Auditdienst Rijk
Ministerie van Financiën

Onderzoeksrapport
Afhandeling datalekken ministerie van Financiën

Versie 1.0

Colofon

Titel	Onderzoek afhandeling datalekken ministerie van Financiën
Uitgebracht aan	ministerie van Financiën
Datum	26 januari 2022
Kenmerk	2022-0000027636
Referentienummer	2020-FIN-028

Inlichtingen
Auditdienst Rijk
070-342 7700

Inhoud

Managementsamenvatting

Binnen het ministerie van Financiën worden datalekken conform procedure afgehandeld

De ADR heeft onderzoek gedaan naar de afhandeling van (mogelijke) datalekken die in de periode van 1 oktober 2019 tot en met 31 maart 2021 gemeld zijn bij het kerndepartement en de Belastingdienst van het ministerie van Financiën. Uitgangspunt voor het onderzoek was de *Procedure meldplicht datalekken*, versie 1.0 d.d. 19 september 2019 van het ministerie van Financiën.

Het onderzoek heeft aangetoond dat binnen het ministerie van Financiën datalekken conform procedure worden afgehandeld en dat hierbij de toepasselijke kaders worden gehanteerd.
De inbreuk en de gevolgen van datalekken worden beschreven. De te treffen maatregelen zijn veelal uit de datalekkenregistratie af te leiden, maar de getroffen maatregelen zijn meestal niet in de datalekkenregistratie opgenomen.
De geïnterviewde functionarissen, betrokken bij de procedure, hebben aangegeven wat er goed gaat rondom de afhandeling van datalekken en welke verbeterpunten er zijn. In hoofdstuk 2 hebben wij de onderzoeksresultaten opgenomen.

Op grond van de onderzoeksresultaten doet de ADR de volgende aanbevelingen:

- Het uitvoeren van een evaluatie van de procedure en eventueel het aanpassen hiervan.
- Het zorgdragen voor een adequate IT-ondersteuning van de afhandeling van datalekken.
- Het geven van aandacht aan het oplossen van de door de ADR geconstateerde bevindingen en het periodiek evalueren van de effectiviteit van de getroffen maatregelen.

1 Inleiding

1.1 Aanleiding onderzoek en opdrachtgever

De Algemene Verordening Gegevensbescherming (AVG) is per 25 mei 2018 van toepassing. Deze Europese verordening vervangt de Wet bescherming persoonsgegevens (Wbp) en heeft onder andere de verplichtingen rond het melden van datalekken aangescherpt. Het ministerie van Financiën beschikt over een Procedure meldplicht datalekken (versie 1.0, d.d. 19 september 2019) die onder meer de rollen beschrijft van de in- en externe partijen betrokken bij de afhandeling van datalekken. De procedure beschrijft ook de stappen die dienen te worden gezet vanaf het moment van ontdekken van een (mogelijk) datalek tot aan de evaluatie en afhandeling van het datalek. De procedure meldplicht datalekken geldt voor alle departementsonderdelen van het ministerie van Financiën waar de minister van Financiën verwerkingsverantwoordelijke voor is.

Om nadere invulling te kunnen geven aan de processtappen zijn afzonderlijke werkinstructies opgesteld voor het kerndepartement en de Belastingdienst. Reden hiervoor is dat er voor is gekozen om vanwege de schaalgrootte van de Belastingdienst binnen het ministerie twee 'meldpunten datalekken' in te richten: één bij het kerndepartement onder de verantwoordelijkheid van de CIO-office van het kerndepartement en één bij de Belastingdienst[1] onder de verantwoordelijkheid van de concerndirectie Informatievoorziening en Databeheersing (IV&D).
Als basisprincipe geldt dat de meldpunten dezelfde uitgangspunten hanteren en processtappen volgen. De invulling van de rollen en verdeling van de verantwoordelijkheden binnen het proces kunnen echter van elkaar verschillen. Dit wordt in de afzonderlijke werkinstructies uitgewerkt.

De Functionaris voor Gegevensbescherming (FG) van het ministerie van Financiën heeft een toezichthoudende rol in de naleving van de AVG en ziet in die rol toe op de afhandeling van datalekken in het werkgebied kerndepartement en Belastingdienst. De FG wil weten in hoeverre de procedure datalekken wordt gevolgd en welke maatregelen de dienstonderdelen hebben genomen om herhaling van datalekken tegen te gaan en/of de risico's van datalekken te beperken. De FG heeft de Auditdienst Rijk (ADR) daarom gevraagd een evaluatie uit te voeren van de afhandeling van datalekken binnen het ministerie van Financiën.

Eind 2020 is een eerste evaluatie uitgevoerd maar niet geheel afgerond. Hervatting van het onderzoek vond plaats in het voorjaar van 2021. De datalekken die in de eerste ronde zijn geëvalueerd zijn hierbij nogmaals bekeken en meer recente datalekken zijn aan die selectie toegevoegd om een actueel beeld te kunnen vormen van de afhandeling van datalekken.

De opdrachtgever voor dit onderzoek is het ministerie van Financiën. De van het ministerie van Financiën, is de gedelegeerd opdrachtgever.

