Auditdienst Rijk
Ministerie van Financiën

Onderzoeksrapport Implementatie AVG bij het Ministerie van Financiën

Definitief

Colofon

Titel	Implementatie AVG bij het Ministerie van Financiën
Uitgebracht aan	Han van Gelder
Datum	10 april 2019
Kenmerk	2019-0000062907

Inlichtingen
Auditdienst Rijk
070-342 7700

Inhoud

Aanleiding opdracht

Aanleiding
Aanleiding voor dit onderzoek is de vraag van Manon Leijten, Secretaris-Generaal (SG), naar het op schema liggen van de opgestelde implementatietrajecten Algemene Verordening Gegevensbescherming (AVG) voor zowel het kerndepartement van Financiën als de Belastingdienst.
De onderzoeksvragen en de gekozen werkwijze zijn in hoofdstuk 4 "Verantwoording van het onderzoek" toegelicht.

Doelstelling
Doelstelling van het onderzoek is om Financiën (kerndepartement en Belastingdienst) extra inzicht te geven in de stand van zaken van een aantal maatregelen uit de implementatieplannen om zodoende op 25 mei 2019 aantoonbaar (op een adequaat niveau) aan de AVG te kunnen voldoen.

Context
Op 25 mei 2018 was de AVG bij Financiën (kerndepartement en Belastingdienst) volgens de inschatting van het Ministerie van Financiën voor een belangrijk deel op een adequaat niveau ingeregeld. Voor openstaande punten zijn er implementatietrajecten gestart. Doel van deze trajecten is om aantoonbaar op een adequaat niveau aan de AVG te voldoen.
De Belastingdienst heeft toegezegd aan de Tweede Kamer, zie Kamerstuk 31 066, nr. 401, dat zij streeft om voor 25 mei 2019 aantoonbaar aan de AVG te voldoen.

Implementatietrajecten AVG lopen: belang is bekend, realisatie is complex

Scope onderzoek
De ADR heeft op basis van de risico inschatting van het kerndepartement en de Belastingdienst een onderzoek gedaan met de volgende scope.

Organisatiedeel	Thema/maatregel
Kerndepartement - DGRB - GT	1. Verwerkersovereenkomst 2. Schoning netwerkschijven 3. Kwaliteit verwerkingenregister 4. Meldplicht datalekken
Belastingdienst - CAP - MKB - IV	1. Verwerkersovereenkomsten 2. Archiveren, schonen en verwijderen *3: Niet archiefwaardige bestanden vernietigen* *5: Toepassen selectielijsten* 3. Autorisaties *4: Beoordeling actualiteit autorisaties* *6: Intrekken autorisaties* 4. Delen van gegevens *16: Uitfaseren datadumping faciliteiten dan wel gebruik afschermen;* *17: Gebruik productiedata in testomgeving stoppen: pseudonimiseren dan wel fictieve testdata gebruiken.*

Context onderzoeksresultaten
Tijdens het onderzoek hebben wij de volgende observaties gedaan, die naast de onderzoeksbevindingen naar voren zijn gekomen en die context geven bij de onderzoeksresultaten;

- Per thema/maatregel is niet altijd de uitgangssituatie/nul situatie vastgelegd, waardoor een uitspraak over de haalbaarheid van de maatregelen voor 25 mei 2019 lastig is te objectiveren. Het voldoen aan de AVG is immers een continu proces, waarbij er altijd nieuwe AVG issues kunnen bijkomen;
- Daarnaast worden in de implementatietrajecten ook aanvullende structurele aanpassingen genoemd, waarbij het niet altijd duidelijk is of deze maatregelen onderdeel zijn van het implementatietraject met de deadline van 25 mei 2019;
- Verder bevindt de Belastingdienst zich midden in een reorganisatie en zijn er diverse AVG gerelateerde thema's/maatregelen die vanwege de reorganisatie aanvullend gedaan moeten worden;
- Tenslotte merken wij op dat de voor AVG project fase II gekozen maatregelen allemaal relevant zijn voor het aantoonbaar voldoen aan de AVG. Wel merken wij op dat bij de start van de vervolgimplementatie medio 2018 een aantal maatregelen niet voldoende was uitgewerkt. Daarnaast ontbreekt in een aantal gevallen het commitment binnen de organisatieonderdelen voor de gekozen aanpak.

Onderzoeksuitkomsten Kerndepartement
Wat is de objectief vast te stellen stand van zaken van een aantal geselecteerde maatregelen uit de implementatieplannen?

- Actualisering verwerkersovereenkomsten vergt aandacht (thema 1, zie paragraaf 1.2.1);
- Verwerkersovereenkomsten conform het model bevatten de benodigde procedureafspraken voor datalekken (thema 1, zie paragraaf 1.2.2);
- Schonen van netwerkschijven is arbeidsintensief evenals het verkrijgen van inzicht in de feitelijke voortgang (thema 2, zie paragraaf 1.3.1);
- Functionaliteit AVG-register[1] voldoende, maar verdere verbetering is mogelijk (thema 3, zie paragraaf 1.4.1);
- Kwaliteit van de vulling van het AVG-register blijft op een aantal punten achter (thema 3, zie paragraaf 1.4.2);
- Uiteindelijke publicatie van alle registraties afhankelijk van voldoende capaciteit (onder andere van FG) (thema 3, zie paragraaf 1.4.4);
- Procedure meldplicht datalekken opgesteld conform AVG en uitgedragen (thema 4, zie paragraaf 1.5.1);
- Datalekkenregister sinds februari 2018 vastgelegd in TopDesk en conform AVG (thema 4, zie paragraaf 1.5.2);
- Procedure meldplicht datalekken is in 2018 toegepast (thema 4, zie paragraaf 1.5.3);
- Aansluiting met incidentprocedure is aandachtspunt (thema 4, zie paragraaf 1.5.4).

Welke factoren zijn van invloed op een goede en tijdige realisatie van de nog uit te voeren geselecteerde maatregelen uit de implementatieplannen?

- Afgesproken werkwijze voor actualiseren verwerkersovereenkomsten (nog) niet altijd uitgevoerd (thema 1, zie paragraaf 1.2.3);
- Geen duidelijke kaders en geen strakke regie op schonen (thema 2, zie paragraaf 1.3.2);
- Proces rondom periodiek schonen is nog niet ingericht (thema 2, zie paragraaf 1.3.3);
- Geen formele werkwijze voor het periodiek actualiseren van verwerkingen (thema 3, zie paragraaf 1.4.3);

Onderzoeksuitkomsten Belastingdienst
Wat is de objectief vast te stellen stand van zaken van een aantal geselecteerde maatregelen uit de implementatieplannen?

[1] Officiële benaming in AVG (art.30) is "register van de verwerkingsactiviteiten"

- Maatregel inzake niet archiefwaardige bestanden vernietigen lijkt haalbaar voor ongestructureerde gegevens specifiek van het eigen dienstonderdeel (thema 1, zie paragraaf 2.2.1);
- Maatregel inzake toepassen selectielijsten lijkt niet haalbaar (thema 1, zie paragraaf 2.2.3);
- Maatregel inzake beoordeling actualiteit autorisaties is reeds gehaald (thema 2, zie paragraaf 2.3.1);
- Maatregel inzake intrekken autorisaties is alleen haalbaar voor dienstonderdeelvreemde rollen (thema 2, zie paragraaf 2.3.2);
- Structurele verbeterslagen in autorisatiebeheer vraagt een langere doorlooptijd (thema 2, zie paragraaf 2.3.3);
- Maatregel inzake datadumping faciliteiten uitfaseren dan wel afschermen is niet voldoende SMART gemaakt (thema 3, zie paragraaf 2.4.1)
- Maatregel gebruik productiedata in testomgeving stoppen is niet voldoende SMART gemaakt (thema 3, zie paragraaf 2.4.3);
- Nog niet alle verwerkersovereenkomsten zijn aanwezig of geactualiseerd (thema 4, zie paragraaf 2.5.2).

Welke factoren zijn van invloed op een goede en tijdige realisatie van de nog uit te voeren geselecteerde maatregelen uit de implementatieplannen?

