Bundel van de MT Belastingdienst van 16 februari 2015

1.1 Communicatie (inclusief TOP-lijst in iBabs)

1.2 Besluiten- en actiepuntenlijst MT Belastingdienst 9 februari 2015 (bijgevoegd)

besluiten- en actiepuntenlijst 9 februari 2015.pdf

1.3 Aansluiting Belastingdienst op Nationaal Detectie Netwerk (bijgevoegd,)

Oplegmemo Aansluiting NDN.pdf

2015-01-22 - Privacy Impact Assessement NDN.pdf

2015-01-29 - Beantwoording vragen MT-BD.pdf

2015-01-26 - Meldingsformulier NDN.pdf

Infosheet Nationaal Detectie Netwerk 1 4.pdf

1.4 MRB (bijgevoegd,)

aanbiedingsbrief MRB jan 2015.pdf

Managementrapportage Belastingdienst januari 2015.pdf

1.5 ICBR (agenda bijgevoegd,)

Agenda ICBR 17 februari.docx

1.6 Actualiteiten, rondvraag, terugkoppeling, mededelingen, komende week/weken

1.7 1BRN (notitie bijgevoegd,)

2015 02 15 Een bankrekeningnummer PvA resterende groep.docx

1.8 Terugkoppeling financiele besluiten (mondeling,)

1.9 Personeel (Alleen vast MT-leden)

2.1 14.00- 15.00 uur Fraude (afzonderlijk in iBabs)

3.1 15.30- 17.30 uur Bezoek SZW P&I (agenda bijgevoegd, locatie Snipzaal)

20150216 Agenda bezoek SZW P&I.docx

BESLUITEN- EN ACTIEPUNTENLIJST MT BELASTINGDIENST

9 februari 2015

Nr.[1]	[2]	Omschrijving	Status
07.01	**C**	Het MT bespreekt de TOPlijst: - De brief alleenstaande ouders met mogelijk recht op kindgebonden budget wordt zes weken uitgesteld. - De brieven die in het kader van 1 BRN zouden worden verstuurd, worden uitgesteld. Dit onderwerp komt volgende week terug op TOPlijst. Wanneer er meer duidelijkheid is met stas bespreken. - IHAK: de gewijzigde brief 'nabetalen' is afgestemd met en goedgekeurd door stas. Er ligt nog een vraag of uitstel ook geldt voor ambtshalve aanslagen. - Bij Toeslagen deze week veel opeenvolgende onderwerpen in de media: Morgen aandacht voor Fraude bij [redacted] bij Tros opgelicht, donderdag volgt aanbieding rapportage door Nationale Ombudsman aan de staatssecretaris, daarnaast wordt aandacht verwacht rond brief uitvoering KOT nieuwe stijl en verwerking inkomens 2008-2011. - Morgenochtend ontvangt TK een brief aangaande [redacted]. - Artikel NTS in Groene Amsterdammer staat voor volgende week gepland. Kan nu eerder in de publiciteit komen. - Morgen volgt voor 12 uur een brief aan TK aangaande rulings (met name aandacht voor Starbucks). - CAO-onderhandelingen: de Belastingdienst verwachtte ongeveer 50 bezwaren. Deze zijn uiteindelijk bij ECO&P binnengekomen en bleken aan minister Blok gericht te zijn. Op korte termijn volgt er een Management Update. Verwacht wordt dat er nog bezwaren zullen binnenkomen van medewerkers van de Belastingdienst. - Onderzoek iSZW: belafspraak met IG gepland voor eind februari. - Aanstaande vrijdag staat een bijeenkomst met stas rondom de aangiftecampagne gepland.	√
07.02	**C**	[redacted] spreekt de actualiteiten door: - Vorige week was een onstuimige week met aandacht voor de uitspraak in de zwartspaarderszaak, zitting Hoge Raad, en aandacht voor HSBC lijst. - Dinsdag wordt uitspraak Hof Den Bosch verwacht in zaak over dwangsom. - Zondag zal stas in Wakker Nederland worden geïnterviewd. Doel is media-aandacht richting de aangifte campagne. Waarschijnlijk is er ook aandacht voor aantal actuele onderwerpen. [redacted] vraagt om input binnen DGBel.	√
07.03		Minister Ploumen heeft een besluit genomen over de sancties tegen Rusland. Er wordt 11 miljoen beschikbaar gesteld en het handhavingniveau blijft gelijk aan de huidige situatie. De Douane heeft een handhavingsplan gereed. Dit levert veel werk op voor	√

