GEGEVENSBESCHERMINGSEFFECTBEOORDELING (GEB) RIJKSDIENST

RAMv1.0

Dit template is gebaseerd op "***Model Gegevensbeschermingseffectbeoordeling Rijksdienst***"; versie 0.2 voorportalen CIO-beraad, IOWJZ, ICBR; 24 Juli 2017.

Revisiegegevens

Versie	Datum	Auteur	Omschrijving
0.1	01-10-2017	Persoonsgegevens	Initiële versie
0.5	13-10		Resultaten interviews en brondocumenten verwerkt
0.8x	18-10		(Collegiale)reviewresultaten verwerkt
0.95	20-10		1e versie voor opdrachtgever
0.96	20-10		Finale conceptversie
1.0	23-10		Versie voor WBP-team

Inhoud

I. SAMENVATTING

Een *Gegevensbeschermingseffectbeoordeling (*GEB), de nieuwe term voor een PIA, legt het vergrootglas op de verwerking van persoonsgegevens met als doel het detecteren van risico's en aanreiken van risico-verminderende maatregelen.

De scope van de GEB is RAM als totaalproduct. RAM is beoordeeld op de huidige werking in 2017 en een eventueel verlengd gebruik na 1/1/2018[1]. Normaliter beoordeelt een GEB een voorgenomen (nieuwe) gegevenswerking. Doordat het in dit geval een meerjarig bestaande verwerking betreft met een voornemen tot uitfasering op zo kort mogelijke termijn, is de risico-beoordeling met bijbehorende maatregelen mede vanuit die context gedaan. Zou het een nieuwe, voorgenomen verwerking betreffen dan zou het risico-oordeel aanmerkelijk zwaarder zijn uitgevallen.

Er zijn interviews gehouden met vertegenwoordigers van de RAM-groep, CIE, CAO en MKB.

RAM is in veel opzichten een product dat heel lang zijn tijd ver vooruit was. In het bijzonder qua gebundelde (72) informatiebronnen. De daarop gebouwde functionaliteit bedoeld voor integraal inzicht op (fiscale)gegevens van burgers en bedrijven maakt RAM het meest complete product voor integraal klantinzicht binnen toezicht. Daarvoor brengt RAM brengt heel veel gegevens bij elkaar die normaliter gescheiden zijn opgeslagen. Gegevens met een hoog vertrouwelijk karakter gezien de fiscale, financiële en/of persoonlijke aard van de gegevens. Vanuit het oogpunt van borging van privacy zijn er de afgelopen jaren diverse, noodzakelijke, verbeteringen aangebracht in RAM ten aanzien van onder andere dataminimalisatie en informatiekwaliteit en-beveiliging.

De infrastructurele / technische opzet van RAM kent desondanks meerdere risico's[2] die in de huidige opzet niet (zomaar) zijn weg te nemen doordat het de onderliggende 'ontwikkelomgeving' betreft. Wetende dat er vanuit de IV-keten en D&A alternatieve, minder risicovolle, voorzieningen geleverd worden[3] leidt dit tot de conclusie dat de in 2016 geaccordeerde, migratie van RAM ook vanuit de in de GEB beschreven risico's onderschreven wordt. Daarnaast wordt een aantal maatregelen, in het bijzonder op basis van onderzoek door CIE onderschreven of vanuit de het assessment zelf benoemd bij het verwachte, verlengde gebruik van RAM na 1/1/2018.

De overall conclusie vanuit de GEB, indachtig de beschreven context in de 2e alinea, is dat er recent voldoende maatregelen zijn genomen of met een implementatiedatum op korte termijn zijn of kunnen worden ingepland, om zowel de 'exploitatie' van RAM in 2017 als het verlengd[4] beschikbaar stellen van RAM vanuit het oogpunt van de beschreven risico's acceptabel te achten. Dit onder de premisse dat zo spoedig mogelijk de migratie van RAM naar een nieuwe infrastructuur wordt gestart. Doe wel aanvullend onderzoek naar een aantal clusters van bronnen (van doorgaans niet (puur) fiscale aard, bv. ISC-data of strafrechtelijke data (FSV, GEFIS)). Hiervan wordt aanvullende toetsing geadviseerd om expliciet vast te stellen dat de verwerking voortgezet kan worden.

In de maatregelen is een aantal scenario's beschreven dat hier mede aan bijdraagt. Afhankelijk van de feitelijke uitfaseringdatum van het huidige RAM, wordt een toetsing op de uitvoering van de aanbevolen maatregelen in deze GEB aanbevolen in geval van een voortgezet gebruik van het huidige RAM na 1-7-2018.

[1] 1 januari 2018 staat sinds begin 2016 als de beoogde datum van uitfaseren (na migratie van RAM en soortgelijke data-sets en risico-/selectiemodellen naar een nieuwe omgeving).
[2] Waaronder ook niet privacy-specifieke risico's die in het SIG-rapport worden beschreven zoals de omvang/complexiteit van de broncode.
[3] Hiermee wordt geen uitspraak gedaan over de rolverdeling tussen partijen en de inplanbaarheid, doorlooptijd. Dat valt buiten de scope van een GEB.
[4] Na 1/1/2018 vanwege een naar verwachting niet voor die tijd afgeronde migratie.

II. VRAGENLIJST GEGEVENSBESCHERMINGSEFFECTBEOORDELING

A. Beschrijving algemene kenmerken gegevensverwerkingen

Beschrijf op gestructureerde wijze de voorgenomen gegevensverwerkingen, de verwerkingsdoeleinden en de belangen bij de gegevensverwerkingen.

1. Voorstel

Beschrijf het voorstel waar de gegevensbeschermingseffectbeoordeling (voorheen PIA) op ziet en de context waarbinnen deze plaatsvindt op hoofdlijnen.

Het onderzoeksobject van de GEB is het volledige product RAM (Risico Analyse Model) bestaande uit:

1. de infrastructurele elementen,
2. de verwerkte (fiscale/persoons)gegevens
3. de functionaliteit, te onderscheiden in de analyse-omgeving en de overige, deels voor gedefinieerde functionaliteit
4. het gebruik door en ten aanzien van medewerkers

Door Persoonsgegevens is in 2016 opdracht gegeven tot uitfaseren van het huidige RAM per 1/1/2018 uitgaande van een migratie van RAM naar een nieuwe omgeving met als beoogd opdrachtnemers D&A en IV'. Voor de periode tot 1/1/2018 zijn zogenoemde 'stutmaatregelen' genomen om de werking van RAM te verbeteren[5].

In deze GEB wordt RAM ten aanzien van twee invalshoeken getoetst; de werking van RAM op dit moment en een verwacht verlengd bestaan van RAM na 1/1/2018 vanwege een niet tijdig afgeronde (lees: nog niet gestarte) migratie van het huidige RAM naar een nieuwe omgeving. Risico's maar vooral ook maatregelen worden vanuit deze context beschreven.

RAM wordt zowel ingezet voor ten aanzien van de informatievoorziening over belastingplichtigen als voor bedrijfsvoeringsdoeleinden waaronder informatievoorziening over / ten aanzien van medewerkers van de Belastingdienst.

De GEB (alhoewel de naam afkomstig is uit de Avg) is geschreven op basis van Wbp. De Avg zal alleen daar worden aangehaald als er risico's / maatregelen worden beschreven die mede vanuit het oogpunt van de Avg behandeling moeten krijgen.

2. Persoonsgegevens

Som alle categorieën persoonsgegevens op die worden verwerkt en deel ze in onder de typen: gewoon, bijzonder of strafrechtelijk en wettelijk identificatienummer. Geef per persoonsgegeven aan op wie het betrekking heeft.