[1] Met als naam: Melddesk Datalekken Belastingdienst (MDB)

1.2 Doelstelling en onderzoeksvragen

Het doel van het onderzoek is om een beeld te krijgen van de afhandeling van (mogelijke) datalekken die in de periode van 1 oktober 2019 tot en met 31 maart 2021 gemeld zijn bij de organisatieonderdelen van het ministerie van Financiën (kerndepartement en Belastingdienst).

De opdrachtgever kan de uitkomsten van het onderzoek gebruiken om de afhandeling van datalekken en opvolging van maatregelen zo nodig te verbeteren, herhaling van datalekken te voorkomen en risico's van datalekken te mitigeren.

De onderzoeksvragen zijn:

1. Op welke wijze zijn de datalekken van het ministerie van Financiën in de periode vanaf 1 oktober 2019 tot en met 31 maart 2021 afgehandeld? Wordt daarbij aan de toepasselijke kaders (procedure, werkinstructies) voor de afhandeling van datalekken voldaan?
2. Specifieke vragen daarbij zijn:
   - Is er een beschrijving van de geconstateerde en vermoedelijke gevolgen van de inbreuk voor de verwerking van persoonsgegevens;
   - Welke maatregelen heeft de verwerkingsverantwoordelijke getroffen om deze gevolgen te verhelpen;
   - Welke maatregelen heeft de verwerkingsverantwoordelijke getroffen om dergelijke incidenten in de toekomst te voorkomen?
3. Wat gaat volgens de betrokken CISO's, privacy officers, FG en BVA, datacoördinatoren en medewerkers van de meldpunten datalekken goed en wat kan beter?
4. Welke aanbevelingen heeft de ADR eventueel ter verbetering van het proces van afhandeling van datalekken?

1.3 Afbakening en aanpak

Object van onderzoek is het proces van afhandeling van de ontvangen meldingen van (mogelijke) datalekken in de periode vanaf 1 oktober 2019 t/m 31 maart 2021 bij het ministerie van Financiën. Het onderzoek heeft plaatsgevonden bij het kerndepartement en de Belastingdienst.

Het onderzoek is uitgevoerd d.m.v. deelwaarnemingen van de gemelde (mogelijke) datalekken bij het kerndepartement en de Belastingdienst en het houden van interviews met betrokken functionarissen.

1.4 Leeswijzer

In hoofdstuk 2 zijn de onderzoeksresultaten opgenomen en worden de onderzoeksvragen 1, 2 en 3 beantwoord. De aanbevelingen zijn terug te vinden in hoofdstuk 3, waarmee onderzoeksvraag 4 wordt beantwoord. De verantwoording van het onderzoek is opgenomen in hoofdstuk 4.

2 Onderzoeksresultaten afhandeling datalekken

2.1 Inleiding

In dit hoofdstuk zijn de onderzoeksresultaten opgenomen. Voor het onderzoek heeft de ADR de afhandeling van de geselecteerde gemelde (mogelijke) datalekken van zowel het kerndepartement als de Belastingdienst getoetst aan de hand van de procedurestappen. De resultaten van deze toets zijn vastgelegd. Bevindingen en de daaruit voortkomende vragen zijn besproken met de contactpersonen. Verder is documentatie bestudeerd en zijn interviews gehouden. Op grond van de resultaten hiervan heeft de ADR de onderzoeksvragen 1, 2 en 3 beantwoord.
Eerst wordt de context van de processen van afhandeling bij het kerndepartement en de Belastingdienst geschetst. Vervolgens worden de onderzoeksvragen beantwoord.

2.2 Context

Binnen het ministerie van Financiën zijn twee meldpunten voor datalekken ingericht:

- Voor het kerndepartement is er een Meldpunt Datalekken;
- Voor de Belastingdienst is er de Melddesk Datalekken Belastingdienst (MDB).

Beide meldpunten hebben een belangrijke rol in de afhandeling van datalekken. Het treffen van maatregelen zowel om de gevolgen van het datalek te herstellen als om een soortgelijk datalek in de toekomst te voorkomen, wordt uitgevoerd door de lijnmanager die verantwoordelijk is voor het proces waar het datalek heeft plaatsgevonden.

Het document *Procedure meldplicht datalekken*, versie 1.0 d.d. 19 september 2019, is bij beide meldpunten het uitgangspunt bij de afhandeling van datalekken. Dit document omvat de procedure en de werkinstructies. Hierin zijn de AVG-vereisten opgenomen die nader zijn uitgewerkt in EU Guidelines. De procedure, inclusief de werkinstructies, vormt het toepasselijke kader.