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

Nr.[1]	[2]	Omschrijving	Status
		binnenland Douane. Er wordt niet afgeschaald maar er is wel extra inzet nodig om andere werkzaamheden ook weer op te pakken.	
07.04		Arke zal vanaf 1 november rechtstreekse vluchten naar de Antillen uit gaan voeren vanaf luchthaven Eindhoven. De Douane is in gesprek wat er voor nodig is om op het gewenste niveau controles te kunnen uitvoeren.	√
07.05	**C**	Volgende week vinden acties vanuit de FIOD plaats bij fiscaal dienstverleners in samenwerking met Belastingen en Toeslagen. Met communicatie zijn afspraken gemaakt over publicitaire aandacht.	√
07.06	**B** **A**	Het memo besluitvorming en communicatie bij verstoringen tijdens de aangiftecampagne wordt aangenomen. - Het MT vraagt voldoende aandacht voor het uitwerken van de what if scenario's. - Bij eventuele verstoring OLAV wordt eerst de oorzaak van de storing vastgesteld en op basis daarvan de communicatie naar de burger bepaald. Criterium moet zijn om burger voor te lichten. De inzet is om maximaal ruimte te houden om Easytax niet in te zetten. [redacted] blijft in de lead en neemt uiteindelijke besluit. De termijnen gelden als leidraad. - Bijlage 3 bevat de nieuwe damageprocedure in wording. Deze wordt nog bestuurlijk afgerond. Tot dat dit is afgerond blijft de oude procedure van kracht.	
07.07		Het MT bespreekt de besluiten- en actiepuntenlijst - 06.10 actiehouder is [redacted] i.p.v. [redacted] - 06.13 deze week opnieuw delegatie met o.a. [redacted] bij broedkamers op bezoek.	√
07.08	**B** **A** **A**	Het jaarplan 2015 wordt als concept aangenomen. - Het plan is ook aangeboden aan de Bestuursraad. Zij geven aan dat er geen jaarplan aan kan worden genomen bij een niet sluitend kader. Wel onderschrijven zij de aanpak voor de komende maanden. - Geen opmerkingen bij de tekst behalve aantal technische zaken die bij FEZ zijn teruggelegd. - Na reces komt [redacted] hierop terug in de Bestuursraad. - Behoefte om in kleine stapjes tot meer inhoudelijke targets te komen. Bij aanmerkelijke veranderingen ruimte nemen om aan te passen. - Per vier maanden wordt de relevantie van dit jaarplan bekeken in verband met bestaande cycli.	
07.09	**B**	Het memo vaststelling strategische projecten wordt aangenomen na toevoeging van beschikbaarheid ODB/HDBS. - Het memo heeft als doel in kaart te brengen welke strategische trajecten er lopen op basis van kosten en strategisch belang. - Nieuw is dat concernbrede releases en programma's ook worden vermeld. - Afronding van projecten wordt expliciet op dit overzicht opgenomen.	√
07.10	**B**	Het memo vaststelling te rapporteren strategische trajecten wordt aangenomen. - Het woord 'deels' bij ad 1 en 2 wordt verwijderd.	√

Nr.[1]	[2]	Omschrijving	Status
07.11	**B**	Het plan van aanpak impactanalyse individuele functies wordt geaccordeerd. Er wordt aandacht gevraagd voor: - Individueel werk en werk in projecten. - Doorstroom - Implementatie (zowel kosten als positionering in de tijd). Om goed in te spelen op implementatievraagstukken wordt in de impactanalyse specifiek gekeken naar de opschaalbaarheid. - Duidelijkheid richting leidinggevenden wat dit voor hen betekent.	√
07.12	**T**	Per 1 april zal [redacted] als [redacted] en [redacted] handhavingsbeleid gaan werken bij de ILT.	√
07.13	**T**	16 februari komt [redacted] SZW P&I op bezoek bij het MT Belastingdienst.	√
07.14	**T**	Met memo MAC campagne 2014-2015 biedt een terugblik op de periode 2014 en de intensieve samenwerking tussen CA en Toeslagen. Aandachtspunten: - Monitoringsfunctie massale proces kan nog beter worden ingericht. - Te hanteren normen zijn erg laat aangeleverd. Dit blijft kwetsbaar. - Tijdspanne tussen releases en uitbetalingsmomenten. Met name rond Aangiftecampagne en MAC. - EBV: dit jaar zowel MAC afgeleverd in berichtenbox als compacte beschikking. Wanneer volgt de eerste volledig digitale MAC? Is het vangnet daar voldoende op ingericht?	√
07.15		[redacted] licht de beoogde prestatie-indicatoren op de website BD (Spoor C) toe. - Voorstel is om te starten met het plaatsen van zeven indicatoren die besproken zijn in de programboard. - Het MT geeft aan graag verschillende soorten indicatoren terug te willen zien. Zowel indicatoren die de stand van zaken op dit moment weergeven ('tellers'), als indicatoren die in de tijd bepaalde trends weergeven, als indicatoren met een positieve formulering (bijvoorbeeld: 98% van de belastingplichtigen voldoet tijdig aan zijn verplichtingen). - Daarnaast is de wens om indicatoren doelmatig in te zetten en te onderzoeken in welke mate er kan worden gestuurd d.m.v. indicatoren. - Indicatoren gebruiken om in bepaalde periode in te zoomen op bepaalde stand van zaken.	
07.16		Forecast massale processen: niet besproken	

Ministerie van Financiën

Aan
MT Belastingdienst

Directoraat-Generaal
Belastingdienst

Inlichtingen
[redacted]
T 06[redacted]
[redacted]@minfin.nl

Datum
5 februari 2015

Van
[redacted]

memo

Aansluiting Belastingdienst op Nationaal Detectie Netwerk

BZK en VenJ hebben de Belastingdienst verzocht aan te sluiten bij het Nationaal Detectie Netwerk (NDN), een samenwerkingsverband dat dreigingsinformatie verzamelt door het monitoren en analyseren van netwerkverkeer. Het kernministerie is als pilot aangesloten bij het NDN. Monitoring betreft ook persoonsgegevens, waarbij de medezeggenschap instemmingsrecht heeft.