Gewone persoonsgegevens

RAM bevat een groot aantal bronnen die persoonsgegevens bevatten waarvan er zowel bronnen rechtstreeks geleverd/ontvangen worden en bronnen middels queries, voornamelijk uitgevoerd binnen CAP/Gegevens/BICC, ontsloten worden. Hieronder staat een indicatief, niet uitputtend, overzicht. In zijn algemeenheid geldt dat vrijwel alle gegevens betreffende alle Belastingmiddelen in RAM zijn opgenomen. RAM verwerkt deze gegevens tot een equivalent van het fenomeen 'datafundament' zoals binnen D&A wordt gecreëerd. Binnen RAM gaat het dan oa 'KernSofi' waarin de oorspronkelijke gegevens uit de diverse

[5] Deze GEB relateert aan maatregel .4 uit het 'Memo RAM beveiliging en toekomstige oplossing', dd 25-08-2017 van de Persoonsgegevens aan Persoonsgegevens

bronnen, aangevuld met berekende velden (rekenkundig en logisch bewerkt) ter beschikking worden gesteld. Dit 'KernSofi' is echter slechts een onderdeel van de mogelijk ter beschikking staande gegevens. Gegevens vanuit de onderstaande bestanden zijn voor de analisten direct beschikbaar tot op het hoogste detailnivo.

Hoofdgroep Type bestand:

a) Convenanten
b) DACAS
c) DOUANE
d) GEFIS-PVS
e) CTR
f) HT
g) IH-VPB
h) IH-VPB Aandeelhouders
i) LH
j) OB
k) Regio-BI-entiteiten-middelen-controles
l) RMLH
m) Toeslagen
n) VAR
o) Verzuimen
p) Voor bouwen Kern Sofinr
q) VPB
r) WOZ
s) Gegevens betreffende fiscale Loongegevens;

Naast deze 'sec' fiscale gegevens bevat RAM verder ook[6] :

t) Relatiegegevens van zowel van Natuurlijke Personen als Niet Natuurlijke Personen waaronder kinderen;
u) NAW-gegevens van zowel Natuurlijke Personen als Niet Natuurlijke Personen waaronder kinderen;
v) Gegevens betreffende de invorderingsadministratie ;
w) Gegevens betreffende Notariële akten;
x) Gegevens betreffende ANBI's;
y) Internet Service Centre
z) Gegevens betreffende Belastingconsulenten;
aa) Gegevens betreffende faillissementen;
bb) Gegevens betreffende Bankrekeningen;
cc) Gegevens betreffende Spaarrekeningen en effecten;
dd) Kadastergegevens ;
ee) Auto-gegevens;
ff) Gegevens betreffende gebouwen (BAG);
gg) Gegevens betreffende VIPS / ambtenarenposten;

Bijzondere persoonsgegevens

Veldnaam	Bron	Betrekking op
Afhankelijk van het gebruik kan Nationaliteit als een bijzonder persoonsgegeven gelden.	BVR, ...	Belastingplichtigen en/of (niet) beschreven

[6] LET OP: Niet limitatieve opsomming!

Strafrechtelijke gegevens

Veldnaam	Bron	Betrekking op
BSN, NAW	GEFIS, PVS?	
Karakter en status vervolging/opsporing		

Wettelijk identificatienummer

Veldnaam	Bron	Betrekking op
BSN	LH	Medewerker
LH-nummer	LH	Inhoudingsplichtige
OB-nummer	OB	OB-plichtige

3. Gegevensverwerkingen

Geef alle voorgenomen gegevensverwerkingen weer.

RAM heeft het karakter van een DataWarehouse en werkt met datafundamenten. Een dergelijke voorziening kent een aantal specifieke verwerkingen.

a) ETL (Extract, Transform en Load) ;

Van alle aanwezige bronnen worden gegevens overgenomen. In dit proces worden deze opgehaald, omgezet naar het te gebruiken formaat en opgeslagen. In dit proces worden de gegevens eventueel ook getransformeerd en verrijkt. De ETL processen in RAM worden, conform aanbevelingen uit het CAO 'stut-rapport' beter beveiligd door het gebruik van beter beveiligde Windowsservers en door het gebruik van Tera data voor opslag van gegevens. De genoemde ETL-processen worden echter uitgevoerd een klein aantal medewerkers. Dit personeel is niet expliciet werkzaam in de IV-keten en voert deze op informele basis uit.

De benodigde programmatuur is (grotendeels) geschreven in ACL, SAS en TD SQL. De software is beschikbaar voor en kan aangepast worden door de personen die (een deel van) deze ETL-processen uitvoeren. Hiermee ontstaat een risico van data-/ procesmanipulatie. Vergelijk dit met de IV-keten waar de applicaties op de productieomgeving gecompileerd zijn en daardoor niet aangepast kunnen worden. In de ORACLE database bestaat voor de gebruikers geen mogelijkheid om de data te manipuleren.

b) Verstrekkingen van gegevens t.b.v. analyses;

Een DataWare House biedt een gelegenheid tot het combineren van gegevens. De gegevens worden verwerkt voor analyse doeleinden. Een deel van analisten is werkzaam binnen het Expertisecentrum Handhaving terwijl anderen werkzaam zijn binnen de diverse projectteams.

Verstrekkingen in een vast formaat:

Binnen de processen van de Belastingdienst bestaat voor een aantal doeleinden de behoefte aan gegevensleveringen in een vast formaat die bijvoorbeeld bedoeld zijn voor behandeling van posten die in de analysefase zijn geselecteerd. Een groot deel van de gebruikers werken met "standaard" schermen en vooraf gedefinieerde gegevenssets die door de gebruiker niet zijn te manipuleren.
In een deel van de regio's worden medewerkers ingezet (als super gebruikers) die voor die regio gegevensvragen vertalen naar een functionele vraag en deze vervolgens extraheren uit RAM. Deze gegevens worden vervolgens ter beschikking gesteld aan de medewerkers die de vraag gesteld hebben. Onduidelijk is of elke regio dezelfde werkwijze hanteert.

4. Verwerkingsdoeleinden

Beschrijf de hoofd- en nevendoeleinden van de voorgenomen gegevensverwerkingen.
RAM is ontstaan binnen het toezicht van de 'Blauwe' Belastingdienst, tegenwoordig primair gepositioneerd binnen MKB. Het handhavingsdoel van de directie MKB is om in het midden- en kleinbedrijf een zo klein mogelijk 'nalevingstekort' te realiseren en daarmee een zo laag mogelijk bedrag aan verschuldigde belasting dat niet binnenkomt ('tax gap'). De directie beoogt het nalevingstekort te verminderen door een effectieve manier van gedragsbeïnvloeding gericht op het verhogen van de compliance en/of het optimaliseren van de belastingopbrengsten. Het uitgangspunt hierbij is dat klanten de aandacht krijgen die ze verdienen, waarbij de beschikbare capaciteit zo efficiënt mogelijk wordt ingezet[7].

RAM wordt ook gebruikt door de FIOD voor opsporingsdoeleinden in de context van fiscale fraude en overige taken van de FIOD.

RAM wordt ook gebruikt door de Douane voor haar VGEM-taken.

RAM wordt ook gebruikt door Toeslagen voor analysetaken.

RAM wordt mede gebruikt voor bedrijfsvoeringsdoeleinden door de Belastingdienst als werkgever waaronder verwerking voor behalen productiedoelen, productiekwaliteit, (anonieme) geaggregeerde overzichten en integriteitsschendingstoetsing.

De verdere verwerking vindt plaats binnen de reguliere processen van de Belastingdienst, FIOD, Toeslagen en Douane en valt als zodanig buiten de scope van deze GEB.

Ter illustratie van de in RAM beschikbare functionaliteit naast de vrije, niet voorgedefinieerde, analyse-mogelijkheden, volgt hieronder een niet-limitatief overzicht van het huidige gebruik van RAM ten behoeve van:

- Nalevingsbeelden;
- Fraudedetectie;
- 'Verwonder'adressen;
- Internationale gegevensuitwisseling;
- Vele tactisch/operationele producten, zoals bijvoorbeeld de arbeidsmarkt (LSI), bouw en dergelijke;
- Startersquerie;
- FD-aanpak
- ANBI;
- Ondersteuning integrale klantbehandeling

5. Betrokken partijen

Benoem welke organisaties betrokken zijn bij welke gegevensverwerkingen. Deel deze organisaties per gegevensverwerking in onder de rollen: verwerkingsverantwoordelijke, verwerker, verstrekker of ontvanger.

