Bundel van de MT Belastingdienst van 6 mei 2014

1 Opening en vaststellen agenda

Aantekeningen.pdf

2 OLAV in aanwezigheid van

20140501 Besluitvorming vrijgave MBD OLAV V1 0.pdf

Aantekeningen.pdf

3 Rondvraag

Aantekeningen.pdf

4 Actualiteiten

Aantekeningen.pdf

5 Besluiten- en actiepuntenlijst MT Belastingdienst 22 april 2014

Besluiten- en actiepuntenlijst MT Belastingdienst 22 april 2014.pdf

Aantekeningen.pdf

6 Controle aan de poort

ontwikkeling controle aan de poort.pdf

Aantekeningen.pdf

7 Informatiebeveiliging en cybercrime en

Oplegmemo MT_BD informatiebeveiliging risico's 20140221 definitief.pdf

20131119 Memo Belastingdienst Risicogebied Cybercrime.pdf

Rapportage risico-inventarisatie 2013 dd 20131104.pdf

Aantekeningen.pdf

8 Protocol Integriteitsonderzoeken Belastingdienst

Onderzoeksprotocol _oplegnota_ 22-04-2014.pdf

PIB 1.0.pdf

Aantekeningen.pdf

9 Houtskoolschets CKC

20140506 Oplegnotitie vaststellen houtskoolschets CKC.pdf

20140506 Houtskoolschets doorontwikkeling CKC - 1.0.pdf

Aantekeningen.pdf

10 Mobiliteitskaart

memo mt mobikaart.docx

07 Richtlijn oneigenlijkgebruik mobiliteitskaart.docx

Aantekeningen.pdf

11 IT-bijstand Curacao, Aruba en Sint-Maarten t.b.v FATCA

Notitie IT bijstand aan MT Belastingdienst 30042014.docx

Notitie Stas IT bijstand CAS 30042014.docx

Aantekeningen.pdf

12 Komende week/weken

Aantekeningen.pdf

12.1 Agenda's komende week (worden verspreid met het weekbericht)

13 Terugkoppelingen/mededelingen

Aantekeningen.pdf

AANTEKENINGEN

Belastingdienst

MT Belastingdienst

Naam dienstonderdeel
BelastingTelefoon
IM Dienstverlening

Contactpersonen
[redacted]
M 06 [redacted]
[redacted]@belastingdienst.nl

[redacted]
M 06 [redacted]
[redacted]@belastingdienst.nl

Datum
01-05-2014

Opdrachtgever
[redacted]

Bijlagen
Geen

memo

Besluitvorming vrijgave MBD / OLAV

Inleiding

MijnBelastingdienst (MBD) en de Onlineaangifte (OLAV) zijn thans zover gevorderd dat besluitvorming over vrijgave en openstelling aan de orde is. MBD en OLAV zijn uitgebreid getest. De resultaten geven het merendeel van de projectboard vertrouwen om beide producten als pilot (zoals ook gedaan is voor de aangifte app) te gaan aanbieden naast Easytax vanaf het moment dat ABS op dagverwerking zit. B/CA geeft er de voorkeur aan nogmaals te testen met de nieuwe ABS-versie en pas op z'n vroegst in augustus in productie te gaan.

Als we een nieuw product live zetten, zijn daar altijd risico's aan verbonden. In dit memo is beschreven welke invoeringsscenario's mogelijk zijn en welke maatregelen we kunnen nemen om deze risico's te mitigeren. De belangrijkste daarvan is dat we MBD/OLAV introduceren als proef en meteen weer kunnen verwijderen, mocht blijken dat de aangiftes niet verwerkbaar zijn.

Wij vragen het MT Belastingdienst om een beslissing over het te kiezen scenario.

Stand van zaken

MBD
Het testtraject is afgerond. Er staan geen bevindingen met risico 'midden' of 'hoog' open. Derhalve is in de projectboard geconcludeerd dat er geen beletselen zijn om MBD vrij te geven. Vooralsnog is openstelling afhankelijk van het gereed zijn van OLAV. Mocht vanuit het perspectief van 1BRN aanleiding gevonden worden om MBD (wijzigen rekeningnummer) open te stellen dan valt dat te overwegen.

OLAV
Er heeft een uitvoerig testtraject plaatsgevonden. Door het laat beschikbaar komen van zowel formulier als testomgevingen zijn testen parallel aan elkaar uitgevoerd. Het

(onbedoeld) gevolg hiervan was dat een veelheid van bevindingen tijdens verschillende tests tegelijkertijd werd geconstateerd. Op dit moment is de stand dat alle voor vrijgave blokkerende bevindingen zijn opgelost en dat alleen nog een regressietest moet worden uitgevoerd. Dit is begin volgende week gepland.

Er is een lijst 'known errors' met bevindingen die niet zijn opgelost. Met betrokken partijen is afgestemd dat geen van de bevindingen op deze lijst blokkerend behoeft te zijn voor vrijgave. Een bevinding wordt als blokkerend aangemerkt wanneer deze leidt tot:
- een foutieve definitieve aanslag
- een foutieve voorspelling
- ondubbelzinnig risico op foutief aangiftegedrag.

De performance voor het aantal te verwachten aangiften in de komende periode is ruim voldoende. Een load van 10.000 aangiftes per uur is haalbaar, dit ligt ruim boven de te verwachten behoefte tot de aangiftecampagne IH 2014. Er loopt inmiddels een actie om te gaan voldoen aan de performance-eis voor de komende campagne.

In de projectboard is geen overeenstemming bereikt over de vrijgave.

B/CA vindt dat de opzet van de uitgevoerde test onvoldoende basis biedt om een vrijgave te kunnen bespreken. Dit komt doordat de afsluitende test is uitgevoerd in een omgeving die naar het oordeel van B/CA, onvoldoende gelijkenis met de productie-omgeving vertoont. Een volwaardige omgeving, die doorgaans voor een ketentest gebruikt wordt, was niet meer beschikbaar. De zorg van B/CA is mede ingegeven door de wetenschap dat B/CA eventuele damages, samen met Belastingen, het hoofd moet bieden. B/CA heeft daarom sterke voorkeur om aan te sluiten bij de ketentest van ABS 14.2 om daarmee meer zekerheid te krijgen over enerzijds de kwaliteit van oplossing van de blokkerende bevindingen en anderzijds de stabiliteit en performance van de keten in een productie like omgeving
Dat zou impliceren dat live gang van OLAV niet voor augustus 2014 te verwachten is.

Belastingen en IM B zijn van mening dat een keuze voor meer zekerheid op de korte termijn evenwel leidt tot meer onzekerheid over het traject voor het komend jaar, we hebben dan immers weinig (leer)ervaringen kunnen opdoen.

Invoeringsscenario's

Er zijn verschillende scenario's mogelijk:

-1- Zekerheid
We kiezen voor een route die vooraf zo veel mogelijk zekerheid geeft dat geen productieverstoringen optreden
-2- Veilig leren
Zo snel mogelijk doch beheerst, bij wijze van proef, live gaan om ervaringen op te doen die nog meegenomen kunnen worden bij het vervolgtraject (VA 2015, IH 2014)

Scenario 1: Zekerheid
Zo min mogelijk onzekerheid accepteren
Ketentest koppelen aan de reguliere ketentest ABS 2014.2, deze vindt op z'n vroegst eind juli plaats
Openstelling dus op z'n vroegst in augustus

Kenmerken:
- ODV is het hoofdspoor, Easytax is minder prominent beschikbaar
- Minder ervaringen en gebruik
- Te laat om ervaringen nog mee te nemen bij VA 2015 en IH 2014
- Geringere gewenningsgraad burger, hoe eerder we live zijn, hoe eerder het publiek immers kennis zou kunnen maken met MBD en OLAV. Daarmee bereiden we de weg voor gebruik in maart 2015 mede voor.

- Biedt de mogelijkheid om MBD eerder open te stellen dan OLAV. Dit vergt echter wel een afzonderlijke inspanning t.a.v. externe positionering/communicatie

Scenario 2: Veilig leren
Op redelijk korte termijn live met MBD en OLAV, bij wijze van proef, om ervaringen op te doen in combinatie met risico-beperkende maatregelen.

Kenmerken:
- We zorgen dat alle bekende blokkerende bevindingen zijn opgelost
- Openstelling vindt plaats wanneer ABS op dagverwerking zit. Dat is naar verwachting eind mei. Het effect hiervan is dat bij eventuele fouten in de applicatie de omvang van het aantal foutieve aangiften, vanwege het ontbreken van grote werkvoorraad, beperkt is (relatief gering aantal aangiften in pijplijn)
- We gebruiken de ervaringen ter voorbereiding/verbetering van de formulieren VA 2015, IH 2014
- De ketentest van ABS 2014.2 is niet randvoorwaardelijk voor vrijgave, maar wel nodig als onderdeel van het testtraject van ABS 2014.2 met in productie zijnde raakvlaksystemen
- We positioneren ODV als 'proef', Easytax is het hoofdspoor. Het positioneren van de proef vereist aanpassing van de communicatieproducten. Onder meer zal in de toelichting duidelijk worden aangegeven waarom deze proef wordt uitgevoerd, wat de reikwijdte is en wat er gebeurt bij eventuele fouten. CKC acht dit haalbaar. Zie bijlage 1.

Risico-beperkende maatregelen:
We treffen in dit scenario een aantal extra risico-beperkende maatregelen:
- We zorgen voor een *gefaseerde* en *gecontroleerde* opstart van de productie vergelijkbaar met de start van de aangifteverwerking in ABS na de aangiftecampagne Zie bijlage 2.
- Deze vindt plaats onder *regie* van *B/CA CMP* (Continuïteit Massale Productie) keten Aanslag in samenwerking met de joint venture Beheer van project ODV
- We verwerken aanvankelijk *druppelsgewijs* een beperkt aantal OLAV-aangiften in ABS om proces en inhoud te controleren.
- Als geen verstoringen blijken, kunnen we de proef stilzwijgend verlengen. Daarom ligt het ook niet in de rede op voorhand een beperking in aantal of tijdsduur te noemen.

Omstandigheden van invloed op afweging van het rest-risico
- Bij geconstateerde fouten na openstelling van het portaal is het in beginsel mogelijk om de toegang tot (het starten van) nieuwe OLAV-aangiften stop te zetten. In dat geval is het nog steeds mogelijk dat burgers via het portaal ingediende aangiften kunnen inzien of wijzigen wanneer wij door het toepassen van de zgn. start-stop-knop nieuwe gebruikers weren. Het spreekt voor zich dat alleen in het uiterste geval tot deze maatregel overgegaan moet worden.
- Mocht een aanpassing van de aangiftesoftware nodig zijn dan heeft dit geen impact op nog niet ingezonden OLAV-aangiften. Deze worden automatisch geconverteerd in het portaal naar de nieuwe software-versie van OLAV, wanneer de aangiften definitief worden gemaakt door de burger.

Geadviseerde beslissing

Gelet op het feitelijk aanwezige (rest)risico, het belang om ervaringen op te doen en de mogelijkheid om aan het licht komende problemen in productie het hoofd te bieden, is het advies te kiezen voor scenario 2 inclusief de risico-beperkende maatregelen.

Definitieve vrijgave voor de aangiftecampagne IH 2014 is niet alleen afhankelijk van de kwaliteit van de producten voor die campagne maar ook van de resultaten van het performance-onderzoek.

Bijlage 1

Burgerperspectief bij scenario 2

Als risico beperkende maatregel wordt de introductie van MBD/OLAV gepositioneerd als proef. Het grote voordeel is dat de burger vooraf wordt gewaarschuwd dat er iets mis kan gaan. Deze positionering heeft wel imagorisico's:

- Wij geven zelf een waarde oordeel af dat we het nog niet voldoende vertrouwen: Beeld dat wij een niet goed product in de markt zetten.
- De burger kan zich gedwongen voelen aan een proef mee te moeten doen.
- Bij het onverhoopt, vervroegd moeten stoppen met de proef zal dit leiden tot minder vertrouwen in het product bij een volgende lancering.

Maatregelen
Deze risico's kunnen worden beperkt met transparante gerichte communicatie met de volgende elementen:

- Door het een proef te noemen zij we transparant dat er nog onvolkomenheden kunnen zijn.
- De keuze om aan een proef mee te doen moet bij de burger liggen; hij moet van te voren weten wat de consequenties van deelname aan de proef zijn. Het aantal mensen dat voor de proef zal kiezen is daarmee aanzienlijk lager dan als OLAV hoofdspoor zou zijn.
- Deze vorm van communicatie is een rationele aanpak. Als de burger een negatieve ervaring krijgt helpt het weinig dat hij het had kunnen weten. Het risico is hiermee beperkt en niet volledig afgedekt.

Kernboodschap
Gaat u aangifte doen? Dan kan u nu meedoen met een proef waarmee u online uw aangifte kan invullen. Dit wordt in de toekomst de manier van aangifte doen. Om dit zorgvuldig te kunnen doen houden we deze proef. We willen ervaring opdoen en zijn ook benieuwd naar uw ervaring.

Vanzelfsprekend moet dit alles goed uitgewerkt worden in een communicatieplan waarbij we uitgaan van pro actieve communicatie.

Bijlage 2

Inregeling productie verwerking OLAV-aangiften[1]

Uitgangspunt
Vanaf 6-5-2014 zit BWA (voorportaal van onder andere ABS, Beheer Werkvoorraad Aanslag) op dagverwerking. Alle garantieposten voor IH2013Nw zijn dan door BWA verwerkt en opgeleverd aan ABS. ABS is op dit moment nog volop bezig met het verwerken van de garantie posten, de verwachting is dat deze eind mei in behandeling zijn genomen. Daarmee zit ook ABS op dagverwerking. Op dat moment kan gestart worden met de invoering conform het scenario "Veilig leren". Dit bestaat uit de volgende stappen:

1. In BWA wordt de kraan voor het berichtsoort "Digitaal aangiften IH2013Nw" dicht gezet. Daarmee wordt tijdelijk voorkomen dat er aangiften van dit type worden doorgegeven aan ABS. Andere IH jaartalen, XBRL, Becon en papier aangiften worden nog wel gewoon doorgegeven

2. ODV wordt volgens de communicatie strategie van CKC als proef live gebracht. Vanaf dat moment wordt het portaal opengesteld voor de burger en kunnen er OLAV-aangiften worden ingediend. Deze worden dan vervolgens in BWA tegengehouden (kraan voor dit bericht type zit dicht). In Splunk kan worden geconstateerd wanneer dat het geval is en welke BSN's dat zijn

3. ABS rondt de verwerking van de garantieposten IH2013Nw (zonder OLAV posten) geheel af (gepland voor eind mei) en controleert dat (lege pijplijn) middels een script. Door dit moment af te wachten wordt eventuele negatieve invloed van de invoering van ODV op de (afronding van) de campagne voorkomen

4. Zodra ABS de status van dagverwerking heeft gemeld, wordt in BWA de kraan voor IH2013Nw (nu incl. Olav posten) kortstondig opengezet. Op basis van het Splunk overzicht worden hierdoor druppelsgewijs voldoende IH2013Nw aangiften doorgelaten, zodanig dat er ook voldoende OLAV-aangiften worden opgeleverd aan ABS

5. ABS start gefaseerd de verwerking op van de nieuwe OLAV-aangiften: hiertoe wordt het volledige proces "gefaseerde opstart" conform het standaard draaiboek uitgevoerd. Daarin zitten de gebruikelijke controles tijdens de afzonderlijke verwerkingsstappen: Fiscale voor-controle, Wegen, Berekenen en Formaliseren. Gestart wordt met een vergelijking van de inhoud van het bericht met de oorspronkelijke opgave van de Burger, zoals deze in DAS is opgenomen.
   Vanuit het eerste aanbod van BWA wordt, zoals bij gefaseerde opstart gebruikelijk is, een nader te bepalen steekproef van ongeveer 40 OLAV aangiften geselecteerd. Bij de samenstelling wordt getracht zoveel mogelijk aangifte-rubrieken te raken. De geselecteerde aangiften worden intensief aan controle onderworpen, tot en met de op te leggen aanslag. Dit wordt zoals gebruikelijk uitgevoerd door de Unit Limburg. De standaard (max.) doorlooptijd van dit proces bedraagt 2 weken. De eindresultaten worden afgestemd met IMB. De reguliere verwerking van aangiften van het type IH2013Nw staat gedurende deze controle tijdelijk volledig stil. De betrokken aantallen zijn op dat moment echter relatief beperkt.
   Deze stap kan herhaald worden wanneer blijkt dat een aantal relevante aangifte-rubrieken niet in deze steekproef is geraakt

6. De controle wordt afgerond met een formele goedkeuring door IMB

7. Zo snel mogelijk na goedkeuring, wordt de BWA kraan voor IH2013Nw weer volledig opengezet zodat de reguliere verwerking, nu incl. OLAV-aangiften kan worden hervat. De in de afgelopen periode (ongeveer 3 weken) ontstane werkvoorraad is dermate klein dat deze vervolgens, zonder extra inspanningen, in een of enkele dagen kan worden weggewerkt. De OLAV-aangiften worden overigens als normale productie beschouwd en krijgen in de verwerking door ABS, indien mogelijk, direct een DA.

---

[1] Verder in te vullen door B/CA CMP (Continuïteit Massale Productie) keten Aanslag in samenwerking met joint venture Beheer ODV.

AANTEKENINGEN

AANTEKENINGEN

AANTEKENINGEN

BESLUITEN- EN ACTIEPUNTENLIJST MT BELASTINGDIENST

22 april 2014

Nr.[1]	[2]	Omschrijving	Status
17.01	**B**	[redacted] verzorgt een presentatie over het vangnet in het kader van (verplicht) elektronisch berichtenverkeer. Opmerkingen vanuit het MT: - Is in budget voorzien? Nee, uitgangspunt is vooralsnog samenwerken met gesloten beurzen; elke partij draagt zijn eigen kosten. Brede bc binnen overheid nodig vanwege financiering - Let op verwachtingspatroon: importeren we met de BB niet een discussie over niet-gebruik van regelingen door mensen die onvoldoende zijn meegenomen? - Positief dat BD lanceert, andere partijen (MFG, BZK, gemeenten) kennen hetzelfde vraagstuk; opletten dat wij niet de hele verantwoordelijkheid naar ons toetrekken; uitstel verplichtstellen helpt hierbij; MFG zet in op kleine pilots - Ei van Columbus t.a.v. triggerfunctie nog niet gevonden; volgorde is: eerst vangnet gereed, dan pas verplichtstellen - Altijd goed actie: papier beperken door niet te sturen [redacted] bedankt [redacted] voor haar presentatie en concludeert: - Heroverweging digitalisering geeft ruimte en tijd; - Belang van overheidsbrede actie - Kleine pilots met anderen prima - Gebruik maken van wat nu al aanwezig is prima insteek - Vangnet biedt geen oplossing voor alle problemen t.a.v. niet-gebruik	√
17.02	**T**	[redacted] meldt dat Opsporing Verzocht op 22/4 aandacht zal besteden aan mensen die geld pinnen van "hun" rekening dankzij bij de post onderschepte bankrekeningnummerformulieren	√
17.03	**T**	[redacted] meldt de stand van zaken huisvesting Nijmegen en Terneuzen. Er zijn kansen voor mensen uit de flexpool bij andere bedrijfsonderdelen. Vanuit Belastingen wordt daarover nog contact gezocht met die andere bo's.	√
17.04	**T**	Op de ETPM-blog zijn 8 reacties gekomen. Met deze mensen wordt een gesprek georganiseerd	√
17.05	**T**	[redacted] kondigt aan dat 22/4 een mail over de mobiliteitskaart zal verschijnen, o.a. over abonnementen o.g.v. gebruik eerste drie maanden. Betrokkenen krijgen begin mei een brief, reactie voor 31 mei, ingangsdatum abonnement 1 juli. Er komt een lijst met namen van mensen voor wie een onderbouwing 1e klas in personeelsdossier ontbreekt; enige tijd voor herstel. Over vier weken opnieuw controle. Degene bij wie dan nog de onderbouwing ontbreekt moet terugbetalen.	

[1] De nummering is als volgt: weeknummer.volgnummer.
[2] **A**=actiepunt; **B**=besluit; **C**=communicatie; **T**=terugkoppeling.

Nr.[1]	[2]	Omschrijving	Status
		In eerstkomende overleg COR staan richtlijnen voor oneigenlijk gebruik op de agenda. Aandacht van de HR-directeuren hiervoor gevraagd. Er bestaan onduidelijkheden over de dossiers en over de vraag hoe je daarop een query doet. Zo nodig overleg [redacted] en [redacted] Kern is dat recht op 1e klas uit dossier moet *blijken*	
17.06	**T** **A**	Ormit: ook zij-instromers, met max twee jaar werkervaring, kunnen in aanmerking komen. Diegenen met een vast dienstverband blijven in dienst van de BD, diegenen met een tijdelijk dienstverband komen in dienst bij Ormit. Binnenkort komt vraag aan alle bedrijfsonderdelen om potentiële opdrachten aan te leveren	 allen
17.07	**T**	Avondsessie transactieverwerking 28 april bij CAOP	√
17.08	**T**	OLAV in MT 6 mei met implementatietraject. Na goede ketentest mogelijk half mei in de lucht	√
17.09	**T**	Vervolg op 15.12: [redacted] heeft O.O.R. bijgewoond. Wordt vervolgd	√
17.10	 **B**	MT bespreekt memo en bijlagen over extern e-mailen. Aan de opmerkingen vanuit vaktechniek Belastingen en cluster Fiscaliteit wordt tegemoet gekomen door het instellen van een werkgroep, waar in de praktijk blijkende knelpunten kunnen worden gemeld. Opgemerkt wordt dat de handleiding sterk vanuit Belastingenperspectief is geschreven. Toeslagen en Douane hebben ruimte om een voor hun dienstonderdelen zinvolle implementatie te kiezen. MT stemt in met het memo en de bijbehorende stukken. [redacted] vraagt naar een mogelijke toepassing voor het buitenland; ook Heerlen buitenland heeft vragen. Afgesproken wordt deze vragen bij de werkgroep in te brengen	√
17.11	 **B**	[redacted] presenteert de [redacted] agenda: - Fase 1: doorontwikkeling [redacted]-kolom; - Fase 2: doorontwikkeling bedrijfsvoeringskolom. Heeft aansluiting gezocht bij MLTP en taskforce [redacted]. [redacted] wijst op Plan-Do-Check-Act en wijst op de uit de taskforce blijkende noodzaak meer naar de processen te kijken. De [redacted]-kolom moet verder kijken dan alleen naar Plan en Check. [redacted] streeft een doorgroei na van alleen financiële kolom naar de bestuurstafel; er gaat daarom meer van mensen gevraagd worden; daarop letten bij werving. Business controllers zowel uit financiële kolom als uit primaire proces. Geen bijzondere communicatie-acties: beweging laten ontstaan in het werk van alledag, passend binnen het tempo van de bedrijfsonderdelen. MT ondersteunt van harte richting en activiteiten uit [redacted]-agenda	√
17.12	**T**	[redacted] licht kort memo met stand van zaken CIO-agenda toe. Viertal punten verdient extra aandacht: verbinding IV-keten met MT, technologie,	√

Nr.[1]	[2]	Omschrijving	Status
	B	rationalisatie, portfolio. MT onderschrijft het beeld dat er veel is gerealiseerd en ondersteunt de keuze voor de vier actiepunten	
17.13	B	[redacted] licht toe dat het anders moet met portfolio: iedereen is nu veel tijd kwijt met herprioriteren, er is onvoldoende regie op de voorkant van het proces. Noodzaak om vanuit het MT BD besluiten te nemen. [redacted] constateert dat we de beschikbare uren opmaken, maar dat maar 60% ervan wordt besteed aan de plannen die we hadden. Zit deels in inefficiency, ontbrekende expertise bij CAO en CIE, omsteltijd/omstelkosten. MT ondersteunt richting: MT moet keuzes maken; krachtiger rol [redacted] prima. MT stemt in met de voorstellen; op MT-tafel besluiten over richting en in geval van escalatie. Aanpak en tijdpad akkoord	√
17.14	B	MT bespreekt rationalisatie aan de hand van een presentatie van [redacted]. MT wil meer urgentie. BO's hebben behoefte aan gestructureerd aanbod en aan informatie over op welke termijn dat beschikbaar is (bouwblokken bijv.) Gesprek gaat in feite over rol van MT waar het gaat om sturen op samenhang en het maken van echte keuzes. Wordt onderwerp van MT-conferentie. Overige conclusies: - Relatie leggen met portfolio - Op MT-tafel spanning tussen rationalisatie en functionaliteit bespreken - Verantwoordelijkheden business enerzijds en [redacted] anderzijds verhelderen - Voorgestelde aanpak en tijdpad akkoord	√
17.15	B	MT stemt in met memo Dienstverlening ERD WGA Belastingdienst	√
17.16	B	MT stemt in met memo Start intern Klanttevredenheidsonderzoek (iKTO) conform optie 3. MT dringt wel aan op het schrappen in de hoeveelheid onderzoeken. De pilotperiode zou voor een actie daartoe kunnen worden gebruikt	√
17.17	T	Het MT ziet in de Managementrapportage maart geen acute risico's. De productieplanningen zijn afgestemd.	√

AANTEKENINGEN

Belastingdienst

Naam dienstonderdeel
BCA, kernteam AFB

Datum
23-04-2014

Versienummer
1.0

Opdrachtgever
MT Fraudebestrijding

Auteur

Behandeld door

Kopie aan

Bijlagen
Geen

memo

Ontwikkeling controle aan de poort

Inleiding.

De visie van de Belastingdienst op fraudebestrijding is uitgewerkt in het zogenaamde "schillenmodel". Twee van deze schillen zijn "Controle aan de poort" en "Profiling". Eén van de maatregelen in de schil "controle aan de poort" is het transactiegericht en realtime (wie is de inzender en welk kanaal en device is gebruikt) kunnen monitoren.
De bij deze monitoring gebruikte logginggegevens zijn waardevolle input voor de profiling. Onderdeel van deze maatregel is het onderzoek naar de toepassing van een digitale fingerprint.
Een andere maatregel is de inrichting van een zogenaamde audittrail. Daarmee wordt geborgd dat voor de hele keten zichtbaar is wat de afkomst is van een aangifte of verzoek en dat alle relevante gelogde gegevens beschikbaar zijn voor toezicht en opsporing.

Er spelen enkele issues, die een duidelijke opdracht en een centrale IV-sturing verdienen. Deze issues worden hierna geschetst. Vervolgens worden aanbevelingen gedaan.

Issues.

1. Zowel het transactiegericht monitoren als de inrichting van een audittrail zijn kleur- en middeloverstijgend. De oorsprong ligt in een gezamenlijk initiatief van Belastingen, Toeslagen, Dienstverlening, FIOD en CA. In de praktijk komen er nu vanuit de business verschillende vragen af op de IV-keten. Er ontbreekt een duidelijke opdracht die ervoor kan zorgen dat deze punten eenduidig en centraal binnen de IV-keten kunnen worden gerealiseerd.

2. Controle in de poort: het proces is informeel ingericht en heeft geen eigenaar.

   De volgende issues spelen op dit punt:
   - Niet beschreven processen en taakuitvoering leidt tot onduidelijkheid. Als voorbeeld dient de recente perikelen rondom OLAV met betrekking tot de ontbrekende logginggegevens t.b.v. fraudebestrijding.
   - Het ontbreken van een eigenaar heeft als risico dat er geen controle kan plaatsvinden op het proces. Bovendien zal er geen aanspreekpunt

zijn in geval van problemen of toekomstige wijzigingen in het IT-landschap.
- Elementen als dataopslag, bewaartermijnen, privacy-issues en veiligheid zijn niet ingeregeld.
- In feite ligt de uitvoering van de real-time monitoring ten behoeve van fraudebestrijding bij het Security Operations Center (B/CIE) bij één persoon en is daarmee bijzonder kwetsbaar.

Advies.

We adviseren zowel aan de businesskant als aan de IV-kant één duidelijke eigenaar van (de inrichting van) dit proces te benoemen. De inrichting van het proces en de ondersteunende middelen vragen om integraal ontwerp, bouw en implementatie. Vanwege de aard en de dynamiek van dit soort fraudebestrijding vraagt dit om een flexibel IV- aanbod. Dat wil zeggen: het proces, de modellen en IT middelen moeten snel aan te passen zijn naar veranderende omstandigheden.

De grootste belanghebbenden aan de businesskant zijn Belastingen, Toeslagen en de FIOD, terwijl de uitvoering van de activiteiten (loggen, monitoren, signaleren) onderdeel is van het massale proces waarin Dienstverlening, Centrale Administratie en CIE belanghebbenden zijn.

Het voorstel is om B/CA (en daarbinnen IM/CA als [redacted]) als eigenaar te laten optreden voor de ontwikkeling van deze maatregelen vanwege het middel- en organisatieoverstijgende karakter en het feit het gegevens betreft die beschikbaar en bruikbaar zijn in de poort.