- Gat tussen beleid en uitvoering, beperkte toetsing op bereiken eindresultaat, geen beschrijving informatiehuishouding (thema 1, zie paragraaf 2.2.2);
- Onvoldoende IV ondersteuning, onduidelijke verantwoordelijkheidsverdeling inzake gebruik gegevens in de keten en implementatie selectielijsten (thema 1, zie paragraaf 2.2.4).
- Reorganisatie Belastingdienst beïnvloedt haalbaarheid uitfaseren dan wel afschermen datadumping faciliteiten negatief (thema 3, zie paragraaf 2.4.2)
- Onvoldoende commitment of het stoppen met productiedata in de testomgeving de juiste uitwerking is om gesignaleerd risico te verminderen (thema 3, zie paragraaf 2.4.4)
- Geen gedeeld beeld binnen de Belastingdienst wanneer een organisatie een verwerker is (thema 4, zie paragraaf 2.5.1)

Leeswijzer
In hoofdstuk 1 worden de twee onderzoeksvragen voor de thema's van het kerndepartement in detail beantwoord en in hoofdstuk 2 worden de twee onderzoeksvragen voor de thema's van de Belastingdienst in detail besproken.
In hoofdstuk 3 staan de mogelijke vervolgstappen voor zowel het kerndepartement als de Belastingdienst vermeld.
In hoofdstuk 4 is de verantwoording van het onderzoek opgenomen.

1 Bevindingen inzake implementatie AVG bij kerndepartement

1.1 Inleiding

Uitgangspunten onderzoek
Bij het implementatieproject AVG fase I, heeft het kerndepartement enkele restpunten/thema's onderkend, die opgepakt zouden moeten worden na 25 mei 2018. De ADR heeft in overleg met de opdrachtgever 4 van deze thema's geselecteerd voor nadere analyse bij het kerndepartement. Ten aanzien van de thema's 1 tot en met 3 zijn gesprekken gevoerd bij de organisatieonderdelen Directoraat Rijksbegroting en Generale Thesaurie. Voor thema 4 is gesproken met de privacy officer en de CISO van het kerndepartement.

De onderzochte thema's zijn:
1. Verwerkersovereenkomsten;
2. Schoning netwerkschijven;
3. Kwaliteit verwerkingsregister;
4. Procedure meldplicht datalekken.

Met betrekking tot de thema's zijn de volgende onderzoeksvragen gesteld:
- Wat is de objectief vast te stellen stand van zaken van een aantal geselecteerde maatregelen uit de implementatieplannen?
- Welke factoren zijn van invloed op een goede en tijdige realisatie van de nog uit te voeren geselecteerde maatregelen uit de implementatieplannen?

Context onderzoeksresultaten
Tijdens het onderzoek hebben wij de volgende observaties gedaan, die naast de onderzoeksuitkomsten naar voren zijn gekomen en die context geven bij de onderzoeksresultaten;
- de activiteiten rondom de implementatie AVG concurreren met andere werkzaamheden;
- de verschillen in kennis van de AVG, capaciteit en motivatie tussen de diverse datacoördinatoren zijn groot;
- ons beeld van de samenwerking tussen de CIO-office kerndepartement en de verschillende data-coördinatoren ten tijde van het onderzoek is dat de data-coördinatoren zelf verantwoordelijk zijn voor de uitvoering van de werkzaamheden en in het geval van vragen bij de CIO-office terecht kunnen;
- doordat met name bij het thema "schoning netwerkschijven" veel handmatig activiteiten dienen te worden uitgevoerd door de diverse organisatie-onderdelen is de werklast voor de betrokkenen hoog en in combinatie met de als gering ervaren waardering, leidt dit in een aantal gevallen tot afnemende motivatie voor het AVG werk.

1.2 Thema 1: Verwerkersovereenkomsten

1.2.1 Actualisering verwerkersovereenkomsten vergt aandacht
Volgens de rapportage van 14 januari 2019 is de stand van zaken inzake de actualisering van de verwerkersovereenkomsten als volgt.

> "Er hebben 1-op-1 gesprekken plaatsgevonden met alle DC. Duidelijk is wat moet gebeuren. Vanuit de CIO-Office KD wordt advies en ondersteuning geboden.

De laatste punten op de i worden gezet op een drietal verwerkersovereenkomsten bij COMM.
Ten behoeve van de overeenkomst van Schuberg Philis dient gebruik te worden gemaakt van de verwerkersovereenkomst onder de ARVODI 2018, ter vervanging van de huidige versie van de verwerkersovereenkomst.
Verwacht wordt volgens planning op 31 maart 2019 gereed te zijn."

Wij hebben op basis van een beoordeling van 10 verwerkersovereenkomsten vastgesteld dat;

- nog niet voor alle verwerkers verwerkingsovereenkomsten zijn opgesteld;
- de verwerkersovereenkomsten vaak in concept zijn of nog niet zijn opgenomen in het AVG-register[2].

De afronding van de actualisering van verwerkersovereenkomsten is gepland voor 31 maart, maar gezien bovenstaande is wellicht meer tijd en aandacht nodig.

1.2.2 *Afgesproken werkwijze voor actualiseren verwerkersovereenkomsten (nog) niet altijd uitgevoerd*

Bij het kerndepartement is de volgende werkwijze afgesproken voor het actualiseren van verwerkersovereenkomsten:

- Er wordt geen nieuwe verwerkersovereenkomst gesloten zolang het bestaande contract met de organisatie/verwerker nog loopt;
- Tot die tijd wordt gewerkt met een addendum met AVG-afspraken; de afdeling inkoop (CDI) zorgt hier voor;
- Bij het afsluiten van een nieuw contract wordt ook een nieuwe verwerkersovereenkomst gesloten.

Uit ons onderzoek is gebleken dat de verwerkersovereenkomsten gedateerd na 25 mei 2018 niet altijd op de ARVODI 2018 zijn gebaseerd. Bij de voor 25 mei 2018 afgesloten verwerkersovereenkomsten (of die geen ondertekeningsdatum hebben) is niet altijd duidelijk welk model is toegepast. Wij hebben bij geen van de door ons onderzochte verwerkersovereenkomsten een addendum aangetroffen.

1.2.3 *Verwerkersovereenkomsten conform het model bevatten de benodigde procedureafspraken voor datalekken*

In de voorgeschreven werkwijze bij de totstandkoming van verwerkingsovereenkomsten wordt verwezen naar het ARVODI-2018 model.
In dit model staat omschreven dat de verwerkingsverantwoordelijke zonder onredelijke vertraging wordt geïnformeerd over een inbreuk in verband met persoonsgegevens. Daarnaast wordt de procedure datalekken als bijlage bijgevoegd bij de verwerkersovereenkomst.

Wij hebben bij geen van de door ons onderzochte verwerkersovereenkomsten een bijlage aangetroffen over de procedure datalekken. Mogelijk is deze procedure wel gedeeld met de verwerker, maar dit blijkt niet uit ons onderzoek.

1.3 Thema 2: Schoning netwerkschijven

1.3.1 *Schonen van netwerkschijven is arbeidsintensief evenals het verkrijgen van inzicht in de feitelijke voortgang*

De werkwijze voor de schoning van netwerkschijven is uitgezet bij alle data-coördinatoren van het kerndepartement. Wij hebben deze werkwijze onderzocht en deze blijkt als erg arbeidsintensief te worden ervaren. Redenen hiervoor zijn:

- De gebruikte "Zoek- en vind tool" levert "false positives" op. De tool meldt dat er in een bestand persoonsgegevens zijn opgeslagen, maar in de praktijk blijkt dat niet het geval te zijn;
- De tool moet gevoed worden met de voor het betreffende dienstonderdeel relevante zoektermen en deze termen dienen ook regelmatig geactualiseerd te worden;

[2] Officiële benaming in AVG (art.30) is "register van de verwerkingsactiviteiten"

- Er is achterstallig mappenonderhoud (bijv. van medewerkers die uit dienst zijn). Daarnaast wordt de schoning soms belemmerd doordat datacoördinatoren niet altijd beschikken over de juiste autorisaties.