[7] Bron: 'MKB intelligence base', auteur Persoonsgegevens, sept. 2017

Benoem tevens welke functionarissen binnen deze organisaties toegang krijgen tot welke persoonsgegevens.

Organisatie[8]	*Rol(len)*	*Functionarissen*
Minister van Financiën namens deze de Persoonsgegevens Persoonsgegevens[9]	*Verwerkingsverantwoordelijke*	
MKB	*ontvanger*	*Beheerders; analisten; specialisten heffing, inning en bedrijfsvoering*
CAP	*verstrekker en ontvanger*	*Beheerders; analisten; specialisten heffing, inning en bedrijfsvoering*
(Z)GO	*ontvanger*	*Beheerders; analisten; specialisten heffing, inning en bedrijfsvoering*
Toeslagen	*verstrekker en ontvanger*	*Beheerders; analisten; specialisten heffing, inning en bedrijfsvoering*
FIOD	*verstrekker en ontvanger*	*Beheerders; analisten; specialisten heffing, inning en bedrijfsvoering*
Douane	*verstrekker en ontvanger*	*Beheerders; analisten; specialisten heffing, inning en bedrijfsvoering*
CAO	*Intern bewerker*	*(technisch) beheerder*
CIE	*Intern bewerker*	*(technisch) beheerder*
RAM-ontwikkelgroep	*Intern bewerker*	*(technisch) beheerder en / of ontwikkelaar*

6. Belangen bij de gegevensverwerking

Beschrijf alle belangen die de verwerkingsverantwoordelijke en anderen hebben bij de voorgenomen gegevensverwerkingen.

De continuïteit van RAM is vanuit het oogpunt van een juiste, zorgvuldige en bedrijfseconomisch zo verantwoord mogelijke wijze van uitvoering van taken van de Belastingdienst van groot belang. Met behulp van de RAM functionaliteiten en gegevens worden diverse processen ondersteund. De belangrijkste zijn:

Analysedoeleinden: RAM wordt grootschalig ingezet voor diverse vormen van onderzoek. Dit onderzoek ondersteunt de handhavingsregisseurs bij de creatie van de handhavingsstrategie. Daarnaast wordt met dergelijke analyseprojecten getracht fiscale onregelmatigheden te vinden en voor de toekomst te voorkomen. Ram ondersteunt voornamelijk een groep analisten welke geen toegang hebben tot andere hulpmiddelen of wiens primaire focus niet op ICT maar op materiekennis ligt.

Ondersteuning primair proces: RAM biedt een volledig klantbeeld aan de medewerkers van de Dienst die de klant bezoeken met een controleopdracht.

Ondersteuning bedrijfsvoering (secundaire processen): er worden persoonsgegevens van medewerkers én belastingplichtigen verwerkt voor bedrijfsvoeringsdoeleinden. Hoewel het eindproduct van de verwerking veelal in anonieme (geaggregeerde) vorm plaatsvindt, kan niet worden uitgesloten dat er ook op niet geanonimiseerde wijze verdere verwerking van persoonsgegevens plaatsvindt.

Gebruikers:
In ieder geval een beperkt aantal users (30-35p) heeft de mogelijkheid om in de rol van super-gebruiker (analisten) alle in RAM aanwezige data massaal te benaderen. Daarnaast heeft een tweede, grotere groep (ong. 90 p) minimaal casusgewijs en rolafhankelijk toegang tot (een deel van) de data. Een derde groep vormen de ontwikkelaars en technisch beheerders die niet zondermeer (ook) een fiscale rol hebben die toegang tot de data rechtvaardigt (bv. CAO-ontwikkelaars/technisch beheerders). Een deel van de medewerkers (de CAO-medewerkers) die geen fiscale rol hebben, worden als gevolg van de verbeterde inlaadprocedure afgesloten van de inhoudelijke toegang tot de data. Voor de technisch beheerders geldt deze beperking niet.

[8] Bij Belastingdienst-bedrijfsonderdelen geldt in alle gevallen dat de verantwoordelijke formeel de Minister van Financiën is en 'namens deze' via mandaat van Persoonsgegevens de directeur van het bedrijfsonderdeel handelt.
[9] Gezien bedrijfsonderdeel-overstijgend gebruik intern BD op DG nivo.

7. Verwerkingslocaties

Benoem in welke landen de voorgenomen gegevensverwerkingen plaatsvinden.

De gehele verwerking vindt in Nederland plaats binnen de infrastructuur van de BD.

8. Technieken en methoden van de gegevensverwerkingen incl. informatiebeveiliging

Beschrijf op welke wijze en met gebruikmaking van welke (technische) middelen en methoden de persoonsgegevens worden verwerkt. Benoem of sprake is van (semi-) geautomatiseerde besluitvorming, profilering of big dataverwerkingen en, zo ja, beschrijf waaruit een en ander bestaat.

De voor RAM beschikbare bronnen worden verwerkt in een voor RAM-specifiek gecreëerde opslagvorm (Oracle database) inclusief de toevoeging van door RAM ' berekende' velden (logisch en rekenkundig). De uitkomst wordt in de RAM-database geplaatst en een aantal bestanden worden omgevormd tot specifieke datafundamenten o.a. het zogenaamde Kern-Sofi datafundament. Deze data is beschikbaar voor analyse-doeleinden door zgn. RAM-super-users of wordt getoond via door de gebruiker aan te roepen voorgedefinieerde schermen en selectiefuncties.

Een deel van de verwerkingen kwalificeert als (semi-) geautomatiseerde besluitvorming (selectie van posten die in behandeling worden genomen of brieven ontvangen), profiling (incl. de mogelijkheid om op nationaliteit) te selecteren zowel ten aanzien van Belastingplichtigen als medewerkers.

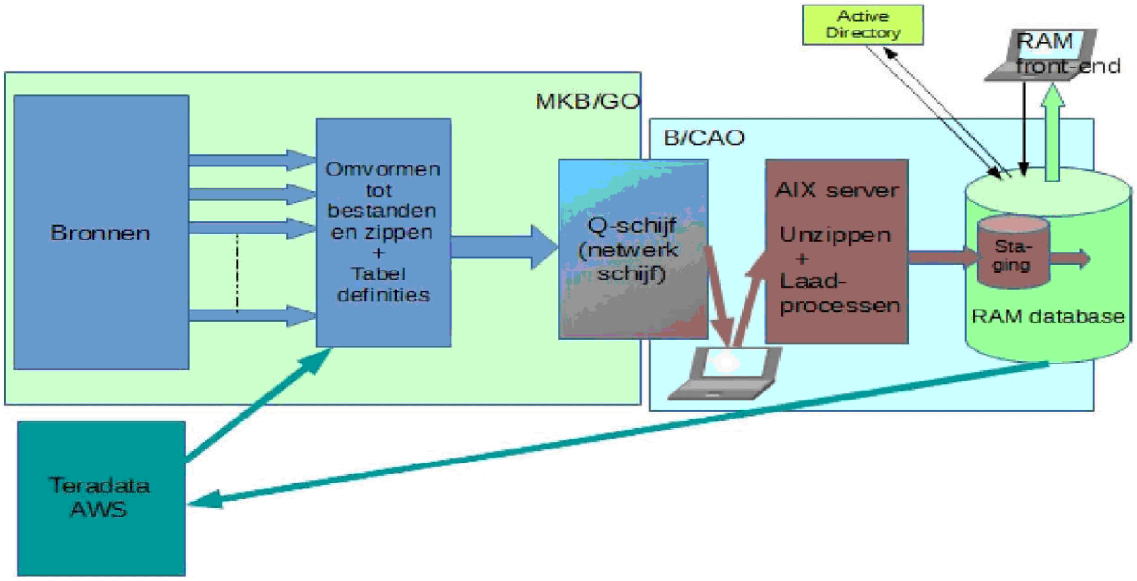
Informatiebeveiliging: Aanvullend op de zgn. 'stutmaatregelen' die zijn genomen om RAM tot eind 2017 te laten functioneren, is in juli 2017 door CIE aanvullend onderzoek gedaan naar specifieke risico's ten aanzien van de informatiebeveiliging. Een aantal bevindingen is of wordt inmiddels opgelost cq kunnen op afzienbare termijn worden opgelost door het feitelijk doorvoeren van de voorgestelde oplossing in combinatie met het ter beschikking stellen van (kwalitatief) voldoende capaciteit en/of het nadrukkelijker toepassen van bestaande voorzieningen binnen RAM. Dit betreft onder andere:

1. Het laadproces dat vereenvoudigt wordt en daardoor veiliger (wijziging wordt momenteel doorgevoerd; zie procesplaten hieronder).
2. Functiescheiding (ihbz in relatie tot toegang tot de gegevens) die onvoldoende is doorgevoerd. (to do, capaciteitstoezegging vanuit Switch geen gestand gedaan)
3. 'Need to know'-toegang tot data die verbeterd kan worden. (samenhang met aspect doelbinding; to do)
4. Gebruik van risicovolle systeemcomponenten (aanroep **activeX** kan worden uitgebouwd door niet meer toepassen MSAccess (to do; capaciteitsissue); **Macro's** zijn vanuit het oogpunt van 'virusvatbaarheid' risicovol maar ook zeer verweven met de opzet RAM icm MS Excel. Daardoor is uitbouw/vermijden van macro's een complexe en bij RAM in haar huidige vorm een naar verwachting onhaalbare aanpassing. Mogelijk dat het werken met beveiligingscertificaten een voortgezet gebruik nader kan beveiligen?
5. Onvoldoende logging[10] en monitoring. Dit is opgelost door het activeren van het loggen en monitoren van de resultaten via CIE/SOC –SPLUNK. RAM zelf logt (alhoewel anders van opzet en structuur) diverse aspecten van gebruik en heeft in ontwerp verbetervoorstellen ten aan zien van logging (en monitoring) in ontwerp/ontwikkeling. Overige bevindingen tav bijvoorbeeld onvoldoende veilig inloggen (bevinding CIE; inmiddels opgelost).
6. Pseudonimisering: RAM kent mogelijkheden om de data pseudoniem te verwerken. Deze optie staat niet standaard aan maar kan wel (door de gebruiker) worden geactiveerd.

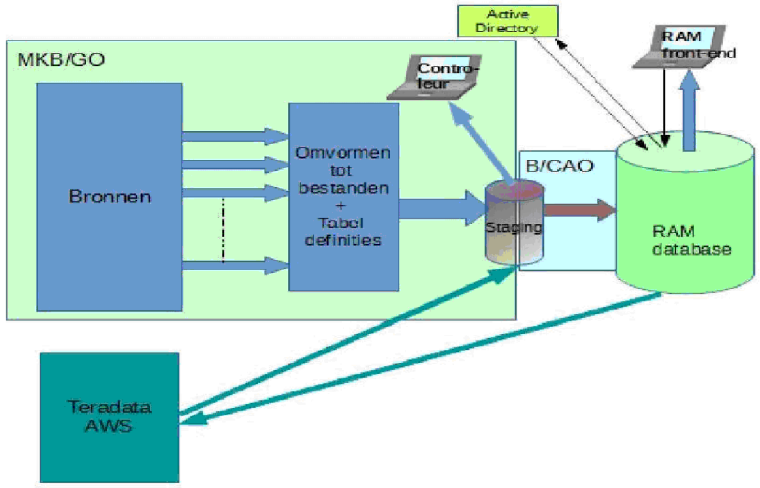
[10] In de documentatie van CIE auditing genoemd. Hier vertaalt in de in een GEB gebruikelijke term logging om verwarring met de binnen privacypraktijk gangbare term auditing in de zin van een toetsing door een (onafhankelijke) derde te voorkomen.

Los van het bovenstaande is tijdens enkele interviews gerefereerd aan het gebrek aan "control". Dit raakt aan het LOA-karakter van RAM waardoor er (inherent aan het karakter van dit type voorzieningen) afwijkingen bestaan ten opzichte van de actuele, centraal gekozen IV/ICT-architectuur.
Zo is er in het verleden (afwijkend van de IV-keten) een keuze gemaakt voor ACL als ontwikkeltaal. ACL werd (en wordt) vooral gebruikt binnen de groep van EDP-medewerkers die het hart van de groep RAM-ontwikkelaars vorm(d)en. Ook is, in overleg met IMB, gekozen voor een inrichting op basis van een Oracle-omgeving.

Daarnaast wordt de personele inzet aan RAM uitgevoerd door een groep (enthousiaste) medewerkers met een soort "gedoogstatus". Hiermee wordt bedoeld dat deze medewerkers een taak uitvoeren naast (of in plaats van) de eigenlijk opgedragen taak. De kantoren kunnen deze ondersteuning intrekken, waarmee de ontwikkeling van RAM in gevaar komt. De directie MKB is uiteindelijk verantwoordelijk voor het inzet van het personeel en draagt zorg voor de (tijdelijke) continuïteit van RAM op dit punt. Deze observaties overstijgen het primaire doel van een GEB maar raken wel aan een relevant onderdelen van de privacy zoals gegevenskwaliteit en -integriteit.



Huidig laadproces data RAM



Verbeterd laadproces o.b.v. bevindingen CIE (wordt momenteel geïmplementeerd).

9. Juridisch en beleidsmatig kader

Benoem de wet- en regelgeving, met uitzondering van de AVG en de Richtlijn, en het beleid met mogelijke gevolgen voor de voorgenomen gegevensverwerkingen.
Het merendeel van de verwerkingen van RAM is gebaseerd op de relatief 'open' norm van art. 11 en 20 Awr waar uit de bevoegdheid tot het opleggen tot aanslagen ook het uitvoeren van toezicht voortvloeit inclusief (volgens de tot nu toe gebruikelijke interpretatie) gegevensverwerkingen als in RAM. Recente rechtspraak van de HR (ANPR) heeft duidelijk gemaakt dat niet alle vormen van persoonsgegevensverwerking in deze generieke wettelijke grondslag gelezen mogen worden. De hoeveelheid door RAM bij elkaar gebrachte gegevens is groot. 72 bronnen (informatiesystemen) worden in enige vorm ontsloten. In zijn algemeenheid kan worden gesteld dat uit de taken van de Belastingdienst rondom Heffen, Innen, VGEM, Accijnzen, Toeslagen en fraude-opsporing de noodzaak tot het verwerken van deze persoonsgegevens kan ontstaan. Per afzonderlijke verwerking zal vervolgens steeds moeten worden bepaald welke gegevens in welke mate verwerkt mogen worden inclusief de constatering dat er geen noodzaak tot verwerking is aangetoond.

10. Bewaartermijnen

Bepaal en motiveer de bewaartermijnen van de persoonsgegevens aan de hand van de verwerkings-doeleinden.

RAM werkt met zgn. jaarlagen. Er worden gegevens van 6 jaar naast het huidige kalenderjaar verwerkt. Gegevens worden na vervallen van 7-jaar tov het actuele jaar verwijderd. Dit correspondeert met de 'gemiddelde' standaard-bewaartermijn uit de Belastingdienst-selectielijsten.

Los van deze (met de structuur van RAM samenhangende) werkwijze, kan er geen garantie gegeven worden over de bewaartermijnen voor de bestanden welke uit RAM geëxtraheerd worden (door de diverse gebruikers). Deze kunnen (en worden) decentraal (op de laptop van de gebruiker) opgeslagen en kunnen niet centraal vernietigd worden.