Gevraagd besluit.

B/CA aan te wijzen als eigenaar van het proces "controle aan de poort" , zodat binnen dat organisatieonderdeel zowel de businessvraag als de vertaling naar IV-middelen kan worden vormgegeven.

AANTEKENINGEN

Belastingdienst

Aan MT Belastingdienst via [redacted] B/CA en FIOD

Apeldoorn

memo

Oplegmemo bij Inventarisatie risico's informatiebeveiliging en cyber crime

Datum
16 april 2014

Auteur

[redacted]

Kopie aan

Bijlagen

Hierbij wordt de rapportage over de inventarisatie van risico's informatiebeveiliging en cyber crime aangeboden.

[redacted] B/CA is in het MT-BD aangewezen als trekker voor het risico "informatiebeveiliging". [redacted] FIOD voor cybercrime.
Afgesproken is een risico-inventarisatie uit te voeren en voorstellen te doen voor vervolgacties waaronder opties als aanscherpen van naleving, instellen van aanvullende maatregelen en dergelijke.

> Met MT BD wordt verzocht in te stemmen met de voorstellen zoals hieronder verwoord.

Informatiebeveiliging
Voor informatiebeveiliging heeft een inventarisatie van mogelijk risico's plaats gevonden; zie bijgevoegde rapportage. Er is nog niet nagegaan of de geconstateerde risico's zich ook voordoen en of er voldoende maatregelen zijn genomen om het risico van optreden te verkleinen c.q. te voorkomen.

Na oplevering van de inventarisatie is besloten aansluiting te zoeken bij de reguliere beveiligingsorganisatie. Daartoe was de inventarisatie op de agenda van het Strategisch Beveiligings Overleg gezet. Als gevolg van de politieke ontwikkelingen rond de vergaderdatum van het SBO kon dit overleg niet doorgaan. Om geen verdere tijd te verliezen is besloten om deze rapportage nu rechtstreeks aan het MT BD aan te bieden.

Voorstel is om de risico analyse op met name de volgende punten uit te werken om vast te stellen of de Belastingdienst voldoende mitigerende maatregelen heeft getroffen en zo nodig maatregelen op te stellen dan wel bestaande maatregelen aan te passen. Dit betreft de volgende gebieden:

- het toegangsbeleid (Rijkspas)
- het gebruik van mobiele devices
- het nieuwe werken.
- Sourcing

Via de in de beveiligingsorganisatie vertegenwoordigde business kan vastgesteld worden wat de meest effectieve en voor de (eind)gebruiker meest efficiënte maatregelen zijn. Het nadrukkelijk betrekken van (eind)gebruikers daarbij is voorwaarde is om naleving van maatregelen en daarmee handhaving van het beveiligingsniveau van de Belastingdienst te waarborgen. De AdR zal gevraagd worden om dit proces met advies en toetsing van eventueel voorgestelde maatregelen te ondersteunen.

CyberCrime
De risico's op het digitale domein onderscheiden we in drie categorieën:
1. de informatiebeveiliging van de huidig in gebruik zijnde systemen
2. de informatiebeveiliging van de toekomstige systemen
3. digitale (identiteits)fraude / phishing / pharming / social engineering

Bij deze driedeling is er uitgegaan van de afspraak dat de eerste twee categorieën gedekt worden door [redacted] (B/CA) en de derde categorie (=cybercrime) opgepakt wordt onder verantwoordelijkheid van de [redacted] FIOD, ondersteund door de [redacted] B/CKC.

In de bespreking van de bij dit risicogebied betrokken directeuren is op basis van de uitgevoerde analyses geconcludeerd dat er veel gedaan wordt op het gebied van cybercrime, met name op operationeel gebied. De vraag is gerezen of wat er gedaan wordt complementair aan elkaar is dan wel verbetering behoeft. Verantwoordelijkheden moeten in bestuurlijke zin voldoende gedekt zijn. Tevens vraagt acteren aan de voorkant aandacht.

Voorstel: geadviseerd wordt om:
- de bestaande structuur voor de governance van Beveiliging (Strategisch Beveilgingsoverleg en Tactisch Beveiligingsoverleg) ook te gebruiken voor de governance van Cybercrime door het inrichten van een cluster Cybercrime;
- blijvend te investeren in het awareness-programma voor leidinggevenden en medewerkers;
- op strategisch niveau de verbinding te zoeken met het NCSC. Een logische plek hiervoor kan het [redacted] Office zijn.

Belastingdienst

MEMO Belastingdienst Risicogebied Cybercrime

19 november 2013

Aan: MT Belastingdienst

B/CKC
Herman Gorterstraat 75
3511 EW Utrecht

Postbus 18200
3501 CE Utrecht
www.belastingdienst.nl

Contactpersoon

M 06
@belastingdienst.nl

Datum
19 november 2013

Versienummer
1.0

Opdrachtgever
-
-

Auteurs
-
-

Kopie aan

Bijlagen
--

1 Aanleiding

In het Managementoverleg Belastingdienst van 25 maart 2013 is onder meer voor 2013 het Risicogebied Cybercrime vastgesteld.

De risico's op het digitale domein onderscheiden we in drie categorieën:
1. de informatiebeveiliging van de huidig in gebruik zijnde systemen
2. de informatiebeveiliging van de toekomstige systemen
3. digitale (identiteits)fraude / phishing / pharming / social engineering

Wij zijn bij deze driedeling uitgegaan van de afspraak dat de eerste twee categorieën gedekt worden door de (B/CA) en de derde categorie (=cybercrime) opgepakt wordt onder verantwoordelijkheid van FIOD, ondersteund door de B/CKC.

In de bespreking van de bij dit risicogebied betrokken directeuren is op basis van de uitgevoerde analyses geconcludeerd dat er veel gedaan wordt op het gebied van cybercrime, met name op operationeel gebied. De vraag is gerezen of wat er gedaan wordt complementair aan elkaar is dan wel verbetering behoeft; verantwoordelijkheden moeten in bestuurlijke zin voldoende gedekt zijn. Tevens vraagt acteren aan de voorkant aandacht.
Van belang is in beeld te krijgen wie waarvoor verantwoordelijk is en waar mogelijk witte plekken te detecteren zijn.

2 Doel memo

Doel van dit memo is:
1. te informeren over de risico's van cybercrime en hoe de Belastingdienst zich daar tegen heeft bewapend;
2. aanbevelingen te geven voor zover het te weer stellen tegen cybercrime (nog) onvoldoende is gebeurd;
3. voorstellen te doen ten aanzien van cybersecurity binnen het geheel van veilig werken[1]:

[1] Veilig werken: werken conform gegevensclassificatie departementaal vertrouwelijk en risicoklasse 2 Wet Bescherming Persoonsgegevens

3 Definitie

Er zijn meer definities van cybercrime in omloop. Een internationaal geaccepteerde en eenduidige definitie is er nog niet.
De houder van het Risicogebied Cybercrime hanteert onderstaande definitie voor de Belastingdienst:
"Cybercrime (in ruime zin) omvat elke strafbare gedraging waarbij het gebruik van geautomatiseerde werken (computers en dergelijke) bij de verwerking en overdracht van gegevens van overwegende betekenis is."

4 Actoren en doel

Cybercrime wordt gepleegd door verschillende actoren met ieder hun eigen doel:

- de "eenvoudige" hacker of script-kiddy: deze is gemotiveerd om te laten zien wat hij kan;
- de ethische hacker: deze is gemotiveerd om gaten in de beveiliging aan te tonen;
- de hacktivist: deze is gericht op het uitdragen van een gedachtengoed
- de terrorist: vaak gedreven door een ideologie of gericht op het zaaien van angst;
- georganiseerde misdaad: gericht op direct of indirect geldelijk gewin, gericht op het doorverkopen van bedrijfsgegevens;
- staten: gericht op het verbeteren van de eigen politieke positie of vergroten van de interne machtspositie;
- interne (ex) medewerkers: gericht op wraak en/of geldelijk gewin.

5 Middelen

De middelen die een cybercrimineel ter vervoeging staan, zijn zeer divers:

- hacken door op diverse manieren (veelal gecombineerde technieken) geautomatiseerde werken binnen te dringen;
- malware besmetting door op computers software te installeren die virussen, worms of Trojans bevatten
- malware aanvallen, bijvoorbeeld pharming (het omleiden van de server waardoor de gebruiker niet in de gaten heeft dat hij/zij met een ander communiceert
- social engineering waarmee door gedragsbeïnvloeding bijvoorbeeld wachtwoorden ontfutseld worden
- DDOS via Botnets

In sommige gevallen kan het gebruik van deze middelen herkend dan wel geblokkeerd worden op technisch niveau. In de meeste gevallen is het een kwestie van combinaties van middelen die het echte gevaar opleveren en is het dus de kunst om combinaties te herkennen en te onderkennen.

6 Ordeningsprincipe activiteiten tegengaan cybercrime

De vraag is hoe je je als organisatie kunt wapenen tegen cybercrime. De activiteiten die verband houden met het *tegengaan van cybercrime* hebben wij als ordeningsprincipe geduid in drie momenten van het inrichten van het handelen: preventie, monitoring en reactie die in zichzelf en tezamen een regelkring vormen.

6.1 Preventie

Preventie begint met governance en organisatie. Het gaat naast de technische maatregelen (veilig programmeren, A&P-testen, etc.) onder andere om het beleggen van de verantwoordelijkheid voor cybercrime in de organisatie en om bewustwordingstrainingen voor medewerkers in ieder geval op sleutelposities. Bedacht moet worden dat 100% veiligheid niet bestaat. Een goede risicoanalyse en een werkend risicomanagement proces zijn randvoorwaarden voor succes. Ook een goede informatievoorziening naar de bestuurders is hierbij van belang. Wat wordt wel geëscaleerd naar boven en wat vooral niet. De bestuurder moet een goed inzicht krijgen/hebben in de risico's die er spelen en hoe relevant deze zijn.

Daar de wereld van cybercrime niet stilstaat is het belangrijk dat de risicoanalyse een continue proces is dat zich aanpast aan de dreigingen en patronen in de buitenwereld. Een samenwerking op het gebied van kennisuitwisseling met andere partijen (binnen en buiten de overheid) is daarbij cruciaal.

6.2 Monitoring

Een organisatie kan door het monitoren van kritieke gebeurtenissen en veiligheidsincidenten en – gebeurtenissen de technologische detectiemaatregelen versterken. Monitoring en datamining vormen samen een uitstekend instrument om vreemde patronen in het gegevensverkeer op het spoor te komen, te signaleren waar de aanvallen zich concentreren en de systeemprestaties te observeren. Van belang hier is dat de organisatie ook leert van gemaakte fouten/incidenten (vgl. luchtvaartindustrie; beloning voor melden van onveilige situaties).

6.3 Reactie

Bij reageren gaat het om het in werking stellen van een vooraf-gedefinieerd plan zodra zich een incident voordoet. Bij een geconstateerde ongewenste activiteit moet een organisatie in staat zijn direct te reageren. Bijvoorbeeld technisch door een systeem uit te schakelen of organisatorisch door een (fraude) onderzoek te starten. Ook hier wordt verwacht dat na het verhelpen van het incident er een evaluatie plaatsvindt en het actieplan daarop zo nodig wordt bijgesteld.

7 Ordeningsprincipe toegepast op Belastingdienst

Wat hebben wij tot nog toe gedaan:

1. Een krachtenveldanalyse is uitgevoerd met als doel om het hele domein van cybercrime, waar deze een bedreiging vormt voor de bedrijfsprocessen van de Belastingdienst, in beeld te krijgen. Het werkveld van de FIOD, B/CIE en B/CA dekt hiervan het overgrote deel.
2. Om de krachtenveldanalyse compleet te maken en de aanpak nog meer te stroomlijnen hebben we alle dienstonderdelen enkele vragen voorgelegd. Met als reden dat we ons kunnen voorstellen dat er op lokaal niveau/dienstonderdeel niveau én ervaring is op dit terrein én mogelijk afspraken zijn gemaakt in dit kader. Dit heeft geleid tot een mindmap onderwerpen en een mindmap krachtenveld.

Op basis van de verzamelde gegevens hebben we genoemde drie momenten van het inrichten van het handelen: preventie, monitoring en reactie toegepast op de Belastingdienst. Wij constateren de volgende situatie met daaraan verbonden conclusies.

7.1 Preventie

De Belastingdienst kent voor de opzet van de beveiligingsorganisatie een viertal beleidsterreinen:

- Informatiebeveiliging
- Persoonlijke veiligheid en Integriteit
- Fysieke beveiliging en
- Business Continuity Management

Deze gebieden zijn alle relevant in het kader van het tegengaan van cybercrime, maar worden niet als zodanig in samenhang bezien:

- Zowel wat betreft governance als organisatie zijn er verantwoordelijken voor veilig werken, maar is er niet een regelkring toegespitst op cybercrime. Ook zijn er overlegvormen waarin de aandacht voor en sturing op veilig werken een plek krijgen, maar ook hier niet toegespitst op cybercrime.

Conclusie: voor wat betreft cybercrime is er op dit moment een onvoldoende ingericht risicomanagementproces cybercrime;

- de Belastingdienst heeft op strategisch, tactisch en operationeel niveau contacten met externe partijen. Niet duidelijk is wat deze contacten in het kader van risico-analyse aan verbinding tussen strategisch, tactisch en operationeel niveau bijdragen.

Conclusie: een regelkring is daartoe niet ingericht. Daarnaast is een belangrijk externe contact nog niet geborgd, terwijl die wens er ligt.

7.2 Monitoring

Zoals aangegeven kan het monitoren van kritieke gebeurtenissen en veiligheidsincidenten de detectie-mogelijkheden en te nemen maatregelen versterken. Deels is de monitoring op het gebied van cybercrime ingeregeld:

- het Security Operations Centre (SOC) voor een klein deel techniek;
- de Anti-Fraudebox (AFB) op het proces en datamining;
- interne controle op basis van HBB-normatiek voor wat betreft toezicht op medewerkers en integriteit in het algemeen;

Conclusie: een onderling samenhangende regelkring is onvoldoende geborgd op strategisch, tactisch en operationeel niveau.

7.3 Reactie

Bij een ongewenste activiteit is het wenselijk om een vooraf-gedefinieerd plan in werking te kunnen stellen (wie beslist wat op welk moment; ook wat betreft escalatie). Deels is een planmatige reactie ingeregeld:

- voor wat betreft een activiteit die vereist dat de infrastructuur en/ of systemen onmiddellijk stopgezet moeten worden, heeft het SOC het zogenaamde “Stekkermandaat”;
- het SOC heeft daarnaast een operationele relatie met de FIOD en de Anti-FraudeBox;
- onder bestuurlijke verantwoordelijkheid van de [redacted] is op strategisch/tactisch niveau het MT Fraudebestrijding ingesteld; de Anti-Fraudebox functioneert onder deze vlag op tactisch/operationeel niveau met een signalerende functie naar het SOC;
- onder bestuurlijke verantwoordelijkheid van [redacted] Belastingen is door het MT Fraude een multidisciplinair samengesteld toezichts-team in het leven geroepen: het Combiteam Aanpak Facilitators (CAF) in het kader van systeemfraude

Conclusie: een planmatig samenhangende aanpak is ons verder niet gebleken; evenmin een daartoe ingerichte overall regelkring.

8 Aanbevelingen

De resultaten van ons onderzoek in samenhang met de daaraan verbonden conclusies brengen ons tot de volgende aanbevelingen:

1. het opnemen in het HBB in de delen A (Strategisch kader) en B (Algemene Uitvoeringsrichtlijnen) van de dreigingen en nader te concretiseren richtlijnen risicobeheersing cybercrime;
2. het inregelen van de governance en organisatie van het risicomanagementproces (preventie, monitoring en reactie) cybercrime waar mogelijk binnen de bestaande structuur SBO en TBO;
3. deelnemers van het TBO opleiden op het gebied van cybersecurity en daarmee samenhangend risicomanagement;
4. de wens van het Nationale Cyber Security Centre (NCSC) te honoreren om op strategisch en tactisch niveau een verbinding met de Belastingdienst te leggen;
5. blijvend te investeren in het awareness-programma voor leidinggevenden en medewerkers.

9 Voorstellen taken en bevoegdheden cybersecurity

9.1 Governance en organisatie

Wij vinden het wenselijk om de aanbevelingen te vertalen in voorstellen, waarbij zoveel als mogelijk wordt aangesloten op bestaande structuren.

Vertrekpunt voor het inregelen van cybersecurity (preventie, monitoring en reactie) is het in het Handboek Beveiliging Belastingdienst verankeren van de verantwoordelijkheid voor cybersecurity beleid bij [redacted]. De verantwoordelijkheid voor de uitvoering hiervan ligt bij de directeuren van de dienstonderdelen. Dit is conform de huidige verantwoordelijkheidsverdeling voor de reeds bestaande beveiligingsaspecten. Hiermee wordt het Strategisch Beveiligingsoverleg (SBO) verantwoordelijk voor een effectief cybersecurity beleid. Zij laat zich hierbij adviseren door het Tactisch Beveiligingsoverleg (TBO).
In dit overleg komen de [redacted] van de dienstonderdelen regelmatig bijeen om gezamenlijk de generieke dreigingen te bespreken. Uiteindelijk doel is om te komen tot een basis-set dreigingen Belastingdienst, die in ieder ontwikkeltraject meegenomen wordt.
Vaststelling van deze basis-set vindt dan plaats in het SBO. Met andere woorden: het SBO stelt de "risk-appetite" voor de Belastingdienst vast op het gebied van beveiliging. De vastlegging van deze basis-set evenals de vastlegging wie doet wat op welk moment bij een ongewenste cyberactiviteit, ook wat betreft escalatie, vindt dan plaats onder het beheer van de [redacted]

Om de basis-set dreigingen up to date te houden, worden de incidenten op het gebied van beveiliging langs het TBO gehouden. Aldaar vindt toetsing plaats.

Hiermee is de governance en organisatie cybersecurity op strategisch, tactisch en operationeel niveau geborgd.

9.2 Samenwerking

Voor het in kaart brengen van de dreigingen en risico's wordt er nu nog onderscheid gemaakt tussen de IV-voortbrenging en het primair proces.
Voor de IV-voortbrenging zijn [redacted] IM, de [redacted] van het dienstonderdeel en [redacted] verantwoordelijk.
Voor het primair proces worden risicoprofielen opgesteld onder verantwoordelijkheid van een M1 van het dienstonderdeel, de [redacted] en de [redacted]. Input voor deze sessies komt onder andere uit de basis-set dreigingen. Resultaat is onder andere een overzicht van te treffen maatregelen.

- Het voorstel is om deze partijen bijeen te brengen en gezamenlijk de risico's en dreigingen in kaart te laten brengen. Per dienstonderdeel kan de [redacted] de spilfunctie vervullen. Zo kunnen in de voortbrenging risico's afgedekt worden die vanuit het primair proces bekend worden en omgekeerd. De [redacted] brengen de risico's in, in het TBO. In het TBO vindt de weging plaats van de risico's die van belang zijn om op te nemen in de basis-set evenals de bijbehorende set maatregelen. Het monitoren van kritische gebeurtenissen en veiligheidsincidenten behoort eveneens tot het aandachtsveld van het TBO; hierin worden zij bijgestaan door de [redacted] (coördinatie), de AFB en het SOC.
- Om niet alleen op operationeel niveau de gebruikte technieken om de organisatie aan te vallen te delen, wordt er ook op strategisch en tactisch niveau aansluiting gezocht met het Nationaal Cyber Security Centre (NCSC). Op operationeel niveau ligt deze verbinding er al via het SOC. Voorgesteld wordt op strategisch niveau de verbinding te leggen door de [redacted] en op tactisch niveau door de [redacted] van B/CIE.

- Om bewustwording en inzicht in het belang van cybersecurity te realiseren is het voorstel om de deelnemers van het TBO op te leiden op het gebied van cybersecurity en het daarmee samenhangend risicomanagementproces. Het initiatief hiertoe wordt genomen door de [redacted] en de [redacted]
- Het management op alle niveaus dient regelmatig met hun medewerkers in gesprek te gaan over cybercrime-awareness; de [redacted] van het betreffende dienstonderdeel ondersteunt daarin het management.

Belastingdienst

Aan [ ], [ ]

RAPPORT

Inventarisatie risico's informatiebeveiliging

B/Centrale Administratie
Apeldoorn

Datum
4 november 2013

Auteurs
[ ]

Kopie aan

Bijlagen
Overzicht interviews

1. Inleiding

Dit memo bevat een beschrijving op hoofdlijnen van risico's waarvan de perceptie bestaat dat mogelijk extra maatregelen nodig zijn ter afdekking ervan. Het Handboek Beveiliging Belastingdienst (HBB) bevat normen en maatregelen die tot doelstelling hebben risico's zoveel mogelijk te reduceren.
Deze inventarisatie is bedoeld om risico's te onderkennen die mogelijk gelopen worden na weging van de reeds genomen maatregelen. Voorstellen worden gedaan om te komen tot een nader onderzoek van deze risico's om te bepalen of de reeds genomen maatregelen voldoende zijn. Zo niet welke maatregelen we alsnog moeten nemen om het risico op een aanvaardbaar niveau te brengen.

2. Opdracht en aanpak

Context
[ ] B/CA is in het MT-BD aangewezen als trekker voor het risico "informatiebeveiliging". Afgesproken is een risico-inventarisatie en een overzicht van de bijbehorende maatregelen (en hun effectiviteit) op te laten stellen. Stap 1 is om allereerst een inventarisatie van risico's uit te voeren. Dat is de inhoud van deze rapportage. Stap 2 is het vervolg om waar nodig extra maatregelen te benoemen.

Opdracht
Gevraagd is een risico inventarisatie op te stellen die inzicht geeft in de reeds uitgevoerde stappen op het gebied van informatiebeveiliging bij de Belastingdienst en de mogelijke hiaten die nog aanwezig zijn. Daarin moet een overzicht zijn opgenomen van de risico's die de Belastingdienst bij de uitvoering van haar eigen taken loopt indien de informatiebeveiliging niet geheel op orde is alsmede de risico's die samenhangen bij onjuist of onbevoegd gebruik door ketenpartners.

Aanpak
De risico inventarisatie is gebaseerd op een serie interviews. Bij de keuze van de gesprekspartners is gekeken naar vertegenwoordiging van de verschillende bedrijfsonderdelen, het fungeren als ketenpartner en de diverse rollen [ ] beleid, architectuur en uitvoering). Zie bijlage 1. Ten behoeve van goede afstemming met de actoren op het gebied van informatiebeveiliging zijn de interviews gevoerd aan de hand van een vooraf opgestelde lijst met onderwerpen en aandachtspunten. Met vertegenwoordigers van de reguliere beveiligingsorganisatie is afstemming geweest over de aanpak.
De interviews zijn vastgelegd in een interviewverslag met terugkoppeling aan de geïnterviewden.
In de aanpak van de inventarisatie worden de reeds genomen acties die zijn gericht op de implementatie en naleving van maatregelen in principe buiten beschouwing gelaten. Tevens is het HBB is een belangrijke uitgangspunt.

3. Risico inventarisatie op hoofdlijnen

In dit onderdeel wordt ingegaan op de hoofdlijn van onze bevindingen. Ons uitgangspunt is daarbij het HBB en de daarin, impliciet, opgenomen risico's. Als eerste wordt daarop ingegaan. Daarna worden de overige uit de inventarisatie naar voren gekomen risico's aangegeven.

3.1 Beveiligingsorganisatie

Binnen de Belastingdienst is een organisatie met betrekking tot informatiebeveiliging aanwezig. Deze is gericht op de risicoafwegingen, zoals vastgelegd in het HBB, en de daaruit voortkomende noodzakelijke maatregelen (zoals die in het HBB als suggesties zijn opgenomen). Via het strategisch beveiligingsoverleg is de leiding van de Belastingdienst betrokken en in staat te sturen. Via het tactisch beveiligingsoverleg zijn alle dienstonderdelen aangesloten en wordt er voortdurend zicht gehouden op de toepassing van de beveiligingsmaatregelen. Dat houdt in dat getoetst wordt op de opzet en het bestaan van de maatregelen binnen de dienstonderdelen. De werking, dat wil zeggen de continue toepassing van de maatregelen in de operatie van alledag, moet zoveel mogelijk aantoonbaar zijn. Daartoe zijn, deels, interne controles opgezet en voeren alle dienstonderdelen zelfevaluaties uit.
Uit de interviews komt naar voren dat veelal wordt voldaan aan opzet en bestaan (het eenmalig vaststellen dat een maatregel is getroffen en op het meetmoment werd toegepast) van beveiligingsmaatregelen, terwijl over de voortdurende toepassing van maatregelen twijfel bestaat.
Daarnaast werkt de PDCA-cirkel niet altijd optimaal: er wordt regelmatig gerapporteerd over bevindingen en voorgestelde oplossingen, maar de '*actfase*' waarin de organisatie aan de slag moeten met de aanbevelingen, wordt niet altijd goed uitgevoerd.

3.2 Risico op gegevens schending of verlies

In het HBB zijn risico's benoemd die gaan over schending van gegevens of gegevensverlies. Uit de interviews is gebleken dat naast de reeds opgenomen risico's, nog andere risico's onderkend worden en dat de wens bestaat om meer nadruk te leggen op deze risico's. Zo komt breed naar voren dat het werken met mobiele *devices* (*smartphones, tablets*) extra aandacht behoeft. Met deze *devices* is bijvoorbeeld gegevensopslag en gegevensuitwisseling mogelijk. Dat houdt in dat het risico bestaat dat gegevens op mobiele *devices* of in *de cloud* worden opgeslagen. Dat betekent een risico op gegevensverlies en gegevensschending in situaties dat het *device* wordt verloren of dat ongeautoriseerden toegang krijgen. Ook aan de mogelijkheden van opslag in een thuissituatie kleven deze risico's. Omdat er steeds meer gebruik gemaakt wordt van deze *devices* is er sprake van een toenemend risico.
Het *rooten of jailbreaken* van devices, waarbij ruimere mogelijkheden van het besturingssysteem van de *devices* wordt verkregen, brengt ook risico's met zich mee.
Een andere tendens die naar voren komt is het toenemend gebruik van email voor de uitwisseling met belastingplichtigen. Formeel is dit niet of slechts beperkt toegestaan. Uit de inventarisatie komt naar voren dat in sommige gevallen email wel op deze manier gebruikt wordt, waarbij het management deze vorm van gebruik soms gedoogt of stimuleert.
Een geheel ander risico is de toenemende afhankelijkheid van de Belastingdienst van informatie die van leveranciers afkomstig is. Bij uitvallen van die gegevensstromen kunnen bedrijfsprocessen van de Belastingdienst niet meer draaien; denk aan Toeslagen.
Door de toename van de snelheden van verbindingen en de toegenomen verwevenheid en complexiteit is het risico op internetaanvallen (via *Denial Of Service* bijvoorbeeld) groter.

3.3 Risico op gegevensmisbruik

Wet- en regelgeving vormen de basis voor de levering van gegevens door de Belastingdienst. Op basis daarvan zijn nadere convenanten afgesloten met de afnemers. Dit kunnen zowel interne bedrijfsonderdelen zijn als externe partijen. Daarin zijn ook bepalingen opgenomen over gebruik van gegevens binnen de doelbinding op grond waarvan deze gegevens worden geleverd.
Uit de inventarisatie komt naar voren dat het risico aanwezig is dat gebruik van de gegevens breder is dan de doelbinding toelaat; het risico is aanwezig dat gegevens ten onrechte naar derden worden doorgestuurd. Wanneer gegevens aan externe partijen verstrekt zijn is er onvoldoende zicht op de manier waarop gegevens gebruikt worden en welke risico's dit gebruik met zich meebrengt. Uit de interviews komt naar voren dat er vermoedens zijn dat dit zich steeds breder voordoet.
Echter ook binnen de Belastingdienst zelf is dit risico aanwezig. En wel bij het gebruik van - van derden - verkregen gegevens die voor een specifiek doel zijn ingewonnen. Gebruik en doorlevering intern (aan bijvoorbeeld andere bedrijfsonderdelen) geeft risico's op inzet van de gegevens, op een manier die strijdig is met de doelbinding die is afgesproken.
Bij beide voorgaande risico's spelen ook regelgeving en convenantafspraken ten aanzien van de bewaartermijn (is er sprake van eenmalig gebruik, mag historie worden opgebouwd, e.d.) en de vernietiging van gegevens een rol. Uit de interviews is naar voren gekomen, dat vernietiging van gegevens niet altijd plaatsvindt.
Verder is uit de inventarisatie naar voren gekomen dat bij *outsourcing* het risico van gegevensopslag buiten de Belastingdienst speelt. Beleid is dat gegevens niet buiten de Belastingdienst worden opgeslagen. Inmiddels zijn er echter ontwikkelingen gaande waarin wel degelijk een volledige *outsourcing* bij commerciële partijen plaatsvindt inclusief gegevensopslag, met alle risico's van dien.