Besluit

Het MT neemt zich voor om de Belastingdienst aan te sluiten bij het NDN en dit voornemen vervolgens ter instemming voor te leggen aan de COR.

Achtergrondinformatie

De Minister van VenJ heeft aan de Tweede Kamer de toezegging gedaan om vanaf 2014 het NDN op- en uit te bouwen. Het NDN is een samenwerkingsverband voor het beter en sneller waarnemen van digitale gevaren en risico's. Door het delen van dreigingsinformatie kunnen partijen vanuit de eigen verantwoordelijkheid tijdig gepaste maatregelen nemen om mogelijke schade te beperken of te voorkomen. Zo werken we samen aan de digitale weerbaarheid van Nederland.
Onder verantwoordelijkheid van VenJ werken NCTV, AIVD, MIVD en BZK/DGOBR samen in het NDN. Daarnaast wordt het NDN ook uitgewerkt met organisaties uit de vitale sectoren, ICT-dienstverleners, belangengroeperingen en verschillende publieke, private en publiek-private samenwerkingsverbanden.

Gevolgde route DGBel/Belastingdienst

Aansluiting op het NDN zal worden uitgevoerd door CIE. Er is een Privacy Impact Assessment (PIA) gedaan, waarbij de [redacted] de [redacted] en [redacted] zijn betrokken.
De eerste bespreking van het NDN in het MT-BD op 27 oktober jl. heeft geleid tot een aantal vragen. Deze vragen zijn beantwoord in het bijgevoegde memo (bijlage 2) en door middel van een aanscherping van de PIA (bijlage 1).
Verder zijn door [redacted], juridisch adviseur bij DGBel, een aantal vragen gesteld naar aanleiding van de review van de PIA. Deze zijn verwerkt en de PIA is vervolgens ter beschikking gesteld aan [redacted]. Haar op- en aanmerkingen zijn eveneens verwerkt in de definitieve versie.

Vervolg

- Dit voorgenomen besluit wordt ter instemming voorgelegd aan de COR. Vertegenwoordigers van CIE en het NDN samenwerkingsverband zullen beschikbaar zijn voor toelichting en de beantwoording van vragen.

- In de PIA zijn een aantal aanbevelingen opgenomen. Deze worden tijdens de uitvoering van de aansluiting geadresseerd in overleg tussen [redacted] en [redacted].

Bijlagen

1. 2015-01-22 - Privacy Impact Assessment NDN
2. 2015-01-29 - Beantwoording vragen MT-BD
3. 2015-01-26 - Meldingsformulier NDN
4. Infosheet Nationaal Detectie Netwerk 1.4

Aansluiting Belastingdienst op het Nationaal Detectie Netwerk (NDN)
Verslag Privacy Impact Assessment (PIA)

Aanleiding

Aansluiting bij NDN van de Belastingdienst infrastructuur

Nederland is één van de meest gedigitaliseerde landen ter wereld. Digitalisering levert grote voordelen op en is een drijvende kracht achter onze welvaart. De keerzijde van digitalisering is echter dat wij ook kwetsbaar worden voor cyberdreigingen. Uit onderzoek van onder meer het Nationaal Cyber Security Centrum (NCSC), de Algemene Inlichtingen- en Veiligheidsdienst (AIVD) en Militaire Inlichtingen- en Veiligheidsdienst (MIVD) blijkt dat de dreiging die uitgaat van digitale aanvallen blijft toenemen. Ook de complexiteit van deze aanvallen neemt toe. De potentiële maatschappelijke en economische impact van een aanval kan groot zijn.

De weerbaarheid van Nederland tegen deze dreigingen heeft geen gelijke tred gehouden met de digitalisering. Daarom is het ministerie van Veiligheid en Justitie gestart met het op- en uitbouwen van een nationaal detectie netwerk (NDN). Het doel van het NDN is om te komen tot een netwerk van samenwerkende publieke en private organisaties uit de kritieke infrastructuur. Het netwerk wordt ondersteund en gefaciliteerd door de AIVD, MIVD en het NCSC. Binnen het netwerk worden detectieactiviteiten uitgevoerd naar digitale dreigingen op basis van hoogwaardige dreigings- en incidenteninformatie. De samenwerking binnen het NDN moet zorgen voor het beter en sneller waarnemen van digitale gevaren en risico's. Door het delen van dreigingsinformatie kunnen partijen op basis van de eigen verantwoordelijkheid tijdig passende maatregelen nemen om mogelijke schade te beperken of te voorkomen.