B. Beoordeling rechtmatigheid gegevensverwerkingen

Beoordeel de rechtsgrond, noodzaak en doelbinding van de voorgenomen gegevensverwerkingen en rechten van de betrokkene.

11. Rechtsgrond

Bepaal op welke rechtsgronden de gegevensverwerkingen worden gebaseerd.
Vanuit de Wbp bezien is de verwerkingsgrondslag voor de BD te baseren op zijn publiekrechtelijke taak (art. 8 sub e Wbp juncto art. 8 sub c Wbp in geval van verwerving van gegevens van derden).

Als Belastingdienst hebben wij te maken met de eis dat een inmenging in de uitoefening van het recht op respect voor het privéleven moet zijn voorzien bij wet ("in accordance with the law"). Dit betekent dat die inmenging moet berusten op een naar behoren bekend gemaakt wettelijk voorschrift waaruit de burger met voldoende precisie kan opmaken welke op zijn privéleven betrekking hebbende gegevens met het oog op de vervulling van een bepaalde overheidstaak kunnen worden verzameld en vastgelegd, en onder welke voorwaarden die gegevens met dat doel kunnen worden bewerkt, bewaard en gebruikt. De woorden "behoudens bij of krachtens de wet te stellen beperkingen" in artikel 10 van de Grondwet brengen bovendien mee dat beperkingen op het recht op eerbiediging van de persoonlijke levenssfeer slechts kunnen worden gerechtvaardigd door of krachtens een wet in formele zin (vgl. HR 19 december 1995, NJ 1996/249, r.o. 6.4.2). Of art. 11 Awr (respectievelijk art. 20 Awr) hierin in de context van gegevensverwerkingen binnen RAM in voorziet lijkt, deels verwerkingsvormafhankelijk, is door in ieder geval de HR ter discussie gesteld (ANPR, HR 2016). Dit risico treft naar onze inschatting ook de vervanger/opvolger van RAM en in zijn algemeenheid ook soortgelijke functionaliteit en voorzieningen die binnen de BD in gebruik zijn. Dit loopt samen met het aspect doelbinding.

Binnen RAM worden persoonsgegevens verwerkt die door ISC van internet zijn verzameld (scraping, crawling al dan niet door tussenkomst van software van derden zoals Coosto). De rechtsgrond voor de verwerking van dergelijke gegevens is (BD-overstijgend) minimaal onderwerp van discussie en in een aantal gevallen niet toegestaan door de AP. Daarnaast verwerkt D&A, als beoogde migratie-partij, primair belastingdienst-eigen gegevens. Mede indachtig aanvullende (kwaliteits)risico's ten aanzien van de herkomst, juistheid en actualiteit van gegevens afkomstig van het internet, wordt geadviseerd om in samenspraak met D&A te bepalen of de huidige van internet afkomstige bronnen blijvend verwerkt of gestopt/verwijderd moeten worden.

12. Bijzondere persoonsgegevens

Indien bijzondere of strafrechtelijke persoonsgegevens worden verwerkt, beoordeel of één van de wettelijke uitzonderingen op het verwerkingsverbod van toepassing is. Bij verwerking van een wettelijk identificatienummer beoordeel of dit is toegestaan.

Het gebruik van het BSN is voor de Belastingdienst (op basis van art. 10 van de Wet Algemene Bepalingen Burgerservicenummer) toegestaan/ verplicht.

Het verwerken van strafrechtelijke informatie is alleen in bepaalde context toegestaan. Bijvoorbeeld voor/door de FIOD maar ook mag strafrechtelijke informatie (GEFIS), hoewel aan restricties onderhevig, betrokken worden in een fiscaal/bestuursrechtelijk onderzoek vanuit het una via-beginsel (artikel 5:44 lid 1 van de Awb) en beleid zoals verwoord in bv. het protcol AAFD[11].

De noodzaak / grondslag voor de verwerking van nationaliteit kan situatieafhankelijk verboden zijn als het kwalificeert als een bijzonder persoonsgegeven, bv. bij (indirecte) selectie op ras via de nationaliteit.

Hoewel geen bijzonder persoonsgegeven / nader onderscheiden kwalificatie vanuit de Wbp is verwerking van VIP-gegevens en ambtenarenposten binnen RAM een verwerking die nadere aandacht verdient. De VIP gegevens en gegevens van ambtenaren wordt primair verwerkt om dergelijke posten te kunnen herkennen en vervolgens af te schermen voor niet geautoriseerde personen. De binnen de BD lopende discussie mbt de wijze van behandelen van dergelijke posten wordt buiten scope van deze GEB geplaatst.

13. Doelbinding

Indien de persoonsgegevens voor een ander doel worden verwerkt dan oorspronkelijk verzameld, beoordeel of deze verdere verwerking verenigbaar is met het doel waarvoor de persoonsgegevens oorspronkelijk zijn verzameld.

Het doel van de gegevensverwerkingen waarvoor RAM wordt ingezet is heel divers. Zonder uitputtend te zijn raakt dit aan (taken op het vlak van):

1. heffing en inning van belastingen;
2. het daarmee gepaard gaand toezicht;
3. accijnzen en VGEM-taken;
4. inkomensafhankelijke regelingen;
5. (interne) bedrijfsvoering;
6. FIOD-taken, gelegen in de opsporingssfeer primair met een fiscale fraude context.

Het (oorspronkelijke) doel van verkrijgen is naar verwachting ook te koppelen aan een van deze onderdelen maar correspondeert bij verdere verwerking niet op voorhand met de oorspronkelijke verwervingsgrond. Zo is het mogelijk binnen RAM om bijvoorbeeld 4 en 5 te koppelen zonder dat er sprake is van doelbinding. Van internet afkomstige gegevens vormen een apart gevalcategorie waar de doelbinding op voorhand lastig van is aan te tonen doordat de 'aanbieder' van de gegevens (al dan niet de betrokkene zelf) waarschijnlijk geen verwerkingsdoel binnen de Belastingdienst voor ogen heeft gehad.

[11] https://zoek.officielebekendmakingen.nl/stcrt-2015-17271.html

Zoals bij elke verwerking voor (statistische en) analysedoeleinden worden in sommige gevallen grote hoeveelheden gegevens opgeslagen (geexporteerd met bv Excel) op lokale apparatuur als laptops en mogelijk externe opslagmedia. Los van beveiligingsissues kan niet worden aangetoond of deze gegevens wel of niet onrechtmatig gebruikt worden voor andere doeleinden.

Door de veelheid aan gegevens die in RAM beschikbaar worden gesteld is het ondoenlijk een integraal oordeel te geven over de doelbinding. In zijn algemeenheid geldt voor data warehouse-achtige voorzieningen door de grote hoeveelheid beschikbare gegevens, dat niet op voorhand met zekerheid kan worden aangetoond dat het oorspronkelijke doel van verwerken correspondeert met de verdere verwerkingen waardoor het risico van onverenigbare doelen aanwezig is. Zeker in geval van de analyse-functie waar massale verwerking mogelijk is vormt dit een risico maar feitelijk bij alle functies van RAM maar dan minder massaal. Nader, gedetailleerd, onderzoek (met name op de clusters niet (puur) fiscale bronnen en de wijze van gebruik wordt geadviseerd. Het onderzoek naar de fiscale gegevens kan (vanuit efficiëntieoverwegingen) wellicht als één geheel (een cluster) plaatsvinden?

Hierna te benoemen maatregelen in de sfeer van geaccordeerde en geregistreerde onderzoeksopdrachten, logging en monitoring, data-compartimentering / rol-gebonden toegang middels formele autorisaties (IMS) in combinatie met bijvoorbeeld data-pseudonimisering dragen bij aan het verminderen van risico's.