De opschoning van netwerkschijven kan bij een aantal organisatie onderdelen een knelpunt worden. Bij O&P omdat hier een reorganisatie plaats vindt. Bij DRZ en het Agentschap omdat de tooling van de eenheid-I bij deze organisatieonderdelen niet toegepast kan worden. De status van de schoning is hierdoor niet bekend.

1.3.2 *Geen duidelijke kaders en geen strakke regie op schonen*

De ADR heeft ten tijde van het onderzoek geen formeel, beheerst proces voor het schonen van de netwerk-schijven aangetroffen. Zo worden de datacoördinatoren er niet op aangesproken als zij geen voortgang boeken op basis van de overzichten die door eenheid-I worden opgeleverd. Een vergelijking van de voortgangsoverzichten van november en januari tonen bij de twee onderzochte dienstonderdelen van het kerndepartement geen specifieke voortgang. Geen van beide dienstonderdelen was op de hoogte van het bestaan van de voortgangsoverzichten. Eén dienstonderdeel gaf aan dat de cijfers over de stagnatie van de schoning niet worden herkend.
CIO Office geeft in een reactie aan dat de opschoning van de netwerkschijven in het datacoördinatorenoverleg wordt besproken. De datacoördinatoren kunnen zelf rapportages vragen bij de eenheid-I.

1.3.3 *Proces rondom periodiek schonen is nog niet formeel ingericht*

De ADR heeft geen formeel proces voor het periodiek schonen van de netwerk-schijven aangetroffen. Wij hebben vernomen dat de IB&P-adviseur en de Eenheid-I op dit moment de procedure voor de periodieke schoning uitwerken. Een eerste concept is inmiddels gereed. Periodiek schoning is nodig om te borgen dat, na afronding van de inhaalslag, er geen nieuwe bestanden met persoonsgegevens op de voor meerdere medewerkers toegankelijke netwerkschijven bij komen.

1.4 Thema 3: Kwaliteit verwerkingenregister

Binnen het Ministerie van Financiën wordt, zoals bij de meeste ministeries, de AVG-tool voor de inrichting van het verwerkingenregister gebruikt. Deze tool is ontwikkeld bij het ministerie van Economische Zaken en biedt mogelijkheden om het gehele proces van de registratie van verwerkingen te ondersteunen, tevens kunnen documenten worden toegevoegd.

1.4.1 *Functionaliteit AVG-register voldoende, maar verdere verbetering is mogelijk*

Gedurende ons onderzoek zijn wij door de datacoördinatoren en het CIO Office op een aantal bugs (software fouten) in het verwerkingenregister gewezen.
Het AVG-register bevat slechts summiere informatie over de afweging om wel of geen PIA uit te voeren en over de informatiebeveiliging indien er doorgifte is van persoonsgegevens buiten de Europese Unie.
Tevens is in het register niet direct te zien of er aan een bestaande verwerkers-overeenkomst (van vóór 25 mei 2018) een addendum met AVG-afspraken is toegevoegd.
Tenslotte is de procesgang rond het wijzigen van reeds goedgekeurde registraties van verwerkingen erg bewerkelijk, waardoor er een vergrote kans is dat de registratie van de verwerking niet actueel kan worden gehouden.

1.4.2 *Kwaliteit van de vulling van het AVG-register blijft op een aantal punten achter*

Op de volgende punten blijft de kwaliteit van het AVG-register achter:

- het doel van de verwerking is niet altijd specifiek geformuleerd. Gebruikerstevredenheid is bijv. een te ruim geformuleerd doel, als de uitvoering van een jaarlijkse enquête het eigenlijke doel van de verwerking van persoonsgegevens is.

- de bijbehorende documenten zijn niet altijd als bijlage toegevoegd, bijvoorbeeld: er ontbreken authenticatieformulieren en/of PIA's;
- bij een aantal door ons onderzochte verwerkingen zijn bepaalde belangrijke gegevens niet ingevuld in het AVG register. Een voorbeeld hiervan is de "bewaartermijn". Soms wordt hier verwezen naar een algemene selectielijst zonder nadere criteria voor de bewaartermijn aan te geven.
- daarnaast worden categorieën van betrokkenen en verstrekkingen vaak (te) algemeen geformuleerd.

1.4.3 Geen vastgelegde werkwijze voor het periodiek actualiseren van verwerkingen

Wij zijn in ons onderzoek geen beschrijving tegen gekomen voor het (periodiek, bijv. jaarlijks) actualiseren van het verwerkingsregister. Ons beeld is dat de datacoördinatoren van de organisatieonderdelen verantwoordelijk zijn voor het actualiseren van het verwerkingsregister. De datacoördinatoren moeten zelf aangeven of zij ondersteuning nodig hebben, van bijv. de CIO-office. Het privacybeleid stelt dat de privacy officer verantwoordelijk is voor de coördinatie van het goede gebruik en een goede vulling van het verwerkingsregister en de datacoördinatoren hierover adviseert. Een meer directieve aanpak richting de datacoördinatoren lijkt gewenst omdat de kwaliteit van de vulling van het verwerkingsregister op een aantal punten achter blijft (zie vorige paragraaf).

1.4.4 Uiteindelijke publicatie van alle registraties afhankelijk van voldoende capaciteit (onder andere van FG)

De laatste stap in het proces is de publicatie van de verwerkingen op "Rijksoverheid.nl". Op 26 februari waren 9 van de 125 verwerkingen gepubliceerd. Dit betekent dat er nog behoorlijk wat werk te doen is. Inmiddels hebben CIO Office en FG er, in overleg met de datacoördinatoren, voor gekozen onderscheid te maken tussen primaire en secundaire verwerkingen: de 55 primaire verwerkingen worden als eerste gepubliceerd, de secundaire verwerkingen eventueel later.
SG/bedrijfsvoering moet nog een aantal PIA's uitvoeren. Ook bij de afdeling O&P is nog veel werk te doen. Voor de publicatie is een actie van de FG nodig, terwijl de FG hier eigenlijk geen tijd voor heeft. Een evaluatie van de werkzaamheden van de FG is aangekondigd voor Medio 2019.

1.5 Thema 4: Procedure meldplicht datalekken

1.5.1 Procedure meldplicht datalekken opgesteld conform AVG en uitgedragen

Het Ministerie van Financiën heeft een procedure meldplicht Datalekken opgesteld. Via het Rijksportaal, lunchlezingen en introductiebijeenkomsten voor nieuwe medewerkers is de procedure bekend gemaakt binnen Financiën. Hierin staan de uitgangspunten, principes en processtappen waar het ministerie en haar medewerkers zich aan dienen te houden omschreven.
De medewerkers van Financiën melden in eerste instantie een mogelijke datalek bij de lijnmanager. Vervolgens vult de medewerker/lijnmanager samen met de data coördinator het document 'Registratie Datalek' in dat gebaseerd is op de informatie die de AP vraagt bij het melden van een datalek. Dit document stuurt de data-coördinator vervolgens naar het Meldpunt Datalekken dat bestaat uit de CISO, de privacy officer en een adviseur informatiebeveiliging.

1.5.2 Datalekkenregister sinds februari 2018 vastgelegd in Topdesk en conform AVG

Iedere melding over een mogelijk datalek wordt in het datalekkenregister bewaard. Hiervoor wordt Topdesk, een incident en change tool gebruikt. In Topdesk staan alle wettelijke verplichte gegevens, zoals gesteld in art. 33.5 van de AVG. De AP kan door middel van een bezoek aan het Ministerie van Financiën het datalekkenregister inzien. De registraties in het datalekkenregister worden tenminste 3 jaar bewaard ten behoeve van rapportage en verantwoording. Of er na het verstrijken van die 3 jaar een beoordeling plaatsvindt van het al dan niet verwijderen van de registratie is nog niet duidelijk.