3.4 Risico's in de voortbrengingsketen

Informatiebeveiliging kan worden ondersteund met voorzieningen in applicaties.
Daarmee kunnen beveiligingsmaatregelen bijvoorbeeld worden afgedwongen door functiescheiding in de applicatie in te bouwen.
Uit de inventarisatie komt naar voren dat bij het ontwerpen van processen en applicaties rekening wordt gehouden met algemene en specifieke eisen ten aanzien van beveiliging. Tijdens de looptijd van een project moeten vaak keuzes worden gemaakt tussen functionaliteit, tijd en middelen. Vaak wordt dan de functionaliteit op gebied van beveiliging teruggebracht tot het minimum, waardoor risico's ontstaan. Om deze af te dekken worden vervolgens ad hoc, "tijdelijke", maatregelen genomen. Deze tijdelijke maatregelen hebben als nadeel dat de kennis daarover slechts bij een beperkt aantal medewerkers aanwezig is en dat deze maatregelen onvoldoende ingebed zijn in het beheer van de applicaties.
Een ander signaal is dat de risicobeheersingsfunctie binnen de voortbrenging onvoldoende stevig is verankerd. Daardoor bestaat het risico dat onvoldoende structurele aandacht aan informatiebeveiliging wordt gegeven.
Technische maatregelen die zijn genomen lopen soms achter op de nieuwste risico's en bedreigingen.

3.5 Risico's bij medewerkers

Uit de interviews komt naar voren dat er zorg is over een mogelijk groter wordend risico dat medewerkers worden aangezet tot frauduleus handelen door invloed van buitenaf, bijvoorbeeld via de georganiseerde misdaad. Aandachtspunt is of de bestaande screening van medewerkers afdoende werkt om dit soort risico's te kunnen ontdekken. Voor nieuwe medewerkers is een Verklaring Omtrent Gedrag (VOG) vereist, maar deze screening wordt daarna nooit herhaald, ook niet als medewerkers lang in dienst zijn of op cruciale (lees: kritische of risicovolle) functies terecht komen.

Verdere signalen uit de interviews zijn dat de bewustwording bij medewerkers en management over houding en gedrag en de noodzaak van bepaalde beveiligingsmaatregelen verbeterd zou moeten worden. Zo komt naar voren dat *clear desk* nog vaak niet wordt toegepast, dat PC's niet worden vergrendeld bij niet-gebruik en dat op flexplekken of in openbare ruimtes informatie in bijzijn van anderen wordt gedeeld. Beveiliging begint bij het inzicht waarom maatregelen getroffen worden. Toelichting en begrip zijn daarom essentieel voor het toepassen van beveiligingsmaatregelen.

4. Mogelijke maatregelen

Zoals aangegeven loopt de Belastingdienst risico's waarvan het noodzakelijk is te onderzoeken in welke mate (kans) dit het geval is.
Indien aanvullende maatregelen nodig blijken te zijn kan, bijvoorbeeld bij gegevensschending, gedacht worden aan het aanscherpen van het uitvoeringsbeleid en de handhaving hierop te versterken. Verder zijn aanvullende technische maatregelen mogelijk in de vorm monitoring of het onmogelijk maken van bepaalde toepassingen.
Bij gegevensmisbruik zijn bijvoorbeeld maatregelen te overwegen ten aanzien van het laten uitvoeren van controles op het nalaven van de doelbinding.
In de voortbrenging bij het ontwikkelen van applicaties is een mogelijke maatregel om te bepalen een hogere prioriteit te geven aan beveiliging.
Indien extra maatregelen gericht op medewerkers noodzakelijk blijken te zijn kan gedacht worden aan een verplichte periodieke bewustwordingstraining.

5. Voorstel vervolg

De inventarisatie geeft aanleiding om te komen tot een voorstel voor een vervolg.
Zoals uit de rapportage naar voren komt zijn er diverse risico's genoemd waarbij de perceptie is dat mogelijk extra maatregelen nodig zijn ter afdekking ervan. Als de meest risicovolle zien wij het lekken van informatie naar derden, het gebruik van onbedoelde mogelijkheden van nieuwe devices, opslag in de cloud (dus buiten BD-omgeving), de LOA's en de outsourcing aan derden inclusief gegevensopslag. Het is noodzakelijk om in ieder geval voor deze risico's gedetailleerder onderzoek te doen of we voldoende mitigerende maatregelen hebben getroffen en zo nodig maatregelen op te stellen dan wel bestaande maatregelen aan te passen.
Wij stellen voor om daarbij aan te sluiten bij de reguliere beveiligingsorganisatie. Via de daarin vertegenwoordigde business kan vastgesteld worden wat de meest effectieve en voor de (eind)gebruiker meest efficiënte maatregelen zijn. Benadrukt wordt dat het betrekken van (eind)gebruikers voorwaarde is om naleving van maatregelen en daarmee handhaving van het beveiligingsniveau van de Belastingdienst te waarborgen.

AANTEKENINGEN

Ministerie van Financiën

Aan
MT Belastingdienst

Directoraat-Generaal
Belastingdienst

Inlichtingen
[redacted]
M 06-[redacted]
E [redacted]@belastingdienst.nl

Datum
23 april 2014

Auteurs
[redacted]

Bijlage 1
Protocol integriteitsonderzoeken Belastingdienst

memo

Betreft: Protocol integriteitsonderzoeken Belastingdienst (PIB)

Hierbij bied ik u het Protocol Integriteitsonderzoeken Belastingdienst (PIB) aan.

1. Inleiding
Sinds 2006 geldt binnen de Rijksoverheid een basisnorm voor het doen van onderzoeken, zoals bepaald in artikel 125 quinqies lid 1 van de Ambtenarenwet. De tekst van het artikel luidt als volgt: '*de organisatie heeft een schriftelijk vastgelegde procedure voor het verrichten van een onderzoek, nadat een vermoeden van een misstand (zoals een integriteitsschending) is gemeld*'.

Bij de Belastingdienst bestaat nog geen uniform onderzoeksprotocol op het gebied van onderzoek naar (vermeende) schendingen van integriteit. Tijdens de uitwerking van het project 'Revitalisering integriteit' (2011-2012) werd het kunnen beschikken over een onderzoeksprotocol als verbeterpunt genoemd[1]. Achterliggende gedachte bij de keuze van dit verbeterpunt is, dat de beschikbaarheid van een uniform onderzoeksprotocol bijdraagt aan de kwaliteit van het onderzoek en het door het bevoegd gezag te nemen besluit. In het in de voetnoot genoemde rapport is ook aandacht gevraagd voor de rol van de onderzoeker, bijvoorbeeld ten aanzien van selectie, opleiding, intervisie etc.

2. Het onderzoeksprotocol
De Kennisgroep Integriteit heeft de door het MT-Belastingdienst geaccordeerde aanbevelingen uit het project 'Revitalisering integriteit' overgenomen en als haar doelstellingen geformuleerd. Het voorliggende document is een beschrijving van een uniforme werkwijze voor het doen van onderzoek naar (vermeende) schendingen. In het protocol is geen nieuw beleid en is geen nieuwe regelgeving opgenomen. Bij de totstandkoming van het protocol zijn de integriteitscoördinatoren van de bedrijfsonderdelen nauw betrokken geweest.

Het protocol is bedoeld als richtlijn en bevat om die reden geen uitputtende beschrijving van onderzoekssituaties en onderzoeksmethoden en geen exacte beschrijving van te volgen procedures. Elk onderzoek vereist namelijk maatwerk.

3. Kwaliteitsverhoging van het proces en het besluit
Geconstateerd is, dat binnen de bedrijfsonderdelen niet eenduidig wordt omgegaan met meldingen over (vermeende) integriteitsschendingen en het

[1] Rapport "Integriteit: vanzelfsprekend onderdeel van ons handelen", par. 6.4 en 6.6.

daarop volgende onderzoek. Dit gegeven vormt mede de noodzaak en urgentie voor de samenstelling van het protocol. Een aanname is, dat een juiste en uniform overeengekomen werkwijze betreffende het melden en het doen van onderzoek, leidt tot verhoging van de kwaliteit van de daaruit voortvloeiende processtappen en de kwaliteit van het besluit, dat door het bevoegd gezag moet worden genomen.

4. Kwaliteit, professionaliteit en inzet van de onderzoeker

Een uniforme werkwijze voor melding en onderzoek biedt nog geen garantie voor het gewenste kwaliteitsniveau van het onderzoeksproces en het uiteindelijke besluit. Om die reden is in het voornoemde rapport[2] ook aanbevolen om aandacht te besteden aan de kwaliteit en professionaliteit van de onderzoeker. Binnen de bedrijfsonderdelen worden momenteel veelal HR-adviseurs, onderzoekers en juridisch (beleids)medewerkers ingezet voor het doen van integriteits-onderzoeken.

Beschikbaarheid en onderhoud competenties:

Voor het vaststellen van het gewenste kwaliteitsniveau van de onderzoeker zijn de volgende vragen relevant:

1. Over welke competenties (kennis, vaardigheden en eigenschappen) dient een onderzoeker te beschikken voor het doen van kwalitatief onderzoek naar (vermeende) integriteitschendingen?
2. Over welke competenties beschikken de huidige onderzoekers?
3. Welk beeld ontstaat per bedrijfsonderdeel?
4. Welke (aanvullende) opleiding en training is wenselijk c.q. noodzakelijk?
5. Op welke wijze kan intervisie tussen de onderzoekers worden georganiseerd, waarin ervaringen en 'best practices' worden gedeeld?

5. Communicatie

Ondanks dat het onderzoeksprotocol geen nieuw beleid en geen nieuwe regelgeving omvat, is kennisname van en dus communicatie over de inhoud van het protocol van groot belang. Gelet op het Belastingdienstbrede karakter van deze aangelegenheid, is de Kennisgroep Integriteit beschikbaar om de coördinatie van de communicatie m.b.t. het doel en de inhoud van het onderzoeksprotocol op zich te nemen, in samenspraak met de integriteitscoördinatoren van de bedrijfsonderdelen. Diverse momenten zullen benut worden om de inhoud en toepassing van het PIB toe te lichten.[3]

6. Beslispunten

Het MT-Belastingdienst wordt voorgesteld om:

a) in te stemmen met de inhoud van het Protocol Integriteitsonderzoeken Belastingdienst (PIB);
b) de Kennisgroep Integriteit (in samenspraak met de integriteitscoördinatoren van de bedrijfsonderdelen) te belasten met het beantwoorden van de in par. 4 gestelde vragen;
c) de Kennisgroep Integriteit (in samenspraak met de integriteitscoördinatoren van de bedrijfsonderdelen) te belasten met de uitvoering van een gecoördineerd communicatietraject (zie 5).

[2] Rapport "Integriteit: vanzelfsprekend onderdeel van ons handelen"
[3] Het PIB is ook een gespreksthema tijdens de Belastingdienstbrede bijeenkomst op 3 juli 2014 in Den Haag

Belastingdienst

Protocol integriteitsonderzoeken Belastingdienst

Inhoudsopgave

1 Inleiding 4

Leeswijzer 4

2 Begripsbepalingen 5

3 Het vermoeden van een integriteitsschending 5

3.1 signalen 5

3.2 het melden 6

3.2.1 anoniem melden? 7

3.2.2 de Klokkenluidersregeling 7

3.3 registratie van de melding 7

3.4 het beoordelen van de melding 7

3.5 de aangifteplicht 8

4 Het onderzoek 9

4.1 de onderzoeksopdracht 10

4.2 de onderzoekers 11

4.3 de betrokkene, de verdachte 12

4.3.1 de betrokkene in een disciplinair onderzoek 12

4.3.2 de verdachte in een strafrechtelijk onderzoek 12

4.4 dossiervorming 12

4.5 informatie-uitwisseling tussen strafrecht en tuchtrecht 13

4.6 ongewenste omgangsvormen 13

5 Het disciplinaire onderzoek 13

5.1 het oriënterend gesprek 14

5.2 het feitenonderzoek 14

5.3 anonieme getuigen 15

5.4 de ordemaatregel 15

5.5 de rapportage 16

5.6 de tenlastelegging 17

5.7 de verantwoording 17

5.8 het besluit 17

6 Het strafrechtelijk onderzoek 17

6.1 de verhoren 18

6.2 de aanhouding 18

6.3 de doorzoeking 18

1873579 00349

6.4 de inbeslagneming 18
6.5 de vordering tot uitlevering 19
6.6 het (eind)proces-verbaal 19
7 Communicatie 19
7.1 algemeen 19
7.2 nazorg 20
7.3 herstelactiviteiten 20
8 Slot 20
Bijlagen 21
A Afkortingen 21
B Bronnen 21
C Integriteitsschendingen 22
D Model onderzoeksopdracht t.b.v. een integriteitsonderzoek 25
E Schema integriteitsonderzoek 26
F Schema aangifteplicht 27

1873579 00349

2 Begripsbepalingen

betrokkene	de ambtenaar van de Belastingdienst (incl. flexwerkers en uitzend- en inhuurkrachten) tegen wie een vermoeden van een integriteitsschending bestaat
bevoegd gezag	de functionarissen genoemd in het Organisatie- en mandaatbesluit directoraat-generaal Belastingdienst; doorgaans de (plaatsvervangend) directeur
integriteitsschending	een schending van wettelijke voorschriften of beleidsregels in relatie tot ambtelijke integriteit (gedrag in strijd met de integriteit en met goed ambtenaarschap; een schending kan plichtsverzuim en/of een strafbaar feit opleveren); zie bijlage C met een *niet-limitatieve* lijst van mogelijke integriteitsschendingen
misdrijf	een strafbare gedraging waarvoor de wet een gevangenisstraf als sanctie heeft bepaald (bijvoorbeeld het Tweede Boek van het Wetboek van Strafrecht (WvSr)) of als zodanig is gekwalificeerd in andere wetgeving
onderzoeker	degene die in opdracht van het bevoegd gezag onderzoek verricht naar een vermoedelijke integriteitsschending
plichtsverzuim	het overtreden van enig voorschrift als het doen of nalaten van iets, hetwelk een goed ambtenaar in gelijke omstandigheden behoort na te laten of te doen (artikel 80 van het Algemeen Rijksambtenarenreglement (ARAR))
strafbaar feit	een gedraging waarop in een wet een sanctie wordt gesteld (dit protocol heeft m.n. betrekking op misdrijven)
verdachte	degene tegen wie uit feiten of omstandigheden een redelijk vermoeden van schuld aan een strafbaar feit bestaat (artikel 27 van het Wetboek van Strafvordering (WvSv))

3 Het vermoeden van een integriteitsschending

3.1 signalen

Mogelijke integriteitsschendingen, gepleegd door medewerkers van alle organisatieonderdelen van de Belastingdienst, kunnen door verschillende bronnen en op diverse manieren bij de Belastingdienst worden gemeld. Deze signalen kunnen afkomstig zijn van burgers (bijvoorbeeld via de Belastingtelefoon, klikbrieven en klachten), maar ook van overheidsinstanties zoals de Politie, de Rijksrecherche en het Openbaar Ministerie (OM). Vanzelfsprekend kunnen ook medewerkers van de Belastingdienst melden (zie onderdeel 3.2).

Het is niet uitzonderlijk dat anoniem wordt gemeld. Het is voor burgers, maar ook voor belastingambtenaren, mogelijk om een melding te doen bij Stichting Meld Misdaad Anoniem (het Meldpunt M).
Het spreekt in het algemeen voor zich dat anonieme signalen extra kritisch worden beoordeeld en dat daarop terughoudend wordt gereageerd (zie onderdeel 3.2.1).

1873579 00349

Uitgangspunt moet zijn dat de Belastingdienst altijd reageert op een melding over een mogelijke integriteitsschending van één van zijn medewerkers. Het is dan ook belangrijk dat deze signalen op de juiste plaats terecht komen waar ze op een professionele wijze verder worden behandeld.

3.2 het melden

Van medewerkers van de Belastingdienst wordt verwacht dat ze hun vermoedens van een integriteitsschending melden binnen de organisatie[1]. Er bestaat geen algemene meldplicht, maar is een medewerker op de hoogte van een (ernstige) integriteitsschending of misstand,

doet. Uitgangspunt is dat elk incident dat de integriteit van de Belastingdienst kan raken moet worden gemeld; dat kan dus ook een strafbaar feit zijn dat in privétijd is begaan, omdat daardoor bijvoorbeeld de akte voor Buitengewoon Opsporingsambtenaar (BOA) niet kan worden verlengd.
Ook kan het de medewerker disciplinair worden verweten als hij wetenschap heeft van een integriteitsschending die het organisatiebelang raakt en deze niet meldt.
Het melden is van belang voor de ontwikkeling van de Belastingdienst, zoals het lerend vermogen en bewustwording ten aanzien van integriteit.
Er is één uitzondering op het ontbreken van een meldplicht. Er bestaat wél een meldplicht bij het vermoeden van een gepleegd (ambts)misdrijf omdat daarvan aangifte moet worden gedaan bij het OM (zie onderdeel 3.5).

Medewerkers kunnen hun melding over een mogelijke integriteitsschending bij voorkeur - doen bij hun (direct) leidinggevende. Ook kunnen zij melden aan een Vertrouwenspersoon (VP), een intern meldpunt van een organisatieonderdeel of bij het Bureau Integriteit en Veiligheid (BIV) van de FIOD.

Als een medewerker tijdens zijn fiscale werkzaamheden het ernstige vermoeden krijgt dat een medewerker van de Belastingdienst plichtsverzuim heeft gepleegd (zich niet heeft gehouden aan zijn fiscale verplichtingen of mogelijkerwijs een andere vorm van plichtsverzuim) moet hij zijn vermoeden, al dan niet via zijn direct leidinggevende, melden aan zijn directeur. Hiervoor is permanente ontheffing van de fiscale geheimhoudingsplicht verleend bij besluit DGB2008-05294 van 2 oktober 2008[2]. De directeur van de meldende medewerker draagt, indien van toepassing, de informatie over aan de directeur van het organisatieonderdeel waar de betrokkene werkzaam is, een en ander na verkregen ontheffing van de geheimhouding.

In bepaalde gevallen moet het managementteam van de Belastingdienst (MO c.q. het Directoraat-Generaal Belastingdienst, DGBel) worden ingelicht (zie hoofdstuk 7 onderdeel 3.2.1. van de Personele Uitvoeringsbepalingen Belastingdienst (PUB)):

- bij het vermoeden van een fiscaal en/of commuun misdrijf;
- als de geheimhoudingsplicht is geschonden;
- als publiciteit valt te verwachten die de Belastingdienst raakt.

De werkgever heeft een zorgplicht met betrekking tot de meldende medewerker; deze mag van een te goeder trouw gedane melding geen nadelige gevolgen ondervinden. Een veilige en transparante cultuur binnen de Belastingdienst is voor het melden een voorwaarde.

[1] zie o.a. Omgaan met integriteitsschendingen; de Gedragscode van de Belastingdienst; het Voorschrift buitengewone voorvallen 2004 (VBV 2004)
[2] zie PUB hoofdstuk 7 onderdeel 3.1

1873579 00349

3.2.1 anoniem melden?

Het beleid van de Belastingdienst is er op gericht om een open en transparante cultuur te bewerkstelligen. Daarin past het anoniem melden in principe niet. Toch zijn er situaties denkbaar waarin deze vorm van melden gewenst is. Als een medewerker toch redenen meent te hebben om anoniem te melden kan hij worden verwezen naar de vertrouwenspersoon (VP) (de vertrouwelijke melding waarbij anonimiteit zoveel mogelijk wordt gewaarborgd maar niet gegarandeerd is) of het meldpunt M.

Bij de Criminele Inlichtingen Eenheid (CIE) van de FIOD is een meldpunt in ontwikkeling voor medewerkers die willen melden in verband met zware georganiseerde criminaliteit. Na akkoord van een officier van justitie van het Functioneel Parket (FP) kan anonimiteit van de medewerker worden gegarandeerd.

3.2.2 de Klokkenluidersregeling

In uitzonderlijke gevallen, als een melder bijvoorbeeld meent niet binnen de Belastingdienst te kunnen melden, kan gebruik worden gemaakt van de Klokkenluidersregeling voor de overheid. Het Adviespunt Klokkenluiders kan daarin adviseren en ondersteunen[3].
Om als klokkenluider te kunnen worden aangemerkt, met de daarbij behorende rechtsbescherming, gelden bepaalde voorwaarden. Deze zijn onder andere weergegeven op de website van de Commissie Integriteit Overheid[4].

3.3 registratie van de melding

Belangrijk is dat de melding, door wie en waar die ook gedaan wordt, professioneel wordt opgepakt en afgehandeld. Dit begint onder andere met een schriftelijke vastlegging van een (mondelinge) melding. Transparantie is namelijk essentieel in zowel de meldprocedure als het onderzoeksproces.

Elke mondelinge en schriftelijke melding over een vermoedelijke integriteitsschending wordt binnen een week geregistreerd in de SAP-applicatie EH&S (registratie vermoedelijke integriteitsschendingen). Deze SAP-applicatie ondersteunt het gehele proces van voortgang (van bijvoorbeeld het disciplinaire onderzoek) en afdoening van de melding. Bij elk organisatieonderdeel van de Belastingdienst is een integriteitcoördinator verantwoordelijk voor deze registratie.

Opgemerkt wordt dat de registratie een *vermoeden* van een integriteitsschending betreft. Als al snel blijkt dat de melding onterecht is, kan de registratie onder vermelding daarvan worden afgesloten. Meldingen die niet terecht zijn gebleken worden jaarlijks - in april van het volgende jaar - geautomatiseerd uit het systeem verwijderd (zie ook onderdeel 3.4).

Bij de registratie wordt ook aandacht besteed aan het vullen van de vrije velden met betrekking tot een korte casusbeschrijving en de overwegingen die tot een disciplinair besluit hebben geleid. Dit kan namelijk mede van belang zijn voor de beleidsvorming op het gebied van integriteit.

3.4 het beoordelen van de melding

De melding wordt na registratie beoordeeld op onder andere de volgende aspecten:

- is de melding voldoende betrouwbaar en concreet;

[3] www.adviespuntklokkenluiders.nl
[4] www.commissieintegriteitoverheid.nl/klokkenluidersregeling

1873579 00349

- is de gemelde gedraging een mogelijke integriteitsschending;
- wat is de aard en de ernst van de gemelde schending (is het bijvoorbeeld een strafbaar feit);
- zijn er aanwijzingen en aanknopingspunten die de melding kunnen onderbouwen;
- is nader onderzoek noodzakelijk en wat zijn dan de onderzoeksmogelijkheden.

In wezen is deze beoordeling een (summier) vooronderzoek.

De melding wordt in opdracht van het bevoegd gezag beoordeeld door bij voorkeur verschillende personen vanuit een verschillende invalshoek. Daardoor wordt objectiviteit zoveel mogelijk gewaarborgd. Het ligt voor de hand om voor deze beoordeling een vaste groep van deskundige medewerkers aan te wijzen.
Deze personen kunnen met name zijn een HR-adviseur, een leidinggevende en een onderzoeker met ervaring op het gebied van integriteitsschendingen.
Het BIV wordt geconsulteerd bij twijfel over de mogelijk strafrechtelijke aard van de integriteitsschending.

De direct leidinggevende kan in dit stadium wel worden geconsulteerd, maar dient niet direct bij de beoordeling te worden betrokken. Bijvoorbeeld omdat hij als melder de mogelijke schending al in zekere zin heeft beoordeeld.

Soms zijn er na deze eerste beoordeling al zulke sterke aanwijzingen voor een (ernstige) integriteitsschending dat een rechtspositionele ordemaatregel onmiddellijk nodig is om bijvoorbeeld een onderzoek te beginnen zonder dat de betrokkene daarop invloed kan uitoefenen (zie onderdeel 5.4).

Indien de melding als niet-onderzoekswaardig wordt beoordeeld, wordt deze in de registratie EH&S gemuteerd als afgedaan. Dat kan bijvoorbeeld het geval zijn als het gaat om een gedraging die niets van doen blijkt te hebben met integriteit, of als er onvoldoende aanwijzingen of aanknopingspunten zijn om nader onderzoek te doen.

In principe wordt de melder op enig moment geïnformeerd over de be- en afhandeling van de melding, waarbij vanwege privacyaspecten veelal geen inhoudelijke mededelingen worden gedaan (zie onderdeel 7.1).

Extra aandacht verdient een melding die betrekking heeft op een BOA. De melding kan aanleiding geven om bij de Dienst Justis van het ministerie van Veiligheid en Justitie te toetsen of bijvoorbeeld een medewerker wordt verdacht van een misdrijf, of dat er zodanige twijfels bestaan over de betrouwbaarheid van de medewerker dat dit van invloed is op de geldigheid of verlenging van de BOA-akte door Justis.

Opgemerkt wordt dat integriteitsschendingen gepleegd door flexwerkers, inhuur- en uitzendkrachten geen plichtsverzuim kunnen opleveren; deze medewerkers zijn geen ambtenaar. Na constatering van een integriteitsschending kan natuurlijk wel het contract met

3.5 de aangifteplicht

Als na de beoordeling de conclusie luidt dat mogelijk sprake is van een strafbaar feit (met name een misdrijf), dan wordt over de vervolgstappen overlegd met het BIV.
Het BIV treedt bij elk vermoeden van een misdrijf in contact met de officier van justitie bij het FP van het OM die ambtelijke integriteit in zijn takenpakket heeft. Deze officier van justitie bepaalt of aangifte moet worden gedaan of dat een andere aanpak de voorkeur geniet, zoals

1873579 00349

een disciplinair onderzoek door de Belastingdienst (waarbij het OM gebruik maakt van het beginsel van opportuniteit).

Als er sprake is van het vermoeden van een misdrijf waarvoor een wettelijke aangifteverplichting voor ambtenaren geldt, wordt door het BIV aangifte gedaan bij het FP. Volgens artikel 162 van het WvSv is daarvan in elk geval sprake bij de ambtsmisdrijven zoals genoemd in de artikelen 355 tot en met 380 van het WvSr (bijvoorbeeld verduistering in dienstbetrekking, omkoping, ambtsdwang en het onbevoegd binnentreden van een woning). Ook wordt aangifte gedaan van een vermoedelijk gepleegd misdrijf

- waarbij een bijzondere ambtsplicht is geschonden, of
- waarbij de een ambtenaar gebruik heeft gemaakt van macht, gelegenheid of middel die aan zijn functie zijn verbonden,
- als daardoor inbreuk wordt gemaakt op een regeling waarvan de uitvoering of de zorg voor naleving aan de Belastingdienst is opgedragen.

Van een aantal andere misdrijven moet door elke burger aangifte worden gedaan, zoals bepaalde levensdelicten (artikel 160 van het WvSv).[5]

4 Het onderzoek

Als besloten is tot een onderzoek naar de vermeende schending zijn enkele algemene aspecten van belang.

Allereerst bepaalt de aard van het onderzoek de verantwoordelijkheden en bevoegdheden. Bij een disciplinair (ook wel: rechtspositioneel, tuchtrechtelijk) onderzoek naar plichtsverzuim is het bevoegd gezag, te weten de (plv) directeur van de Belastingdienst, leidend. de onderzoeker heeft bij dit onderzoek andere bevoegdheden dan bij een strafrechtelijk onderzoek. In laatstgenoemd onderzoek gebruikt de opsporingsambtenaar (bijzondere) opsporingsbevoegdheden onder leiding en gezag van de officier van justitie van het OM. de onderzoeker is daarbij gehouden aan de wetgeving van het WvSr en het WvSv.

Het onderzoek is in beide gevallen gericht op waarheidsvinding. Er is wel een nadrukkelijk onderscheid: in een disciplinair onderzoek zal het vermoedelijke plichtsverzuim op basis van deugdelijk vastgestelde gegevens aannemelijk moeten worden gemaakt, terwijl in een strafrechtelijk onderzoek het vermoedelijke strafbare feit wettig en overtuigend moet worden bewezen.

Het onderzoek moet door deskundige onderzoekers professioneel worden uitgevoerd. Daarbij spelen onafhankelijkheid, objectiviteit, zorgvuldigheid, volledigheid en transparantie een grote rol. Het spreekt voor zich dat onderzoeken naar integriteitsschendingen uitermate vertrouwelijk zijn.

Het onderzoek moet in verhouding staan tot de ernst en aard van de schending. Het te verrichten onderzoek moet proportioneel zijn (bijvoorbeeld qua diepgang of tijdsduur), dus in verhouding staan tot de norm die is geschonden.
Ook de onderzoeksmethode moet in verhouding staan tot de schending: als een minder ingrijpende onderzoeksmethode kan leiden tot het gestelde doel dan heeft deze methode de voorkeur (het beginsel van subsidiariteit).