In de uitvoering zijn er verschillen tussen het kerndepartement en de Belastingdienst. Deze verschillen betreffen met name aard en omvang van de datalekken.
In de onderzoeksperiode (1 oktober 2019 – 31 maart 2021) heeft het kerndepartement een zestigtal meldingen van datalekken ontvangen; dit betreft voornamelijk persoonsgegevens van de eigen medewerkers.
De Belastingdienst houdt zich als uitvoeringsorganisatie bezig met het massaal inwinnen en verstrekken van gegevens. Dit ten behoeve van o.a. de inkomstenbelasting van ongeveer negen miljoen burgers en de toeslagen voor ongeveer zes miljoen huishoudens. In de onderzoeksperiode had de Belastingdienst ongeveer 5500 gemelde datalekken af te handelen.
Zowel het kerndepartement als de Belastingdienst hebben te maken met externe verwerkers. In het geval van het kerndepartement gaat het om verwerkers die personeels- en ICT-diensten verlenen. Bij de Belastingdienst is sprake van postbezorging door een extern bedrijf. Het ontstaan en melden van datalekken bij deze externe verwerkers ligt buiten de directe invloedsfeer van het kerndepartement en de Belastingdienst; zij zijn echter wel verantwoordelijk voor de afhandeling van deze datalekken.

Het kerndepartement en de Belastingdienst stimuleren het melden van mogelijke datalekken. Als logisch gevolg hiervan komen er meldingen binnen die na onderzoek geen datalek blijken te zijn. Ook voor deze meldingen moet de procedure grotendeels worden doorlopen.

Voor de vastlegging van de meldingen maken het kerndepartement en de Belastingdienst gebruik van diverse registratiesystemen.
Het kerndepartement gebruikt TOPdesk, een service managementsysteem ('helpdesk' voor o.a. incidentenregistratie).
De Belastingdienst maakt gebruik van meerdere registratiemiddelen:

- ITSM (IT Service Management), een applicatie waarmee de IT-processen van de Belastingdienst worden ondersteund (o.a. incidents, changes, service-aanvragen);
- LotusNotes (mailsysteem, archivering mails en bijlagen in mappen);
- Excel (handmatige registratie voortgang individuele datalekken in een excelsheet); en
- ConnectPeople (samenwerkingsplatform) waar een aantal documenten waaronder een kopie van de excelsheet worden opgeslagen.

2.3 Binnen het ministerie van Financiën worden datalekken conform procedure afgehandeld

Het onderzoek heeft aangetoond dat binnen het ministerie van Financiën datalekken conform procedure worden afgehandeld.
Zowel uit de interviews als uit de deelwaarnemingen blijkt dat bij beide meldpunten het privacy-bewustzijn van de medewerkers hoog is en dat ernaar wordt gestreefd om gemelde datalekken tijdig en conform de procedure af te handelen.

De ADR heeft tijdens het onderzoek een aantal bevindingen gedaan en zaken opgemerkt die we als observaties terug willen geven. Deze komen in de volgende paragrafen aan de orde.

2.4 Op hoofdlijnen wordt gewerkt volgens het toepasselijke kader; op enkele punten zijn er bevindingen

Uit de deelwaarnemingen en de interviews komt naar voren dat de procedure grotendeels wordt gevolgd bij de afhandeling van datalekken.
Op enkele punten wordt de procedure niet geheel gevolgd of is hier geen vastlegging van in het registratiesysteem. Deze punten zijn door ons onderverdeeld in drie categorieën:

- Bevindingen; afwijkingen van de procedure bij de afhandeling van datalekken.
- Observaties m.b.t. de procedure; stappen uit de procedure die in de praktijk lastig uitvoerbaar zijn, geen vereiste zijn in het kader van de AVG en/of onduidelijkheden betreffen met betrekking tot het toedelen van verantwoordelijkheden.
- Observaties m.b.t. IT-ondersteuning; beperkingen van de gebruikte registratiesystemen.

2.4.1 Bevindingen

- Kerndepartement: verloren en gestolen devices worden via de maandrapportages van SSC-ICT gemeld waardoor deze per definitie te laat worden gemeld aan de Autoriteit Persoonsgegevens (AP).
  Het kerndepartement is in overleg met SSC-ICT over een manier waarop deze meldingen real-time beschikbaar kunnen komen voor het Meldpunt om op te nemen in de datalekkenregistratie (TOPdesk).
- Kerndepartement: de verwerkingsverantwoordelijke wordt niet expliciet vermeld (niet in TOPdesk noch in het datalekregistratieformulier).
  Dit is veelal wel af te leiden uit de in TOPdesk opgenomen informatie.
- Belastingdienst: vanaf medio 2020 tot en met begin 2021 lukte het de Belastingdienst niet om meldplichtige datalekken binnen 72 uur te melden aan de AP.
  De Belastingdienst heeft bij deze meldingen steeds als reden voor vertraging gemeld: "door capaciteitsproblemen bij de Melddesk datalekken

Belastingdienst worden incidenten later in behandeling genomen". In april 2021 heeft de AP aan de Belastingdienst gevraagd welke maatregelen getroffen worden om deze vertragingen in de toekomst te voorkomen. De Belastingdienst heeft in een reactie aangegeven welke maatregelen zijn genomen (o.a. uitbreiding capaciteit MDB) waarmee het probleem is opgelost.

- Kerndepartement en Belastingdienst: een van de eerste stappen in de procedure is "Een medewerker meldt het mogelijke datalek ook bij zijn/haar leidinggevende". Dit is in de vastlegging niet altijd expliciet terug te vinden. In de praktijk wordt dit ondervangen door de leidinggevende (indirect) te betrekken in de afhandeling van het datalek.