14. Noodzaak en evenredigheid

Beoordeeld of de voorgenomen gegevensverwerkingen noodzakelijk zijn voor het verwezenlijken van de nagestreefde doeleinden. Ga hierbij in ieder geval in op:

1. *Proportionaliteit: staat de inbreuk op de persoonlijke levenssfeer en de bescherming van de persoonsgegevens van de betrokkenen in evenredige verhouding tot de verwerkingsdoeleinden?*
   Negatief gesteld zijn de mogelijkheden om inbreuk te maken op de persoonlijke levenssfeer met een voorziening als RAM, inherent aan het fenomeen data warehouse, zonder beperkende maatregelen groot. Er wordt veel gevoelige data van heel veel personen bij elkaar gebracht die voor de (beperkt in aantal) gebruikers inzicht in 'alles op alles' biedt.

   In zijn algemeenheid kan worden vastgesteld dat met bestaande en in deze PIA genoemde aanvullende maatregelen het risico van een 'evenredige verhouding tussen rechten van betrokkenen en de verwerkingsdoeleinden' van de Belastingdienst, mede vanwege het zicht op uitfasering / migratie kan voldoende worden gewaarborgd. Dan gaat het om data compartimentering, 'need to know'-autorisaties, logging, monitoring en 'awareness' bij RAM-gebruikers ten aanzien van dit aspect.

2. *Subsidiariteit: kunnen de verwerkingsdoeleinden in redelijkheid niet op een andere, voor de betrokkenen minder nadelige wijze, worden verwezenlijkt?*
   De Belastingdienst werkt aan een verbeterde proceslogistiek waardoor data alleen casusgewijs naar bijvoorbeeld een behandelaar wordt doorgezet. Integrale toegang tot data fundamenten en/of bronnen is in de toekomst meer en meer voorbehouden aan een beperkte groep van beheerders en analisten die zorgen een juiste informatievoorziening. Een werkend, gelijkwaardig alternatief voor RAM is er op dit moment echter niet. Het huidige RAM in combinatie met een aantal maatregelen voortvloeiend uit deze GEB beoogt te voorzien in een aanvaardbaar risico-gehalte ten aanzien van de persoonsgegevensverwerking uitgaande van een aanstaande migratie van RAM naar een nieuwe omgeving.

15. Rechten van de betrokkenen

Geef aan hoe invulling wordt gegeven aan de rechten van de betrokkenen. Indien de rechten van de betrokkene worden beperkt, bepaal op grond van welke wettelijke uitzondering dat is toegestaan.

Het is onbekend of de gegevensverwerking in RAM aan Persoonsgegevens gemeld conform de verplichting daartoe in

de Wbp. In algemene zin is verwerking van persoonsgegevens voor Toezicht kenbaar gemaakt[12]. De in het voornoemde document opgesomde gegevens omvatten niet de berekende velden uit RAM. Het is binnen het bereik van dit onderzoek niet duidelijk geworden of in geval van een beroep door een betrokkene op het inzagerecht, in RAM verwerkte / gecreëerde gegevens (zullen) worden vermeld.

Eén van de rechten van betrokkenen bestaat uit de garantie dat de gegevens juist, volledig en tijdig zijn. Omdat het ontwikkeltraject en de productieprocessen van RAM niet centraal geregisseerd en niet volgens harde en vastgelegde uitgangspunten bestuurd wordt, bestaat de mogelijkheid dat (door het genoemde gebrek aan control) hier niet volledig aan voldaan wordt. In het verleden is hier overigens niets van gebleken.

C. Beschrijving en beoordeling risico's voor de betrokkenen

Beschrijf en beoordeel de risico's van de voorgenomen gegevensverwerkingen voor de rechten en vrijheden van de betrokkenen. Houd hierbij rekening met de aard, omvang, context en doelen van de voorgenomen gegevensverwerkingen.

16. Risico's

Beschrijf en beoordeel de risico's van de voorgenomen gegevensverwerkingen voor de rechten en vrijheden van de betrokkenen. Ga in ieder geval in op:

- *a. welke negatieve gevolgen de gegevensverwerkingen kunnen hebben voor de rechten en vrijheden van betrokkene;*
- *b. de oorsprong van deze gevolgen;*
- *c. de waarschijnlijkheid (kans) dat deze gevolgen zullen intreden en*
- *d. de ernst (impact) van deze gevolgen voor de betrokkene wanneer deze intreden.*

Hou bij elk aspect rekening met de aard, omvang, context en doelen van de gegevensverwerking.

1. Rechtmatigheid en noodzaak van verwerking

RAM ondersteunt in feite hergebruik van veel van binnen de Belastingdienst aanwezige gegevens. De rechtmatigheid van verkrijging en daarna ter beschikking stellen is voor het merendeel van de gegevens (voldoende) duidelijk met als uitzondering van internet verzamelde gegevens, gegevens die recent ter discussie zijn komen te staan zoals een deel van de IB-47 renseignementen en bijzondere persoonsgegevens. Het risico ontstaat vooral bij de (verdere) verwerking van de gegevens. Wat wordt aan welke medewerker(s) voor welk doel ter beschikking gesteld? Vanuit het perspectief van betrokkenen bestaat het risico dat noodzaak van deze verwerkingen onvoldoende of niet kan worden aangetoond. Om dit risico aanvaardbaar te maken en tegelijkertijd transparantie van de verwerking te vergroten wordt opdrachtgestuurd verwerken geadviseerd in combinatie met de overige in deze GEB genoemde maatregelen.

2. Doelbinding

In RAM worden heel veel gegevens bij elkaar gebracht en (rolafhankelijk) voor een aantal gebruikers integraal ter beschikking gesteld of zichtbaar via de voorgedefinieerde RAM-schermen. Vanuit het perspectief van de betrokkene betekent dit dat niet duidelijk is of kan worden gemaakt, in geval van bijvoorbeeld een verwerkingsinzageverzoek, of diens gegevens vanuit het oogpunt van doelbinding juist zijn verwerkt. In ieder geval is het risico reëel aanwezig dat gegevens doelbinding overstijgend verwerkt worden. Dit geldt ook voor gegevens van medewerkers met de Belastingdienst in de rol van verwerkingsverantwoordelijke werkgever. RAM biedt bijvoorbeeld voor de (ongeveer 35) supergebruikers en (ongeveer 90) analisten de mogelijkheid om nagenoeg 'alles aan alles' te relateren. Logging en monitoring en autorisatieprofielen dragen bij aan het beperken van dit risico.

3. Proportionaliteit en subsidiariteit

In RAM worden heel veel gegevens bij elkaar gebracht en (rolafhankelijk) voor een aantal gebruikers integraal ter beschikking gesteld of rol-afhankelijk zichtbaar via de voorgedefinieerde RAM-schermen. Vanuit het perspectief van de betrokkene betekent dit ten aanzien van proportionaliteit en subsidiariteit, dat niet met zekerheid kan worden gegarandeerd dat er geen bovenmatige verwerking

[12] https://download.belastingdienst.nl/belastingdienst/docs/meldingen_belastingdienst_2008_al5303z4fd.pdf

heeft plaatsgevonden cq er een minder belastend alternatief voorhanden was.
In ieder geval is het risico reëel aanwezig dat gegevens disproportioneel (bovenmatig) verwerkt worden. RAM biedt bijvoorbeeld voor de (ongeveer 35) supergebruikers en (ongeveer 90) analisten de mogelijkheid om nagenoeg 'alles aan alles' te relateren. Er is een alternatief (subsidiariteit) in de vorm van een migratie-scenario in wording, dat op termijn vanuit het oogpunt van de zorgvuldigheid van verwerking van persoonsgegevens meer garanties biedt. Logging en monitoring en autorisatieprofielen en integriteits en zorgvuldigheidsregels dragen daarnaast bij aan het beperken van dit risico.