1.5.3 *Procedure meldplicht datalekken is in 2018 toegepast*

In 2018 zijn er 7 meldingen gedaan aan de AP. De criteria die ten grondslag liggen aan het wel of niet melden aan de AP en eventueel de betrokkene(n) komen uit de AVG en zijn door het Meldpunt Datalekken op hoofdlijnen uitgewerkt. De privacy officer voert het datalek onderzoek uit. Het definitieve besluit voor een melding aan de AP en eventueel de betrokkene(n) wordt genomen door de CISO na afstemming met de PO en FG. De termijn van 72 uur was in 2018 geen probleem. Zo nodig is er een voorlopige melding gedaan bij de AP.
De melding aan de AP wordt gedaan door de CISO waardoor het takenpakket van de CISO ruimer is dan de functienaam suggereert. Of hier sprake is van een geldig mandaat moet nog worden uitgezocht. Dit is bekend bij DJZ en wordt opgepakt. Het recent ontwikkelde document 'Registratie Datalek' dat door de data-coördinator wordt aangeleverd aan het meldpunt datalekken is gebaseerd op het meldingsformulier van de AP. Dit maakt het opvoeren van de gegevens door de CISO bij de AP gemakkelijk.

Wanneer de inbreuk waarschijnlijk een hoog risico heeft voor de rechten en vrijheden van de betrokkene, dan worden de betrokkene geïnformeerd door de verwerkingsverantwoordelijke. Dit is in 2018 een aantal keer gebeurd. Het Meldpunt Datalekken, in overleg met de FG, levert input voor de benodigde informatie die aan de betrokkene(n) medegedeeld dient te worden conform de AVG.

1.5.4 *Aansluiting met incidentprocedure is aandachtspunt*

Een mogelijk datalek is altijd een informatiebeveiligingsincident, maar een informatiebeveiligingsincident waar geen persoonsgegevens bij betrokken zijn is geen datalek. De privacy officer schrijft op dit moment een notitie waarin de definitie en het proces van informatiebeveiligingsincidenten en datalekken worden verduidelijkt.

2 Bevindingen inzake implementatie AVG bij Belastingdienst

2.1 Inleiding

Uitgangspunten onderzoek
Na de invoering van de AVG op 25 mei 2018, heeft de Belastingdienst een aantal punten onderkend die buiten de basispositie AVG voor de Belastingdienst vielen. In het DT van de Belastingdienst van 24 mei, 7 juni en 19 juli 2018 is besloten om deze punten op te pakken en zijn er dienstonderdelen als actiehouder benoemd conform de besturingsfilosofie van de Belastingdienst, die uitgaat van lijnsturing. In oktober/november zijn de maatregellijsten door B/IV&D (in oprichting) in één-op-één gesprekken met alle data-coördinatoren van de diverse belastingdienstonderdelen doorgesproken.
De ADR heeft in overleg met de opdrachtgever 4 van deze maatregelen/thema's geselecteerd voor nadere analyse bij de Belastingdienst. Ten aanzien van de thema's 1, 2 en 4 zijn gesprekken gevoerd bij de dienstonderdelen MKB en CAP[3]. Ten aanzien van thema 3 is een gesprek gevoerd bij het dienstonderdeel IV.

De onderzochte thema's zijn:
1. Archiveren, schonen en verwijderen;
2. Beoordelen en actualiseren autorisaties;
3. Delen van gegevens;
4. Verwerkersovereenkomsten.

Met betrekking tot deze thema's zijn de volgende onderzoeksvragen gesteld:
- Wat is de objectief vast te stellen stand van zaken van een aantal geselecteerde maatregelen uit de implementatieplannen?
- Welke factoren zijn van invloed op een goede en tijdige realisatie van de nog uit te voeren geselecteerde maatregelen uit de implementatieplannen?

Context onderzoeksresultaten
Tijdens het onderzoek hebben wij de volgende observaties gedaan, die naast de onderzoeksuitkomsten naar voren zijn gekomen en die context geven bij de onderzoeksresultaten:
- De belastingdienstonderdelen zijn zich bewust van het belang van de AVG implementatie en doen zoveel als mogelijk wat binnen hun eigen beïnvloedingsvermogen ligt;
- De Belastingdienst is transparant in de openstaande punten. Zo is de maatregelenlijst met de Autoriteit Persoonsgegevens gedeeld;
- Voor de maatregelen zijn niet altijd plannen van aanpak uitgewerkt;
- De onderdelen hebben veelal zelf kaders opgesteld als deze kaders niet beschikbaar waren. Er is op dit moment geen gemeenschappelijk beeld tussen de uitvoerende onderdelen en de beleidsonderdelen, welke beleidskaders inzake de AVG er zouden moeten zijn. Ook is soms een ander beeld over de aanpak, over de rol van de B/IV&D en de rol van de data-coördinatoren;
- Een complicerende factor is dat er naast de AVG veel aanpalende wetgeving is die ook geïmplementeerd moet worden, zoals bijvoorbeeld de archiefwet.

[3] Voor toelichting keuze MKB, CAP, zie hoofdstuk 4

2.2 Thema 1: Archiveren, schonen en verwijderen

De Belastingdienst heeft "Archiveren, schonen en verwijderen van gegevens" als belangrijk handhavingsrisico onderkend om aantoonbaar te voldoen aan de AVG. Om te voldoen aan het AVG-principe van dataminimalisatie zijn de volgende maatregelen benoemd:

3 : Niet archiefwaardige bestanden vernietigen
5 : Toepassen selectielijsten

Hierbij zijn gegevens onder te verdelen in:
- Gestructureerde gegevens;
- Ongestructureerde gegevens.

De gestructureerde gegevens zijn alle gegevens die opgeslagen zijn in formele systemen, Robuuste Tijdelijke Voorzieningen (RTV's) en Locaal Ontwikkelde Applicaties (LOA's). De ongestructureerde gegevens zijn de gegevens die opgeslagen staan op de samenwerkingsgebieden, communities (bijvoorbeeld Connect People), persoonlijke schijven en de Email postvakken.
Een selectielijst is een systematische opsomming van archiefbescheiden. Deze opsomming bevat de categorieën te bewaren en te vernietigen archiefbescheiden

2.2.1 Maatregel inzake niet archiefwaardige bestanden vernietigen lijkt haalbaar voor ongestructureerde gegevens specifiek van het eigen dienstonderdeel

Het belastingdienstonderdeel CAP geeft zelf aan dat inzake het vernietigen van "Niet archiefwaardige bestanden" nog veel werk is te verrichten. Dit geldt zowel voor gestructureerde gegevens als voor ongestructureerde gegevens. CAP heeft geen plan van aanpak uitgewerkt voor deze maatregel, maar wel een werkwijze opgesteld voor het opschonen van de ongestructureerde gegevens.
Deze werkwijze houdt in dat acties zijn ondernomen om te werken aan het bewustwordingsaspect onder CAP medewerkers en teamleiders. Zo heeft elke medewerker een AVG awareness training gevolgd. Ook is door de plaatsvervangende directeuren een mail verstuurd met werkinstructies aan de teamleiders ten behoeve van schoning van de persoonlijke schijf.
Voor het vernietigen van gestructureerde gegevens loopt de pilot 'datahygiëne' bij Particulieren, de uitkomsten waren ten tijde van het onderzoek nog niet bekend.

Bij het belastingdienstonderdeel MKB zijn er onder aansturing van een eigen projectleider AVG, inzake het vernietigen van "Niet archiefwaardige bestanden" de volgende activiteiten ontplooid. Allereerst is er een pilot in Eindhoven uitgevoerd. Dit heeft input opgeleverd voor het zelf ontwikkelen van kaders en een handleiding. Hierbij is samengewerkt met CAP en Particulieren.
Gemeenschappelijk beleid ontbreekt, maar MKB heeft wel stappen gemaakt voor wat betreft die zaken die volgens MKB binnen haar eigen beïnvloedingsvermogen liggen. Dit betreft voornamelijk de ongestructureerde gegevens.
Op 1 februari 2019 heeft ongeveer 65% van de medewerkers van MKB verklaard dat schoning heeft plaatsgevonden conform kaders en de werkinstructie.