Het is van belang om tijd te nemen voor de onderzoeksopzet en de strategie. Voordat wordt begonnen met daadwerkelijk onderzoek zal eerst een goede informatiepositie moeten worden

[5] zie bijlage F, schema aangifteplicht

1873579 00349

gecreëerd. Ook is het belangrijk om vanaf het begin rekening te houden met verschillende
nnen bepalen).

Het komt voor dat een disciplinair en een strafrechtelijk onderzoek min of meer gelijktijdig worden verricht. Deze onderzoeken zijn evenwel strikt van elkaar gescheiden en vallen onder verschillende privacy-regimes (zie onderdeel 4.5). Soms kan het disciplinaire traject pas worden aangevangen of worden voortgezet nadat informatie, met toestemming van de officier van justitie, vanuit het strafrechtelijk onderzoek aan de Belastingdienst ter beschikking is gesteld. Het kan ook voorkomen dat een disciplinair onderzoek wordt opgeschort hangende het strafrechtelijke onderzoek; laatstgenoemd onderzoek heeft dan prioriteit.
Beslissingen in het ene traject kunnen overigens wel degelijk van invloed zijn op het andere traject. Een stevige disciplinaire aanpak kan voor het OM aanleiding zijn om van (verdere) vervolging af te zien. En een disciplinaire straf kan voor de rechter bij het vonnis weer van belang zijn bij de afweging van de op te leggen strafrechtelijke straf.
Overigens wordt opgemerkt dat het nooit is aan te bevelen om met de disciplinaire procedure te wachten tot het strafrechtelijk onderzoek is afgerond. Het bevoegd gezag heeft hierin namelijk een eigen verantwoordelijkheid. Een strafrechtelijk onderzoek vraagt doorgaans veel tijd en het duurt nog langer voordat een strafzaak bij de rechter wordt behandeld (zie ook onderdeel 4.5).[6]

Tot slot wordt opgemerkt dat er geen strikte, formele scheiding is te maken tussen vooronderzoek, oriënterend onderzoek en feitenonderzoek: het gaat altijd om onderzoek naar een complex van feiten en omstandigheden.

4.1 de onderzoeksopdracht

Een disciplinair onderzoek start met het opmaken van een opdracht voor het onderzoek.
opeenvolgende
onderzoeksopdrachten waarmee de onduidelijkheid voor de betrokkene onnodig lang voortduurt.
Na het vooronderzoek (de beoordeling) geeft het bevoegd gezag, bij voorkeur schriftelijk, opdracht tot het instellen van een nader (feiten)onderzoek[7]. Een mondelinge opdracht wordt zo spoedig mogelijk schriftelijk vastgelegd. De onderzoeksopdracht bevat in principe de volgende onderdelen:

- de aanleiding voor het onderzoek;
- de opdracht zelf (wat moet worden onderzocht; het is bijvoorbeeld ongewenst om naar aanleiding van een concreet feit het gehele ambtelijke verleden van betrokkene te onderzoeken, het zogenaamde);
- de onderzoeksvragen;
- de onderzoeksmethode(n);
- de onderzoekscapaciteit, wie voert het onderzoek uit (gesprekken worden bijvoorbeeld altijd door twee personen gevoerd);
- de periode die het onderzoek beslaat (ook in verband met het voornoemde ;
- de vermoedelijke duur van het onderzoek.

De onderzoeksopdracht geeft een heldere afbakening en biedt duidelijkheid aan zowel onderzoekers als (zij het doorgaans in een later stadium) aan betrokkene. De opdracht wordt opgenomen in het onderzoeksdossier en de uiteindelijke rapportage.

[6] zie bijlage E, schema integriteitsonderzoek
[7] zie bijlage D, modelformulier onderzoeksopdracht

1873579 00349

Als er tijdens een onderzoek redenen zijn om de onderzoeksopdracht uit te breiden (de integriteitsschending kan bijvoorbeeld ingewikkelder of omvangrijker blijken), dan wordt dit ook schriftelijk vastgelegd.

Vorenstaande geldt ook bij een strafrechtelijk onderzoek; de officier van justitie geeft aan de opsporingsambtenaren een specifieke opdracht om een strafrechtelijk onderzoek in te stellen naar het vermoeden van een bepaald strafbaar feit. Deze opdracht wordt in het proces-verbaal vastgelegd. Met het OM worden onder andere schriftelijke afspraken gemaakt over tijdsduur en wijze van onderzoek.

Het bevoegd gezag blijft, evenals de officier van justitie, verantwoordelijk voor de wijze waarop het onderzoek wordt verricht.

4.2 de onderzoekers

Het (reiten)onderzoek wordt verricht door deskundige en professionele medewerkers. Zij dienen bepaalde basisvaardigheden te hebben, zoals gespreksvaardigheden en vaardigheden met betrekking tot onderzoek en verslaglegging, en bij voorkeur ervaring met het verrichten van onderzoeken naar vermeende integriteitsschendingen.

Disciplinaire onderzoeken kunnen worden verricht door HR-adviseurs, juridische beleidsmedewerkers, arbeidsjuristen en door leidinggevenden van het organisatieonderdeel. Andere medewerkers kunnen, indien gewenst, door de directeur speciaal worden aangesteld voor het verrichten van integriteitsonderzoeken.
In een enkel geval is een onderzoekscommissie met verschillende disciplines en expertises aan te bevelen. De Directeur-generaal Belastingdienst beslist op een daartoe gedaan verzoek[8].

Onderzoek door een direct leidinggevende van de betrokkene gebeurt in principe niet. De direct leidinggevende voert een dergelijk onderzoek in elk geval nooit alleen uit. De noodzakelijke objectiviteit kan in het gedrang komen en deze direct leidinggevende moet tijdens en na het onderzoek verder met het team van medewerkers en/of betrokkene.
Bovendien kan de direct leidinggevende een rol hebben gespeeld bij de integriteitsschending (bijvoorbeeld door niet tijdig in te grijpen).
Wel kan de direct leidinggevende betrokken worden bij het eerste gesprek met de betreffende medewerker over de vermeende schending.

In disciplinaire onderzoeken mag geen gebruik worden gemaakt van opsporingsbevoegdheden. De bevoegdheden zoals de Belastingdienst die in verschillende voorschriften heeft vastgelegd, met name in het PUB, zijn van toepassing.

Het BIV van de FIOD kan in bepaalde gevallen, na overleg met Juridische Zaken van DGBel, (reiten)onderzoek naar een vermoeden van plichtsverzuim verrichten namens, en in opdracht van, het bevoegd gezag (de directeur). De medewerkers van het BIV treden dan niet op als opsporingsambtenaren en gebruiken dus geen opsporingsbevoegdheden.

Strafrechtelijke onderzoeken worden verricht door daartoe bevoegde opsporingsambtenaren van de FIOD, de Rijksrecherche, de Politie of de Koninklijke Marechaussee. Het officier van justitie bepaalt welke opsporingsinstantie het onderzoek verricht.

[8] zie het PUB hoofdstuk 7 onderdeel 3.2

1873579 00349

4.3 de betrokkene, de verdachte

4.3.1 de betrokkene in een disciplinair onderzoek

De betrokken medewerker heeft in een disciplinair onderzoek bepaalde rechten, maar ook plichten. De betrokkene hoeft zijn onschuld niet te bewijzen, maar hij dient wel elke twijfel omtrent zijn integriteit weg te nemen en mee te werken aan het disciplinaire onderzoek (het geven van openheid van zaken). Hij dient zich immers te gedragen zoals een goed ambtenaar betaamt. Wil de betrokkene niet meewerken dan kan dit (nogmaals) plichtsverzuim opleveren. Het is aan het bevoegd gezag om aannemelijk te maken dat betrokkene zich schuldig heeft gemaakt aan plichtsverzuim.

De betrokkene wordt, als het onderzoeksbelang zich daartegen niet verzet, zo snel mogelijk op de hoogte gesteld van het feit dat een onderzoek naar hem wordt ingesteld. Hij wordt dan geinformeerd over hetgeen hem verweten wordt en over zijn rechten (zoals bijstand door een raadsman of vertrouwenspersoon) en plichten (medewerking aan het onderzoek). Bij aanvang van het formele disciplinaire traject ontvangt de betrokkene in ieder geval een schriftelijke mededeling (de tenlastelegging).

De betrokkene wordt, als het onderzoek op enig moment wordt gestopt, in principe geinformeerd over het feit dat een onderzoek naar hem is ingesteld, tenzij er zwaarwegende redenen zijn om dat niet te doen. Dit hangt van de situatie af.

4.3.2 de verdachte in een strafrechtelijk onderzoek

De verdachte in het strafrechtelijk onderzoek heeft de rechten zoals die zijn vastgelegd in het WvSv (zoals het zwijgrecht, bijstand van een raadsman). De aangehouden verdachte heeft recht op bijstand van een raadsman voordat het eerste verhoor plaatsvindt. Hij hoeft niet mee te werken aan het onderzoek en dat moet hem worden medegedeeld (de zogenaamde cautie). Ook zal aan de verdachte op het geëigende moment worden medegedeeld waarvan hij wordt verdacht. Aan de verdachte mogen geen vorderingen worden gedaan tot het verstrekken van gegevens, informatie en dergelijke.
De officier van justitie deelt de verdachte mede als er bijzondere opsporingsbevoegdheden zijn toegepast. De verdachte krijgt verder onder andere mededelingen over de (niet-) verdere vervolging.

4.4 dossiervorming

Het feitencomplex en het onderzoek daarnaar dient zorgvuldig en objectief te worden vastgelegd. Schriftelijke vastleggingen zijn onder andere van belang voor de transparantie van het onderzoek en het zo nodig achteraf afleggen van verantwoording over (de wijze van) het onderzoek en genomen beslissingen. Het verdient bijvoorbeeld aanbeveling om onderzoekshandelingen, besluitvorming en afspraken vast te leggen in een journaal.

Het onderzoeksdossier bestaat in elk geval uit:

- de onderzoeksopdracht;
- het journaal;
- relevante bescheiden of (soms) voorwerpen;
- gespreksverslagen;
- onderzoeksverslagen;
- processen-verbaal en/of rapporten;
- een eindrapportage.

1873579 00349

In een disciplinair onderzoek maakt het onderzoeksdossier deel uit van het plichtsverzuimdossier. Verder maken hiervan deel uit de onderzoeksopdracht, de tenlastelegging, de verantwoording van betrokkene en het besluit van het bevoegd gezag.

4.5 informatie-uitwisseling tussen strafrecht en tuchtrecht

De disciplinaire procedure en het strafrechtelijk onderzoek vallen onder verschillende privacywetgeving: eerstgenoemde onder de Wet bescherming persoonsgegevens (Wbp) en de tweede onder de Wet politiegegevens (Wpg) en de Wet justitiële en strafvorderlijke gegevens (Wjsg). Terbeschikkingstelling van informatie vanuit de ene naar de andere procedure is aan strenge regels gebonden. De belangen van de medewerker en die van de Belastingdienst worden daarbij afgewogen door de instantie die de informatie bezit.

Het BIV verzorgt in voorkomende gevallen de afstemming en overdracht van relevante informatie uit de disciplinaire of de strafrechtelijke procedure aan de andere belanghebbende instantie. Hierbij wordt nogmaals opgemerkt dat er doorgaans geruime tijd verstrijkt voordat het OM toestemming heeft gegeven voor verstrekking van informatie uit een strafdossier.

Als het OM (nog) geen toestemming heeft verleend voor informatieverstrekking aan de Belastingdienst en er is al wel een terechtzitting gepland, dan is het uitermate zinvol om deze zitting bij te wonen. De zitting is immers openbaar en kan veel informatie geven over het feitencomplex en de rol van de verdachte daarbij.

4.6 ongewenste omgangsvormen

Het vermoeden van plichtsverzuim kan bestaan op grond van gedragingen die als ongewenste omgangsvormen worden omschreven. Het kan gaan om discriminatie of seksuele intimidatie,

omgangsvormen kunnen worden benoemd als een strafbaar feit (bijvoorbeeld belediging, stalking, bedreiging of aanranding).
Onderzoek naar ongewenste omgangsvormen moet uiterst zorgvuldig en behoedzaam gebeuren. Sturende vragen of opmerkingen, met name ingegeven door het tonen van inlevingsvermogen met het (vermeende) slachtoffer bij seksuele intimidatie, liggen op de loer, evenals vooringenomenheid of tunnelvisie.
Een zorgvuldige voorbereiding van te voeren gesprekken is met name in een onderzoek naar ongewenste omgangsvormen van groot belang. Daarnaast is het – in het algemeen – belangrijk dat dergelijke onderzoeken worden verricht door een vrouwelijke en mannelijke onderzoeker in koppelverband.

5 Het disciplinaire onderzoek

In dit protocol zijn reeds veel onderwerpen aan de orde gekomen die van belang zijn in het disciplinaire onderzoek. Daarom zal in dit hoofdstuk (iets meer) worden ingegaan op enkele specifieke aandachtspunten. Bovendien staat de disciplinaire procedure al uitvoerig

De disciplinaire procedure heeft als doel om op basis van deugdelijk vastgestelde feiten aannemelijk te maken dat betrokkene zich heeft schuldig gemaakt aan plichtsverzuim, en kent een aantal fasen:

- het vermoeden van plichtsverzuim;
- het oriënterend gesprek;
- het feitenonderzoek;
- het dossier en de rapportage;

1873579 00349

- de tenlastelegging;
- de verantwoording;
- het (straf)besluit.

Hierna wordt ingegaan op enkele aspecten van het disciplinaire onderzoek.

5.1 het oriënterend gesprek

Het beginsel van hoor en wederhoor is ook in het disciplinaire onderzoek belangrijk.
De betrokkene wordt in principe schriftelijk uitgenodigd voor het oriënterend gesprek waarin hij kan reageren op het vermoeden van plichtsverzuim. In de uitnodiging wordt betrokkene op de hoogte gesteld van de aard en het doel van het gesprek. Hij wordt ook gewezen op zijn rechten en plichten (zoals zijn medewerking aan het onderzoek). Tijdens dit gesprek kan betrokkene zich laten bijstaan, bijvoorbeeld door een raadsman of een vertrouwenspersoon.
Van het gesprek wordt een verslag gemaakt, zoveel mogelijk in de eigen bewoordingen van de betrokkene. Het verslag wordt door alle aanwezigen getekend voor akkoord of gezien.
Het verdient aanbeveling dit verslag tijdens het gesprek op te maken en onmiddellijk na het gesprek te laten ondertekenen. Als de betrokkene een achteraf opgemaakt gespreksverslag niet wil ondertekenen dan wordt diens reden om niet te tekenen aan het verslag toegevoegd.
In sommige gevallen kan het gewenst zijn om het gesprek op te nemen en achteraf uit te werken. Dit kan alleen met toestemming van alle gespreksdeelnemers.

Er moet tijdens het gesprek voor worden gewaakt om ongeoorloofde druk uit te oefenen. De onderzoeker dient zich objectief op te stellen en zich, zoveel als mogelijk, te onthouden van sturende opmerkingen, suggesties of insinuaties.

5.2 het feitenonderzoek

Het feitenonderzoek is doorgaans het vervolg op het vooronderzoek (de beoordeling van de melding, die
oriënterend gesprek waarin betrokkene wordt geïnformeerd over het vermoeden van plichtsverzuim.
Tijdens het tuchtrechtelijk feitenonderzoek proberen de onderzoekers onder verantwoordelijkheid van het bevoegd gezag het feitencomplex (de feiten én de omstandigheden) objectief vast te stellen.

Zij kunnen daarvoor verschillende onderzoekshandelingen verrichten, zoals bijvoorbeeld:

- het voeren van gesprekken met de betrokkene (in het kader van hoor en wederhoor);
- het voeren van gesprekken met getuigen of andere personen;
- het raadplegen van diverse openbare bronnen (internet, sociale media, etc.);
- het raadplegen van gesloten, vertrouwelijke bronnen;
- het doen van onderzoek in de (digitale) werkomgeving, zoals de computer, smartphone, tablet, e-mail en het bureau en/of de kast;
- het onderzoeken van tijd- en werkregistraties en declaraties;
- het onderzoeken van toegangsregistraties;
- het onderzoeken van rittenadministraties;
- het onderzoeken van telecommunicatiegegevens (met uitzondering van afluisteren);
- het observeren van locaties en/of de betrokkene, al dan niet met behulp van een camera.

Het is belangrijk gesprekken (interviews) met betrokkene en met anderen altijd met twee onderzoekers te voeren, waarbij één van de twee zich richt op de verslaglegging. Eventueel kan worden gekozen voor een aparte notulist.

1873579 00349

Voordat databestanden met vertrouwelijke fiscale gegevens worden geraadpleegd (zoals BVR, Fibase, Dacas, HSB, ABS, etc.) moet de directeur van het organisatieonderdeel van betrokkene een schriftelijke ontheffing van de fiscale geheimhoudingsplicht vragen aan Juridische Zaken van DGBel. De verleende ontheffing geldt vervolgens ook voor het confronteren van betrokkene met de resultaten van het fiscale onderzoek en voor de rapportage over het plichtsverzuim.

De Algemene wet inkomensafhankelijke regelingen (Awir) en de Algemene wet bestuursrecht (Awb) kennen een eigen geheimhoudingsverplichting die niet geldt als medewerkers met toeslagen hebben gefraudeerd. De geheimhouding geldt slechts voor de informatie waarvan een medewerker van de Belastingdienst/Toeslagen in zijn functie en uit de aard van de zaak (toezicht op toeslagen) kennis heeft. Dit geldt uiteraard niet voor fraude met toeslagen[9].

Voor het onderzoeken van persoonsregistraties of bestanden die behoren bij de bedrijfsmiddelen van de Belastingdienst, waarbij inbreuk kan worden gemaakt op de persoonlijke levenssfeer van betrokkene, dient de directeur van het organisatieonderdeel schriftelijk toestemming te vragen aan Juridische Zaken van DGBel. Daarvan is in elk geval sprake als toegangsregistraties, rittenadministraties, camerabeelden, computers en gegevens van telecommunicatieverkeer moeten worden onderzocht. Toestemming wordt alleen verleend als sprake is van een ernstig vermoeden van plichtsverzuim. De toestemming geldt ook voor gebruik van het onderzoeksresultaat in de disciplinaire procedure.

B/CAO), zoals specifieke loggings of mutaties gekoppeld aan user- het verzoekende organisatieonderdeel de vraag schriftelijk aan de directeur van B/CIE en/or B/CAO. Soms moet daarbij een toestemming van DGBel worden gevoegd, zoals voor onderzoek van e-mailverkeer en telefoonverkeer. Voor een dergelijk verzoek is een speciale postbus beschikbaar in Lotus Notes (BCIE Vertrouwelijkeonderzoeken_Postbus).

Het BIV kan op verzoek van het bevoegd gezag bijstand verlenen aan een disciplinair reitenonderzoek. Daarvoor is overleg met en instemming vereist van Juridische Zaken van DGBel. De medewerkers van het BIV verrichten hun werkzaamheden dan in opdracht van het bevoegd gezag (de directeur) en treden in dat geval niet op als opsporingsambtenaar.

5.3 anonieme getuigen

Het gebruik van anonieme getuigen tegen een betrokkene is weliswaar in principe niet ontoelaatbaar, maar is alleen toegestaan in combinatie met ander verifieerbaar bewijsmateriaal en alleen dan als de anonimiteit op zeer zwaarwegende gronden noodzakelijk is. Van een ambtenaar mag in beginsel worden verwacht dat hij zijn verantwoordelijkheid als overheidsfunctionaris neemt en onder naam verklaringen aflegt.

De afzonderlijke verklaringen van de anonieme getuigen moeten voor betrokkene controleerbaar zijn (bijvoorbeeld door inzage). Daarnaast moet duidelijk zijn volgens welke procedure de getuigen zijn geselecteerd, welke vragen zijn voorgelegd en hoeveel getuigen verklaringen hebben afgelegd. Dit wordt des te belangrijker als de betrokkene de anoniem afgelegde verklaringen betwist.

5.4 de ordemaatregel

Tijdens de disciplinaire procedure zijn er verschillende momenten waarop ordemaatregelen noodzakelijk kunnen zijn. Dat kan al zijn direct na het ontstaan van een concreet en actueel

[9] zie het PUB hoofdstuk 7 onderdeel 3.1

1873579 00349

vermoeden van plichtsverzuim (is er bijvoorbeeld gevaar voor het wegmaken van bewijzen of voor verstoring van het onderzoek, maar ook in verband met onrust in het team). Soms ontstaat pas in de loop van het onderzoek de noodzaak tot een ordemaatregel.

Een ordemaatregel is geen strafmaatregel en wordt, na een afweging van de belangen van de betrokkene en van de organisatie, opgelegd in het belang van de Belastingdienst en van het onderzoek. Ontzegging van de toegang tot de gebouwen van de Belastingdienst of een schorsing zijn ordemaatregelen die regelmatig tijdens een disciplinair onderzoek worden toegepast.
Bij deze beide ordemaatregelen dienen doorgaans de toegangspas en het legitimatiebewijs te worden ingenomen. Ook worden bedrijfsmiddelen als de smartphone, tablet en notebook ingenomen. Verder is het meestal noodzakelijk dat wordt voorkomen dat betrokkene nog op enigerlei wijze toegang krijgt tot databestanden van de Belastingdienst: autorisaties moeten worden geblokkeerd (een verzoek via Lotus Notes: BCIE Vertrouwelijkeonderzoeken_Postbus).
Om de genomen ordemaatregelen effectief te laten zijn moeten deze (meestal) binnen de dienst aan medewerkers van hetzelfde kantoor worden kenbaar gemaakt (zie onderdeel 7).
Opgemerkt wordt dat een aangehouden verdachte, wiens vrijheid wordt beperkt, van rechtswege in zijn ambt is geschorst.

De betrokkene mag tijdens diensttijd door het bevoegd gezag zelfs aan lichaam, kleding en goederen worden onderzocht (artikel 125d van de Ambtenarenwet (AW)). Het spreekt voor zich dat deze handeling een forse inbreuk maakt op de persoonlijke levenssfeer en alleen wordt toegepast als er duidelijke en gerechtvaardigde aanwijzingen zijn dat betrokkene bijvoorbeeld gestolen bedrijfsmiddelen of ander bewijsmateriaal bij zich heeft.

5.5 de rapportage

Na het onderzoek wordt daarvan een rapportage gemaakt ten behoeve van het bevoegd gezag. Deze rapportage is ook bestemd voor de betrokken medewerker.
In dit rapport worden alle feiten en omstandigheden, belastende maar ook ontlastende, opgenomen. De onderzoekers leggen het onderzoek objectief vast en onthouden zich van persoonlijke meningen of oordelen.
Als van de onderzoekers wordt verwacht dat zij conclusies of adviezen aan het onderzoek verbinden worden deze separaat bij het rapport gevoegd.

De onderzoeksrapportage, onderdeel van het onderzoeksdossier, bevat in elk geval:

- de onderzoeksopdracht (met het vermoeden/verwijt);
- de vermelding van relevante wet- en regelgeving (de normstelling);
- de onderzoeksmiddelen, -methoden;
- een weergave van alle relevante feiten en omstandigheden;
- alle relevante schriftelijke stukken;
- het onderzoeksresultaat.

De rapportage wordt door het bevoegd gezag gebruikt voor het vervolg van de disciplinaire procedure. Allereerst betreft dit de beoordeling of de onderzochte gedragingen inderdaad kunnen worden gekwalificeerd als plichtsverzuim, of er een tenlastelegging moet volgen en vervolgens of een rechtspositionele maatregel (zoals een straf) moet worden opgelegd.
Als het oordeel luidt dat er geen grond meer is voor een vervolg van de disciplinaire procedure stopt het onderzoek en volgt er geen tenlastelegging. Betrokkene wordt hiervan schriftelijk op de hoogte gesteld.

5.6 de tenlastelegging

In de tenlastelegging verwoordt het bevoegd gezag de conclusie welke gedragingen betrokkene als plichtsverzuim worden verweten. Het is de afsluiting van de onderzoeksfase en het formele begin van het disciplinaire traject dat moet leiden tot een besluit van het bevoegd gezag. Alle feiten en omstandigheden die hebben geleid tot de conclusie het vermoeden van plichtsverzuim worden beschreven. De omstandigheden moeten vooral antwoord geven op de vraag omtrent de verwijtbaarheid van de gedraging. Vanzelfsprekend staat in de tenlastelegging ook welk voorschrift of welke (gedrags)norm is overtreden. In de tenlastelegging wordt betrokkene er op gewezen dat hij in de gelegenheid wordt gesteld zich te verantwoorden.

5.7 de verantwoording

De betrokkene kan zich op de tenlastelegging mondeling of (bij voorkeur) schriftelijk verantwoorden. Een schriftelijke verantwoording door betrokkene kan mondeling worden toegelicht. Bij een mondelinge verantwoording wordt zo spoedig mogelijk een gespreksverslag gemaakt dat door betrokkene, eventueel diens raadsman en door de verslaglegger voor akkoord wordt ondertekend. Bij weigering om te ondertekenen wordt vermeld waarom betrokkene niet wenst te ondertekenen.

5.8 het besluit

Een professioneel uitgevoerd onderzoek moet leiden tot een verantwoord en goed onderbouwd besluit van het bevoegd gezag. De feiten en omstandigheden zoals die in het onderzoek zijn gebleken worden zorgvuldig afgewogen. Daarbij komen altijd de volgende vragen aan de orde: is er sprake van plichtsverzuim; zo ja, is dat plichtsverzuim verwijtbaar of toerekenbaar; wordt gebruik gemaakt van de bevoegdheid om te straffen en is deze straf evenredig aan het gepleegde plichtsverzuim?
Voorafgaand aan het definitieve besluit wordt betrokkene het voornemen tot het opleggen van een straf medegedeeld en wordt hij in de gelegenheid gesteld om zijn zienswijze te geven.

Vanzelfsprekend kan de betrokkene binnen vastgestelde termijnen tegen het besluit nog bezwaar en beroep aantekenen.

6 Het strafrechtelijk onderzoek

Als uit de melding van een integriteitsschending het vermoeden van een gepleegd strafbaar feit ontstaat, moet in een aantal gevallen aangifte worden gedaan bij de officier van justitie van het FP (zie onderdeel 3.5).
Bij twijfel over de aard van de vermoende schending dient het BIV te worden geraadpleegd.
In dit verband wordt ook gewezen op de Gedragslijn bij strafbare feiten begaan door ambtenaren van de Belastingdienst in functie[10]. Deze gedragslijn geldt ook voor uitzendkrachten en flexwerkers en betreft, in bepaalde gevallen, ook strafbare feiten begaan in de privésfeer.

Het strafrechtelijk onderzoek wordt uitgevoerd onder gezag van de officier van justitie. Deze bepaalt ook welke opsporingsinstantie met het onderzoek wordt belast.
Gezien alle formaliteiten (het onderzoek wordt verricht conform de wetgeving van het WvSv) kent dit onderzoek doorgaans een lange doorlooptijd. Gedurende het onderzoek kunnen in het

[10] besluit van 7 maart 2001 nummer BOB2001/518M

1873579 00349

algemeen, zonder toestemming van de officier van justitie, geen mededelingen worden gedaan over voortgang of resultaten van het onderzoek.

Binnen het strafrechtelijk onderzoek hebben de opsporingsambtenaren, afhankelijk van het vermoedelijke strafbare feit, vergaande (bijzondere) opsporingsbevoegdheden. Toepassing van deze bevoegdheden, die een aanzienlijke inbreuk kunnen maken op de privacy van de verdachte, is doorgaans afhankelijk van toestemming van de officier van justitie en/of de rechter-commissaris.

Tijdens het strafrechtelijk onderzoek kan gebruik worden gemaakt van bijvoorbeeld de volgende opsporingsbevoegdheden:

- het verhoren van verdachten en getuigen;
- de aanhouding van de verdachte (inverzekeringstelling, bewaring);
- de doorzoeking van de woning of het kantoor;
- inbeslagneming van voorwerpen of gegevens;
- vorderingen tot uitlevering van voorwerpen of gegevens;
- opnemen en afluisteren van tele- of datacommunicatie;
- observatie;
- pseudokoop;
- stelselmatige informatie-inwinning.

Hierna zullen enkele opmerkingen bij sommige bevoegdheden worden gemaakt.

6.1 de verhoren

Verklaringen van verdachten en getuigen worden zoveel mogelijk in de eigen bewoordingen van de gehoorde geverbaliseerd. Deze verklaringen worden door de verbalisanten op ambtseed of de belofte opgemaakt en in ieder geval door de verbalisanten ondertekend.
De verdachte krijgt slechts na toestemming van de officier van justitie een kopie van zijn verhoor.