Onder verantwoordelijkheid van het ministerie van Veiligheid en Justitie werken de Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV), de AIVD en MIVD en het directoraat-generaal Organisatie en Bedrijfsvoering Rijk (DGOBR) van het ministerie van Binnenlandse Zaken en Koninkrijksrelaties samen in een pilot NDN. De verwachting is dat dat wanneer de pilot NDN eindigt dit wordt omgezet in een definitieve voorziening. De Belastingdienst zal gebruik maken van de definitieve voorziening. Daarnaast wordt het NDN ook verder uitgewerkt met organisaties uit de vitale sectoren, ICT-dienstverleners, belangengroeperingen en verschillende publieke, private en publiek-private samenwerkingsverbanden.

Om de risico's van de niet-naleving van de eisen die de Wet bescherming persoonsgegevens (Wbp) stelt aan verwerkingen van persoonsgegevens te beoordelen, is al eerder rijksbreed een privacy impact assessment (PIA) uitgevoerd. Uit die rijksbrede-PIA kwam een aantal risico's naar voren waarvan een samenvatting is opgenomen aan het eind van dit verslag. De onderhavige PIA betreft de aansluiting van de Belastingdienst op het NDN. Voor zover dat mogelijk is worden de eerder gesignaleerde risico's in de onderhavige PIA geadresseerd en zullen er mitigerende maatregelen worden voorgesteld

.

De aansluiting van de Belastingdienst op het NDN behelst concreet het plaatsen van twee typen sensoren. De aansluiting is beperkt tot de volgende digitale netwerken van de Belastingdienst: Belastingdienst kantoornetwerk, Belastingdienst WiFi netwerk, inclusief

BYOD en Gasten, en het Open Internet netwerk. De sensoren die worden gebruikt om cyberdreigingen te detecteren zijn van het NCSC en de AIVD. Deze sensoren detecteren de aanwezigheid van zogenoemde Indicators of Compromise (IOC's) binnen het netwerkverkeer. Deze IOC's worden samengesteld door het NCSC en de AIVD zelf. Zodra een IOC wordt geraakt, wordt een signaal afgegeven en wordt een pakketje informatie rondom de IOC apart gezet. De opvolging van het signaal is de taak van de eigenaar van de sensor: NCSC of AIVD. Dit gebeurt echter niet zonder de tussenkomst van het Security Operations Center (SOC) van de Belastingdienst/Centrum voor infrastructuur en exploitatie (B/CIE). Het beheer van de sensoren is in handen van het SOC. In een plan van aanpak zullen de beheersafspraken en de procesafspraken tussen NCSC en AIVD en het SOC nauwgezet beschreven worden.

Vragen PIA volgens het Toetsmodel Rijksdienst

I Basisinformatie: type persoonsgegevens, type verwerking en noodzaak/ gegevensminimalisering

1. **Wilt u als verantwoordelijke persoonsgegevens gaan gebruiken voor de verwerking die u voorziet? Zo ja, van welk type?**

Ja. In het kader van de Wbp is [redacted] Belastingdienst de verantwoordelijke voor de aansluiting van de Belastingdienst op het NDN; de Belastingdienst/Centrum voor infrastructuur en exploitatie (B/CIE) is de beheerder. Het SOC voert de werkzaamheden feitelijk uit.
De betrokkenen van wie de persoonsgegevens worden verwerkt, zijn medewerkers van de Belastingdienst, de personen die via het internet communiceren met de medewerkers van de Belastingdienst en (potentiële) dreigers die doorgaans anoniem willen blijven.

De typen persoonsgegevens die worden verwerkt, zijn variabel. Dit zal hieronder worden toegelicht.

Al het digitale netwerkverkeer wordt getoetst aan de digitale patronen van digitale aanvallen. Dit is vergelijkbaar met netwerkcomponenten als firewalls, anti-spam en anti-malware oplossingen, zoals deze ook al worden gebruikt door B/CIE. Op het moment dat er een match is met een IOC die duidt op een digitale aanval, wordt hier een melding van gemaakt aan het SOC. Dit stukje netwerkverkeer wordt op de server, die bij B/CIE geplaatst is, voor een beperkte periode van 30 dagen opgeslagen. We kunnen hier spreken van pakketjes informatie rondom de match. Al het andere netwerkverkeer wordt niet opgeslagen. Het enige verschil met de huidige gang van zaken is dat door aansluiting bij het NDN twee externe partijen zijn betrokken, te weten het NCSC en de AIVD.

Hoe werkt het ongeveer?
De verwerking van persoonsgegevens bestaat uit het plaatsen van AIVD- en NCSC-sensoren op een vooraf bepaald gedeelte van het in- en uitgaande digitale netwerkverkeer van de Belastingdienst. Deze sensoren werken met IOC's. De IOC's kunnen zijn opgebouwd uit verschillende componenten , zij zullen echter vaak een IP-adres bevatten. Het actuele dreigingsbeeld bepaalt de precieze inhoud van de IOC's. Nadat de sensoren in het in- en uitgaande netwerkverkeer een match met een IOC hebben vastgesteld, wordt een pakketje informatie klaargezet bij het SOC. Dat pakketje zal doorgaans persoonsgegevens omvatten.