2.2.2 Gat tussen beleid en uitvoering, beperkte toetsing op bereiken eindresultaat, geen beschrijving informatiehuishouding

Onderstaande factoren zijn van invloed op een goede en tijdige realisatie van het vernietigen van niet archiefwaardige bestanden:

1. Gat tussen beleid en uitvoering inzake vernietigen bestanden op samenwerkingsgebieden;
2. Beperkte toetsing op bereiken eindresultaat;
3. Geen beschrijving informatiehuishouding.

Ad.1) Gat tussen beleid en uitvoering
Voor het vernietigen van archiefbestanden op samenwerkingsgebieden voelen een aantal dienstonderdelen zich afhankelijk van IV&D. Mede door de ruimte tussen de beleidskaders en de uitvoeringspraktijk ten aanzien van het vernietigen van archiefbestanden op de samenwerkingsgebieden, is het voor een aantal dienstonderdelen moeilijk om tot een eigen aanpak te komen.

Ad.2) Beperkte toetsing op bereiken eindresultaat
Er is beperkte toetsing op het bereiken van de doelstelling "vernietigen van niet archiefwaardige bestanden". Het dienstonderdeel Grote Ondernemingen heeft de beschikking over een Q-scanner, waarmee de samenwerkingsgebieden kunnen worden getoetst op de aanwezigheid van persoonsgegevens. De Q-scanner kan door een medewerker worden gebruikt om op basis van zijn of haar user-id te achterhalen in welke directories op de Q-schijf (het samenwerkingsgebied) er bestanden staan waarvan hij/zij 'eigenaar' is. De scanner scant niet op inhoud. Er loopt momenteel een onderzoek door het dienstonderdeel IV of deze Q-scanner breder binnen de Belastingdienst kan worden ingezet.

Ad.3) Geen beschrijving informatiehuishouding
De informatiehuishuishouding van de Belastingdienst is niet formeel uitgewerkt in allemaal Domeinarchitecturen. Ook is er geen ondersteunde tooling voor de informatiehuishouding, bijvoorbeeld door middel van een Documentair Managementsysteem zoals Digidoc. Daarnaast zijn bedrijfsvoeringfunctionaliteiten voor schonen en/of archiveren niet standaard in de Belastingdienstapplicaties ingebouwd. Dit betekent dat het vernietigen van bestanden een handmatig en daarmee tijdrovend proces is.

2.2.3 *Maatregel inzake toepassen selectielijsten lijkt niet haalbaar*

Bij CAP zijn de selectielijsten nog niet toegepast op de gestructureerde gegevens. CAP geeft aan dat deze maatregel op het kritieke pad ligt. Als factoren worden genoemd:
- geen volledig beeld/inzicht over het gebruik van gegevens in de keten;
- onvoldoende IV ondersteuning;
- onduidelijkheid over de van toepassing zijnde bewaartermijnen.

Aangezien deze factoren niet eenvoudig zijn op te lossen en voor de oplossing interne afstemming met de andere dienstonderdelen noodzakelijk is, lijkt deze maatregel niet voor 25 mei 2019 haalbaar.

MKB heeft de intentie om de selectielijsten toe te gaan passen. MKB geeft in de rapportage[4] aan dat deze maatregel op schema ligt.
Wel geeft MKB aan dat er onduidelijkheid is over begin en eindverantwoordelijkheid van de gegevens. Door ontbreken van eenduidig beleid en juiste tooling worden samenwerkingsgebieden naar eigen inzicht gearchiveerd. Daarom lijkt deze maatregel niet voor 25 mei 2019 haalbaar.

2.2.4 *Onvoldoende IV ondersteuning, onduidelijke verantwoordelijkheidsverdeling inzake gebruik gegevens in de keten en implementatie selectielijsten*

Onderstaande factoren zijn van invloed op een goede en tijdige realisatie bij toepassen selectielijsten:
1. Onvoldoende IV ondersteuning;
2. Geen volledig beeld/inzicht over het gebruik van gegevens in de keten, waardoor er onduidelijkheid is over de van toepassing zijnde bewaartermijnen;
3. Feitelijke implementatie selectielijsten.

[4] Rapportage: januari 2019

Ad.1) Onvoldoende IV ondersteuning
Om de selectielijsten niet handmatig, maar geautomatiseerd toe te kunnen passen zijn IV aanpassingen nodig. Door prioriteitstelling in de IV, komen deze aanpassingen tot op heden niet aan bod.

Ad.2) Geen volledig beeld gebruik gegevens in keten
Door het ontbreken van een volledig beeld van het gebruik van gegevens in de keten, ontstaat er onduidelijkheid over welke selectielijsten toegepast moeten worden en daarmee ook welke bewaartermijn gehanteerd moet worden.

Ad.3) Feitelijke implementatie selectielijsten
De selectielijsten die door CFD zijn opgesteld zijn nog niet door de uitvoerende dienstonderdelen geïmplementeerd. Dit betekent dat het toepassen van de selectielijsten niet op korte termijn kan worden uitgevoerd en afgerond.
Het toepassen moet met voldoende aandacht gebeuren, anders zou dit veel onrust en onzekerheid kunnen geven, omdat onder druk van de AVG wellicht bestanden worden weggegooid die later nog nodig blijken.

2.3 Thema 2: Beoordelen en actualiseren autorisaties

De Belastingdienst heeft "autorisaties" ook als handhavingsrisico onderkend om aantoonbaar te voldoen aan de AVG. Om het risico op te brede toegang tot gegevens te verminderen zijn de volgende maatregelen benoemd:
4 : Beoordeling actualiteit autorisaties
6 : Intrekken autorisaties

2.3.1 Maatregel inzake beoordeling actualiteit autorisaties is reeds gehaald

Alle dienstonderdelen moesten vóór 1 oktober 2018 rapporteren over de actualiteit van de bestaande autorisaties. Wij hebben de situatie voor CAP en MKB onderzocht.

CAP heeft invulling gegeven aan deze verplichting door een uitvraag te doen naar de actualiteit van de autorisaties bij alle onderdelen van CAP. De uitkomsten van de uitvraag gaven een grillig beeld en is beschreven in een memo "Rapportage AVG toets". CAP benoemt als oorzaak van het grillige beeld, dat CAP een bedrijfsonderdeel is met meer dan 190 teams met onderling een grote diversiteit aan werkzaamheden.
Bij de meer op de standaardwerkwijze georiënteerde semi-massale processen zijn de autorisaties over het algemeen met behulp van standaardprofielen ingericht en toebedeeld. Deze standaardprofielen zijn er niet bij de minder gestandaardiseerde werkzaamheden (bijvoorbeeld rond functioneel beheer en de diverse taken rond inwinnen en verstrekken van gegevens).
Om een koppeling van rollen aan functies mogelijk te maken moet het functiehuis beter worden ingericht. Aangezien dit een actie is die niet sec gedaan hoeft te worden volgens de AVG, is dit geen onderdeel van de huidige implementatie AVG die loopt tot 25 mei 2019. De realisatie van het functiehuis zal in afstemming met SSO F&MI moeten plaatsvinden en heeft een doorlooptijd die loopt tot na 25 mei 2019.

MKB heeft de verplichting om te rapporteren over de actualiteit van de bestaande autorisaties ingevuld door een 3 stappenplan op te stellen op het thema autorisaties:
Stap 1 : korte termijnacties tot 25 mei 2019 (onderdeel vervolgimplementatie AVG)
Stap 2 : inrichten generieke structuur en werkwijze
Stap 3 : borging van de inrichting (AO/IC) en uitvoeren checks en balances.

Voor stap 1 is MKB gestart met een inventarisatie van de bij de medewerkers aanwezige autorisaties. In de analysefase heeft de rollenbeheerder IMS[5] veel

[5] IMS (Identity Management System) is de geautomatiseerde IV-voorziening die het proces van Logisch Toegangs Beheer (LTB) ondersteunt.

voorbereidend werk verricht. De ruim 6600 MKB-medewerkers hebben ongeveer 96.000 autorisaties, waarvan 11.000 dienstonderdeel overstijgende rollen.
Op basis van de analyse is een plan gemaakt voor het intrekken van autorisaties, zie paragraaf 2.2.2.