6.2 de aanhouding

De verdachte kan in opdracht van de officier van justitie worden aangehouden, waarna hij voor een periode van maximaal tweemaal 3 dagen in verzekering kan worden gesteld. Deze vrijheidsbeneming vindt doorgaans plaats in een politiebureau.
De verdachte kan daarna eventueel in bewaring worden gesteld door de rechter-commissaris (maximaal 14 dagen), en vervolgens kan de gevangenhouding worden bevolen door de rechtbank (ten hoogste 90 dagen).
Tijdens deze vrijheidsbeneming is de verdachte ambtenaar van rechtswege in zijn ambt geschorst.

6.3 de doorzoeking

Een doorzoeking ter inbeslagneming in de kantoorruimte geschied onder leiding van de officier van justitie, terwijl deze in een woning plaats vindt onder leiding van de rechter-commissaris. Beiden zullen aan de belanghebbende altijd eerst verzoeken tot medewerking aan de doorzoeking.
Binnentreden in een woning gebeurt, als de bewoner geen toestemming verleent, slechts met een machtiging tot binnentreden van een (hulp)officier van justitie.

6.4 de inbeslagneming

Voorwerpen die de waarheid aan het licht kunnen brengen, die kunnen worden verbeurd verklaard of die kunnen worden onttrokken aan het verkeer zijn voor inbeslagneming vatbaar.
Opsporingsambtenaren kunnen in bepaalde gevallen zelfstandig in beslag nemen. In andere gevallen neemt de (hulp)officier van justitie of de rechter-commissaris voorwerpen in beslag. De belanghebbende ontvangt altijd een bewijs van inbeslagneming.

1873579 00349

6.5 de vordering tot uitlevering

Opsporingsambtenaren en de (hulp)officier van justitie kunnen voorwerpen en gegevens van de (directeur van de) Belastingdienst vorderen. Als het gaat om gegevens uit persoonsregistraties of uit bestanden die behoren bij bedrijfsmiddelen verdient een schriftelijke vordering van de officier van justitie ex artikel 126nd van het WvSv de voorkeur.
Aan dergelijke vorderingen moet binnen een bepaalde termijn worden voldaan door of namens de directeur van de Belastingdienst. In de vordering is ook een geheimhoudingsclausule opgenomen. Een vordering tot uitlevering wordt niet aan de verdachte gedaan.

6.6 het (eind)proces-verbaal

Gedurende het onderzoek worden onderzoekshandelingen (zoals verhoren, observaties en dergelijke) in een proces-verbaal vastgelegd. Ook alle relevante bijlagen worden bij het proces-verbaal gevoegd.
Het uiteindelijke proces-verbaal wordt naar de officier van justitie gezonden. Deze beoordeelt het proces-verbaal op de haalbaarheid van de verdere vervolging.
Daarna moet aan de verdachte een dagvaarding voor de terechtzitting worden uitgereikt.

Er kan geruime tijd zitten tussen het inleveren van het proces-verbaal bij het OM en de eventuele transactie, strafbeschikking of de behandeling van een zaak door een rechter. Deze lange doorlooptijd is ook van invloed op de verstrekking van relevante informatie uit het strafdossier ten behoeve van het eventuele disciplinaire traject.

7 Communicatie

7.1 algemeen

Communicatie over een integriteitsschending is belangrijk, onder andere voor de bewustwording en preventie. Het kan onrust, geruchten en een onveilig gevoel bij medewerkers voorkomen of wegnemen.

Tijdens het onderzoek moet terughoudend en weloverwogen worden omgegaan met (het moment van) communicatie over de integriteitsschending naar zowel betrokkene als naar (het belang van de Belastingdienst) staat bij de afweging voorop, maar de privacy van de betrokkene telt daarbij zwaar mee.
Soms moet, onder vermelding van de naam van betrokkene, worden gecommuniceerd over is ontzegd en/of is geschorst. Ook strafontslag moet worden kenbaar gemaakt, al was het maar om ongewenste contacten vanuit betrokkene met oud- (bijvoorbeeld om vertrouwelijke informatie te verkrijgen). Als de naam van betrokkene wordt vermeld kan dit alleen na instemming van betrokkene. Als betrokkene geen toestemming geeft dient de directeur, vóór publicatie, een onderbouwde belangenafweging ter goedkeuring voor te leggen aan Juridische Zaken van DGBel[11].

De direct leidinggevende houdt gedurende het onderzoek contact met betrokkene waarbij hij deze begeleidt en de nodige zorg geeft.

[11] zie de Handreiking communicatie bij een integriteitsschending

1873579 00349

De melder zal, indien mogelijk en gewenst, worden geïnformeerd over het resultaat van zijn melding. Het tijdstip waarop dit gebeurt dient zorgvuldig te worden afgewogen.

In geval van een onterecht gebleken vermoeden van plichtsverzuim zal dit, uitsluitend na overleg met de betrokken medewerker, worden medegedeeld aan het (relevante onderdeel van het) organisatieonderdeel. Rehabilitatie vraagt een zeer zorgvuldige en intensieve begeleiding van de medewerker waarbij communicatie een belangrijke rol speelt.

In geval van een strafrechtelijk onderzoek wordt daarover binnen de Belastingdienst uitsluitend gecommuniceerd na toestemming van de officier van justitie.

7.2 nazorg

Soms blijkt dat een intern onderzoek zoveel commotie in de naaste werkomgeving van betrokkene heeft veroorzaakt dat nazorg nodig is. In een gesprek met belanghebbenden (zoals teamleden) kan bijvoorbeeld worden uitgelegd waarom een onderzoek is ingesteld en waarom voor bepaalde onderzoeksmethoden is gekozen. Verder kan onjuiste beeldvorming (geruchten) worden gecorrigeerd. Een dergelijk gesprek kan ook van belang zijn in het kader van het lerend vermogen van de medewerkers en ten behoeve van preventie.
Bij de nazorg kunnen leidinggevenden en HR-adviseurs worden betrokken, maar ook de onderzoekers.
Met name na een strafrechtelijk onderzoek kan uitleg over bepaalde gebeurtenissen (zoals de keuze voor een aanhouding of doorzoeking) van belang zijn. Het BIV kan hiervoor worden benaderd.

Uiteraard moet aandacht worden besteed aan de betrokkene, met name wanneer de betrokkene weer moet integreren in op een (andere) werkplek. In geval van een rehabilitatie zal betrokkene en zijn directe werkomgeving intensief moeten worden begeleid.

7.3 herstelactiviteiten

Na een integriteitsschending kan het van belang zijn om een aantal vragen te stellen, zoals:

- enst onderkend en afgedekt;
- zijn de datasystemen nog integer;
- moet financiële, proces- of imagoschade worden hersteld of beperkt;
- moet de Auditdienst Rijk (ADR) worden geïnformeerd (moeten bijvoorbeeld (beheers)procedures worden verbeterd of gewijzigd);
- moeten anderszins activiteiten worden ontplooid ter voorkoming van soortgelijke incidenten.

8 Slot

Dit onderzoeksprotocol is door het Managementteam Belastingdienst vastgesteld.
Het kan worden aangehaald als Protocol integriteitsonderzoeken Belastingdienst (PIB).

1873579 00349

Bijlagen

A Afkortingen

ADR	Auditdienst Rijk
AW	Ambtenarenwet 1929
Awb	Algemene wet bestuursrecht
Awir	Algemene wet inkomensafhankelijke regelingen
ARAR	Algemeen Rijksambtenarenreglement
BOA	buitengewoon opsporingsambtenaar
BIV	Bureau Integriteit en Veiligheid (FIOD)
CIE	Criminele Inlichtingen Eenheid (FIOD)
DGBel	Directoraat-generaal Belastingdienst
FP	Functioneel Parket van het Openbaar Ministerie (OM)
Gedragslijn	Gedragslijn bij strafbare feiten begaan door ambtenaren van de Belastingdienst in functie (Besluit BOB2001/518M)
HR	Human Resource
PUB	Personele Uitvoeringsbepalingen Belastingdienst
VBV 2004	Voorschrift buitengewone voorvallen 2004 (onderdeel 8 van het PUB)
VP	Vertrouwenspersoon (integriteit en ongewenste omgangsvormen)
Wbp	Wet bescherming persoonsgegevens
Wjsg	Wet justitiele en strafvorderlijke gegevens
Wpg	Wet politiegegevens
WvSr	Wetboek van strafrecht
WvSv	Wetboek van strafvordering

B Bronnen

- www.integriteitoverheid.nl, m.n. BIOS (handreiking Zorgvuldige handhaving)
- http://intranet.belastingdienst/integriteit, intranet Belastingdienst,
- http://portal.rp.rijksweb.nl/irj/portal/anonymous/personeel, voor het PUB doorlinken

- de brochure Een integere Belastingdienst (de Gedragscode, zie intranet)
- de brochure Omgaan met integriteitsschendingen (intranet)
- de brochure Handreiking communicatie bij een integriteitsschending (intranet)
- het Voorschrift buitengewone voorvallen 2004
- de Gedragslijn bij strafbare feiten begaan door ambtenaren van de Belastingdienst in functie
- het Besluit melden van vermoedens van missstanden voor Rijk en Politie 2009

1873579 00349

C Integriteitsschendingen

Hierna volgt een niet-limitatieve opsomming van mogelijke integriteitsschendingen.
(bron: Registratie integriteitsschendingen openbaar bestuur en politie (2008), aangevuld met enkele specifieke omschrijvingen voor de Belastingdienst)

1. Financiële schendingen

Diefstal / verduistering

Opzettelijk enig goed dat geheel of ten dele aan een ander toebehoort zichzelf toe-eigenen.

Fraude

Betreft intern misbruik, zoals bij vervalsing van administratie of ontduiking van voorschriften. Een concreet voorbeeld is declaratiefraude. Doel van de fraude is materieel persoonlijk gewin.

Overig

Bijvoorbeeld afpersing, afdreiging en oplichting.

2. Misbruik positie en belangenverstrengeling

Ongeoorloofde nevenactiviteiten

Het verrichten van nevenwerkzaamheden die de belangen van de Belastingdienst (kunnen) schaden.

Ongeoorloofde financiële belangen

Het hebben van bepaalde (niet gemelde) financiële belangen of het verrichten van bepaalde financiële transacties kan (de schijn van) belangenverstrengeling oproepen.
Denk hierbij aan de Insiderregeling.

Omkoping (corruptie)

Van corruptie is sprake wanneer een persoon een gift , dienst of belofte vraagt en/of aanneemt; en (vermoedelijk) als doel heeft om in zijn functie iets te doen of na te laten, al dan niet in strijd met zijn plicht (een ambtsmisdrijf).

Aannemen / vragen van geschenken, uitnodigingen etc.

Hieronder vallen zowel het aannemen van geschenken boven de vijftig euro, als ook het niet melden van geschenken.

Favoritisme

Oneigenlijke bevoordeling van medewerkers, vrienden, familie, partijgenoten.

Misbruik van legitimatiebewijs

In sommige functies kan een functioneel bewijs misbruikt worden voor het verkrijgen van enig persoonlijk voordeel. Bijvoorbeeld om korting of gratis toegang te bedingen, of om toegang te verkrijgen tot anders niet toegankelijke plaatsen.

Overig

Voorbeelden zijn draaideurconstructies, vriendjespolitiek, deelname aan aanbestedingen, leveringen aan openbare diensten.

3. Lekken en misbruik van informatie

Lekken van informatie

Het bewust of onbewust geven van vertrouwelijke informatie aan onbevoegde derden.

Misbruik van informatie

Het misbruik maken van informatie ten voordele van de eigen persoon of derden, of ten nadele van derden.

Raadplegen informatie uit vertrouwelijke registers

Het raadplegen van vertrouwelijke systemen van de Belastingdienst anders dan voor zakelijk gebruik.

Verlies / diefstal van informatiedragers

Verlies of diefstal van computers, laptops, usb-sticks, cd-roms et cetera.

Overig

Overige vormen van lekken en misbruik van informatie die de integriteit van de Belastingdienst aantasten, bijvoorbeeld het achterhouden van informatie.

1873579 00349

4. Misbruik bevoegdheden

Ongeoorloofde opsporingsmethoden en dwangmiddelen

Het inzetten van bepaalde opsporingsmethoden en/of dwangmiddelen zonder de daarvoor vereiste officiële goedkeuring of zonder enige gegronde noodzaak.

Meineed

Het onder eed of belofte verkondigen van een onwaarheid.

Valsheid in geschrifte

Indien onwaarheid in officiële stukken wordt verkondigd. Ook het aanbrengen van veranderingen in stukken waarop moet kunnen worden vertrouwd, valt hieronder

Afgifte van vergunningen en legitimatiebewijzen

Het in afwijking van geldende voorschriften afgeven van vergunningen, legitimatiebewijzen, sluiting van huwelijken en dergelijke.

Overig

Overige vormen van misbruik van bevoegdheden die de integriteit van de Belastingdienst aantasten.

5. Misbruik geweldsbevoegdheid

Fysiek geweld

Het niet subsidiair en proportioneel toepassen van geweld in de uitoefening van de functie.

Vuurwapengebruik

Het niet subsidiair en proportioneel toepassen van het vuurwapen in de uitoefening van de functie.

Overig

Overige vormen van het niet subsidiair en proportioneel toepassen van de geweldsbevoegdheid.

6. Ongewenste omgangsvormen

Discriminatie

Discriminatie is het maken van een ongerechtvaardigd onderscheid (bijvoorbeeld in de vorm van een belediging of het achterstellen van individuen). Het betreft onderscheid op grond van godsdienst, levensovertuiging, politieke gezindheid, ras, geslacht, nationaliteit, seksuele geaardheid, handicap, chronische ziekte of leeftijd.

Seksuele intimidatie

Variërend van dubbelzinnige opmerkingen, seksuele grappen of mededelingen over lichamelijke kenmerken tot aan ongewenste handtastelijkheden en poging tot aanranding en verkrachting.

Overig

Overige ongewenste omgangsvormen die de integriteit van de Belastingdienst aantasten.

7. Misbruik bedrijfsmiddelen en overtreding interne regels

Ongewenst gebruik e-mail / internet

Dit betreft niet alleen het (buitensporig) gebruikmaken van email/internet voor privédoeleinden, maar ook het gebruik van email/internet voor het bekijken en/of verspreiden van informatie die de integriteit van de Belastingdienst aantast.

Misbruik van bedrijfsmiddelen

Het (buitensporig) gebruikmaken van bedrijfsmiddelen voor privédoeleinden.
Zoals (mobiele) telefoon, tablets en bedrijfsauto, vervoersbewijzen.

Werkverzuim

Het op zodanige wijze niet naleven van werkuren of het misbruik maken van ziekteverzuim, dat disciplinair optreden passend is.

Niet volgen van de procedures

Door het niet naleven van procedures kan een goede taakvervulling van de organisatie in gevaar worden gebracht.

Slordig omgaan met bedrijfsmateriaal

Het op zodanig wijze omgaan met bedrijfsmateriaal dat deze beschadigd raken of zoekraken.

Gebruik van alcohol of drugs

Het op zodanig wijze gebruikmaken van alcohol- of drugs, dat disciplinair optreden passend is. Dit staat los van een eventuele begeleidingstraject met het bedrijfsmaatschappelijk werk.

Overig

Overige vormen van misbruik bedrijfsmiddelen en overtreding van interne regels die de integriteit van de Belastingdienst aantasten.

8. Misdragingen in privésfeer

Financiële schendingen

Zoals diefstal, fraude, oplichting.

Ongewenste omgangsvormen

Zoals discriminatie, seksuele intimidatie en agressie en geweld. Dit kan ook huiselijk geweld betreffen.

Alcohol of drugs

Dit betreft niet alleen alcohol- en drugsmisbruik, maar ook (gelegenheid geven tot) drugshandel. Bijvoorbeeld door het kweken van hennepplanten.

Ongewenste contacten

Het onderhouden van ongewenste contacten in de privésfeer. Bijvoorbeeld het aangaan van een relatie met een persoon met criminele antecedenten. Zie ook de Circulaire ongewenste privécontacten rijksambtenaren.

Overig

Overige vormen van misdragingen in de privésfeer die de integriteit of het aanzien van de Belastingdienst aantasten. Voor ambtenaren van de Belastingdienst vallen hieronder bijvoorbeeld het niet nakomen van fiscale verplichtingen (bijvoorbeeld onjuiste belastingaangifte), fraude met toeslagen en loonbeslag.

9. Misstanden volgens de klokkenluidersregeling

De specifieke invulling van dit type misstanden hangt af van de klokkenluidersregeling die voor de eigen organisatie geldt.

Het kan betrekking hebben op :

Een schending van wettelijke voorschriften of beleidsregels.

Een gevaar voor de gezondheid, de veiligheid of het milieu.

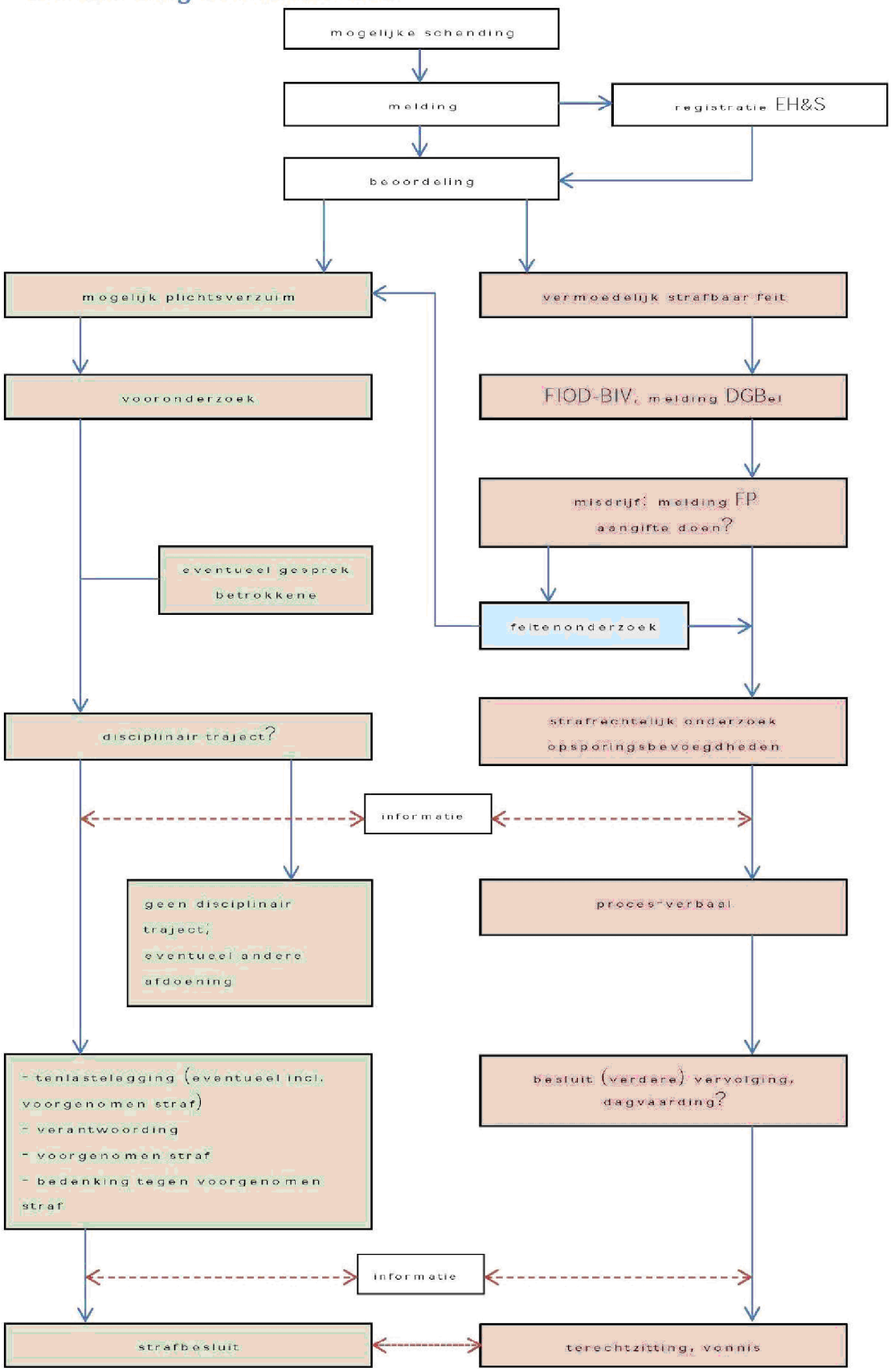
Een onbehoorlijke wijze van functioneren die een gevaar vormt voor het goed functioneren van de openbare dienst.

D Model onderzoeksopdracht t.b.v. een integriteitsonderzoek

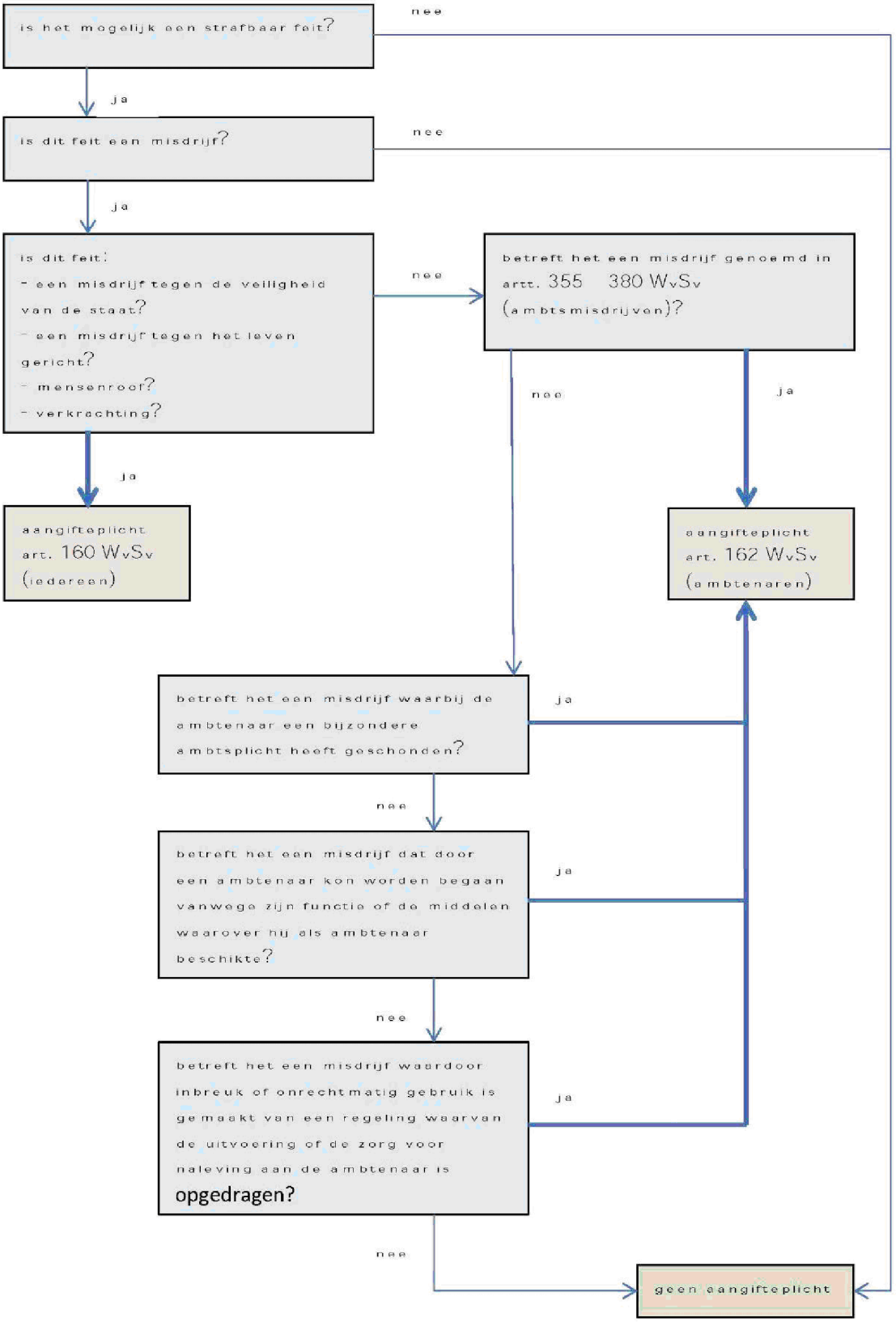
opdrachtgever *(naam, functie, organisatieonderdeel)*	
betrokkene *(naam, functie, werklocatie)*	
aanleiding onderzoek *(korte summiere beschrijving)*	
opdracht *(zo beperkt mogelijk, indien nodig uit te breiden)*	
onderzoeksvragen *(beschrijf de essentiële vragen)*	
onderzoeksmethode *(welke middelen worden gebruikt *)*	
onderzoeksperiode *(welke periode moet worden onderzocht)*	
onderzoekscapaciteit *(naam onderzoekers, geschatte duur van het onderzoek)*	
handtekening opdrachtgever, datum	

* denk aan een tijdige ontheffing van de fiscale geheimhoudingsplicht en een toestemming voor onderzoek in bestanden die behoren bij bedrijfsmiddelen (DGBel)

E Schema integriteitsonderzoek



F Schema aangifteplicht



AANTEKENINGEN

Ministerie van Financiën

Aan
MT Belastingdienst

Directoraat-Generaal
Belastingdienst

Inlichtingen

T
F
minfin.nl

Datum
6 mei 2014

Auteur

memo

Doorontwikkeling CKC: houtskoolschets

Het MTBD wordt gevraagd

Kennis te nemen van de houtskoolschets doorontwikkeling B/CKC, inclusief onderliggende rapportages.

1. Aanleiding voor MT/BD besluit

De Belastingdienst werkt aan zijn toekomst. In 2013 is onderzoek gedaan naar de kennisfunctie binnen de Belastingdienst en is op basis van dit onderzoek een concept houtskoolschets voor een centrale kennissupportorganisatie opgesteld. In de periode januari – maart 2014 is op verzoek van en CHRO de verbinding met de richting en inrichting van centrale communicatie en HR uitgewerkt.

Gezamenlijk vormen de verschillende onderzoeken het fundament voor de doorontwikkeling van B/CKC als centraal organisatieonderdeel op het gebied van kennis, communicatie en HR. Dit fundament is uitgewerkt in een integrale houtskoolschets Doorontwikkeling B/CKC. Tijdens de avondbijeenkomst van het MT/BD 22 april is de richting van B/CKC verder toegelicht. Tevens zijn de noodzakelijke voorwaarden en aandachtspunten om deze richting te effectueren ter bespreking voorgelegd.

Tijdens deze bespreking is door geconcludeerd en besloten dat de rapporten met betrekking tot HR, Kennis en Lopende zaken voldoende fundament bieden om de doorontwikkeling van B/CKC tot volwaardig partner op het gebied van kennis, communicatie en HR te effectueren. Met betrekking tot het onderzoek naar Communicatie /Dienstverlening is vastgesteld dat de bevindingen worden meegenomen door de taskforce communicatie. De uitkomsten van die taskforce zijn bepalend voor de verdere richting en inrichting van de bij B/CKC.
B/CKC heeft op grond van de houtskoolschets, de onderliggende rapporten en de uitkomsten van de avondsessie de opdracht gekregen de inrichting van B/CKC te effectueren.

2. Totstandkoming documenten

De integrale doorontwikkeling van B/CKC als centraal organisatieonderdeel op het gebied van kennis, communicatie en HR vraagt een evenwichtige uitwerking van deze drie domeinen. In de periode januari – maart 2014 zijn hiertoe verschillende onderzoeken uitgevoerd. De aanpak van deze onderzoeken is op hoofdlijnen vergelijkbaar. Op basis van een inventarisatie van de huidige (organisatie van de) activiteiten is een dialoogfase gestart met stakeholders. Insteek van die gesprekken was een verkenning van de beelden die er zijn ten aanzien van het functioneren van een centraal dienstonderdeel op het terrein van (respectievelijk) kennis, communicatie en HR. Op basis van deze gesprekken en de onderzoeken zijn de onderliggende rapportages van de houtskoolschets opgesteld. Gezamenlijk vormen de houtskoolschets en de onderliggende notities een integraal richtinggevend kader voor de inrichting en doorontwikkeling van B/CKC.

3. Vervolgproces

[redacted]B/CKC heeft de opdracht gekregen om de doorontwikkeling van B/CKC te effectueren in lijn met de houtskoolschets en onderliggende documenten, rekeninghoudende met de uitkomsten van de avondbijeenkomst van 22 april. Doelstelling daarbij is om per 1 januari 2015 een organisatie te hebben ingericht in lijn met de in de integrale houtskoolschets uitgewerkte richting (zie bijlage).

In de periode mei - september wordt de inrichting verder uitgewerkt en geconcretiseerd. Met onderdelen die geen onderwerp van discussie zijn (geweest) wordt begonnen met richten en inrichten. In september wordt de uitkomst van dit proces, inclusief veranderplan, wederom besproken in een avondsessie met het MT/BD.