2.4.2 Observaties m.b.t. de procedure

- De procedure is ingericht op individuele afhandeling van een mogelijk datalek waarbij alle stappen doorlopen moeten worden. Dit zorgt bij aanzienlijke aantallen gemelde mogelijke datalekken (Belastingdienst) voor een grote werklast.
- In de procedure wordt gevraagd naar datum en tijdstip van melding aan de AP en melding aan betrokkene. Datum en tijdstip van melding aan AP zijn vastgelegd in de ontvangstbevestiging van de melding. Van de melding aan betrokkene ligt de datum vast in de datering van brief of mailbericht; een specifiek tijdstip van de melding aan betrokkene is geen AVG-vereiste en niet relevant voor de afhandeling.
- Een onderdeel van de procedure betreft het vastleggen van een samenvatting van de communicatie met de toezichthoudende autoriteit en de betrokkene(n). De communicatie ligt reeds vast in de registratiesystemen; een specifieke samenvatting is niet aanwezig.
- In de EU Guidelines wordt de rol en taak van de verwerkings-verantwoordelijke beschreven. In de procedure van Financiën wordt de term 'verwerkingsverantwoordelijke' nauwelijks gehanteerd. De taken die in de EU Guidelines aan de verwerkingsverantwoordelijke worden toebedeeld, worden in de procedure verdeeld tussen het meldpunt en de verantwoordelijke lijnmanager. Naast de registratie, de administratieve afhandeling en de monitoring van een datalek, is ook de analyse van het datalek en het bepalen welke maatregelen nodig zijn, belegd bij het meldpunt. De verwerkingsverantwoordelijkheid, zoals bedoeld in de EU Guidelines, ligt hierdoor minder expliciet bij de lijnmanager.
- Kerndepartement: Het tijdstip van de initiële registratie van het (mogelijke) datalek in TOPdesk wordt door het kerndepartement genomen als feitelijke start van de 72 uurstermijn. Dit is in principe vroeger dan de AVG vraagt en ook vroeger dan de eigen werkinstructie aangeeft. Het realiseren van de melding binnen de 72 uurstermijn is een AVG-vereiste. Om hierover verantwoording af te kunnen leggen, is het van belang om het tijdstip van aanvang van de 72 uurstermijn vast te leggen en dit expliciet op te nemen in de werkinstructie en/of te registreren in TOPdesk.

2.4.3 Observaties m.b.t. IT-ondersteuning

- Kerndepartement: TOPdesk als registratiesysteem voor datalekken volstaat voor het kerndepartement gezien het aantal datalekken dat zich voordoet. TOPdesk voorziet niet in specifieke velden of rubrieken voor de vastlegging van alle benodigde AVG-aspecten zoals bv. de verwerkingsverantwoordelijke of het melden aan betrokkene(n).
  Deze AVG-aspecten worden vastgelegd in het door het kerndepartement gebruikte datalekregistratieformulier.
- Belastingdienst: Gelet op de grote aantallen datalekken biedt het registreren in ITSM, LotusNotes, ConnectPeople en Excel geen goede ondersteuning

voor het proces afhandelen datalekken (o.a. veel handmatig werk, weinig zicht op afhandeling).
Er wordt momenteel gewerkt aan de ontwikkeling van een centraal registratiesysteem voor de Belastingdienst waarmee zowel MDB als de dienstonderdelen de voortgang van de afhandeling van datalekken kunnen registreren.

2.5 De inbreuk en de gevolgen van datalekken worden beschreven; de te treffen maatregelen zijn veelal uit de datalekkenregistratie af te leiden; de getroffen maatregelen zijn meestal niet in de datalekkenregistratie opgenomen

Op basis van de deelwaarnemingen heeft de ADR vastgesteld dat de inbreuk en de geconstateerde en vermoedelijke gevolgen hiervan in het datalekkenregister zijn beschreven. De te treffen maatregelen om de gevolgen van het datalek te verhelpen zijn veelal uit de omschrijving van het datalek in het register af te leiden. De lijnmanager, verantwoordelijk voor de uitvoering van deze maatregelen, kan de daadwerkelijke uitvoering hiervan niet registreren in het datalekkenregister. Het monitoren van de uitvoering van de maatregelen door de meldpunten moet daarom handmatig plaatsvinden.
In veel gevallen betreft een datalek een menselijke fout zoals het verkeerd bezorgen van post, het omwisselen van twee cijfers in een BSN-nummer of het verliezen van een telefoon. In deze gevallen is het naar aanleiding van het specifieke datalek treffen van maatregelen om dergelijke fouten in de toekomst te voorkomen meestal niet van toepassing. Wanneer echter sprake is van meerdere gelijksoortige datalekken/fouten dan wel dat er sprake is van een groot incident, nemen de meldpunten het initiatief om met de lijnmanager passende maatregelen te bespreken.

De onderzoeksresultaten worden hierna weer in de drie categorieën onderverdeeld.