Inhoud pakketje
Uit welke persoonsgegevens het genoemde pakketje bestaat, wordt bepaald door de gegevens die er op het moment van de match met een IOC over het netwerk gaan. Hierbij zal het doorgaans gaan om IP-adressen, e-mailadressen, URL's en domeinnamen. Het is vooraf onmogelijk om te bepalen welke persoonsgegevens er over het netwerk gaan. Daarom kan een netwerkpakketje fragmenten bevatten van uiteenlopende type informatie. Voorbeelden hiervan zijn e-mailbijlagen, bestanden, metadata van bestanden, documenten, internetverkeer van medewerkers, gegevens van netwerkapplicaties, chatverkeer.

AIVD- en NCSC-sensor
Voor de verwerking van het netwerkverkeer is op de externe router van de Belastingdienst een SPAN-poort gecreëerd waaraan de sensoren worden aangesloten. Op de SPAN-poort wordt een filter geplaatst door de Belastingdienst. Middels dit filter wordt alleen verkeer van en naar de beoogde netwerken (Belastingdienst kantoornetwerk, Belastingdienst WiFi netwerk, inclusief BYOD en Gasten en het Open Internet netwerk) zichtbaar in de sensor. Dit filter wordt door de Belastingdienst beheerd. De AIVD en NCSC hebben geen toegang tot dit filter. Op de plek waar de sensoren worden geplaatst, is er geen zicht meer op de originele cliënt IP-adressen van de binnen de Belastingdienst aangesloten systemen. Dit heeft als effect dat de AIVD en het NCSC de match niet meer rechtstreeks kunnen linken aan een systeem binnen de Belastingdienst. Verder zorgt het filter ervoor dat personen die de websites van de Belastingdienst bezoeken niet door de sensoren heen gaan. Hierdoor krijgen de AIVD en het NCSC geen inzage in de aangifte- en toeslagenverkeersstromen. Hierdoor is in de praktijk sprake van dataminimalisatie.

De NCSC-sensoren worden aangesloten op het logmanagement systeem van B/CIE. Een match met een IOC gaat dus automatisch ook naar het logmanagement systeem van B/CIE. Door deze maatregel heeft B/CIE inzage in welke informatie er tussen het NDN en het NCSC wordt uitgewisseld. Bij de AIVD is er vanuit B/CIE een soortgelijke functionele vraag neergelegd. Vooralsnog geldt hetgeen hiervoor is opgemerkt over een automatische link naar het logmanagementsysteem van het SOC (nog) niet voor de AIVD-sensoren.

Match met een IOC en wat nu? De melding.
Op het moment dat een match gesignaleerd wordt, wordt het SOC door de sensor ingelicht. Daarna gaat, na een instelbare periode, een melding van de match naar het NCSC en de AIVD.

In het geval van de NCSC-sensor is deze melding handmatig door de Belastingdienst te stoppen. De melding bevat slechts een hashwaarde van het IP-adres en een tijdstip. Bij het oppikken van een signaal kan het NCSC de bij de match behorende informatie nog niet inzien. De bij de match behorende informatie belandt pas bij NCSC zodra B/CIE zelf heeft kunnen beslissen of deze die informatie met NCSC wil delen.

Voor de AIVD verloopt het proces anders. De AIVD kan de eerder genoemde pakketjes (hashwaarde van het IP-adres en een tijdstip) al op afstand bekijken en analyseren op basis van artikel 6, lid2, sub c (de C-taak) van de Wet op de Inlichtingen- en Veiligheidsdiensten 2002 (Wiv 2002). Dit is de reden dat de AIVD-sensor aan de buitenkant van de Belastingdienst infrastructuur wordt geplaatst, omdat het beleid van de Belastingdienst niet toe staat dat er directe verbinding vanaf het internet naar het kantoornetwerk worden opgezet. Een dergelijke verbinding wordt door de Belastingdienst als risicovol bestempeld. De informatie in deze pakketjes is beperkt. Voor aanvullende gegevens en/of verdere analyse wordt contact opgenomen met het SOC. Bij incidenten zal B/CIE zelf de respons verzorgen, al dan niet ondersteund door NCSC of AIVD.

Voor de incidentafhandeling door het SOC zal het standard ITIL-proces worden gebruikt. De melding wordt in de ITSM-tooling geregistreerd als security incident. Als het gaat om integriteitsschending zal het normale proces rond integriteitsschendingen worden gebruikt.

2. Andere specifieke persoonsgegevens?

2a. Is het de bedoeling om gegevens over de financiële of economische situatie van betrokkenen, of andere gegevens die kunnen leiden tot stigmatisering of uitsluiting te verwerken?
Nee.

2b. Is het de bedoeling om gegevens over kwetsbare groepen of personen te verwerken?
Nee.

2c. Is het de bedoeling gebruikersnamen, wachtwoorden en andere inloggegevens te verwerken?
Uit welke persoonsgegevens het netwerkverkeer bestaat, wordt bepaald door de gegevens die er op het moment van de match over het netwerk gaan. Het is niet uit te sluiten dat het hierbij gaat om gebruikersnamen, wachtwoorden of inloggegevens.