De uitkomst van deze avond is de opmaat naar het functioneren van B/CKC als centrale organisatie voor HR - Kennis en communicatie per 1 januari 2015. Parallel aan dit proces vinden gesprekken plaats met de OR B/CKC en de [redacted]

Bijlage: houtskoolschets doorontwikkeling B/CKC

In co-creatie proactief en professioneel werken aan ruimte en resultaat

Richten van B/CKC als centraal organisatieonderdeel van de Belastingdienst op het gebied van kennis, communicatie en HR

HOUTSKOOLSCHETS

April 2014 versie 1.0

1873579 00349

Inhoud

Inleiding **3**

1. Beweegreden: samen doen wat samen kan **4**

2. Richting geven aan B/CKC als partner bij doelrealisatie **5**

2.1 B/CKC als partner bij doelrealisatie *5*

2.2 De spil waar B/CKC om draait *6*

2.3 Voorwaarden om professioneel partnerschap te realiseren *6*

2.4 Aandachtspunten voor succesvolle implementatie *8*

3. Inrichten B/CKC als centraal organisatieonderdeel op het gebied van kennis, communicatie en HR **9**

3.1 Uitgangspunten voor inrichting centrale activiteiten B/CKC *9*

3.2 Uitwerking domeinen B/CKC *10*

3.2.1 Domein - Onderzoek & Innovatie *10*

3.2.2 Domein - Leren & Ontwikkelen *11*

3.2.3 Domein - Communicatie *12*

3.2.4 Domein - Organisatieontwikkeling *13*

3.2.5 Domein - Mobiliteit (arbeidsmarktontwikkeling, in-, door- en uitstroom) *13*

3.2.6 Domein - Werkgever- en werknemerschap *14*

Colofon

Dit document is een coproductie van de Belastingdienst en TEN HAVE Change Management.

Datum: april 2014
Versie: 1.0
Opdrachtgever:
Auteurs:

Inleiding

De Belastingdienst werkt gericht en gestructureerd aan een perspectief op de toekomst. In het nieuwe MLTP – getiteld *Resultaat en Ruimte* – wordt de koers voor de periode 2014 – 2017 uitgewerkt. Leidende vragen zijn (1) hoe kan de Belastingdienst waarmaken dat elke burger en elk bedrijf de behandeling krijgt die men verdient en (2) hoe kan de dienst uitgaan van verantwoordelijkheid, kansen en professionele ruimte voor elke medewerker. Dit wordt gerealiseerd met behulp van vier speerpunten:

- kansen voor medewerkers;
- handhavingsregie;
- digitalisering, en;
- samenwerking.

De speerpunten vormen individueel en in samenhang de basis voor de verdere ontwikkeling van de Belastingdienst. Essentiële bijdragen daaraan worden geleverd vanuit de vakgebieden kennis, communicatie en HR. De combinatie met recente ontwikkelingen maakt dat de organisatie van de werkzaamheden op deze drie gebieden aan belang is toegenomen.

De opdracht voor B/CKC is om de Belastingdienst, zowel in zijn geheel als voor de verschillende delen, in staat te stellen om de maatschappelijke doelen te realiseren. Dit betekent meer dan alleen een dienstverlenende houding richting dienstonderdelen. Het betekent dat er centraal activiteiten op het gebied van kennis, communicatie en HR worden ingevuld omdat dit de gehele dienst ten goede komt. Samen doen wat samen kan, en zorgen voor verbinding in plaats van fragmentatie, ook daar waar de diversiteit van dienstonderdelen om maatwerk vraagt.

Aan de hand van deze houtskoolschets wordt de komende jaren gewerkt aan de centrale invulling van de werkzaamheden die B/CKC uitvoert voor de Belastingdienst op het gebied van kennis, communicatie en HR. In lijn met de in het MLTP beschreven ruimte en verantwoordelijkheid organiseert de Belastingdienst kennis, communicatie en HR dicht tegen het werk aan. In het licht van zowel effectiviteit en *efficiency* als samenhang en consistentie wordt de verbinding en ondersteuning van de kennis-, communicatie-, en HR-functie centraal georganiseerd. Dit vraagt een doorontwikkeling van B/CKC, met zicht op toegevoegde waarde en structurering van de centraal georganiseerde werkzaamheden, zowel voor de Belastingdienst in zijn geheel als voor de dienstonderdelen.

De houtskoolschets geeft richting aan en kader voor de doorontwikkeling van B/CKC, welke verder vorm zal krijgen langs de lijnen, voorgestelde besluiten en denkrichtingen zoals beschreven in de onderliggende notities. De notitie bouwt verder op de inzichten die zijn voortgekomen uit het scenariotraject voor B/CKC, de rapportage *'Verkenning van de kennisfunctie binnen de Belastingdienst – kennis als kerncompetentie voor de Belastingdienst'*, de *Houtskoolschets kennissupport* en de aanvullende opdrachten die in de periode januari – maart 2014 zijn uitgevoerd op het gebied van kennis-, communicatie- en HR-support. De concretisering en effectuering in de geschetste richting is onderdeel van de vervolgopdracht doorontwikkeling B/CKC. Binnen het uitgewerkte kader worden in lijn daarmee voor specifieke dossiers benodigde besluitvorming in het MT/BD geëxpliciteerd.

De onderliggende rapportages zijn opgesteld op basis van onderzoek en gesprekken met diverse stakeholders uit dienst. De individuele bijdragen en zienswijzen van stakeholders komen niet expliciet terug in deze houtskoolschets. De onderliggende notities zijn opgenomen in separate bijlagen van dit document.

Naast B/CKC worden ook centrale werkzaamheden uitgevoerd vanuit andere dienstonderdelen, zoals B/CA, de IV-keten en B/CFD. Deze werkzaamheden maken geen onderdeel uit van deze houtskoolschets. Raakvlakken worden, waar dit nuttig en nodig, is geëxpliciteerd.

1. Beweegreden: samen doen wat samen kan

De Belastingdienst verbetert zich voortdurend om modern en efficiënt – gedreven vanuit het resultaat voor burgers en bedrijven – te kunnen zijn en werken. Daarmee werkt de dienst aan zijn toekomstbestendigheid en richt de dienst zich op het, nu en in de toekomst, adequaat vervullen van zijn maatschappelijke opdracht. De Belastingdienst zet daarbij in op het maximaal vergroten van de mate waarin burgers en bedrijven vrijwillig hun verplichtingen nakomen (*compliance*), zodat een klimaat ontstaat waarin regelnaleving vanzelfsprekend is en waarin burgers en bedrijven de interne intrinsieke motivatie voelen om verplichtingen na te komen. Om burgers en bedrijven de behandeling te kunnen geven die ze verdienen, krijgen medewerkers verantwoordelijkheid, kansen en professionele ruimte.

De afgelopen jaren heeft de Belastingdienst flinke stappen gezet en stond de dienst onder meer in het teken van een aantal grote reorganisaties om duurzaam het primaire proces te verbeteren. Daarmee staat in beginsel de basisstructuur waarbinnen uitvoering kan worden gegeven aan het MLTP 2014 – 2017. Tegelijkertijd is er nog veel fragmentatie en diversiteit, in aantal, organisatie en sturing van activiteiten.

De realisatie van de permanente opdracht van de Belastingdienst en de daarmee verbonden belangen van burgers en bedrijven, overheid en maatschappij (*high stakes*) vraagt onder meer adequate communicatie, de absorptie, diffusie, generatie en exploitatie van kennis en de juiste medewerkers op het juiste moment op de juiste plaats. Daarenboven hebben interne en externe ontwikkelingen, zoals de instroom van nieuwe medewerkers, de toenemende aandacht voor fraude, de afnemende tolerantie in de samenleving voor fouten van overheidsorganisaties en de samensmelting van de off- en online woon-, werk en leefomgeving, een nadrukkelijke verbinding met zowel kennis, communicatie als HR.

Het kader van eenheid in beleid en uitvoering, de behoefte aan kwalitatief hoogwaardige producten en diensten, het bewaken van de *corporate image* & *identity*, de positie van de Belastingdienst als (mede-)uitvoerder van rijksbrede taken (denk aan categoriemanagement Leren & Ontwikkelen), het hebben van één interne arbeidsmarkt en het voorkomen van (verdere) versnippering van initiatieven op het gebied van kennis, communicatie en HR, zijn stuk voor stuk redenen voor de Belastingdienst om een deel van de expertise en ondersteuning ten behoeve van de kennis-, communicatie en HR-functie te bundelen in een centraal dienstonderdeel. Het beleggen van activiteiten in een centraal dienstonderdeel draagt er aan bij, dat er concernbreed weloverwogen keuzes worden gemaakt zodat de beschikbare middelen passend worden besteed. Op dit moment worden vraagstukken veelal opgepakt binnen het eigen dienstonderdeel, terwijl het vraagstuk bij meerdere onderdelen speelt. Gekozen oplossingen zijn vaak toereikend, maar kunnen door samenwerking en bundeling van krachten en kennis vaak effectiever en efficiënter worden toegepast.

Door vanuit een MTBD breed gedragen kader B/CKC als centraal dienstonderdeel voor kennis, communicatie en HRte richten en in te richten worden schaalvoordelen, professionaliteit en kwaliteit stevig verankerd. Het adagium daarbij is samen doen wat samen kan, vanuit eigen verantwoordelijkheid en rol. Dit vraagt heldere keuzes met betrekking tot rollen, verantwoordelijkheid en toegevoegde waarde. Zonder deze keuzes leidt het samen doen tot polderen, bureaucratie en gedoogde ongehoorzaamheid. Samen doen staat juist voor samen richting geven en samen richting houden. Dat vraagt afspreken en aanspreken, en uit zich onder meer in *checks-and-balances, countervailling power* en professioneel opdrachtgever- en opdrachtnemerschap. Dit betekent dat business en B/CKC in verbinding zijn door middel van een zakelijke, constructieve dialoog over inhoud, toegevoegde waarde en uniforme kaders.

B/CKC stelt de dienstonderdelen in staat zich te focussen op hun primaire taken. Vanuit het centrale dienstonderdeel wordt op secundaire taken ontzorgd en daardoor ondersteund bij het realiseren van de organisatiedoelstellingen. Binnen B/CKC wordt expertise waar nodig gebundeld en bij elkaar gehouden (kritische massa), zodat deze kan blijven renderen voor de dienst. Wanneer dienstonderdelen werkzaamheden nodig hebben die niet binnen B/CKC worden georganiseerd of ingekocht, organiseren ze het zelf.

2. Richting geven aan B/CKC als partner bij doelrealisatie

Het realiseren van B/CKC als effectief en efficiënt centraal dienstonderdeel op het gebied van kennis, communicatie en HR vraagt om een duidelijke richting, expliciete keuzes en rekenschap van een aantal uitgangspunten, voorwaarden en aandachtspunten. Concreet betekent het dat B/CKC de in deze notitie beschreven rol pakt en dat de Belastingdienst zorgt voor de voorwaarden waaronder B/CKC zijn rol ook kan pakken. In dit hoofdstuk wordt de richting B/CKC uitgewerkt.

2.1 B/CKC als partner bij doelrealisatie

Kennis, communicatie en HR zijn cruciale pijlers voor de ontwikkeling van vak, mens en organisatie. Ze dragen bij aan de realisatie van de missie en de doelen, de vervulling van de primaire functie en een goede uitvoering van het primaire proces en de daarvoor benodigde management- en ondersteunende processen van de gehele Belastingdienstorganisatie. Kennis, communicatie en HR krijgen daarmee de aandacht en positie die ze verdienen in een organisatie als de Belastingdienst en zijn tegelijkertijd niet het antwoord op alles.

Binnen de Belastingdienst worden kennis, communicatie en HR waar mogelijk dicht tegen het werk aan georganiseerd, in de ketens en bij dienstonderdelen. In lijn hiermee, passend bij het *governancemodel* van de Belastingdienst en de eigen verantwoordelijkheden van dienstonderdelen, worden kennis, communicatie en HR ingevuld binnen de gestelde kaders vanuit het MLTP 2014 – 2017. Vanuit een uniforme basis is daarbij ruimte voor diversiteit op basis van werk en aard van de dienstonderdelen. Tegelijkertijd is het vanuit het integrale, overkoepelende belang van de dienst noodzakelijk om consistentie en samenhang te borgen. De Belastingdienst en zijn onderdelen vormen één organisatie met een gedeelde maatschappelijke opdracht en handelen daar ook naar. Waar vanuit een dienstonderdeel optimalisatie kan worden voorzien, brengt gebrek aan verbinding het risico van sub-optimalisatie voor het geheel met zich mee. Daarnaast ligt het gevaar van het versnipperen en verwateren van expertise op de loer.

B/CKC streeft er naar om de Belastingdienst en zijn dienstonderdelen in staat te stellen adequaat antwoord te bieden op de uitdagingen en ontwikkelingen waar zij voor staan en hun doelstellingen te realiseren. De kernfunctie is het stimuleren en ondersteunen van de ontwikkeling van de Belastingdienst en zijn medewerkers. In lijn met het MLTP gaat het om de ontwikkeling van vak, mens en organisatie.

B/CKC streeft er naar om een gewaardeerde professionele partner te zijn op het gebied van kennis, communicatie en HR. Als *business partner* werkt B/CKC proactief en in verbinding met zowel de business als andere ondersteunende organisatieonderdelen. De organisatie functioneert als *enabler* en maakt het realiseren van de doelen en concrete resultaten van de Belastingdienst mede mogelijk. In de volledige keten – van beleidsvorming tot beleidsuitvoering – werkt B/CKC vanuit expertise in co-creatie mee aan het realiseren van beoogde effecten. B/CKC heeft daarmee een wederkerige relatie met de gehele dienst en de dienstonderdelen. Co-creatie staat immers voor samenwerking waarbij partners vanuit hun eigen rol en verantwoordelijkheid samen werken aan doelrealisatie. Dat betekent een wederzijdse verplichting om verantwoordelijkheden te erkennen en elkaar in staat te stellen waarde toe te voegen.

De optelsom van partnerschap, expertise en verbinding leidt tot kwaliteit. Het partnerschap zorgt er voor dat B/CKC weet en begrijpt welke kwaliteit wordt verwacht. De expertise en verbondenheid maakt dat ze dit kunnen leveren, passend bij het vraagstuk, vaktechnisch kloppend en in lijn met de uniforme kaders. Dat maakt het dienstonderdeel tot een proactieve, professionele, kwalitatieve partner, die werkt vanuit de opgaven van de business, aandacht heeft voor diversiteit en werkt aan concrete resultaten binnen vooraf gestelde, uniforme, kaders. In alle activiteiten streeft ze ernaar om meetbare, toegevoegde waarde te demonstreren.

Passend bij de door de Belastingdienst beoogde ontwikkeling van vak, mens en organisatie richt B/CKC zich binnen kennis, communicatie en HR op het proactief, kwalitatief en professioneel uitvoeren van dienstonderdeel-overstijgende activiteiten binnen de domeinen Onderzoek &

Innovatie, Leren & Ontwikkelen, Communicatie, Organisatieontwikkeling, Mobiliteit en Werkgever- & werknemerschap.[1]

2.2 De spil waar B/CKC om draait

B/CKC werkt aan de ontwikkeling van vak, mens en organisatie. Deze ontwikkeling stelt de Belastingdienst in staat om de permanente opdracht in dienst van de maatschappij duurzaam te realiseren, nu en in de toekomst. Centraal staat het werk van de dienst, de werkzaamheden die worden uitgevoerd om de doelstellingen te realiseren. De complexiteit van opgaven waar de dienst mee wordt geconfronteerd vraagt om adequate expertise. Tegelijkertijd lopen er op dit moment veel onsamenhangende en inconsistente initiatieven. Als centraal dienstonderdeel heeft B/CKC de opdracht om versnippering en het verwateren van expertise te voorkomen. Zij ondersteunt en versterkt de organisatie, door 'diepe kennis' in te brengen en 'verbinding' te realiseren en te bewaken. De primaire focus ligt daarbij op de proactieve, kwalitatieve, professionele invulling en uitvoering van dienstonderdeel overstijgende thema's.

- ***Diepe kennis*:** staat voor de expertise die binnen de organisatie aanwezig is. Kennis inspireert en zit in de haarvaten van B/CKC. De organisatie werkt dan ook op een systematische en methodische manier op basis van *state of the art kennis.* Deze invulling past bij het, ook in het MLTP geaccentueerde, vakmanschap. B/CKC onderscheidt zich door de specialistische kennis over productieve methoden, gekoppeld aan goed zicht op de opgaven en uitdagingen van de Belastingdienst en zijn onderdelen op de domeinen Onderzoek & Innovatie, Leren & Ontwikkelen, Communicatie, Organisatieontwikkeling, Mobiliteit en Werkgever- & werknemerschap.

- ***Verbinding:*** staat voor de samenhang die de organisatie aanbrengt in de werkzaamheden en initiatieven op het gebied van kennis, communicatie en HR. De verantwoordelijkheid voor het werk en de bijdrage van kennis, communicatie en HR daaraan, ligt bij [redacted] of de dienstonderdelen. B/CKC zorgt voor een integrale benadering, waardoor consistentie en samenhang aangebracht en geborgd kunnen worden. Het gaat daarbij zowel om verbinding van doelen en opgaven als om de verbinding van initiatieven in de organisatie op het gebied van kennis, communicatie als HR.

Het inbrengen van expertise en verbinding gedurende de gehele beleidscyclus stelt B/CKC in staat om samen met de dienst en zijn onderdelen de leercirkel op de centrale domeinen HR, kennis en communicatie te sluiten. Door betrokkenheid bij het stellen van doelen en de beleidsformulering, bij het organiseren, implementeren en uitvoeren, bij de evaluatie en bijsturing sluit de cirkel en wordt de Belastingdienst in staat gesteld continu te verbeteren.

2.3 Voorwaarden om professioneel partnerschap te realiseren

Het daadwerkelijk realiseren van een volwaardig partnerschap tussen B/CKC en de dienst heeft consequenties voor de wijze waarop binnen de Belastingdienst wordt gewerkt, gestuurd en georganiseerd. Specifieke voorwaarden voor het komen tot een proactief, kwalitatief, professioneel centraal organisatieonderdeel op het gebied van kennis, communicatie en HR zijn:

- heldere keuzes over de richting en inrichting van de Belastingdienst - Het productief maken van een centraal organisatieonderdeel op het gebied van kennis, communicatie en HR vraagt om richtinggevende keuzes op het gebied van:
    - het richten en inrichten van de communicatiefunctie (externe-, intern- en corporate communicatie) binnen de Belastingdienst, waarbij:
        - de verantwoordelijkheden, bevoegdheden en taken binnen de communicatiefunctie worden geëxpliciteerd;
        - dienstonderdelen verantwoordelijk worden voor zowel effect als contentcreatie;
        - kanalenregie een volwaardige positie (incl. bevoegdheden) binnen de communicatieketen krijgt.

[1] Samenhang en complementariteit met taken die door andere dienstonderdelen worden uitgevoerd (bijvoorbeeld door eHI Belastingen, dienstverlening, B/CIE, B/CAO et cetera) worden bij de concretisering en inrichting van B/CKC zorgvuldig geborgd.

    - een integrale visie op het gebied van internationale betrekkingen als kader voor handelen voor alle dienstonderdelen;
    - de samenwerking en taakverdeling tussen [redacted] centraal belegde programma's en B/CKC op het gebied van kennis, communicatie en HR;
- heldere positionering van eencentraal organisatieonderdeel op het gebied van kennis, communicatie en HR en de invulling van *countervailing power* (kracht en tegenkracht die samen evenwicht bewaren) - B/CKC zal in het kader van verbinding en vanuit het algemeen belang van de Belastingdienst tegendruk kunnen bieden tegen besluiten en wensen van individuele dienstonderdelen. Op deze manier blijft het handelen van de dienst in balans. Vanzelfsprekend dient deze *countervailing power* geborgd te worden in de structuur, maar kan deze enkel worden waargemaakt door de wijze van handelen en acteren vanuit B/CKC;
- het gebruiken van *spelregels* en *stelregels* - Bovenstaande vraagt niet alleen aandacht voor de wijze waarop uitvoering wordt gegeven aan beoogd of gewenst gedrag en samenspel tussen business en B/CKC (de spelregels), maar ook voor de wijze waarop de Belastingdienst, en het dagelijks bestuur in het bijzonder, een centraal organisatieonderdeel op het gebied van kennis, communicatie en HR steunt en positioneert, wanneer in concrete situaties de centrale en decentrale belangen op spanning staan (stelregels);
- het hebben van *sponsorship* van een centraal organisatieonderdeel op het gebied van kennis, communicatie en HR en domeinen daarbinnen – Het in de dagelijkse praktijk realiseren van de doorontwikkeling van B/CKC als geheel en de inhoudelijke domeinen daarbinnen, vraagt een gedragen beeld van de richting en sponsors in het MTBD om de organisatie ook in staat te stellen deze toegevoegde waarde te realiseren;
- werken vanuit de business - Bij de uitvoering van werkzaamheden werkt de B/CKC altijd vanuit de opgaven van de dienst en zijn dienstonderdelen. Dit betekent niet dat B/CKC een 'u vraagt, wij draaien'-houding aanneemt, maar werkt met professioneel portfoliomanagement. De organisatie neemt in beginsel geen zaken over die qua aard en karakter in de business moeten worden georganiseerd. Ze is ook geen loket waar kan worden gewinkeld wanneer het past. De organisatie vraagt een proactieve, initiatiefrijke houding van B/CKC. Ze profileert zich sterk en is daardoor zichtbaar voor de gehele organisatie. Door haar expertise, haar flexibiliteit en door uitstekend in verbinding te staan met alle dienstonderdelen en de buitenwereld, bewijst B/CKC haar meerwaarde. Daardoor is het centraal organisatieonderdeel op het gebied van kennis, communicatie en HR de vanzelfsprekende partner voor de business, die steeds weer goed, snel en efficiënt presteert op haar domeinen;
- accepteren van professioneel portfoliomanagement - B/CKC zal werken met geprofessionaliseerd portfoliomanagement op basis waarvan financiering en capaciteit worden gestuurd en beheerd. De rol van opdrachtnemer of 'u vraagt wij draaien' vervalt, dienstverlening zit straks net zozeer in *de goede dingen doen*, als in *de dingen goed doen*. Dit vraagt proactieve afstemming en continue dialoog met de business;
- helder(e) zeggenschap/verantwoordelijkheidsverdeling ten aanzien van werkzaamheden - Taken, verantwoordelijkheden en bevoegdheden in relatie tot de domeinen moeten helder gedefinieerd worden (rolduidelijkheid), binnen de Belastingdienst dient daar overeenstemming over te zijn (rolbewustzijn) en men dient daar naar te handelen en elkaar op aan te spreken (rolvastheid);
- behouden en versterken van herkenbaarheid - Het Employability Center en de BelastingdienstAcademie hebben de afgelopen jaren een herkenbaar profiel opgebouwd binnen de Belastingdienst. Bij de doorontwikkeling van B/CKC wordt deze herkenbaarheid behouden en wordt gewerkt aan het versterken van herkenbaarheid van andere domeinen.
- signaleren is niet gelijk aan corrigeren - B/CKC levert expertise ten behoeve van de dienstonderdelen, brengt verbinding en signaleert fragmentatie. Correctie is een lijnverantwoordelijkheid en geen taak van B/CKC als centraal organisatieonderdeel.. Alleen daar waar expliciete opdrachten vanuit het MTBD worden geformuleerd, corrigeert de organisatie ook;
- organiseren van adequate IM-functie - Veel van de werkzaamheden van B/CKChebben een nauwe relatie met IM (denk bijvoorbeeld aan de digitale leeromgeving). Het realiseren van een organisatie zonder eigen IM-functie vereist dat vanuit B/CKC op basis van een agenda in samenhang op basis van een meerjarenplan de vraag wordt gesteld.

2.4 Aandachtspunten voor succesvolle implementatie

Naast voorwaarden geldt voor het realiseren van een proactieve, kwalitatieve en professionele centraal organisatieonderdeel op het gebied van kennis, communicatie en HR dat er aandacht nodig is voor het:

- houden van commitment - Commitment op het niveau van het MTBD en vervolgens de MT's van de verschillende dienstonderdelen op de werking en toegevoegde waarde van een centraal organisatieonderdeel op het gebied van kennis, communicatie en HR is essentieel voor het realiseren van een volwaardige business partner. Het betreft zowel commitment op strategische richting en de verdeling van taken en verantwoordelijkheden als op de afspraken om deze lijn vast te houden bij conflicterende belangen. Vanuit de CHRO zal sturing moeten plaatsvinden op deze visie, op uniformiteit en op het vanzelfsprekend laten zijn dat ook daadwerkelijk gevolg wordt gegeven aan het commitment dat is gegeven op de hoofdlijnen;
- voorkomen van concurrentie - Bij de uitvoering van werkzaamheden voorkomt B/CKC een concurrentie- of competentiestrijd met dienstonderdelen, door geen lijnverantwoordelijkheden over te nemen, helder te zijn over ruimte en resultaat en niet te redeneren vanuit positie (ik heb) maar vanuit bijdrage (ik voeg toe);
- tijd nemen en krijgen - Het inregelen van een goed functionerend centraal organisatieonderdeel op het gebied van kennis, communicatie en HR vraagt tijd. De gewenste kwaliteit, welke op lange termijn wordt gevraagd en geleverd, zal in het begin niet direct kunnen worden geleverd. B/CKC moet de tijd nemen en krijgen om de werkprocessen goed in te regelen;
- omgaan met interne belangentegenstellingen - Bij de inrichting van B/CKC wordt een continue dialoog georganiseerd over eigen belang van een organisatieonderdeel versus het brede organisatiebelang en de wijze waarop daar mee om wordt gegaan (handelingskader) – zowel op abstract niveau als bij concrete cases. Zodra deze tegenstellingen raken aan een centrale opdracht moet duidelijk zijn hoe dergelijke spanningen worden opgelost en welke rol/mandaat een centraal organisatieonderdeel op het gebied van kennis, communicatie en HR daarbij heeft.

3. Inrichten B/CKC als centraal organisatieonderdeel op het gebied van kennis, communicatie en HR

De inhoudelijke inrichting van de organisatie moet ertoe bijdragen dat optimaal invulling wordt gegeven aan de doorontwikkeling van B/CKC en de opdracht en verantwoordelijkheid op het gebied van kennis, communicatie en HR binnen de Belastingdienst. In dit hoofdstuk worden de uitgangspunten voor activiteiten en de domeinen waar de B/CKC zich op richt uitgewerkt.[2]. Aan de hand hiervan wordt de doorontwikkeling van B/CKC verder geconcretiseerd en kan in gesprek worden gegaan met de verschillende dienstonderdelen over de definitieve invulling van een centraal organisatieonderdeel op het gebied van kennis, communicatie en HR binnen de Belastingdienst.