2.3.2 *Maatregel inzake intrekken autorisaties is alleen haalbaar voor dienstonderdeel overstijgende rollen*

Zowel bij CAP als bij MKB is de maatregel intrekken autorisaties voor de termijn tot 25 mei 2019 toegespitst op de analyse en het voor zover mogelijk intrekken van autorisaties die dienstonderdeel vreemd zijn. Het realiseren van deze toegespitste maatregel is voor zowel MKB als voor CAP haalbaar.

MKB heeft op basis van de uitkomsten van de analyse een pilot opgesteld om een eerste schoning uit te voeren. Na de pilot is inmiddels de schoning MKB breed uitgevoerd. Er zijn nu nog 2% (ongeveer 2000) dienstonderdeelvreemde autorisaties over die om nader onderzoek vragen (noodzaak, continuïteit proces)

Dit zal tot een van de volgende vervolgacties leiden:

- als nog schonen;
- in een andere bedrijfsrol van MKB opnemen van de rechten;
- in een bedrijfsrol van een ander dienstonderdeel opnemen, waarbij dat dienstonderdeel dan ook de verantwoordelijkheid (goedkeuring) krijgt.
- is er geen MKB rol en is deze wel nodig, dan wordt de vreemde rol in overleg met andere bedrijfsonderdelen omgezet naar een MKB rol.

De voortgang van de stap 1 acties, zoals toegelicht in paragraaf 2.2.1, is opgenomen in rapportages van het MT.

CAP gaat het intrekken van dienstonderdeel vreemde autorisaties nog uitvoeren. De werkwijze is vastgesteld evenals het rapportageformat. Eind februari is door CAP een instructie opgesteld voor de teamleiders die deze actie moeten gaan uitvoeren.

2.3.3 *Structurele verbeterslagen in autorisatiebeheer vraagt een langere doorlooptijd*

De beoordeling van de autorisaties heeft meerdere aandachtspunten rond het inrichten en beheren van autorisaties opgeleverd. Het oplossen van deze aandachtspunten vraagt een lange doorlooptijd waarin de nodige afstemming zal moeten plaatsvinden tussen de diverse dienstonderdelen en de SSO F&MI.

Na het realiseren van de korte termijnacties gaan zowel CAP als MKB verder met het nemen van stappen om het autorisatieproces als geheel te verbeteren.
MKB heeft daar al initiatieven in genomen. Stap 2 is inmiddels ook opgepakt. MKB werkt aan een soort blauwdruk waarin de autorisatieprofielen allereerst worden gekoppeld aan de Functieprofielen Rijk en vervolgens, met name voor de toezichts-gerelateerde profielen, aan de specifieke inrichting van MKB. Dit resulteert naar verwachting in ongeveer 30 tot 50 functie en rolspecifieke autorisatiepakketten.
Het resultaat wordt vervolgens afgestemd met de portefeuillehouders en de procesregisseurs binnen het eigen dienstonderdeel en rollenbeheer binnen de SSO F&MI. Na alle afstemmingen zal de feitelijke omzetting in de applicatie IMS moeten plaatsvinden. Dit is nog een grote operatie.
Stap 3 betreft aanpassingen die nodig zijn om te komen tot een structureel AVG-conform autorisatiebeheer door de inrichting en uitvoering van checks en balances in het autorisatiebeheerproces.

2.4 Thema 3 : Delen van gegevens

De Belastingdienst heeft "Delen van gegevens" ook als handhavingsrisico onderkend om aantoonbaar te voldoen aan de AVG. Om het risico op ongebreideld (her)gebruik en te brede toegang tot gegevens te verminderen zijn de volgende maatregelen benoemd:
16 : Uitfaseren datadumping faciliteiten dan wel gebruik afschermen

17 : Gebruik productiedata in testomgeving stoppen: pseudonimiseren dan wel fictieve testdata gebruiken.

2.4.1 *Maatregel inzake datadumping faciliteiten uitfaseren dan wel afschermen is niet voldoende SMART gemaakt*

Een objectieve vaststelling hoever de Belastingdienst is met de maatregel inzake datadumping faciliteiten uitfaseren dan wel afschermen, hebben wij niet kunnen maken.

De reden hiervoor is dat deze actie niet uitgewerkt is in een plan met doelstelling, die we kunnen toetsen.

2.4.2 *Reorganisatie Belastingdienst beïnvloedt haalbaarheid uitfaseren dan wel afschermen datadumping faciliteiten negatief*

De Belastingdienst rapporteert zelf dat deze maatregel op schema ligt. Aangezien deze maatregel ligt bij IV en de Directie IV technisch gezien de datadumping (bulkexport) met onmiddellijke ingang kan stopzetten, lijkt dit een goede inschatting.
Echter door het onmiddellijk stopzetten van de datadumping faciliteit kan er binnen de Belastingdienst een continuïteitsprobleem in een primair of ondersteunend proces ontstaan. Dit roept de vraag op of deze maatregel niet eerder bij de uitvoerende dienstonderdelen zou moeten zijn belegd, aangezien zij formeel juridisch de zorgplichtigen voor de persoonsgegevens zijn.

2.4.3 *Maatregel gebruik productiedata in testomgeving stoppen is niet voldoende SMART gemaakt*

Directie IV heeft een uitvraag gedaan in de markt naar producten die het mogelijk maken testdata te anonimiseren dan wel pseudonimiseren. Een onderliggend plan met doelstelling hiervoor hebben we niet aangetroffen.

2.4.4 *Onvoldoende commitment of het stoppen met productiedata in de testomgeving de juiste uitwerking is om gesignaleerd risico te verminderen*

De voornaamste belemmering voor het tijdig realiseren is, dat er onvoldoende commitment is voor de gekozen uitwerking om in principe helemaal te stoppen met het gebruik van productiedata in de testomgeving[6]. De AVG verbiedt het gebruik van productiedata, tenzij hiervoor een noodzaak is.
Niet duidelijk is welke argumenten/onderbouwingen er zijn om het gebruik van productiedata voor testdoeleinden volledig stop te zetten gelet op risico's voor de kwaliteit van de mededelingen van de Belastingdienst.

De Belastingdienst heeft een bestaande procedure die voorziet in het op beheerste wijze gebruik maken van een kopie van productiedata in de gebruikersacceptatie-testomgeving.
De procedure Gebruik productiedata in Test en Acceptatieomgevingen (versie 2.0 van 22-10-2015) kent onder meer een aanvraag en toestemmingstraject, het selectief toewijzen van autorisaties en het vernietigen van testoutput en de kopie productiedata.

2.5 Thema 4: Verwerkersovereenkomsten

Het thema verwerkersovereenkomsten is door de Belastingdienst niet als belangrijk handhavingsrisico benoemd. Dit heeft als voornaamste reden dat de Belastingdienst voor nagenoeg alle geautomatiseerde gegevensverwerkingen gebruik maakt van het Data Center Services (DCS) dat valt onder het dienstonderdeel directie IV.

---

[6] Op 24 mei 2018 heeft DT BD besloten: Er worden geen productiedata gebruikt voor testdoeleinden; testen geschiedt met fictieve testdata dan wel met gepseudonimiseerde productiedata. Aangesloten wordt bij rijksbrede initiatieven zoals het 'testdorp'. Als testen zonder (gepseudonimiseerde) productiedata onvermijdelijk is, wordt extra maatregelen getroffen om de bescherming van de gegevens te waarborgen

Op basis van gesprekken met de opdrachtgever hebben wij dit thema wel betrokken in het onderzoek. Mede ook in verband met de vergelijkbaarheid met het kerndepartement.

De volgende verwerkingen[7] zijn in het AVG-register aangetroffen bij de dienstonderdelen die in scope waren, waarbij een verwerker staat geregistreerd, stand 28 februari 2019.