2d. Is het de bedoeling om uniek identificerende gegevens, zoals biometrische gegevens, te verwerken?
Nee

2e. Is het de bedoeling om het BSN-nummer, of een ander persoonsgebonden nummer te verwerken?
Nee. Het criterium dat ingegeven wordt als zoekterm in de IOC zal veelal een IP-adres bevatten en daarmee een persoonsgegeven. Het IP-adres dat wordt vermeld in de IOC, is het IP-adres van de potentiële dreiger. In het vervolgonderzoek naar het mogelijk verdachte verkeer zal de systeemeigenaar, net als in de huidige situatie, te maken kunnen krijgen met andere persoonsgegevens dan IP-adressen. Daar kunnen BSN's in voorkomen.

3. Kan van elk van de onder vraag I.1 en vraag I.2 opgevoerde typen persoonsgegevens worden gesteld dat zij beleidsmatig of technisch direct van belang en onontbeerlijk zijn voor het bereiken van de beleidsdoelstelling? Wat zou er precies niet inzichtelijk worden als ervoor wordt gekozen bepaalde gegevens niet te verwerken? Licht per te verwerken persoonsgegeven toe.
Ja. De verwerking beperkt zich tot die persoonsgegevens die in het kader van de detectie technisch noodzakelijk zijn om te komen tot een match met een IOC. Zie ook I.1.

4. Kan als het gaat om gevoelige persoonsgegevens hetzelfde beleidseffect of technisch resultaat worden bereikt op een van de volgende wijzen: (a) door (gecombineerd) gebruik van normale persoonsgegevens, (b) door gebruik van geanonimiseerde of gepseudonimiseerde gegevens?
Nee.

5. In welk breder wettelijk, beleidsmatig of technisch kader wordt het voorziene beleid/databestand/informatiesysteem ontwikkeld en wat voor soort(en) verwerking(en) van persoonsgegevens gaan hiervan deel uitmaken bij het voorziene

traject? Wordt hierbij gebruikt gemaakt van (nieuwe) technologie of informatiesystemen?

Het (beleidsmatig) kader op grond waarvan de Belastingdienst verplicht is te beveiligen, is beschreven in het Handboek Beveiliging Belastingdienst. Specifiek ten aanzien van de verwerking van persoonsgegevens door de Belastingdienst geldt artikel 13 van de Wbp, dat regelt dat 'passende technische en organisatorische maatregelen' moeten worden genomen. Deze zijn uitgewerkt in de richtsnoeren van het CBP voor de beveiliging van persoonsgegevens. NDN is dienstbaar aan de beveiliging van de (persoons)gegevens die verwerkt worden bij de Belastingdienst en maakt gebruik van nieuwe technologie om beter weerstand te kunnen bieden aan digitale dreigingen.

II. Doelbinding, koppeling, kwaliteit en profilering

1. **Hebt u het/de specifieke doel(en) waarvoor u de persoonsgegevens gaat verwerken in detail vastgesteld? Geldt hiervoor één en hetzelfde specifieke doel?**

Het doel van het NDN is om te komen tot een netwerk van samenwerkende publieke en private organisaties uit de kritieke infrastructuur. Het netwerk wordt ondersteund en gefaciliteerd door de AIVD, MIVD en het NCSC. Binnen het netwerk worden detectieactiviteiten uitgevoerd naar digitale dreigingen op basis van hoogwaardige dreigings- en incidenteninformatie. Door als Belastingdienst deel te nemen aan het NDN zal de infrastructuur van de Belastingdienst weerbaarder worden tegen digitale aanvallen.

2. **Gaat het bij het project/systeem om gebruik van nieuwe persoonsgegevens voor een bestaand doel, of bestaande doelen binnen al bestaande systemen? (scenario toevoeging nieuwe persoonsgegevens).**

Het gaat om een bestaand doel. Logging van netwerkverkeer vindt reeds plaats door B/CIE en deze verwerking is gemeld bij [redacted] van het ministerie van Financiën. Het verschil is gelegen in het feit dat er nu persoonsgegevens worden gedeeld met externe partijen, het NCSC en de AIVD.

3. **Gaat het bij het project/systeem om het nastreven van nieuwe/aanvullende doeleinden door bestaande persoonsgegevens, of verzamelingen daarvan, te gebruiken, vergelijken, delen, koppelen of anderszins verder te verwerken? (scenario toevoeging doeleinden). Zo ja, hebben alle personen/instanties/systemen die betrokken zijn bij de verwerking dezelfde doelstelling met de verwerking van de desbetreffende persoonsgegevens of is daarmee spanning mogelijk gelet op hun taak of hun belang? Gelden dezelfde doelen voor het hele proces?**

Er worden geen andere persoonsgegevens verwerkt binnen het NDN dan nu al worden verwerkt binnen de standaard Security Operations tooling die nu al wordt gebruikt. Er zijn nieuwe partijen waar persoonsgegevens aan worden verstrekt te weten het NCSC en de AIVD. Deze partijen gebruiken de persoonsgegevens voor hetzelfde doel als de Belastingdienst. Dat doel is een netwerk van samenwerkende publieke organisaties en private organisaties uit de kritieke infrastructuur die detectieactiviteiten uitvoeren naar digitale dreigingen op basis van hoogwaardige dreigings- en incidenteninformatie die binnen dit netwerk wordt uitgewisseld. Het netwerk wordt hierbij ondersteund en gefaciliteerd door de AIVD, MIVD en het NCSC. Het verschil is dus gelegen in het feit dat de

Belastingdienst het NDN gebruikt om haar eigen infrastructuur weerbaarder te maken tegen digitale aanvallen en dat de AIVD en het NCSC dit voor verschillende organisaties doen.