3.1 Uitgangspunten voor inrichting centrale activiteiten B/CKC

Op basis van inzichten die zijn voortgekomen uit het scenariotraject voor B/CKC, de rapportage *'Verkenning van de kennisfunctie binnen de Belastingdienst – kennis als kerncompetentie voor de Belastingdienst'*, de *Houtskoolschets kennissupport* en de aanvullende opdrachten die in de periode januari – maart 2014 zijn uitgevoerd op het gebied van Kennis-, Communicatie- en HR-support wordt voor de richting en inrichting van B/CKC uitgegaan van de volgende kaders en uitgangspunten:

- B/CKC richt een organisatie in die de in dit hoofdstuk beschreven domeinen op een proactieve, professionele, kwalitatieve wijze uit kan voeren;
- Centrale activiteiten die op dit moment zijn ondergebracht in de IV-keten (B/CIE en B/CAO) en bij de onderdelen B/CFD, B/CA en DG-Bel zijn geen onderdeel van de activiteiten van B/CKC. Noodzakelijke afstemming vindt plaats;
- Versnippering van specifieke kennis (<10fte) wordt voorkomen en op een robuuste wijze geborgd binnen B/CKC als het centrale organisatieonderdeel op het gebied van kennis, communicatie en HR;
- De onderzoeksfunctie van de Belastingdienst wordt zowel in de dienstonderdelen als op centraal niveau georganiseerd en uitgevoerd. Daarbij wordt onderscheid gemaakt tussen 1ste orde en 2de orde onderzoek. 1ste orde onderzoek staat voor onderzoek gericht op de sturing en verbetering van eigen (primaire) processen van dienstonderdelen (denk aan: analyse doorloopsnelheid, bottlenecks gevolgen ITI op versnelling invorderingsproces, evaluatie van kwaliteit van risico-selectieregels). 2de orde onderzoek staat voor onderzoek met een bredere vraagstelling, met een meer complex of strategisch karakter (denk aan: effecten van invoering VIA op compliance, effecten doelgroepacties, onderzoek naar determinanten van compliant gedrag van ondernemers). De centrale onderzoeksafdeling richt zich op 2de orde onderzoek, waarbij geldt dat:
    - De centrale onderzoeksafdeling onderdeel is van B/CKC
    - Vanuit de centrale onderzoeksafdeling de huidige dialoog over lopende en nieuwe vraagstellingen met de dienstonderdelen en MT/BD periodiek (meerdere keren per jaar) wordt gecontinueerd
    - Per onderzoeksprogramma een adviesraad bestaande uit (top)experts en management uit de dienst wordt ingesteld, om te ondersteunen en adviseren over de voorbereiding en alignment van de onderzoeksprogramma's
    - De onderzoeksafdeling een eigenstandige verantwoordelijkheid heeft voor het initiëren van (2de orde) onderzoek in het belang van de dienst.
    - De dienstonderdelen zijn zelf verantwoordelijk voor 1ste orde onderzoek, waarbij waar opportuun gebruik wordt gemaakt van de bij B/CKC aanwezige expertise.
    - De centrale onderzoeksafdeling vanuit methodekennis bijdraagt aan de verbinding van zowel 1ste als 2de orde onderzoek over dienstonderdelen heen
- Naar aanleiding van de uitkomst van de voorgestelde besluiten in de rapportage over de communicatiesupport en de bevindingen van de *taskforce communicatie* worden eventuele wijzigingen in het beschreven activiteitenpakket van B/CKC doorgevoerd. Vooralsnog blijft B/CKC kanaaleigenaar internet en de belangrijkste uitvoeringspartner op het gebied van communicatie van de Belastingdienst en zijn dienstonderdelen;

[2] De opsomming van kenmerkende activiteiten is niet limitatief

1873579 00349

- De sturing van en verantwoordelijkheden voor contentcreatie en contentmanagement (het verzamelen, valideren, metadateren, publiceren, verspreiden en beheren van de content afkomstig van de dienstonderdelen en DG-bel) worden geëxpliciteerd. De dienstonderdelen zijn verantwoordelijk voor de contentcreatie bij externe communicatie. Voor interne en corporate communicatie veranderen deze verantwoordelijkheden niet ten opzichte van de huidige situatie;
- Het *Employability Center* wordt volledig geïntegreerd in B/CKC als centraal organisatieonderdeel op het gebied van kennis, communicatie en HR. Werving en selectie blijft een centraal georganiseerde activiteit welke vanuit B/CKC wordt georganiseerd;
- Leren en ontwikkelen blijft een centraal georganiseerde activiteit die van aanbod- naar vraaggericht verschuift;
- Op het gebied van Evenementen bestaat het onderscheid tussen het begeleiden en organiseren van evenementen met een leer-, veranderkundige of bestuurlijke doelstelling (denk aan: top 1500, M-dagen, etc.) en het begeleiden en faciliteren van bijeenkomsten (denk aan: recepties, openingen van gebouwen, de nationale vlaggendag, etc.). B/CKC blijft verantwoordelijk voor de organisatie van deze inhoudelijke evenementen. Faciliteren wordt verzorgd vanuit B/CFD. Onderling wordt gewerkt aan het versterken van de afstemming en synergie bij de uitvoering van werk;
- Op het gebied van Internationaal verzorgt B/CKC het verbinden en veredelen van kennis uit de verschillende internationale contacten. De beleidsinhoudelijke, tactische en operationele ondersteuning van internationale activiteiten van het primair proces worden respectievelijk bij DG-Bel en de betrokken dienstonderdelen onderbracht. Concreet betekent dit dat:
    - De verantwoordelijkheid en uitvoering van strategie- en beleidsvorming en coördinatie hiervan wordt belegd bij DG-Bel.
    - De voorgenomen samenvoeging tussen CKC team internationaal en Belastingen ABC/Internationaal voor de activiteiten die in het verlengde van het primaire proces liggen past binnen de richting van een centraal organisatieonderdeel op het gebied van kennis, communicatie en HR.
    - B/CKC vanuit kennissupport de internationale activiteiten ondersteunt om kennisdeling en samenwerking te optimaliseren.
    - B/CKC de HR ondersteuning voor langdurig uitgezonden personeel uit blijft voeren, zodat een eenduidige behandeling en rechtspositie gegarandeerd blijft.
    - Facilitaire werkzaamheden (reisbureau) passen niet direct binnen de werkzaamheden van een centraal organisatieonderdeel op het gebied van kennis, communicatie en HR. Wanneer deze activiteiten niet vanwege pragmatische redenen binnen B/CKC moeten worden georganiseerd kunnen deze – tot het moment dat deze in het kader van de rijksbrede ontwikkelingen worden ondergebracht bij het Ministerie van Buitenlandse Zaken – bij B/CFD worden belegd.
- De verbinding van het *Future Center* met de strategische doelen van de Belastingdienst wordt versterkt. Inhoudelijke initiatieven worden vanuit dit kader getoetst op impact en alignment Het *Future Center* valt binnen de verantwoordelijkheid van één van de plaatsvervangend directeuren van B/CKC. De Raad van Advies van het *Future Center* wordt versterkt met interne stakeholders – mede met het oog op het versterken van de verbinding tussen bottum-up innovatie en impact van initiatieven op imago en identiteit van de dienst;

3.2 Uitwerking domeinen B/CKC

Het centrale organisatieonderdeel op het gebied van kennis, communicatie en HR richt zich op het leveren en organiseren van diepe kennis en verbinding vanuit de domeinen Onderzoek & Innovatie, Leren & Ontwikkelen, Communicatie, Organisatieontwikkeling, Mobiliteit en Werkgever- & werknemerschap. Onderstaand wordt de *core business* van B/CKC toegelicht aan de hand van de invulling van de zes gekozen domeinen en bijbehorende kenmerkende activiteiten.

3.2.1 Domein - Onderzoek & Innovatie

Vanuit Onderzoek & Innovatie werkt B/CKC aan de absorptie en generatie van kennis ten behoeve van de Belastingdienst. Vanuit dit domein wordt kennis gecreëerd en gevalideerd door zowel het halen van nieuwe kennis vanuit de omgeving, het coördineren van onderzoek, het genereren van kennis door middel van (wetenschappelijk) onderzoek, het verbeteren en vernieuwen van werk en

werkwijzen op basis van onderzoek ten behoeve van de gehele dienst of het leveren van kennis over methoden en technieken aan dienstonderdelen. Vanzelfsprekend kan dit kennis zijn over thema's uit het primair proces, maar ook voor bijvoorbeeld communicatie of HR.

Kenmerkende activiteiten bij de invulling van dit domein zijn onder andere:

- het uitvoeren van specifieke studies naar strategische thema's van de Belastingdienst;
- het coördineren en waar nodig uitvoeren van meerjarige onderzoekprogramma's;
- het coördineren van de kennisagenda;
- het creëren en faciliteren van effectmetingen op lange termijn van dienstonderdelen (2de orde onderzoek);
- het coördineren en uitvoeren van verdiepend onderzoek naar gedrag van burger en bedrijf (*compliance*-gericht onderzoek);
- het coördineren en uitvoeren van (intern) onderzoek naar de rol en bijdrage van medewerkers (*performance*-gericht onderzoek);
- het innoveren van communicatie en interactie en het instrumentarium dat daarbij hoort op basis van *usability*/gebruiksvriendelijkheid;
- het stimuleren van *bottom-up* innovatie.

De uitvoering van de opdracht rondom 'innovatie' vindt – passend bij de verantwoordelijkheid van dienstonderdelen – vanzelfsprekend dicht in op primaire proces plaats, daar waar de meeste toegepaste kennis aanwezig is en direct zicht is op behoefte, toepasbaarheid en toegevoegde waarde. Tegelijkertijd vraagt innovatie om een integrale benadering vanuit de Belastingdienst als één organisatie. Het vraagt om het maken van ongebruikelijke verbindingen, zicht op ontwikkelingen die niet direct passen bij de opdracht van het primaire proces en om ruimte om te zoeken, te experimenteren, fouten te maken en ideeën samen te brengen (ideeënmanagement), zonder direct te worden geconfronteerd met de grote complexe processen binnen de Belastingdienst en zonder risico's voor het primaire proces. Tevens vraagt innovatie om kennis over innovatie: hoe doe je het, wat is ervoor nodig, hoe maak je het productief, etc.

B/CKC borgt en levert de specialistische kennis over innovatie die nodig is om (ook) het primaire proces in staat te stellen om innovaties zelf werkbaar te maken. Daarnaast werkt B/CKC ook zelfstandig aan innovaties voor de Belastingdienst, door de aanwezige specialistische kennis te combineren met de benodigde ruimte. . De relatie tussen B/CKCen concreet uitgevoerd(e) werk/activiteit (binnen B/CKC) wordt na de innovatieperiode beëindigd omdat deze of in de lijnorganisatie is ondergebracht of niet geslaagd is.

3.2.2 Domein - Leren & Ontwikkelen

Leren en ontwikkelen staat binnen de Belastingdienst voor het bevorderen van een goede connectie tussen werk en medewerkers (person-job-fit) voor alle 30.000 medewerkers. Het draait om de juiste medewerker, op de juiste plaats, op het juiste moment. Dit is nauw verbonden met de invulling van de leerfunctie van de Belastingdienst. Daarbij wordt meer geboden dan fiscale kennis alleen; er is een breed portfolio aan mogelijkheden voor opleiding en ontwikkeling. Leren & Ontwikkelen wordt gezien als een constante factor, welke zoveel mogelijk is geïntegreerd in het dagelijkse werk. Werkend leren en lerend werken. Aan de hand van de 70:20:10 wordt het leeraanbod samengesteld. Dit wordt ingevuld door innovatieve en succesvolle onderwijsvormen en leermodellen te koppelen aan de vragen die vanuit de organisatie worden gesteld. De business is in the lead. Het accent ligt op leren en ontwikkelen in het werk, aangevuld met inzet van het kennisnetwerk, klassikaal leren en het gebruik van innovatieve digitale middelen en (sociale) media. Het gaat om de duurzame inzetbaarheid van managers en medewerkers. Voor managers is daarbij aandacht voor zowel management als leiderschap, zowel op individueel als collectief niveau.

Kenmerkende activiteiten bij de invulling van dit domein zijn onder andere:

- het verzorgen van een passend, effectief en zoveel mogelijk markterkend professionaliseringsaanbod, variërend van online modules, klassikale trainingen, online en fysieke intervisie groepen tot duale trajecten en traineeships.;
- het stimuleren en ondersteunen van experts binnen de Belastingdienst die in co-design/co-creatie zorgen voor professionalisering en kenniscreatie;
- het volgen, waarderen en erkennen van professionalisering door middel van een adequaat Leer Management Systeem;
- het verzorgen van de leercontent op de digitale leerinfrastructuur;
- het verzorgen van eenduidige toegang tot en contact met universiteiten, HBO-instellingen, ROC's en andere kennisinstellingen;

1873579 00349

- het coördineren van stages behorende bij het certificeren of opleiden van (toekomstige) managers en medewerkers van de Belastingdienst.
- het invullen van de psychologische adviesfunctie (ontwikkelen en uitvoeren van assessments, psychologisch onderzoek en –instrumenten en hieraan gerelateerde adviezen);
- het landelijk coördineren en professionaliseren van specialistische functie (o.a. coachpool);
- het continu verbeteren van activiteiten op dit domein, op grond van relevante data-analyse (effectmeting).

De invulling van de activiteiten in het domein Leren & Ontwikkelen past binnen de huidige koers van de BelastingdienstAcademie. Daarnaast bestaat hier, mede in het licht van de opgaven met betrekking tot de in-, door- en uitstroom van medewerkers, nauwe samenhang met de doorontwikkeling van het *Employability Center*. Voor het versterken van leiderschap binnen de Belastingdienst is er nauwe verbondenheid met de werkzaamheden uit het domein Organisatieontwikkeling. Dat blijkt ook uit het feit dat huidige programmatisch aangepakte (en bij HR passende) thema's als LEAN, HNW en Leiderschap veel gebruik maken van producten en diensten die vanuit de domeinen Leren & Ontwikkelen en Organisatieontwikkeling worden geleverd.

3.2.3 Domein - Communicatie

Vanuit het domein Communicatie levert B/CKC een bijdrage aan de communicatiefunctie van de Belastingdienst. Het domein is nauw verbonden met zowel het ontsluiten en publiceren van kennis en informatie als het productief maken van kennis en richt zich zowel op externe, interne en corporate communicatie.

Vanuit het uitgangspunt dat de Belastingdienst en zijn onderdelen één organisatie vormt met een gedeelde maatschappelijke opdracht is het fundament voor communicatie - en daarmee voor de organisatie en sturing van communicatie - het beoogde effect dat de dienst nastreeft. Als adagium daarbij geldt 'alles wat je doet is communicatie'. Dat geldt zowel voor burgers en bedrijven, voor medewerkers, als voor maatschappij en politiek. Binnen dat kader wordt vanuit het domein Communicatie gewerkt aan de creatie en executie van externe, interne en corporate communicatie die invloed heeft op de dienst als geheel. Centraal staat het borgen en verzorgen van de *corporate image* & *identity*. Het gaat daarbij om eenheid, samenhang en consistentie in communicatie-uitingen, zowel binnen als buiten de dienst. In het licht van de grote belangen die verbonden zijn met het werk van de dienst, zowel voor de politiek, maatschappij en voor de individuele burgers en bedrijven wordt versnippering en inconsistentie voorkomen.

Vanuit de communicatiestrategie worden communicatie-instrumenten (of kaders hiervoor) gericht op de gewenste effecten. Er wordt daarbij vanuit dezelfde competenties gewerkt aan het realiseren van effecten op het gedrag van enerzijds burgers en bedrijven (*compliance*) en anderzijds medewerkers en managers (*performance*). Om dit te bewerkstelligen is specialistische kennis over communicatie en gedragsbeïnvloeding een must en het borgen van adequate methodekennis over communicatie noodzakelijk voor de Belastingdienst. Concurrerende perspectieven, zoals bijvoorbeeld de plicht tot voorlichten en bedrijfseconomische impact op dienstverleningskanalen, vragen om het adequaat borgen van *countervailing power*. De Belastingdienst waakt daarmee voor een introverte benadering van externe communicatie, waarin bedrijfseconomische belangen boven impact en effect van communicatie-uitingen worden geprioriteerd.

Kenmerkende activiteiten bij de invulling van dit domein zijn onder andere:
- het (mede) vormgeven aan *corporate image & identity*;
- het opstellen, onderhouden en toetsen van richtlijnen voor externe, interne en corporate communicatie;
- het creëren en productief maken van vakkennis (expertisecentrum communicatie);
- het uitvoeren en co-creëren van de *corporate* communicatiestrategie;
- het verzorgen van crossmediale campagnes;
- het co-creëren van en adviseren over handhavingscommunicatie;
- het organiseren en faciliteren van de bedrijfscommunicatie;
- het organiseren en faciliteren van de interne communicatiedialoog;
- het beheren van het communicatie-instrumentarium als onderdeel van de *corporate* communicatie (waaronder intranet);
- het adviseren over externe en interne communicatie van de Belastingdienst en dienstonderdelen;
- het beheren en ontwikkelen van de externe website;

- het beheren en ontwikkelen van de *owned*, en *paid* kanalen voor interne en corporate communicatie;
- het verzorgen van generieke contentvraagstukken en generiek contentbeheer (denk aan: één contentbron, generiek documentenbeheer, metadateren, thesaurus, taxonomie, modellen en sjablonen);
- Het meten van effecten van (concernbrede) interne- en corporate communicatie

De activiteiten die worden uitgevoerd in dit domein worden op dit moment – in het licht van de complete communicatiefunctie van de Belastingdienst – herzien. Het in het kader van communicatiesupport uitgevoerde onderzoek is daar input voor. Eventuele conclusies en aanbevelingen van de *taskforce* worden meegenomen bij de verdere doorontwikkeling van B/CKC. Specifieke conclusies op het gebied van contentmanagement, positionering van communicatieadvies en verdeling van verantwoordelijkheden die raken aan dit domein worden daarbij expliciet met het MT/BD besproken door de CHRO en [redacted] B/CKC van de Belastingdienst.

3.2.4 Domein - Organisatieontwikkeling

Organisatieontwikkeling staat voor het richting geven aan de organisatie vanuit het continu vooruitkijken met oog voor de interne en externe omgeving. Deze richting wordt vertaald naar de consequenties voor de organisatie (op het gebied van werk en mens) om bewegingen te initiëren, te monitoren en ervan te leren. B/CKC draagt daarmee bij aan het blijvend equiperen van de Belastingdienst en zijn medewerkers, om hun werk te kunnen doen in een voortdurend veranderende omgeving. Het vraagt om een continue dialoog met zowel de organisatie als zijn omgeving.

Kenmerkende activiteiten voor de invulling van dit domein zijn onder andere:

- het adviseren en begeleiden van leidinggevenden en medewerkers bij de realisatie van organisatievraagstukken en organisatiebrede ontwikkelprogramma's op het gebied van:
  - het richten van werk en organisatie (MLTP als kader);
  - het inrichten van werk en organisatie;
  - het verrichten van werk (structureren, processen) en verbeteren van de performance;
  - het begeleiden van samenwerken in de keten (intern en extern).
- het adviseren over invoeringsstrategie en wijze van implementatie om het gebruik van instrumenten mogelijk te maken (HR-instrumenten zoals Exittooling, Vlootschouw, Gesprekkencyclus, Functiegebouw rijk, Exitmonitor, etc.);
- het adviseren en ondersteunen bij implementatie van BD-brede projecten met betrekking tot HR-beleid (inclusief: Quotumregeling, Onboarding en Werkplus);
- het monitoren, signaleren en vertalen van externe en interne ontwikkelingen op het gebied van HR ten behoeve van beleidsvoorbereiding;
- Het continu verbeteren van activiteiten op dit domein op grond van relevante data-analyse (effectmeting).

3.2.5 Domein - Mobiliteit (arbeidsmarktontwikkeling, in-, door- en uitstroom)

Mobiliteit staat voor arbeidsmarktontwikkeling en de in-, door- en uitstroom van medewerkers bij de Belastingdienst. Het draait om het verkrijgen van de juiste medewerker op de juiste plaats op het juiste moment, waarbij de Belastingdienst zich profileert als aantrekkelijke werkgever. B/CKC werkt aan een eenduidig beeld over werken bij de Belastingdienst (zowel voor potentiële als huidige medewerkers), biedt zicht op en inzicht in (ontwikkelingen in) de (externe) arbeidsmarkt en draagt bij aan de verbinding tussen werk en mens.

Kenmerkende activiteiten bij de invulling van dit domein zijn onder andere:

- het bewerken van de arbeidsmarkt door het kennen van trends en kunnen bereiken van doelgroepen;
- het adviseren over employabilityvraagstukken en projecten;
- het centraal uitvoeren van werving en selectie;
- het uitvoeren van trajecten en projecten gericht op in-, door- en uitstroom (denk aan: trainees, RNI, stages duaal, het coördineren van stages behorende bij het certificeren of opleiden van (toekomstige) managers en medewerkers van de Belastingdienst, loopbaanbegeleiding en werk-naar-werk-trajecten);
- het monitoren, signaleren en vertalen van externe en interne ontwikkelingen op het gebied van arbeidsmarkt en in-, door- en uitstroom;

- het implementeren van en adviseren over de uitvoering van relevante wet- en regelgeving (denk aan: de wet WAADI en het rijksbreed afgesproken participatiequotum);
- het adviseren van dienstonderdelen bij introductie en begeleiding van nieuwe medewerkers (onboarding);
- het ontwikkelen en inzetten van instrumenten ondersteunend aan in-, door- en uitstroom (denk aan: werkplus, etc.);
- het invullen van de psychologische adviesfunctie (ontwikkelen en uitvoeren van assessments, psychologisch onderzoek en –instrumenten en hieraan gerelateerde adviezen);
- het continu verbeteren van activiteiten op dit domein op grond van relevante data-analyse (effectmeting).

De invulling van de activiteiten in het domein Mobiliteit past binnen de huidige werkzaamheden van het *Employability Center*.

3.2.6 Domein - Werkgever- en werknemerschap

Werkgever- en werknemerschap staat voor het faciliteren, borgen, uitvoeren en effectueren van de rechten en plichten van werkgever en werknemer. Het draait om goed werknemerschap én goed werkgeverschap, op gebieden als gezondheid, welzijn en recht. Een belangrijk deel van de activiteiten binnen dit domein is opgenomen in het takenpakket van B/CFD. Het adviseren en uitvoeren van individuele rechtspositionele casuïstiek is centraal ondergebracht bij DG-Bel. Vanuit de het centrale organisatieonderdeel op het gebied van kennis, communicatie en HR wordt vooral gewerkt aan het borgen van expertise en aanbrengen van verbinding.

Kenmerkende activiteiten bij de invulling van dit domein zijn onder andere:
- het landelijk coördineren van HR-mediation, professionaliseren van mediators en uitvoeren van mediation op HR-gebied;
- het coördineren en professionaliseren van de vertrouwenspersonen op het gebied van integriteit en ongewenste omgangsvormen;
- het versterken en stimuleren van synergie en verbinding tussen activiteiten en actoren actief binnen dit domein;
- het continu verbeteren van activiteiten op dit domein op grond van relevante data-analyse (effectmeting).

Aantekeningen

Ministerie van Financiën

Aan
MT Belastingdienst

Directoraat-Generaal
Belastingdienst

Inlichtingen

T
F
@minfin.nl

Datum
1 mei 2014

Auteur

memo

Richtlijn oneigenlijk gebruik mobiliteitskaart

Bijlage
Brief COR met richtlijn oneigenlijk gebruik mobiliteitskaart

Aanleiding

Afgelopen overleg met de COR is gesproken over de richtlijn oneigenlijk gebruik mobiliteitskaart en het controleprotocol.
De COR heeft in dat overleg ingestemd met het controleprotocol en de controle op de aanwezigheid van verklaringen in de personeelsdossiers wanneer medewerkers standaard een eerste klasse kaart hebben aangevraagd op arbeidsvoorwaardelijke of op medische grond.

De COR heeft niet ingestemd met de richtlijn. Met name omdat deze te rigide gevonden werd ten aanzien van eventuele gemiste check-outs.

Gevraagd besluit

Akkoord gaan met de in de bijlage voorgestelde aangepaste richtlijn als handelswijze bij constatering van oneigenlijk gebruik van de mobiliteitskaart.

Vervolg

- bespreking met de COR
- publicatie op beeldkrant

Toelichting

Met het oog op publicatie begint de brief met het nogmaals geven van achtergrondinformatie en het waarom van controles. De eigenlijke richtlijn begint op pagina 3.

Ten aanzien van gemiste check-outs is nu aangepast dat een 'eerste gesprek' pas plaatsvindt na 5 gemiste check-outs (in geval van NS, ten aanzien van stads- en streekvervoer gelden 10 gemiste checkouts). Dit is in lijn met hetgeen besproken is in de rijksbrede stuurgroep mobiliteitskaart. Bij constatering van privégebruik zal overigens nog steeds direct het gesprek aangegaan worden. Ook zijn er termijnen toegevoegd waarbinnen 'een vorige stap' in de richtlijn moet hebben plaatsgevonden wil men naar een zwaardere stap gaan. Dit zodat er niet oneindig gestapeld kan worden.

1873579 00349

Ministerie van Financiën

> Retouradres Postbus 20201 2500 EE Den Haag

Concernondernemingsraad Belastingdienst

Directoraat-Generaal
Belastingdienst

Korte Voorhout 7
2511 CW Den Haag
Postbus 20201
2500 EE Den Haag
www.rijksoverheid.nl

Inlichtingen

T
F
@minfin.nl

Ons kenmerk

Datum 6 mei 2014
Betreft Richtlijn oneigenlijk gebruik mobiliteitskaart

Geachte leden,

Inleiding
De afgelopen maanden hebben wij de mobiliteitskaart van Mobility Mixx ingevoerd. De kaart wordt aan medewerkers verstrekt voor het maken van dienstreizen of ten behoeve van woon-werkverkeer. In onze overlegvergadering van 20 maart jl. hebben wij gesproken over de controles op het gebruik van de mobiliteitskaart. Om controle mogelijk te maken diende er een controleprotocol te worden vastgesteld. In dat protocol staat aangegeven welke gegevens worden gecontroleerd en wie toegang heeft tot gecontroleerde gegevens. In onze overlegvergadering van 17 april jl. heeft u ingestemd met het controleprotocol.

Tevens heb ik u toen op uw verzoek een richtlijn voorgelegd ter bevordering van een gelijke handelswijze in gelijke gevallen wanneer oneigenlijk gebruik van de mobiliteitskaart wordt geconstateerd. Hiervan heeft u toen aangegeven daar niet volledig mee in te kunnen stemmen, omdat u de regels rondom gemiste check-outs te rigide vond.

Dit heb ik besproken in het MT Belastingdienst van 6 mei jl. Naar aanleiding van deze bespreking en met inachtneming van hetgeen dat in de stuurgroep mobiliteitskaart rijksoverheid in dit verband ook al is besproken, leg ik u hierbij een nieuwe richtlijn voor.

Waarom controle op het gebruik van de mobiliteitskaart
Medewerkers van de Belastingdienst wordt de mobiliteitskaart van Mobility Mixx ter beschikking gesteld voor zakelijk gebruik. Bij de verstrekking van de kaarten wordt uitgegaan van vertrouwen. Medewerkers kunnen de kaart zelf aanvragen en een met de kaart te maken reis hoeft niet vooraf te worden goedgekeurd. B/CFD voert in samenwerking met B/CA periodiek en op verzoek controles uit op het gebruik van de kaart en op het op orde zijn van het P-dossier wanneer een standaard eerste klasse kaart op arbeidsvoorwaardelijke of medische gronden wordt aangevraagd. Controles vinden plaats ten behoeve van gerechtvaardigd vertrouwen in het ter beschikking stellen van de kaarten voor zakelijke reizen en ter controle op een doelmatige uitgave van overheidsgeld.

Wat wordt er eigenlijk gecontroleerd
Ten aanzien van de mobiliteitskaart onderscheiden we twee soorten controles.

1. Controle op reisgegevens
In ons overleg van 17 april jl. heeft u ingestemd met het rijksbrede controleprotocol. Hierin staat exact aangegeven welke gegevens over de reizen die medewerkers maken worden bijgehouden, wie toegang tot de gegevens heeft en aan wie rapportages ten aanzien van de gegevens worden verzonden.

Directoraat-Generaal Belastingdienst

Ons kenmerk
DGB/2014/2123

U heeft eerder aangegeven niet te willen dat met de invoering van de kaart een vorm van een 'medewerkersvolgsysteem' wordt geïntroduceerd. Ook de dienstleiding vindt dit onwenselijk. Om dit te voorkomen is het aantal functionarissen dat toegang heeft tot alle gegevens beperkt tot twee. Deze twee medewerkers zijn de enigen bij de Belastingdienst die toegang hebben tot alle gegevens, maar ze zijn niet bevoegd om die te gebruiken, anders dan voor de in het controle protocol vastgestelde rapportages, of op verzoek van directoraat-generaal Belastingdienst, wanneer een uitvraag wordt gedaan in het kader van een integriteitsonderzoek bij een ernstig vermoeden van plichtsverzuim.

2. Controle op personeelsdossiers
De mobiliteitskaart staat bij aanvraag standaard ingesteld op tweede klasse ten behoeve van woon-werkverkeer. Er kunnen 3 redenen zijn om de kaart standaard op eerste klasse in te stellen: arbeidsvoorwaardelijke grond, medische grond of de kaart wordt alleen gebruikt voor dienstreizen. Indien een medewerker een eerste klasse kaart op arbeidsvoorwaardelijke of medische grond heeft dan dient hiervan een verklaring aanwezig te zijn in het personeelsdossier. Dit wordt in de aanvraagmodule ook zo gecommuniceerd aan de medewerkers en ook leidinggevenden hebben hier een e-mailbericht over ontvangen.

Het vastleggen van personele afspraken in het p-dossier is, naast dat het voor een medewerker zelf handig is om op terug te kunnen vallen, verplicht ter controle op een doelmatige besteding van overheidsgelden (personeelskosten zoals salaris en ook reiskostenvergoedingen vormen een grote uitgavenpost van de overheid. Afspraken die aan de uitgaven ten grondslag liggen dienen te worden vastgelegd, zo ook deze. Hierom voeren wij, maar ook een instantie als de Algemene Rekenkamer, daar controles op uit).

B/CA/UCA (die belast is met de concernadministratie en daarmee ook de controle op doelmatige besteding van gelden en vanuit die functie toegang heeft tot P-direkt) controleert of de verklaringen in het P-dossier zijn opgenomen. Tevens wordt de kwaliteit van de verklaring gecontroleerd (van recente datum, reden van afwijking, einddatum en ondertekening door het bevoegd gezag van de betreffende medewerker). Wanneer uit de controle blijkt dat er geen verklaring of een verklaring van onvoldoende kwaliteit zit opgenomen in het personeelsdossier, dan wordt de medewerker gevraagd dit binnen vier weken in orde te maken. Indien na hercontrole blijkt dat dit nog niet in orde is, dan wordt het door de betreffende medewerker maken van eerste klasse reizen voor woon-werkverkeer aangemerkt als oneigenlijk gebruik. De aangepaste richtlijn op de volgende pagina zal vervolgens gehanteerd worden. Over de niet op orde zijnde P-dossiers zal worden gerapporteerd via B/CA in de managementrapportages.