2.5.1 Bevindingen

- De te treffen maatregelen zijn veelal uit de datalekkenregistratie op te maken, maar niet expliciet vastgelegd. Ook in het geval er geen maatregelen nodig zijn, is dit niet expliciet in de registratie vastgelegd. De zichtbare invulling van de rol van de verwerkingsverantwoordelijke door de lijnmanager ontbreekt hierdoor.
- Welke maatregelen daadwerkelijk zijn getroffen is meestal niet na te gaan, omdat deze niet in de datalekkenregistratie zijn opgenomen.
- Belastingdienst: De procedure schrijft voor dat een datalek wordt gemeld aan de betrokkene(n) wanneer de inbreuk een waarschijnlijk hoog risico oplevert voor de rechten en vrijheden van natuurlijke personen.
  De Belastingdienst meldt ook zekerheidshalve aan betrokkene(n) wanneer de kans klein is op gevolgen voor de persoonlijke levenssfeer ('ongunstige gevolgen voor de persoonlijke levenssfeer van de betrokkene kan niet uitgesloten worden'), maar de impact groot kan zijn wanneer de rechten en vrijheden wel (bewust) worden aangetast.

2.5.2 Observaties m.b.t. de procedure

- De procedure is ingericht op individuele afhandeling van een mogelijk datalek waarbij alle stappen doorlopen moeten worden inclusief het treffen van maatregelen ter voorkoming van dergelijke incidenten in de toekomst. Bij de meeste datalekken is dit niet aan de orde, omdat het een menselijke fout betreft. Zowel de procedure als de registratiesystemen voorzien niet in de vastlegging “niet van toepassing” wanneer het dergelijke datalekken betreft.
- De huidige procedure voorziet niet in het vormen van een overkoepelend beeld van de geregistreerde datalekken (trendanalyse).

Een analyse wordt in de praktijk wel uitgevoerd bij zowel het kerndepartement als de Belastingdienst in de vorm van periodieke datalekkenrapportages die in diverse gremia worden besproken.

2.5.3 Observaties m.b.t. IT-ondersteuning

- Belastingdienst: De vier registratiesystemen die de Belastingdienst gebruikt bieden geen functionaliteiten om de voortgang van de afhandeling van datalekken te kunnen monitoren.
  Met de onder 2.4.3 genoemde ontwikkeling van een centraal registratiesysteem zal ook de voortgang van de afhandeling van datalekken kunnen worden gemonitord.

2.6 Wat gaat goed en wat kan beter?

Voor de beantwoording van onderzoeksvraag 3 is in de interviews met de betreffende functionarissen gevraagd wat er volgens hen goed gaat en wat eventueel beter kan.

2.6.1 Wat gaat goed?

Aangegeven wordt dat het goed is dat medewerkers de meldpunten weten te vinden, zowel bij het kerndepartement als bij de Belastingdienst.

Verder worden de korte communicatielijnen met de datacoördinatoren genoemd als positief punt bij het kerndepartement.

Bij de Belastingdienst heerst in het algemeen tevredenheid over de afhandeling van de datalekken. Maandelijks wordt door de melddesk van de Belastingdienst aan alle dienstonderdelen gerapporteerd over de incidentmeldingen en wat daarvan gemeld is aan de AP. Daarmee zijn de dienstonderdelen in de gelegenheid vast te stellen of de aantallen en soorten in overeenstemming zijn met de door hen ontvangen en centraal (door de melddesk) verwerkte meldingen. Dit voorziet in een behoefte zolang er geen applicatie is die decentraal inzicht geeft.

2.6.2 Wat kan beter?

De organisatorische plaats van het meldpunt van het kerndepartement wordt als een mogelijk verbeterpunt genoemd. Het meldpunt datalekken van het kerndepartement is nu geplaatst bij de Privacy Officer in de tweede lijn (tactisch niveau), terwijl dit een eerstelijns (operationele) activiteit is.

Het functioneren van het registratiesysteem/de registratiesystemen[2] kan worden verbeterd door uitbreiding met een monitoringsfaciliteit.

De Belastingdienst geeft aan dat wanneer een ernstig incident gebeurt, medewerkers soms de procedure en afspraken vergeten. Het bewustzijn van datalekken en de kennis van de procedure onder medewerkers in de dienstonderdelen kan beter, zodat zij weten wat er van hen wordt verwacht.
Bij sommige dienstonderdelen worden meldingen van datalekken ook nog alleen door de ‘oude’ contactpersonen behandeld terwijl de datacoördinator, die een sleutelrol heeft toebedeeld gekregen in de (nieuwe) procedure, verantwoordelijk is voor het afhandelen van datalekken.

Bij de Belastingdienst is er behoefte aan een registratietool met meer mogelijkheden tot opname/integratie van documentatie en met een betere afscherming/beveiliging. Doordat veel belastingdienstmedewerkers toegang (moeten) hebben tot ITSM, kunnen zij allemaal ook de gemelde datalekken inclusief eventueel opgenomen persoonsgegevens raadplegen.

[2] m.n. bij grote aantallen (mogelijke) datalekken bij de Belastingdienst

3 Aanbevelingen

Dit hoofdstuk bevat het antwoord op onderzoeksvraag 4: Welke aanbevelingen heeft de ADR eventueel ter verbetering van het proces van afhandeling van datalekken?