CAP

Naam verwerking	Verwerker	Verwerkers-overeenkomst aanwezig
M882 - Verstrekken van persoonsgegevens M937 - Verstrekking BSN aan Binnenlandse Zaken	Logius	JA NEE (niet geregistreerd bij deze verwerking)
M880 - Inwinnen van persoonsgegevens voor de taken van de Belastingdienst	stichting RINIS	NEE
M687 - Behandelen aangifte BZM (Belasting Zware Motorrijtuigen); M738 - Betalen BZM (Belasting Zware Motorrijtuigen)	AGES GMBH	NEE

MKB

Naam verwerking	Verwerker	Verwerkers-overeenkomst aanwezig
M1234 - Opleggen naheffingsaanslag omzetbelasting; M871 - In beheer nemen loonaangiftebericht; M1270 - In beheer nemen Eerstedagmelding; M1235 - Omzetbelasting, intracommunautaire prestaties, Toezicht verwervingen; M1225 - Afhandelen aangifte en correctie op aangifte OB nationaal; M1097 - Omzetbelasting, Intracommunautaire prestaties, afhandelen opgaaf en correctie; M1057 - registreren verklaring Uitsluitend zakelijk gebruik bestelauto; M1307 - Aangifteverzuimbehandeling Loonheffingen	Logius	JA
M3638 – Deelname fora Fiscaal Dienstverleners, Salaris en Horizontaal Toezicht	Pleio	NEE
M1083 - Het afhandelen specifieke doelgroep TBZ	CAK	NEE
M1650 - Toezicht houden op rangschikking Natuurschoonwet (NSW); M1429 - Beoordelen verzoek (rangschikking, wijziging of vooroverleg) ikv Natuurschoonwet	DocDirekt	JA

2.5.1 *Geen gedeeld beeld binnen de Belastingdienst wanneer een organisatie een verwerker is*

De ADR ziet geen consistente lijn in het AVG-register ten aanzien van het gebruik van de term verwerker. Uit gesprekken met de data-coördinatoren komt naar voren dat niet duidelijk is hoe binnen de Belastingdienst omgegaan dient te worden met het begrip verwerker.

2.5.2 *Nog niet alle verwerkersovereenkomsten aanwezig of geactualiseerd*

De belangrijkste verwerker voor de Belastingdienst is Logius. De verwerkersovereenkomst van Logius hebben we getoetst en dat leidde tot de volgende opmerkingen:

- Het toenmalige meest recente ARVODI model is gebruikt bij de opstelling van de verwerkersovereenkomst in 2016, een addendum in verband met de huidige ARVODI 2018 model is niet aangetroffen. Overigens voldoet de overeenkomst wel aan de belangrijkste eisen van de AVG;
- In de verwerkersovereenkomst staat dat Logius en de Belastingdienst nog moeten bepalen wie van beiden de melding van het datalek aan de AP gaat

[7] Teruggetrokken verwerkingen zijn buiten scope geplaatst

doen. Dit laatste is in strijd met het privacy beleid van het Ministerie van Financiën. Uitgangspunt in het privacy beleid is, dat de verwerker zelf geen melding van het datalek mag doen bij de Autoriteit Persoonsgegevens.

Er is geen getekende verwerkersovereenkomst van de Belastingdienst met de verwerker "Rinis". Wel is er een concept.

3 Aanbevelingen en/of vervolgstappen

3.1 Situatie kerndepartement

Op basis van onze bevindingen uit hoofdstuk 1, denken wij dat de volgende vervolgstappen wenselijk zijn om op 25 mei 2019 aantoonbaar (op een adequaat niveau) aan de AVG te voldoen:

1. Een duidelijke vastlegging wat nog gedaan moet worden. Dit is met name van toepassing voor het thema "Schoning netwerkschijven", zodat duidelijk is wat een oud issue is en wat een nieuw issue is, zodat er beter en sneller inzicht is in de feitelijke voortgang;

2. Om strakker te sturen bevelen wij een meer projectmatige aanpak aan. Wij denken hierbij aan de volgende key-elementen:
   - op welke manier je de doelen wilt realiseren, met andere woorden de aanpak;
   - wie wat moet doen;
   - wie regie voert;
   - wie controleert op realisatie;
   - wie ondersteunt waarbij;
   - wie voert kwaliteitscontroles uit.

   Dit betekent dat er meer controle en regie op de uitvoering van de AVG acties door de data-coördinatoren ontstaat en dat er indien nodig sneller bijgestuurd kan worden en de data-coördinatoren gerichter ondersteund kunnen worden. Dit is bij alle thema's relevant;

3. Te overwegen valt om de aanpak van de verschillende thema's tot 25 mei 2019 te prioriteren. De schoning van netwerkschijven is een continu proces dat ook na 25 mei doorgaat. Er zou, in het geval van capaciteitsproblemen, voor gekozen kunnen worden de registratie van verwerkingen en verwerkersovereenkomsten prioriteit te geven en de schoning van netwerkschijven pas na 25 mei te intensiveren met een periodieke ("batch-gewijze") aanpak.

4. Positief inzake de governance is het periodieke overleg tussen de data-coördinatoren en de Privacy Officer. Aanvullend bevelen wij aan om de CIO Office kerndepartement inclusief de Privacy Officer een pro-actievere rol toe te delen in het ondersteunen van de data-coördinatoren.
   Een mogelijke invulling zou kunnen zijn dat vanuit de CIO Office Kerndepartement "vliegende brigades" worden georganiseerd die langs de dienstonderdelen gaan voor ondersteuning op maat.

5. Tenslotte bevelen wij aan om de benodigde aandacht te geven aan het inrichten van een aantal procedures gericht op de borging van de kwaliteit. De feitelijke inrichting van deze procedures dient natuurlijk in lijn te zijn met het reeds vastgestelde "Privacy Beleid". Voorbeelden die aansluiten op de onderzochte thema's zijn:
   - de periodieke controle op het schonen van netwerkschijven;
   - het periodiek actualiseren van het verwerkingenregister; en
   - het periodiek actualiseren van de verwerkersovereenkomsten.

   Voor het uitvoeren van deze kwaliteitschecks is het van belang dat de nodige inhoudelijke expertise beschikbaar is, en wordt geborgd. Met behulp van deze procedures kan de Check van de PDCA-cyclus voor privacy worden ingevuld.

3.2 Situatie Belastingdienst

Op basis van onze bevindingen uit hoofdstuk 2, denken wij dat de volgende vervolgstappen wenselijk zijn om op 25 mei 2019 aantoonbaar (op een adequaat niveau) aan de AVG te voldoen:

1. Een korte heroverweging/hertoets te doen van alle issues (AVG acties) die nu gepland staan. Enerzijds om zeker te zijn dat deze acties noodzakelijk zijn voor het aantoonbaar voldoen aan de AVG en anderzijds om vast te stellen dat de eerder onderkende risico's door de voorgestelde AVG-acties op een zo effectief mogelijke wijze worden afgedekt en dat er geen betere alternatieven voorhanden zijn. Tenslotte dient het te bereiken doel voor elke AVG actie heel concreet te worden uitgewerkt om daadwerkelijk te kunnen meten of het doel op 25 mei 2019 is gehaald;

2. Om strakker te kunnen sturen bevelen wij een meer projectmatige aanpak aan. Dit betekent dat er meer regie op de uitvoering is van de AVG acties door de data-coördinatoren en dat er indien nodig sneller bijgestuurd kan gaan worden. Wij denken hierbij dat decentrale projectleiders die worden ondersteund door een centraal projectbureau, het best aansluit bij de huidige besturingsfilosofie van de Belastingdienst.
   Wij benadrukken hierbij het feit dat de projectleiders voldoende inhoudelijke expertise dienen te hebben.

3. Positief inzake de governance is de maandelijkse rapportage door middel van het AVG dash-board dat door de directie IV&D wordt gefaciliteerd. Aanvullend bevelen wij aan om de CIO Office Belastingdienst en dan met name de Privacy Officer een pro-actievere rol toe te delen in het ondersteunen van de data-coördinatoren.
   Een mogelijke invulling zou kunnen zijn dat vanuit de CIO Office Belastingdienst "vliegende brigades" worden georganiseerd die langs de Belastingdienst dienstonderdelen gaan voor ondersteuning op maat;

4. Uitgangspunt van de nieuwe topstructuur is: scheiding tussen beleid en uitvoering. Aangezien hier binnen de Belastingdienst nog niet zoveel ervaring mee is opgedaan, bevelen wij aan dat inzake de AVG (naast IV&D ook CFD en SSO-FM&I) de beleidsdirecties in nauwe samenwerking met de uitvoerende dienstonderdelen de beleidskaders opstellen.