In ons overleg van 17 april jl. heeft u ten aanzien van deze controle op de rechtmatigheid van de kaartverstrekking ook aangegeven hiermee in te stemmen.

Wat gebeurt er wanneer er sprake is van oneigenlijk gebruik
U heeft gevraagd om een richtlijn hoe te handelen wanneer oneigenlijk gebruik van de kaart wordt geconstateerd, zodat wordt bevorderd dat in gelijksoortige gevallen gelijk opgetreden wordt. U heeft tevens gevraagd er op te letten dat de richtlijn niet te rigide vormen aanneemt.

Directoraat-Generaal
Belastingdienst

Ons kenmerk
DGB/2014/2123

Mijn belangrijkste uitgangspunt voor een dergelijke richtlijn vind ik in onze basiswaarden: geloofwaardigheid, verantwoordelijkheid en zorgvuldigheid. Het beeld dat burgers en bedrijven hebben van de Belastingdienst, bepaalt voor een groot deel de bereidheid om (fiscale) verplichtingen na te komen. Integriteit is dus van groot belang. Ook in iets dat zo eenvoudig kan lijken al het maken van een dienstreis of woon-werkverkeer moeten we onze basiswaarden betrachten. Zorgvuldig omgaan met de ter beschikking gestelde kaart en de uitgave van overheidsgelden die daarmee samenhangt, is hierom vanzelfsprekend.

Overweging voor de richtlijn
De regelgeving omtrent woon-werkverkeer en dienstreizen dient bij medewerkers bekend te zijn. Ter bevordering hiervan is er actief gecommuniceerd rondom de invoering van de kaart, met de mogelijkheid voor medewerkers om vragen te stellen. De regelgeving is daarnaast permanent beschikbaar op intranet/rijksportaal en is tevens opgenomen in de aanvraagmodule voor de kaart. Medewerkers die in het bezit zijn van de kaart hebben zich dus van de regelgeving op de hoogte kunnen stellen bij de aanvraagprocedure. Om extra de aandacht hierop te vestigen stel ik voor na bespreking van dit onderwerp deze brief te communiceren op de beeldkrant en te verspreiden onder leidinggevenden ter eventuele bespreking in de teamoverleggen.

Richtlijn bij oneigenlijk gebruik mobiliteitskaart
1. Er zijn 3 vormen van oneigenlijk gebruik van de mobiliteitskaart. Dit zijn:
    a) Gemiste of onjuiste Check In
    Bij controle in het voertuig kan blijken dat een medewerker vergeten is in te checken, in de verkeerde klasse reist of bijvoorbeeld niet opgewaardeerd heeft voor het reizen met treinen waarvoor een toeslag dient te worden betaald. In deze gevallen kan de medewerker hiervoor een boete op naam ontvangen. Deze boetes worden niet door de werkgever vergoed.
    b) Gemiste Check Out
    Een medewerker kan na een reis vergeten uit te checken, waardoor een boetetarief in rekening wordt gebracht bij de werkgever.
    c) De kaart wordt niet-zakelijk gebruikt
    Voorbeelden van niet-zakelijk gebruik zijn het gebruiken van de kaart: voor reizen die niet in opdracht van de werkgever gemaakt worden; in de pauze om naar de stad te gaan; om van en naar een andere plek dan de geregistreerde woonplaats te reizen als woon-werkverkeer; voor het betalen van parkeerkosten wanneer er sprake is van woon-werkverkeer of onterecht een reis eerste klasse met de kaart maken.

2. Bij de constatering van oneigenlijk gebruik is sprake van plichtsverzuim.

3. Ongeacht het al dan niet nemen van een disciplinaire maatregel, dient de medewerker bij wie oneigenlijk gebruik is geconstateerd de gemaakte meerkosten in verband met het oneigenlijk gebruik door middel van inhouding op het salaris terug te betalen aan de werkgever / Staat der Nederlanden.

4. Wanneer oneigenlijk gebruik genoemd onder 1A en 1B meer dan incidenteel (vastgesteld op 5 keer op jaarbasis wanneer gebruik wordt gemaakt van reizen met de NS en 10 keer op jaarbasis wanneer gebruik wordt gemaakt van reizen in het stads- en streekvervoer) voorkomt of wanneer oneigenlijk gebruik zoals genoemd onder 1C wordt geconstateerd leidt dit tot een eerste gesprek tussen leidinggevende en medewerker.
   In het eerste gesprek wordt de aandacht gevestigd op de integriteit en de basiswaarden van de Belastingdienst en wordt nog eens extra gewezen op deze richtlijn. Het gesprek wordt vastgelegd en opgenomen in het personeelsdossier.

5. Bij constatering van oneigenlijk gebruik binnen een jaar na een eerste gesprek, leidt dit tot een tweede gesprek tussen de leidinggevende en de betreffende medewerker. Het gesprek wordt vastgelegd en opgenomen in het personeelsdossier. In dit gesprek wordt de aandacht gevestigd op de integriteit en de basiswaarden van de Belastingdienst en wordt nog eens extra gewezen op deze richtlijn. Daarnaast kan een lichte disciplinaire straf worden opgelegd. Voor disciplinaire bestraffingen wordt verwezen naar hoofdstuk 7 van de PUB.

6. Bij constatering van oneigenlijk gebruik binnen een jaar na een tweede gesprek, leidt dit tot een derde gesprek tussen leidinggevende en de betreffende medewerker, waarbij dit maal ook de naast hogere leidinggevende aanschuift. Ook dit gesprek wordt vastgelegd en opgenomen in het personeelsdossier. Dit derde gesprek leidt tot een disciplinair traject dat wordt afgerond met een voorstel aan DGBel/Cluster bedrijf/ Juridische Zaken om de disciplinaire straf van voorwaardelijk ontslag (met een proeftijd van half jaar) op te leggen.

7. Bij een constatering van oneigenlijk gebruik binnen een half jaar na een derde gesprek, leidt dit niet tot het voeren van een gesprek, omdat in dat geval direct het disciplinaire traject wordt ingezet. Dit traject wordt afgerond met een voorstel aan DGBel/Cluster bedrijf/ Juridische Zaken om de voorwaardelijk opgelegde disciplinaire straf van ontslag ten uitvoer te leggen (en deze dus onvoorwaardelijk te maken).

De richtlijn heeft geen bindend karakter waar het de disciplinaire gevolgen betreft, omdat van geval tot geval de voor de collega nadelige gevolgen van een strafbesluit moeten worden afgewogen tegen de met dat besluit te dienen doelen. Het bevoegd gezag zal altijd de feiten en omstandigheden moeten wegen.

In dat verband speelt de al dan niet aanwezigheid van strafverminderende of strafverzwarende omstandigheden een rol. Van een strafverminderende omstandigheid kan bijvoorbeeld sprake zijn wanneer een medewerker het direct bij zijn leidinggevende meldt wanneer hij is vergeten uit te checken en aangeeft de eventuele meerkosten voor de werkgever te willen vergoeden. Een strafverzwarende omstandigheid kan zich voordoen wanneer geconstateerd wordt dat een medewerker veelvuldig en op regelmatige basis privé heeft gereisd met de kaart. Kortom: het hiervoor geschetste traject kan soms sneller en soms langzamer doorlopen worden.

Tenslotte
Met het vaststellen een algemene richtlijn bij oneigenlijk gebruik nemen we de laatste stappen die samenhangen met de ingebruikname van de rijksbrede mobiliteitskaart. Ik begrijp dat dit voor sommige collega's de volgende werk-gerelateerde wijziging in korte tijd is geweest. De zorgen die u geuit heeft ten

aanzien van het vervallen van mogelijke eerdere privévoordelen die medewerkers hadden, zijn door de vakbonden aangekaart op rijksniveau.

Ten aanzien van de invoering als proces op zich ben ik blij dat dit in een relatief korte periode voor het overgrote deel vlekkeloos is verlopen. Dit is mede gelukt doordat u zich intensief heeft bemoeid met het invoeringsproces, heeft meegedacht en tips heeft gegeven om de invoering voor medewerkers zo goed mogelijk te laten verlopen. Hiervoor dank ik u hartelijk.

Deze brief en de hierin voorgestelde richtlijn wil ik agenderen voor onze overlegvergadering van 15 mei a.s. Ik hoop u hiermee voldoende te hebben geïnformeerd.

Hoogachtend,

namens deze,

Directoraat-Generaal
Belastingdienst

Ons kenmerk
DGB/2014/2123

Aantekeningen

Ministerie van Financiën

TER BESLISSING
Aan
MT Belastingdienst

Directoraat-Generaal
Belastingdienst

Inlichtingen
[redacted]
T
F
[redacted]@minfin.nl

Datum
30 april 2014

Notitienummer
DGB/2014-2788

Rubriek
Curaçao, Aruba ,St. Maarten

Technische bijstand

Auteur
[redacted]

Van
Cluster Fiscaliteit

Kopie aan
[redacted]

Bijlage
Concept notitie aan de staatssecretaris

notitie

IT bijstand aan Curaçao, Aruba en St. Maarten voor FATCA-CRS

Aanleiding

In dit memo wordt het MT Belastingdienst gevraagd te beslissen over de wijze van bijstand die de Belastingdienst moet verlenen richting Curaçao, Aruba en St. Maarten (CAS eilanden) voor de bouw van een IT systeem voor automatische inlichtingenuitwisseling, en wie de kosten moet betalen. Het gaat hier voor de goede orde niet om de normale technische bijstand voor operationele zaken, zoals het wegwerken van achterstanden.

Staatssecretaris Weekers heeft in het kader van de totstandkoming van de Belastingregeling met Curaçao bijstand van de Belastingdienst toegezegd voor de bouw van een IT systeem voor automatische inlichtingenuitwisseling in ruil voor een FATCA overeenkomst met Nederland. Curaçao heeft het IT systeem nodig om te voldoen aan de Foreign Account Tax Compliance Act (FATCA), de EU Spaarrenterichtlijn en de OESO Common Reporting Standard (CRS). IFZ onderhandelt momenteel ook met Aruba en St. Maarten over vergelijkbare bijstand omdat die om dezelfde redenen nodig is. Er is nooit gesproken over de mate van bijstand of over wie de kosten voor de bijstand moet betalen.

Kern

Gaat u akkoord met het voorstel dat:

- De Belastingdienst/CA onder verantwoordelijkheid van de CAS eilanden bijstand verleent in een adviserende en begeleidende rol;
- Volgens de actieve variant, en dat
- De kosten van de hele operatie door de CAS eilanden wordt gedragen maar dat de Belastingdienst ook een deel voor zijn rekening neemt (25% van de ontwerp en advieskosten die geschat worden op € 415.000 en in uiterste instantie ook 25% van de bouwkosten die geschat worden op € 500.000 = max. € 228.750).

Vervolgtraject

Naar aanleiding van uw beslissing wordt een notitie naar de Staatssecretaris ter beslissing gestuurd (zie bijlage voor een concept)

met het verzoek om een informerende brief richting Curaçao te sturen indien akkoord. IFZ kan dan de onderhandelingen met Aruba en St. Maarten afronden.

Toelichting

Achtergrond
De CAS eilanden zijn fiscaal zelfstandig. Dit betekent dat de eilanden zelfstandig met de VS moeten onderhandelen over de toepassing van FATCA en zelfstandig financiële gegevens aan de VS moeten zenden over Amerikanen die klant zijn bij financiële instellingen op de CAS. Curaçao heeft daarbij hulp gevraagd aan NL omdat Curaçao niet beschikt over de middelen om gegevens over Amerikaanse personen automatisch richting de VS uit te wisselen.

Staatssecretaris Weekers heeft niet gespecificeerde bijstand bij de bouw van een IT systeem aangeboden aan minister Jardim in ruil voor een overeenkomst op grond waarvan Curaçao ook FATCA informatie over Nederlandse inwoners met tegoeden aldaar gaat uitwisselen. Dit is vastgelegd in een in december 2013 ondertekende intentieverklaring.

Met het IT systeem zal Curaçao voor FATCA zelfstandig financiële gegevens over Amerikaanse personen aan de VS kunnen toesturen en ook over Nederlands belastingplichtigen richting Nederland. Bovendien moet het systeem Curaçao in staat stellen om informatie uit te wisselen voor de EU Spaarrenterichtlijn en op termijn ook voor de door de OESO ontwikkelde CRS met de rest van de wereld.

Gebruik door Curaçao van de nieuwe CRS standaard van wereldwijde inlichtingenuitwisseling is zeer wenselijk. Het VK verplicht zijn overzeese gebiedsonderdelen (o.a. Bermuda, Barbados en de Kaaimaneilanden) mee te doen. Het is voor Nederland niet handig als een offshore financieel centrum zoals Curaçao als onderdeel van het Koninkrijk niet meedoet in deze internationale ontwikkeling van vergrote transparantie en samenwerking tegen internationale belastingontduiking. Het Global Forum bij de OESO gaat nu ook proberen om financiële centra in de wereld gecommitteerd te krijgen voor de CRS.

Het bovenstaande geldt ook voor de eilanden Aruba en St. Maarten. IFZ bespreekt deze bijstand momenteel ook met Aruba en St. Maarten tijdens de onderhandelingen over een Belastingregeling met die eilanden. Als voor alle drie de eilanden in één keer bijstand wordt verleend voor de ontwikkeling van eenzelfde benodigd systeem, scheelt dat kosten.

Verantwoordelijkheid
De verantwoordelijkheid voor de (tijdige) ontwikkeling van een IT systeem blijft bij de CAS eilanden; de Belastingdienst adviseert. Op deze wijze wordt bereikt dat de CAS eilanden zelf verantwoordelijk blijven en Nederland niet aansprakelijk kan worden gesteld als implementatie en uitwisseling richting de VS per september 2015 niet lukt. Bovendien is het de bedoeling dat de CAS eilanden uiteindelijk zelfstandig de IT

systemen kunnen bedienen en onderhouden. Het houden van de verantwoordelijkheid bij de CAS eilanden voorkomt een passieve lokale houding.

Actieve vs passieve variant
Het is goed om te realiseren dat bijstand verder gaat dan alleen een IT systeem. Het IT systeem is één schakel in een lange keten. Er zit een heel proces omheen, zoals wetgeving, een overlegplatform met de plaatselijke financiële instellingen, bronnenbeheer, uitvalbehandeling compliance, beheer en onderhoud. Om gegevens uit te gaan wisselen zal het project naast de IT ook een uitvoerend (lijn)team en een overleg platform met de plaatselijke financiële instellingen moeten inrichten.

Wij adviseren u in te zetten op bijstand in de actieve variant, omdat wij inschatten dat de eilanden te weinig personeel en middelen hebben om zo'n project te trekken met alleen passieve advisering. Ook denken wij dat de eilanden in de passieve variant niet op tijd klaar zullen zijn richting de VS. Bovendien is Nederland zelf gebaat bij een zo snel mogelijk werkend systeem om zelf de informatie te verkrijgen. Tenslotte is de kans groter dat de eilanden bij de keuze voor een actieve adviserende rol sneller mee gaan doen met wereldwijde uitwisseling in de CRS.

In de actieve variant is er een intensieve samenwerking met de eilanden. Het projectplan wordt samen met de Belastingdienst opgesteld en er komt een Nederlandse projectmanager ter plaatse met actieve ondersteuning door Nederlandse procesdeskundigen en IV ontwerpers. Ook in de actieve variant zijn de CAS eilanden zelf verantwoordelijk voor de implementatie, en zullen de eilanden eigen personeel beschikbaar moeten stellen dat meewerkt aan het project en dat wordt opgeleid om zelfstandig verder te kunnen werken.

In de passieve variant moeten de CAS eilanden zelf voor een projectmanager zorgen en zelf een projectplan opstellen waarin de ondersteuning van Nederland wordt besproken. De nadruk ligt dan op kennisdeling en ondersteuning in de vorm van reviews. Planning, initiatief en verantwoordelijkheid en het opstellen van ontwerpen en sturingsdocumenten liggen dan bij de eilanden.

Kosten
Er zijn drie scenario's wie de kosten moet dragen:
- Nederland draagt alle kosten;
- De CAS eilanden dragen alle kosten;
- Een combinatie in de vorm van cofinanciering, NL draagt 25% van een deel van de kosten.

Het is niet handig om Nederland alle kosten te laten dragen. Ten eerste gaat dit meer ten nadele van de budgetten van de Belastingdienst. Ten tweede is het vanuit een project invalshoek logischer als degene die verantwoordelijk is voor(de voortgang van) het project, ook verantwoordelijk is voor de kosten. Gebeurt dat niet, dan bestaat het

risico dat de CAS eilanden minder logische beslissingen nemen of minder efficiënt zullen zijn, omdat de kosten toch door een ander worden gedragen. Dit betekent een verhoogd risico dat het project niet op tijd af is en met hogere kosten aan de kant van Nederland.

Vanuit een projectmatige insteek bezien is het dus beter dat de CAS eilanden alle kosten dragen, omdat zij ook de verantwoordelijkheid dragen voor (de voortgang van) het project. In de gesprekken tussen Staatssecretaris Weekers en Minister Jardim van Curaçao (zonder ambtelijke ondersteuning) is er echter niet gesproken over de kosten, zodat dit scenario achteraf gevoeld kan worden als een sigaar uit eigen doos. Ook tijdens de onderhandelingen met Aruba en St. Maarten heeft IFZ bijstand voor de bouw van een IT systeem beloofd in ruil voor meer tegemoetkomingen van St. Maarten over de Regeling, zonder dat over de kosten is gesproken.

Daarnaast heeft Nederland er een belang bij als de CAS eilanden snel beschikken over dit IT systeem, omdat we dan snel ook informatie over Nederlands belastingplichtigen kunnen krijgen van de eilanden. Ten slotte heeft Nederland een politiek belang dat de CAS eilanden kunnen voldoen aan de nieuwe internationale transparantie standaarden. Het imago van een non-compliant financieel centrum 'in de achtertuin' kan schadelijk zijn voor het imago van Nederland zelf. Het opleggen van alle kosten aan de CAS eilanden kan dan leiden tot weerstand en onnodige vertraging wat ook niet in het belang van Nederland zelf is.

De bouw en onderhoudskosten voor de ICT voorziening worden door B/CA geschat op € 500.000. Werken de CAS eilanden samen, dan kan dit bedrag door de drie eilanden gedeeld worden.
De kosten voor de inzet van de Belastingdienst in de vorm van ontwerp- en advieskosten worden geschat op € 330.000 (actief) en € 110.000 (passief) voor bijstand alleen aan Curaçao. Voor bijstand aan alle CAS landen bedragen deze kosten € 415.000 (actief) respectievelijk € 140.000 (passief).

Voorstel
Om aan het bovenstaande tegemoet te komen zou een cofinanciering kunnen werken. De CAS eilanden dragen alle drie zelf de bouw- en onderhoudskosten voor de ICT voorziening, en Nederland draagt een gedeelte bij van de bijstand in de vorm van expertise, bijvoorbeeld 25% van de ontwerp- en advieskosten.

Voor alle hulp die de Belastingdienst biedt in de vorm van kennis, expertise en begeleiding betaalt elk eiland en de Belastingdienst dan 25%. Op deze manier ligt de verantwoordelijkheid en de uiteindelijke draagplicht voor de kosten voor het grootste deel bij de eilanden zelf. Daarmee wordt recht gedaan aan het projectmatig uitgangspunt dat degene die verantwoordelijk is ook betaalt, en wordt tevens recht gedaan aan geschapen verwachtingen, terwijl dit ook het voordeel reflecteert dat Nederland zelf heeft bij het eindresultaat.

De [redacted] van het ministerie van Financiën, [redacted], peilt momenteel de reactie van de eilanden op dit voorstel.
Als dit aanbod onverhoopt tot weerstand in de besprekingen met de eilanden leidt zou de Belastingdienst ook in uiterste instantie 25% van zowel de bouw- en onderhoudskosten, als de ontwerp- en advieskosten kunnen dragen. Alle kosten worden dan door vier gedeeld.

De Nederlandse bijdrage is dan in principe 25% van € 415.000 = € 103.750 en in geval van weerstand in uiterste instantie 25% van de totale kosten ad € 915.000 = € 228.750. Deze kosten worden dan ten laste van het [redacted] budget gebracht.

Ministerie van Financiën

TER BESLISSING
Aan
De Staatssecretaris

Directoraat-Generaal
Belastingdienst

Inlichtingen
[redacted]
T
F
[redacted]@minfin.nl

Datum
mei2014

Notitienummer
DGB/2014-2787

Rubriek
Curaçao, Aruba, St. Maarten

Auteur
[redacted]

Van
Cluster Fiscaliteit

Kopie aan
[redacted] (Uitvoeringsbeleid)
(Belastingen)
(IFZ)
(AFP EU)

Bijlage
1. Intentieverklaring NL-CUR
2. Concept brief aan minister Jardim

notitie

Bijstand Belastingdienst voor IT systeem Curaçao, Aruba en St. Maarten

Paraaf
De Staatssecretaris

Via
[redacted]

Via
[redacted] voor
Fiscale Zaken

Via
[redacted]

Medeparaaf
Managementteam
Belastingdienst

Medeparaaf
[redacted]

Medeparaaf
[redacted]

Aanleiding

Uw ambtsvoorganger heeft in het kader van de onderhandelingen over de Belastingregeling met Curaçao (BRC) aan minister Jardim bijstand toegezegd van de Belastingdienst bij de bouw van een IT systeem voor automatische inlichtingenuitwisseling. Bij Curaçao bestaat de behoefte om te weten in welke vorm dat gebeurt. Curaçao heeft het IT systeem nodig om te voldoen aan de Foreign Account Tax Compliance Act (FATCA) en de Common Reporting Standard (CRS).

Kern

Gaat u akkoord met het voorstel dat:

- De Belastingdienst onder verantwoordelijkheid van Curaçao bijstand verleent in een adviserende en begeleidende rol;
- Volgens de actieve variant;
- De kosten van deze bijstand door Curaçao worden gedragen, maar wel met een bijdrage van 25% van de ontwerp –en advieskosten van Nederland;
- Hetzelfde geldt richting Aruba en St. Maarten en
- U de in de bijlage aangegeven brief verstuurt aan minister Jardim?

Toelichting

Algemeen

De bijstand die in deze notitie wordt besproken staat los van de technische bijstand die de Belastingdienst op verzoek van Curaçao, Aruba en St. Maarten (CAS eilanden) zou moeten verlenen voor operationele activiteiten, zoals bijstand bij het wegwerken van achterstanden. U wordt daar separaat nog over geïnformeerd.

Achtergrond

De CAS eilanden zijn fiscaal zelfstandig. Dit betekent dat de eilanden zelfstandig met de VS moeten onderhandelen over de toepassing van FATCA en zelfstandig financiële gegevens aan de VS moeten zenden over Amerikanen die klant zijn bij financiële instellingen op de CAS. Curaçao heeft daarbij hulp gevraagd aan uw ambtsvoorganger omdat Curaçao niet beschikt over de middelen om gegevens over Amerikaanse personen automatisch richting de VS uit te wisselen.

Uw ambtsvoorganger heeft niet gespecificeerde bijstand bij de bouw van een IT systeem aangeboden aan minister Jardim in ruil voor een overeenkomst op grond waarvan Curaçao ook FATCA informatie over Nederlandse inwoners met tegoeden aldaar gaat uitwisselen met Nederland. Dit is vastgelegd in een in december 2013 ondertekende intentieverklaring (zie bijlage).

Met het IT systeem zal Curaçao voor FATCA zelfstandig financiële gegevens over Amerikaanse personen aan de VS kunnen toesturen en ook over Nederlands belastingplichtigen richting Nederland. Bovendien moet het systeem Curaçao in staat stellen om informatie uit te wisselen voor de EU Spaarrenterichtlijn en op termijn ook voor de door de OESO ontwikkelde CRS met de rest van de wereld.

Gebruik door Curaçao van de nieuwe CRS standaard van wereldwijde inlichtingenuitwisseling is zeer wenselijk. Het VK verplicht zijn overzeese gebiedsonderdelen (o.a. Bermuda, Barbados en de Kaaimaneilanden) mee te doen. Het is voor Nederland niet handig als een offshore financieel centrum zoals Curaçao als onderdeel van het Koninkrijk niet meedoet in deze internationale ontwikkeling van vergrote transparantie en samenwerking tegen internationale belastingontduiking. Het Global Forum bij de OESO gaat nu ook proberen om financiële centra in de wereld gecommitteerd te krijgen voor de CRS.

Het bovenstaande geldt ook voor de eilanden Aruba en St. Maarten. IFZ bespreekt deze bijstand momenteel ook met Aruba en St. Maarten tijdens de onderhandelingen over een Belastingregeling met die eilanden. Als voor alle drie de eilanden in één keer bijstand wordt verleend voor de ontwikkeling van eenzelfde benodigd systeem, scheelt dat kosten.

Adviserende rol

De verantwoordelijkheid voor de (tijdige) ontwikkeling van een IT systeem blijft bij de CAS eilanden; de Belastingdienst adviseert. Op deze

wijze wordt bereikt dat Curaçao zelf verantwoordelijk blijft en Nederland niet aansprakelijk kan worden gesteld als implementatie en uitwisseling richting de VS per september 2015 niet lukt.

Actieve vs passieve variant
Het is goed om te realiseren dat bijstand verder gaat dan alleen een IT systeem. Het IT systeem is één schakel in een lange keten. Er zit een heel proces omheen, zoals wetgeving, een overlegplatform met de plaatselijke financiële instellingen, bronnenbeheer, uitvalbehandeling compliance, beheer en onderhoud. Om gegevens uit te gaan wisselen zal het project naast de IT ook een uitvoerend (lijn)team en een overleg platform met de plaatselijke financiële instellingen moeten inrichten.

Wij adviseren u in te zetten op bijstand in de actieve variant, omdat wij inschatten dat de eilanden te weinig personeel en middelen hebben om zo'n project te trekken met alleen passieve advisering. Ook denken wij dat de eilanden in de passieve variant niet op tijd klaar zullen zijn richting de VS. Bovendien is Nederland zelf gebaat bij een zo snel mogelijk werkend systeem om zelf de informatie te verkrijgen. Tenslotte is de kans groter dat de eilanden bij de keuze voor een actieve adviserende rol sneller mee gaan doen met wereldwijde uitwisseling in de CRS.

In de actieve variant is er een intensieve samenwerking met Curaçao. Het projectplan wordt samen met de Belastingdienst opgesteld en er komt een Nederlandse projectmanager ter plaatse met actieve ondersteuning door Nederlandse procesdeskundigen en IV ontwerpers. Ook in de actieve variant is Curaçao zelf verantwoordelijk voor de implementatie, en zal Curaçao eigen personeel beschikbaar moeten stellen dat meewerkt aan het project en dat wordt opgeleid om zelfstandig verder te kunnen werken.

In de passieve variant moet Curaçao zelf voor een projectmanager zorgen en zelf een projectplan opstellen waarin de ondersteuning van Nederland wordt besproken. De nadruk ligt dan op kennisdeling en ondersteuning in de vorm van reviews. Planning, initiatief en verantwoordelijkheid en het opstellen van ontwerpen en sturingsdocumenten liggen dan bij Curaçao.

Kosten
Zowel in de actieve als de passieve variant zal Curaçao de bouw- en onderhoudskosten voor de ICT voorziening zelf moeten betalen. Deze worden door B/CA geschat op € 500.000. Werken de CAS eilanden samen, dan kunnen alle kosten door de drie eilanden gedeeld worden.

De kosten voor de inzet van de Belastingdienst in de vorm van ontwerp- en advieskosten moeten in principe ook worden vergoed. Deze kosten worden geschat op € 330.000 (actief) en € 110.000 (passief) voor bijstand alleen aan Curaçao. Voor bijstand aan alle CAS landen bedragen deze kosten € 415.000 (actief) respectievelijk € 140.000 (passief). In de

gesprekken met de eilanden is tot nu toe nooit over vergoeding van deze kosten gesproken.

Wij raden aan dat de Belastingdienst 25 % van deze kosten voor zijn rekening neemt, zodat de pijn in gelijke mate verdeeld wordt tussen de drie eilanden en Nederland. Hiermee wordt voorkomen dat de eilanden zich achteraf bekocht voelen en het gevoel hebben een sigaar uit eigen doos te krijgen, omdat er over vergoeding van dit soort kosten nooit is gesproken tijdens de onderhandelingen. Ook reflecteert dit de baat die Nederland zelf heeft bij een zo snel mogelijke bouw van de IT systemen en dus compliance van de eilanden aan internationale standaarden.

Aantekeningen

AANTEKENINGEN

AANTEKENINGEN