3.1 Voer evaluatie uit op procedure datalekken en pas deze eventueel aan

- Procedure evalueren en waar mogelijk aanpassen aan de praktijk (nl. niet alle procedurestappen zijn in de praktijk goed uitvoerbaar en het doel/toegevoegde waarde van sommige procedurestappen is niet duidelijk) met inachtneming van de AVG-vereisten. (Zie ook paragrafen 2.4 en 2.5).
- Procedure is ingericht om elke melding individueel af te handelen; dit betekent dat voor elk melding in principe alle procedurestappen doorlopen moeten worden. Dit is veel werk, zeker bij grote aantallen meldingen. Aanbeveling is om te onderzoeken of in de procedure, en in de vastlegging ervan in het registratiesysteem, een melding eerder afgesloten kan worden wanneer wordt vastgesteld dat het niet om een datalek gaat of wanneer duidelijk is dat volgende procedurestappen niet aan de orde zijn.
- Het bepalen van de te treffen maatregelen wordt in de procedure, processtappen 5 en 6, belegd bij de CISO en het meldpunt; niet bij de verwerkingsverantwoordelijke.

De ADR is tijdens het onderzoek op de hoogte gesteld van de evaluatie en herijking van het bestaande Privacybeleid en de onderliggende procedures. Waar nodig worden de onderliggende procedures aangepast.

3.2 Zorg voor adequate IT-ondersteuning

- Belastingdienst: onderzoek de mogelijkheden voor een adequate ondersteuning van de afhandeling van datalekken waarbij o.a. grote aantallen verwerkt kunnen worden, minder handmatig werk noodzakelijk is en de voortgang van afhandeling inclusief de te treffen en getroffen maatregelen (centraal en decentraal) gemonitord kan worden.
  De Belastingdienst is bezig met onderzoek voor selectie of ontwikkeling van een nieuwe tool hiervoor. Gelet op het belang van een beheerst proces van de afhandeling van datalekken, is de aanbeveling hier voortvarend mee door te gaan.
- Het kerndepartement: onderzoek of en hoe AVG-vereisten (artikel 33 en 34 AVG) in TOPdesk opgenomen kunnen worden in specifieke velden/rubrieken bv. voor te treffen en getroffen maatregelen.
- Onderzoek mogelijkheden voor geautomatiseerde ondersteuning voor het genereren van (trend)analyses en managementinformatie.

3.3 Overige aanbevelingen

- Aanbeveling is om de in hoofdstuk 2 opgenomen bevindingen in de evaluatie van de procedure mee te nemen dan wel separaat hiervoor een oplossing te formuleren.
- In paragraaf 2.5.1 wordt aangegeven dat meestal niet is na te gaan welke maatregelen daadwerkelijk zijn getroffen, omdat deze niet in de datalekkenregistratie zijn opgenomen. Hiervoor zijn in paragraaf 3.2 aanbevelingen geformuleerd om het mogelijk te maken de te treffen en getroffen maatregelen in de registratie vast te leggen. Aanvullend hierop is de aanbeveling om periodiek de effectiviteit van de getroffen maatregelen te evalueren.

4 Verantwoording onderzoek

4.1 Werkzaamheden en afbakening

Object van het onderzoek is het proces van afhandeling van de ontvangen meldingen van (mogelijke) datalekken in de periode vanaf 1 oktober 2019 t/m 31 maart 2021 bij het ministerie van Financiën (kerndepartement en Belastingdienst).

Eind 2020 is een eerste evaluatie uitgevoerd maar niet geheel afgerond. Hervatting van het onderzoek vond plaats in het voorjaar van 2021. De datalekken die in de eerste ronde zijn geëvalueerd, zijn hierbij nogmaals bekeken en meer recente datalekken zijn aan die selectie toegevoegd om een actueel beeld te kunnen vormen van de afhandeling van datalekken.

Het onderzoek is uitgevoerd d.m.v. deelwaarnemingen van de gemelde (mogelijke) datalekken bij het kerndepartement en de Belastingdienst en het houden van interviews met betrokken functionarissen:

- Functionaris Gegevensbescherming (FG);
- Chief Information Security Officer (CISO) kerndepartement;
- Privacy Officers kerndepartement en Belastingdienst;
- Coördinator Melddesk Datalekken Belastingdienst;
- Weger Melddesk Datalekken Belastingdienst;
- Datacoördinator en Security Officer Douane.

Voor dit onderzoek is de ADR uitgegaan van de Procedure meldplicht datalekken van het Ministerie van Financiën (d.d. 19 september 2019).

De beoordeling van de afhandeling van de datalekken is vervolgens samen met informatie uit de interviews verwerkt tot deze rapportage.

4.2 Gehanteerde standaard en kwaliteitsborging

Deze opdracht is uitgevoerd in overeenstemming met de Internationale Standaarden voor de Beroepsuitoefening van Internal Auditing. Dit onderzoek verschaft geen zekerheid in de vorm van een oordeel of conclusie, omdat het een onderzoeksopdracht betreft en geen controle-, beoordelings- of andere assurance-opdracht. Als hier wel sprake van was geweest, dan zou de ADR wellicht andere zaken hebben geconstateerd en gerapporteerd.

De opdracht is uitgevoerd conform de algemene uitgangspunten voor de uitoefening van de interne auditfunctie bij de rijksdienst. Daarbij hoort ook een stelsel van kwaliteitsborging. Een onderdeel daarvan is dat er een onafhankelijke kwaliteitstoetsing heeft plaatsgevonden op deze onderzoeksopdracht.