   Mede ook omdat er een extra inspanning nodig is om zicht te krijgen op de noodzakelijke beleidskaders als uitwerking van de opgestelde beleidslijnen. Vanuit de onderzochte thema's denken wij hierbij in eerste instantie aan de volgende beleidskaders;
   - Uitgangspunten bij toepassing selectielijsten;
   - uitgangspunten vernietiging bestanden op samenwerkingsgebieden;
   - verantwoordelijkheidsverdeling van de dienstonderdelen bij gebruik gegevens in een ketens;
   - uitgangspunten bepaling noodzaak maken verwerkersafspraken.

5. Inzake de structurele verbeteracties die van belang zijn voor de naleving van de AVG, maar in feite een breder bereik hebben bevelen wij aan om dit op te nemen in een separaat project, dit belastingdienstbreed af te stemmen en hier ook een projectmatige aanpak op te zetten.

   Dit betreft in ieder geval de volgende onderwerpen:
   - de implementatie van de selectielijsten;
   - het op orde brengen van de informatiehuishouding (bijvoorbeeld langs de lijnen van het 'Rijksprogramma voor Duurzaam Digitale Informatiehuishouding').

6. Uit het onderzoek kwamen ook nog de volgende aandachtspunten naar voren die van belang zijn voor de aantoonbare naleving van de AVG. Wij bevelen aan om hier structureel aandacht aan te geven:
   - het verbeteren van het inzicht in het gebruik van persoonsgegevens in de keten;
   - het zodanig managen van de prioriteitstelling in de IV dat de functionaliteiten t.b.v. schonen en bewaartermijnen in de applicaties kunnen worden aangebracht;
   - het ontwikkelen van een voldoende dekkend AVG-normenkader om AVG-toetsing beter mogelijk te maken.

3.3 Slotopmerking

Tenslotte bevelen wij aan om te onderzoeken in hoeverre de bovenstaande aanbevelingen kunnen worden doorgetrokken naar de niet-onderzochte thema's en dienstonderdelen. Hierdoor kunnen de aanbevelingen ook ruimere werking hebben en mogelijk leiden tot structurele verbeteringen van de AVG-governance.

4 Verantwoording onderzoek

4.1 Werkzaamheden en afbakening

De werkzaamheden zijn uitgevoerd conform de beschrijving in de opdracht-bevestiging met kenmerk 2019-0000015300, d.d. 25 januari 2019, waarbij de peildatum van het onderzoek 28 februari 2019 betrof.

Hierbij merkt de ADR op, dat een uitspraak over het aantoonbaar voldoen aan de AVG op dit moment lastig is vanwege het ontbreken van een voldoende dekkend en geaccepteerd normenkader. Daarnaast is het voldoen aan de AVG een continu proces en dus niet op een bepaald moment "af".

Onderzoeksvragen:

1. Wat is de objectief vast te stellen stand van zaken van een aantal geselecteerde maatregelen uit de implementatieplannen van het kerndepartement en de Belastingdienst?
2. Welke factoren zijn van invloed op een goede en tijdige realisatie van de nog uit te voeren geselecteerde maatregelen uit de implementatieplannen?

Allereerst heeft de ADR een vooronderzoek uitgevoerd, waarbij een aantal thema's /maatregelen zijn geselecteerd. Deze selectie is afgestemd met het desbetreffende organisatiedeel. Wij willen benadrukken dat de ADR slechts een deel van alle thema's heeft onderzocht en nog maar bij een beperkt aantal dienstonderdelen, daarom trekken wij geen overall conclusie voor het Ministerie van Financiën.

Organisatiedeel	Thema/maatregel
Kerndepartement	1. Verwerkersovereenkomst 2. Schoning netwerkschijven 3. Kwaliteit verwerkingenregister 4. Meldplicht datalekken
Belastingdienst	1. Verwerkersovereenkomsten 2. Archiveren, schonen en verwijderen *3: Niet archiefwaardige bestanden vernietigen* *5: Toepassen selectielijsten* 3. Autorisaties *4: Beoordeling actualiteit autorisaties* *6: Intrekken autorisaties* 4. Delen van gegevens *16: Uitfaseren datadumping faciliteiten dan wel gebruik afschermen;* *17: Gebruik productiedata in testomgeving stoppen: pseudonimiseren dan wel fictieve testdata gebruiken.*

NB: In deze rapportage is het eerste thema van de Belastingdienst als laatste thema beschreven om beter aan te sluiten op de risico inschatting van de Belastingdienst.

Bij het kerndepartement is bij de eerste 3 thema's ingezoomd op de dienst-onderdelen: DG Rijksbegroting en de Generale Thesaurie. Daarvoor zijn gesprekken gevoerd met de desbetreffende data-coördinatoren. Ook is met de privacy officer en de projectleider AVG fase 2 gesproken over de eerste 3 thema's. Daarnaast is een analyse gemaakt van alle actuele verwerkingen van het kerndepartement in het AVG-register, stand 28 februari 2019. Met de CISO en de privacy officer is tenslotte gesproken over thema 4.

Bij de Belastingdienst is bij thema 1, de belangrijkste verwerkersovereenkomst onderzocht, namelijk Logius. Bij de thema's 2 en 3 is ingezoomd op de dienstonderdelen: MKB en CAP. Gekozen is voor deze dienstonderdelen omdat wij vooraf konden bepalen dat zij met persoonsgegevens werken en met heel veel gegevens werken. Daarvoor zijn gesprekken gevoerd met de desbetreffende data-coördinatoren. Ook is met een privacy deskundige en de CISO van de Belastingdienst gesproken over alle thema's inclusief de governance. Met de data-coördinator van IV is gesproken over thema 4.

4.2 Gehanteerde Standaard

Deze opdracht is uitgevoerd in overeenstemming met de Internationale Standaarden voor de Beroepsuitoefening van Internal Auditing.

In dit rapport wordt geen zekerheid verschaft, omdat er geen assurance-opdracht is uitgevoerd.

4.3 Verspreiding rapport

De opdrachtgever, pSG - Han van Gelder, is eigenaar van dit rapport.

De ADR is de interne auditdienst van het Rijk. Dit rapport is primair bestemd voor de opdrachtgever met wie wij deze opdracht zijn overeengekomen. In de ministerraad is besloten dat het opdrachtgevende ministerie waarvoor de 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 door de ADR uitgebrachte rapporten en plaatst dit overzicht op de website.

5 Ondertekening

Den Haag, 10 april 2019

Bijlage 1: Management Response

Managementreactie n.a.v. het onderzoeksrapport Implementatie AVG bij het Ministerie van Financiën

Aan de ADR als onafhankelijke partij heb ik gevraagd onderzoek te doen naar het op schema liggen van de opgestelde implementatietrajecten Algemene Verordening Gegevensbescherming (AVG) voor zowel het kerndepartement van Financiën als de Belastingdienst.

De ADR heeft dit onderzoek uitgevoerd en stelt terecht dat het belang van het implementeren van de AVG bekend is, maar de realisatie complex. De ADR heeft zowel voor het kerndepartement als voor de Belastingdienst aanbevelingen en vervolgstappen geformuleerd. Ik dank de ADR voor het onderzoek en voor de geformuleerde aanbevelingen/vervolgstappen.

De conclusies en aanbevelingen uit het onderzoek onderschrijf ik. De aanbevelingen zullen worden overgenomen en worden betrokken bij het vervolg van de implementatie van de AVG bij het kerndepartement en de Belastingdienst.

De Belastingdienst geeft aan actief te sturen op het mitigeren van de risico's die de ADR identificeert en verwacht de mitigerende maatregelen - met uitzondering van het archiveren en schonen van bestanden - voor eind mei 2019 afdoende gerealiseerd te hebben.

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