4. **Indien u positief hebt geantwoord op vragen II.2 of II.3, hoe wordt een dergelijk voorgenomen gebruik (d.w.z. gebruik van nieuwe persoonsgegevens in bestaande systemen of van bestaande persoonsgegevens voor nieuwe doeleinden) gemeld aan: (a) , of (b) het Cbp indien er geen FG is?**

De verwerking zal worden gemeld bij .

5. **Indien u positief geantwoord hebt op vragen II.2 of II.3, welke (nadere) controles op een dergelijk gebruik (d.w.z. gebruik van nieuwe persoonsgegevens in bestaande systemen of van bestaande persoonsgegevens voor nieuwe doeleinden) zijn voorzien?**

Er zal periodiek worden gecontroleerd welke gegevens met het NCSC en de AIVD worden uitgewisseld. Het NCSC en AIVD zullen moeten bewaken en bevorderen dat de persoonsgegevens niet zonder een andere Wbp-toets voor andere doeleinden zullen worden gebruikt. Hiervoor zal nog een controle-opdracht aan de Auditdienst Rijk (AdR) moeten worden verstrekt.

Aanbeveling 1:
Maak een plan van aanpak (of afsprakendocument) tussen B/CIE, NCSC en AIVD met duidelijke proces- en beheersafspraken. Zie ook III.1 hierna.

Aanbeveling 2:
Verstrek een controleopdracht aan de AdR om periodiek de naleving van de Wbp en met name de doelbinding (artikel 7, 8 en 9 Wbp) te controleren.

6. **Welke periodieke en incidentele controles zijn voorzien om de juistheid, nauwkeurigheid en actualiteit van de in het beleidsvoorstel, wetsvoorstel op overheidsICT-systeem verwerkte persoonsgegevens na te gaan?**

Er zal periodiek worden gecontroleerd welke gegevens met het NCSC en de AIVD worden uitgewisseld en of de eisen van doelbinding worden nageleefd. Hiervoor zal nog een opdracht aan de AdR moeten worden verstrekt.

Aanbeveling 2:
Verstrek een controleopdracht aan de AdR om periodiek de naleving van de Wbp en met name de doelbinding (artikel 7, 8 en 9 Wbp) te controleren.

7. **Zullen de verzamelde/verwerkte persoonsgegevens gebruikt worden om het gedrag, de aanwezigheid of de prestaties van mensen in kaart te brengen en/of te beoordelen en/of te voorspellen? Zijn de betrokkenen daarvan op de hoogte? Zijn de gegevens die hiervoor worden gebruikt, afkomstig uit verschillende (eventueel externe) bronnen en zijn zij oorspronkelijk voor andere doelen verzameld?**

Nee. Er is geen sprake van persoonlijke profilering. Dreigingsprofilering vindt wel plaats. Middels de dreigingsprofilering kan beter in kaart worden gebracht waar een bepaald risico wordt gelopen. Het doel is om de Belastingdienst beter te beschermen tegen dreigingen van buitenaf. De medewerkers van de Belastingdienst zijn op de hoogte van het van hen

gewenste gedrag door middel van de internetgedragscode. Andere betrokkenen worden over het NDN geïnformeerd via de openbare websites van de rijksoverheid.

8. **Wordt bij deze analyse/beoordeling/voorspelling gebruik gemaakt van vergelijking van persoonsgegevens die technisch geautomatiseerd is (d.w.z. niet door mensen zelf wordt uitgevoerd)? Zo ja, hoe wordt geregeld dat, indien dit geautomatiseerde proces tot een beoordeling of voorspelling over een bepaalde persoon leidt, hierop pas concrete actie wordt ondernomen na tussenkomst en (tweede) controle van (menselijk) personeel?**

Nee. Een match met een IOC zal nooit zonder tussenkomst van een menselijke beoordeling leiden tot concrete actie.

III. Betrokken instanties/systemen en verantwoordelijkheid

1. **Welke interne en externe instantie(s) en/of systemen is/zijn betrokken bij de voorziene verwerking in elk van de onder I.5 onderscheiden fasen? Welke verstrekkers zijn er en welke ontvangers? Welke bestanden of deelbestanden en welke infrastructuren?**

Organisaties die persoonsgegevens gaan ontvangen zijn AIVD, NCSC en B/CIE. Het NCSC en de AIVD stellen maandelijks ieder afzonderlijk een bevindingenrapportage op. De rapportages worden naar B/CIE gestuurd. Het SOC verwerkt de rapportages in de SOC-rapportage. Alleen direct belanghebbenden binnen B/CIE ontvangen de SOC-rapportage. De SOC-rapportage komt in geaggregeerde vorm terug in de Business Continuity Rapportage (BCR). De bijdrage van het SOC aan de BCR rapportage bevat geen persoonsgegevens.