4.3 Verspreiding rapport

De opdrachtgever, , is eigenaar van dit rapport. Dit rapport is primair bestemd voor de opdrachtgever met wie de ADR deze opdracht is overeengekomen. Hoewel het rapport de context van het onderzoek zo goed mogelijk probeert te beschrijven, is het mogelijk dat iemand die de context niet (volledig) kent de uitkomsten anders interpreteert dan bedoeld.

In de ministerraad is besloten dat het opdrachtgevende ministerie waarvoor de Auditdienst Rijk (ADR) een rapport heeft geschreven, het rapport binnen zes weken op de website van de Rijksoverheid plaatst, tenzij daarvoor een uitzondering geldt. De minister van Financiën stuurt elk halfjaar een overzicht naar de Tweede Kamer met de titels van rapporten die de ADR heeft uitgebracht en plaatst dit overzicht op www.rijksoverheid.nl.

5 Ondertekening

Apeldoorn, 26 januari 2022

6 Managementreactie

Managementreactie n.a.v. het onderzoek Afhandelen datalekken bij het Ministerie van Financiën

De Belastingdienst, Toeslagen, Douane en het Kerndepartement danken de ADR voor de uitgevoerde audit en de vaststelling dat het ministerie van Financiën datalekken conform procedure afhandelt en dat hierbij de toepasselijke kaders worden gehanteerd.
De aanbevelingen die u heeft gedaan nemen we, zoals aangegeven, mee in de verbeteracties in 2021/2022, deze zullen we verwerken in de actieplannen die eind Q1 2022 aan de BR worden aangeboden. Zo scherpen we onder meer de genoemde procedures aan, versterken daar waar nodig de toerusting van de ondersteuning en borgen dat we voortdurend leren in de PDCA-cyclus, onder meer via periodieke evaluaties.

In aanvulling hierop reageert de Belastingdienst als volgt.
In deze reactie gaan we in op de aanbevelingen in het rapport van de Auditdienst Rijk “Rapport onderzoek afhandeling datalekken minFin” van oktober 2021.
De onderzoeksvragen die in het rapport zijn gedefinieerd zijn:

1. Op welke wijze zijn de datalekken van het ministerie van Financiën in de periode vanaf 1 oktober 2019 tot en met 31 maart 2021 afgehandeld? Wordt daarbij aan de toepasselijke kaders (procedure, werkinstructies) voor de afhandeling van datalekken voldaan?
2. Specifieke vragen daarbij zijn:
   - Is er een beschrijving van de geconstateerde en vermoedelijke gevolgen van de inbreuk voor de verwerking van persoonsgegevens;
   - Welke maatregelen heeft de verwerkingsverantwoordelijke getroffen om deze gevolgen te verhelpen;
   - Welke maatregelen heeft de verwerkingsverantwoordelijke getroffen om dergelijke incidenten in de toekomst te voorkomen?
3. Wat gaat volgens de betrokken CISO’s, privacy officers, FG en BVA, datacoördinatoren en medewerkers van de meldpunten datalekken goed en wat kan beter?
4. Welke aanbevelingen heeft de ADR eventueel ter verbetering van het proces van afhandeling van datalekken?

De Belastingdienst heeft in 2015 de melddesk voor datalekken ingericht. Douane en Toeslagen maakten destijds onderdeel uit van de Belastingdienst. Deze melddesk behandelt ook de datalekken van Douane en Toeslagen. Mogelijk worden na de volledige ontvlechting nog andere afspraken gemaakt over het behandelen van datalekken. In deze memo wordt voor elk van de drie aanbevelingen een reactie gegeven.

1. Aanbeveling opgenomen onder 3.1 in het rapport
Voer evaluatie uit op procedure datalekken en pas deze eventueel aan
- Procedure evalueren en waar mogelijk aanpassen aan de praktijk (nl. niet alle procedurestappen zijn in de praktijk goed uitvoerbaar en het doel/toegevoegde waarde van sommige procedurestappen is niet duidelijk) met inachtneming van de AVG-vereisten. (Zie ook paragrafen 2.4 en 2.5).
- Procedure is ingericht om elke melding individueel af te handelen; dit betekent dat voor elk melding in principe alle procedurestappen doorlopen moeten worden. Dit is

veel werk, zeker bij grote aantallen meldingen. Aanbeveling is om te onderzoeken of in de procedure, en in de vastlegging ervan in het registratiesysteem, een melding eerder afgesloten kan worden wanneer wordt vastgesteld dat het niet om een datalek gaat of wanneer duidelijk is dat volgende procedurestappen niet aan de orde zijn.
- Het bepalen van de te treffen maatregelen wordt in de procedure, processtappen 5 en 6, belegd bij de CISO en het meldpunt; niet bij de verwerkingsverantwoordelijke.

De ADR is tijdens het onderzoek op de hoogte gesteld van de evaluatie en herijking van het bestaande Privacybeleid en de onderliggende procedures. Waar nodig worden de onderliggende procedures aangepast.