4. **Informatiebeveiliging**
Op dit moment zijn de fiscale persoonsgegevens zoals verwerkt binnen RAM, ook toegankelijk voor medewerkers die alleen een (technisch/functionele) beheerdersrol vervullen. Mede indachtig het gegeven dat logging en monitoring tot voor kort niet of slechts beperkt was ingevuld en het feit dat het ook externe inhuurkrachten betreft, vormt dit een risico. Logging en monitoring zou ten tijde van het schrijven van deze GEB binnen het SOC geactiveerd moeten zijn. Een aantal toegekende rechten kan en moet beperkt worden (conform het advies van CIE).

De analysefunctionaliteit van RAM geeft een beperkt aantal medewerkers toegang tot alle data in een niet standaard gepseudonimiseerde vorm. Wel bevat RAM mogelijkheden om de gegevens (optioneel) pseudoniem te verwerken. Door de optionele wijze waarin dit is vormgegeven in combinatie met het nog niet standaard integraal ingeregeld zijn van logging en monitoring vormt dit een risico.

RAM kent een aantal, in onbruik geraakte, onderdelen dat uitgefaseerd/uitgebouwd kan worden, in het bijzonder de ActiveX-componenten. Daarnaast vormen de gebruikte macro's een risico door de virusgevoeligheid van macro's. Het aanvragen en implementeren van SSL-certificaten kan het beveiligingsniveau verhogen. Hoewel dit risico zich niet in een feitelijke casus heeft voorgedaan, verdient het afbouwen van het gebruik (door migratie van RAM naar een nieuwe omgeving)mede om niet privacy-gerelateerde redenen aanbeveling.

Het laadproces van gegevens voor RAM is verbeterd. Hoewel het nog steeds een, deels handmatige, stappen buiten de reguliere centrale ICT-voorzieningen kent, lijkt de verbeterde versie door het zoveel mogelijk beperken van het aantal (handmatige) stappen en , gezien het advies van CIE, het maximaal haalbare.

5. **Gegevenskwaliteit (waaronder data integriteit)**
In RAM worden originele brongegevens opgeslagen aangevuld met door RAM berekende gegevenselementen. Dit kunnen zowel rekenkundige (bv sommaties of ratio's) als logische bewerkingen (als X en Y dan (conclusie) Z). Hoewel er geen praktijkvoorbeelden zijn gevonden tijdens het assessment kan niet worden gegarandeerd dat in de veelheid aan bewerkingsslagen die beide categorieën gegevens ondergaan, er kwaliteitsissues bestaan ten aanzien van de juistheid, volledigheid en actualiteit van de verwerkte persoonsgegevens. Wel is juist vanwege dit risico het laadproces vereenvoudigd en zijn er 'vierkants-controle'-achtige maatregelen fouten zoveel mogelijk te voorkomen of daarna alsnog te detecteren. De onvoldoende bevonden functiescheiding tussen de rol van (technisch) beheerders en functionaris met mutatierechten op de data- en bijbehorende bewerkingsalgorithmen vormt aan aanverwant risico dat van invloed kan zijn op de datakwaliteit en daardoor op de belangen en rechten van betrokkenen. Afspraken op dit gebied, onder andere door het leveren van capaciteit vanuit SWITCH zijn nog niet geeffectueerd. Er zijn geen voorbeelden bekend geworden gedurende het assessment waaruit dit feitelijk is gebleken.

6. **Data Governance (control, beheer)**
Feitelijk een risico dat de voorgaande vier risico's overstijgt: het gehele stelsel van processenstappen ten behoeve van RAM, geautomatiseerd en handmatig, levert een overall risico op het gebied van data governance op door de, deels a-typische, gegevensverwerking afgezet tegen binnen de Belastingdienst gebruikelijke verwerkingsvormen in soortgelijke situaties (onder centrale regie binnen de IV-keten). Ook hier geldt dat er gedurende het assessment geen voorbeelden zijn gevonden waarmee is aangetoond dat het risico zich feitelijk heeft voorgedaan in de vorm van bijvoorbeeld een

incident.

7. **Awareness gebruikers**
   Op de gebruikers van RAM (super gebruikers met veel rechten en gebruikers voor wie middels maatwerk deelverzamelingen ter beschikking worden gesteld) rust, afgezet tegen de rechten van betrokkenen, de verantwoordelijkheid om zorgvuldig met de gegevens om te gaan. Integriteits- en zorgvuldigheids voorschriften voorzien hier in ieder geval in. iBewustzijn en trainingen op het vlak privacy-awareness zijn ook beschikbaar om hier een extra bijdrage aan te leveren te vermindering van dit risico.

8. **Secundaire persoonsgegevensverwerking (waaronder bedrijfsvoering): RAM-gebruik ten aanzien van BD-medewerkers**
   De medewerkers gelden in dit geval dus als betrokkene en de BD is hier verwerkingsverantwoordelijke in haar rol als werkgever. RAM wordt mede ingezet om persoonsgegevens van medewerkers te verwerken, bijvoorbeeld om inzicht in de productie / correctieopbrengsten tot op medewerker te krijgen. Functioneel biedt RAM de mogelijkheid om op medewerkerniveau op niet geanonimiseerde wijze gegevens te verwerken (verzamelen, presenteren) zonder structureel inzicht in de mate van verwerking/verspreiding. Gekoppeld aan het feit dat er specifieke afspraken intern Belastingdienst zijn gemaakt over de (beperkte) wijze waarop dergelijke gegevens (al dan niet geanonimiseerd) mogen worden verwerkt, vormt deze functionaliteit binnen RAM een risico ten aanzien van de rechten van BD-medewerkers, doordat er onvoldoende transparantie is over de wijze waarop en de mate waarin persoonsgegevens van medewerkers via RAM worden verwerkt

D. Beschrijving voorgenomen maatregelen

Beschrijf de voorgenomen maatregelen om de hiervoor beschreven risico's van de voorgenomen gegevensverwerkingen voor de vrijheden en rechten van betrokkene aan te pakken.

17. Maatregelen

Beoordeel welke technische, organisatorische en juridische maatregelen in redelijkheid kunnen worden getroffen om de hiervoor beschreven risico's te voorkomen of te verminderen. Beschrijf welke maatregel welk risico aanpakt en wat het restrisico is na het uitvoeren van de maatregel. Indien de maatregel het risico niet volledig afdekt, motiveer waarom het restrisico acceptabel is.

Generieke maatregel (scenario korte-lange(re)termijn):
RAM wordt, in samenhang met soortgelijke functionaliteit, gemigreerd naar een nieuwe configuratie die gaat fungeren als een MKB-intelligence voorziening ten behoeve van centrale regie, risicodetectie en -selectie en klantinzicht. De uitwerking hiervan bevindt zich in de opdrachtformuleringsfase. Gezien de hieronder meer in detail uitgewerkte risico's is een van de risico borgende maatregelen het 'as is' overnemen van de door RAM gecreëerde datafundamenten, mede op basis van de door CIE voorgestelde beveiligingsmaatregelen zoals het dit najaar opgeleverde 'verbeterde' laadproces. Op basis van het datafundament kan de aandacht/ IV-investering van IV' en D&A in deze fase vooral gericht worden op het ontwerpen en (her)inrichten van de analysefuncties en migratie en doorontwikkeling van bestaande RAM-functionaliteit. Op termijn is dan een verdere verbetering gewenst door ook de datafundament waar nodig te herontwerpen. Bij de keuze voor dit scenario is een doelbindingstoetsing op de clusters niet-sec-fiscale gegevens noodzakelijk om eventuele verwerkingsbeperkingen ten aanzien van het aantal bronnen of elementen binnen de bronnen aan te brengen. Uit efficiëntieoverwegingen kan het cluster fiscale gegevens in één toetsing beschouwd worden.

Het per direct stopzetten van RAM is, voor de volledigheid, een tweede scenario dat alle hieronder genoemde (kansen op) risico's voorkomt. Dit scenario vloeit niet voort als totaalconclusie uit deze GEB. Door de meer integrale business impact die een dergelijke beslissing zal hebben wordt bij nadere verkenning van het migratiescenario een instrument als een WMK-toets in combinatie met bijvoorbeeld een BIA (Business Impact Analyse) geadviseerd.

1. **Rechtmatigheid en noodzaak van verwerking**
   Implementeer / verbeter opdrachtgestuurde verwerking. Alleen expliciete opdrachten van vooraf bepaalde opdrachtgevers worden in behandeling genomen.

2. **Doelbinding**
   Door de introductie van rollen en het expliciet toekennen en beperken van autorisaties is al ten dele voorzien in risico borgende maatregelen. Dit kan verder worden uitgebreid door in overleg met de business meer gebruikersgroepen met specifieke rechten aan te maken. De Belastingdienst wil in de nabije toekomst casusgewijs gaan werken waarbij gegevens alleen op een need-to-know, casusgewijze basis worden verwerkt. Middels centrale regie worden de, hiervoor noodzakelijke, massale gegevensverwerkingen ontkoppeld van de casusgewijze verwerking. In RAM is dit, anders dan door maatregelen op het vlak van autorisatie en bijvoorbeeld (binnenkort) logging en monitoring, niet in eenzelfde mate te scheiden. Door implementatie van de reeds voorziene maatregelen op het hiervoor genoemde vlak van autorisatie en bijvoorbeeld logging en monitoring wordt het risico, indachtig de gewenste maar niet op heel korte termijn effectueerbare migratie van RAM, aanvaardbaar geacht. Verbeter daarnaast het inzicht in de gegevensverwerkingen door een expliciete, kenbare opdrachtverstrekking tot gegevensverwerking van een daartoe gerechtigde opdrachtgever te registreren en monitoren.

3. **Proportionaliteit**
   Door de introductie van rollen en het expliciet toekennen én beperken van autorisaties en het binnenkort te implementeren loggen en monitoren via CIE/SOC, wordt ten dele voorzien in risico borgende maatregelen. De Belastingdienst wil in de nabije toekomst casusgewijs gaan werken waarbij gegevens alleen op een need-to-know, casusgewijze basis worden verwerkt. Middels centrale regie worden de, hiervoor noodzakelijke, massale gegevensverwerkingen ontkoppeld van de casusgewijze verwerking. In RAM is dit, anders dan door de genoemde maatregelen op het vlak van autorisatie en bijvoorbeeld logging en monitoring, niet integraal in eenzelfde mate te scheiden. Voor de korte termijn, met een migratie van RAM in het vooruitzicht, wordt het risico voor dit moment aanvaardbaar geacht. Verbeter daarnaast het inzicht in gegevensverwerking een expliciete, kenbare opdrachtverstrekking van een daartoe gerechtigde opdrachtgever te registreren in of buiten RAM. ISC ...

4. **Informatiebeveiliging**
   Door CIE is in juli/augustus 2017 onderzoek gedaan naar de beveiligingsaspecten van RAM. Een aantal in voorgestelde maatregelen is of wordt momenteel geïmplementeerd. Zeker daar waar de voorgestelde maatregelen ook de beveiliging van persoonsgegevens betreft, nemen wij de maatregelen in deze GEB over, in het bijzonder ten aanzien van:

   a. Het beperken van de rechten van medewerkers met een technische (beheer)rol binnen RAM, bijvoorbeeld bij medewerkers in de IV-keten al dan niet in combinatie met functie(rol)scheiding. Een technische beheerrol betekent in principe geen noodzaak tot inhoudelijke toegang op data-element niveau. Waar mogelijk moet deze mogelijkheid tot raadplegen van de data worden uit de autorisaties worden verwijderd, indien onmogelijk zal er minimaal een maatregel op het niveau van logging en monitoring en functiescheiding moeten worden genomen.

   b. Naast het functioneel inrichten van logging en monitoring via Splunk onder beheer van CIE/SOC zijn aanvullende maatregelen om een kwalitatief juiste, actieve vorm van monitoring in te regelen en beleggen. Benoem en implementeer daarom ook controle-aspecten waarop, mede vanuit het perspectief van de fiscale-verantwoordelijkheden, actief getoetst gaat worden.

   c. De-activeer / verwijder zgn. Active-X-componenten uit RAM. Naar verluidt is dit een niet meer in gebruik zijnde 'erfenis' gekoppeld aan het inmiddels niet meer gebruikte van MS-Access. De aanwezigheid van dit component levert een risico op voor de informatiebeveiliging. Onderzoek implementatie van (SSL)beveiligingscertificaten voor het veilig werken met Excel-macro's. Er wordt dan een digitale handtekening meegegeven die het activeren van een

hoger beveiligingsniveau binnen Excel-macro's mogelijk maakt.

d. Pseudonimisering van data is momenteel in RAM een optionele verwerkingsvorm. Standaard kiezen voor pseudoniem verwerken (tenzij, beargumenteerd en gelogd) wordt aanbevolen, vooruitlopend op een overgang naar een nieuwe omgeving waarin dit (naar verwachting) de (privacy by default) standaard is (bv. de 'statistische enclave' waaraan D&A momenteel werkt). Doe nader onderzoek naar de implementatie(effecten) en implementeer deze maatregel zo snel mogelijk.

5. **Gegevenskwaliteit (waaronder data integriteit)**
Onder informatiebeveiliging a. en b. zijn twee voor dit risico relevante maatregelen genoemd: beperken van rechten/functiescheiding en logging en monitoring. Dit bevordert de data integriteit en vermindert het risico op het voordoen van het risico.

Ten aanzien kwaliteit van de gegevens verdient het aanbeveling hierop nader te investeren door toetsingsmaatregelen te nemen/verbeteren ten aanzien van de bestaande wijze van gegevensverwerking in RAM. In eerste instantie lijkt dit een maatregel die op het herontwerp/migreren van RAM moet worden toegepast. Wanneer de doorlooptijd van het migratiescenario Q1&2 van 2018 overstijgt, wordt geadviseerd om bij een voortgezet gebruik van (een voldoende substantieel deel van) RAM, deze maatregel mede op het huidige RAM toe te passen.

6. **Data Governance (control, beheer)**
De beste maatregel die dit meta-risico zoveel mogelijk beperkt is, buiten het scenario om per direct te stoppen met RAM, een zo spoedig mogelijke migratie naar een nieuwe infrastructuur/voorziening. In de periode daarvoor zullen de in gang gezette verbeteringen die vanuit een oogpunt van 'passende technische en organisatorische maatregelen..' '..rekening houdend met de stand der techniek..' (art. 13 Wbp) mogelijk zijn, kunnen gelden als het maximaal haalbare.

7. **Awareness gebruikers**
Het bewustzijn ten aanzien van zorgvuldig handelen met (fiscale) persoonsgegevens wordt al geraakt door bestaande verantwoordelijkheden c.q. maatregelen op het vlak van geheimhouding, zorgvuldigheid en integriteit. Als aanvullende maatregel kan het perspectief van de betrokkene (belastingplichtige) worden toegevoegd. Door de rechten (en plichten) vanuit het oogpunt van de betrokkene te beschouwen wordt een juiste, zorgvuldige verwerking van persoonsgegevens zoveel mogelijk geborgd. Dit kan worden gerelateerd aan bv. IBewustzijn is door RAM gebruikers gevolgd. Communicatie behorende bij de implementatie van de Avg kan het bewustzijn m.b.t. privacy verbeteren.

8. **Secundaire persoonsgegevensverwerking (waaronder bedrijfsvoering): RAM gebruik ten aanzien van BD-medewerkers**
Verbeter het inzicht in gegevensverwerking op deze grond door bijvoorbeeld expliciete, kenbare opdrachtverstrekking van een daartoe gerechtigde opdrachtgever en logging en monitoring van de verwerking.
De maatregel kan mede in het perspectief van awareness worden betrokken: toets en verbeter het bewustzijn van RAM-gebruikers maar ook 'opdrachtgevers' voor RAM-onderzoeken ten aanzien van de 'spelregels' hoe om te gaan met persoonsgegevens over medewerkers in relatie tot de mogelijkheden die RAM biedt.