De aanbeveling wordt overgenomen met de volgende toelichting:
- Samen met het kerndepartement zullen de Belastingdienst, Douane en Toeslagen een evaluatie uitvoeren in 2022. De procedurestappen worden beoordeeld en waar nodig aangepast aan de praktijk ook rekening houdend met de meldingen die ontvangen worden en die niet leiden tot een datalek.
- Het herbeleggen van de processtappen 5 en 6 wordt daarbij ook beoordeeld.

2. Aanbeveling opgenomen onder 3.2 in het rapport

Zorg voor adequate IT-ondersteuning
- Belastingdienst: onderzoek de mogelijkheden voor een adequate ondersteuning van de afhandeling van datalekken waarbij o.a. grote aantallen verwerkt kunnen worden, minder handmatig werk noodzakelijk is en de voortgang van afhandeling inclusief de te treffen en getroffen maatregelen (centraal en decentraal) gemonitord kan worden. De Belastingdienst is bezig met onderzoek voor selectie of ontwikkeling van een nieuwe tool hiervoor. Gelet op het belang van een beheerst proces van de afhandeling van datalekken, is de aanbeveling hier voortvarend mee door te gaan.
- Het kerndepartement: onderzoek of en hoe AVG-vereisten (artikel 33 en 34 AVG) in TOPdesk opgenomen kunnen worden in specifieke velden/rubrieken bv. voor te treffen en getroffen maatregelen.
- Onderzoek mogelijkheden voor geautomatiseerde ondersteuning voor het genereren van (trend)analyses en managementinformatie.

De aanbeveling wordt overgenomen met de volgende toelichting:
- De huidige IT-ondersteuning bij de Melddesk Datalekken Belastingdienst, Douane en Toeslagen is onvoldoende en daarom loopt al enige tijd onderzoek en selectie voor een tool waarbij de registratie en dossiervorming zijn gewaarborgd en eenvoudig inzicht kan worden verkregen in de status van meldingen. (zie eerste bullet in de aanbeveling)
- Doel is dit in 2022 te hebben gerealiseerd en dan kan ook onderzocht worden of trendanalyses of managementinformatie eenvoudiger kunnen worden gegenereerd. (zie derde bullet in de aanbeveling)

3. Aanbeveling opgenomen onder 3.3 in het rapport

Overige aanbevelingen
- Aanbeveling is om de in hoofdstuk 2 opgenomen bevindingen in de evaluatie van de procedure mee te nemen dan wel separaat hiervoor een oplossing te formuleren.
- In paragraaf 2.5.1 wordt aangegeven dat meestal niet is na te gaan welke maatregelen daadwerkelijk zijn getroffen, omdat deze niet in de datalekkenregistratie zijn opgenomen. Hiervoor zijn in paragraaf 3.2 aanbevelingen geformuleerd om het mogelijk te maken de te treffen en getroffen maatregelen in de registratie vast te

leggen. Aanvullend hierop is de aanbeveling om periodiek de effectiviteit van de getroffen maatregelen te evalueren.

De twee aanbevelingen worden overgenomen met de volgende toelichting:

Eerste bullet: de hieronder genoemde bevindingen van hoofdstuk 2 zijn relevant voor de afhandeling bij de Belastingdienst, Douane en Toeslagen:
Opgenomen in het rapport onder 2.4.1. onder bullet 3, kort samengevat: De tijdelijke achterstand in de onderzoeksperiode. In de onderzoeksperiode is reeds voorzien in uitbreiding met 1 FTE. Verder wordt onderzocht of voor piekmomenten nog een stand-by kan worden ingericht van 0,5 of 1 FTE.
Opgenomen in het rapport onder 2.4.1. onder bullet 4, kort samengevat: Leg ook vast of de leidinggevende is/wordt geïnformeerd. Dit wordt in de praktijk wel gedaan maar niet expliciet vastgelegd. Dit kan voor de Belastingdienst, Douane en Toeslagen worden meegenomen in de inrichting van de nieuwe IT-ondersteuning in 2022.
Opgenomen in het rapport onder 2.5.1. wordt bij de eerste twee bullets aangegeven dat aanbeveling van te treffen maatregelen en de getroffen maatregelen niet expliciet worden vastgelegd en ook als geen maatregelen nodig zijn wordt dit niet vastgelegd in de administratie. Dit moet nu blijken uit correspondentie. De aanbeveling wordt zo mogelijk meegenomen in de inrichting van de IT-ondersteuning in 2022.
Opgenomen in het rapport onder 2.5.1. wordt bij het derde bullet aangegeven dat de Belastingdienst ook meldt aan betrokkene(n) als de kans klein is op gevolgen voor de persoonlijke levenssfeer. Door deze bevinding zal vaktechnisch afstemming worden gezocht met de privacy officer en de Functionaris Gegevensbescherming voor een herbeoordeling.
Tweede bullet: Aanbevolen wordt om periodiek de effectiviteit van getroffen maatregelen te evalueren. Hiervoor is nodig dat de vastlegging eerst wordt ingericht, zoals hiervoor benoemd.
In 2022 zal een evaluatie op maatregelen worden uitgevoerd.

Auditdienst Rijk
Postbus 20201
2500 EE Den Haag
(070) 342 77 00