Er wordt gewerkt met afspraken tussen de genoemde betrokken organisaties (B/CIE, AIVD en NCSC) die zelf verantwoordelijke zijn in de zin van de Wbp. In de eerste fase van het NDN zal er geen centrale omgeving zijn waar de persoonsgegevens worden opgeslagen. Er zal dan ook geen correlatie plaatsvinden over deelnemers van het NDN heen.

Er zullen in het kader van NDN door B/CIE met de AIVD en het NCSC afspraken worden gemaakt of er voldoende waarborgen zijn getroffen betreffende de technische en organisatorische beveiligingsmaatregelen. Deze afspraken zullen worden vastgelegd in een afsprakendocument.

Aanbeveling 1:
Maak een plan van aanpak (of afsprakendocument) tussen B/CIE, NCSC en AIVD met duidelijke proces- en beheersafspraken.

2. **Is (in ieder stadium) duidelijk wie verantwoordelijk is voor de verwerking van de persoonsgegevens? Zo ja, is deze persoon of organisatie daarop voldoende voorbereid en geëquipeerd wat betreft de nodige voorzieningen en maatregelen, waaronder middelen, beleid, taakverdeling, procedures en intern toezicht?**

Ja, zie ook het antwoord op vraag III.1. Bovendien wordt er een netwerkverkeer beperkend filter geplaatst op de SPAN-poort waaraan de sensoren zijn gekoppeld. Middels dit filter wordt alleen verkeer van en naar de beoogde netwerken (Belastingdienst kantoornetwerk,

Belastingdienst WiFi netwerk, inclusief BYOD en Gasten, en het Open Internet netwerk) zichtbaar in de sensoren. Dit filter wordt door de B/CIE beheerd. De AIVD en het NCSC hebben geen toegang tot dit filter. Op de plek waar de sensoren zijn geplaatst, is er geen zicht meer op de originele cliënt IP-adressen van de binnen de Belastingdienst aangesloten systemen. Dit heeft als effect dat de AIVD en het NCSC de match niet meer rechtstreeks kunnen linken aan een systeem binnen de Belastingdienst.

3. **Wie binnen uw organisatie, en elk van de andere betrokken organisaties, krijgen precies toegang tot de persoonsgegevens? Bestaat de kans dat bij het gebruik ervan de gegevens ter beschikking komen van onbevoegden?**

De medewerkers van het SOC hebben toegang tot de persoonsgegevens. Echter, het gaat hier om dezelfde persoonsgegevens die in het kader van de uitvoering van het proces security operations al door het SOC worden gemonitord. De persoonsgegevens kunnen in het kader van NDN ook, in het geval van het NCSC na overdracht door de Belastingdienst, door derden worden ingezien. Dit kan alleen wanneer de Belastingdienst daartoe toestemming voor heeft gegeven. De AIVD heeft inzage in de persoonsgegevens op basis de Wiv 2002. Binnen het NCSC zullen de medewerkers van het 'Monitoring en Response'-team inzage hebben en binnen de AIVD de AIVD-analisten. Zowel voor de AIVD als het NCSC geldt het dat de betrokken medewerkers een geldige AIVD A-Screening hebben.

4. **Geldt voor een of meer van de betrokken instanties een beperking van de mogelijkheid om persoonsgegevens te verwerken als gevolg van geheimhoudingsverplichtingen (in verband met functie/wet)?**

Ja, op grond van artikel 67 van de Algemene wet inzake rijksbelastingen (Awr), artikel 15 van het Communautair douanewetboek (Cdw) en artikel 2:5 van de Algemene wet bestuursrecht (Awb) geldt er een geheimhoudingsplicht voor een ieder die betrokken is bij uitvoering van de belastingwetgeving, douanewetgeving en toeslagenwetgeving. Deze geheimhoudingsplicht kan in een beperkt aantal gevallen worden doorbroken.

Binnen het NDN zijn twee typen sensoren in gebruik. Geheimhoudingsplicht geldt niet voor de persoonsgegevens die door de AIVD-sensor worden verwerkt op grond van artikel 43c, eerste lid, onder b, ten eerste, van de Uitvoeringsregeling Awr (Uitv.reg. Awr). Gelet op het feit dat de signaleringen over het algemeen geen fiscale gegevens zullen bevatten (alleen identificerende persoonsgegevens), is toepassing van de uitzondering voor de AIVD in artikel 43c van de Uitv.reg. Awr niet aan de orde.

Voor de NCSC-sensor geldt dat doorbreking van de geheimhoudingsplicht van artikel 67 van de Awr zou moeten geschieden op basis van een ontheffing (voor de NCSC geldt geen uitzonderingsgrond in 43c van de Uitv.reg. Awr). Het verlenen van een ontheffing is naar verwachting niet nodig om dezelfde reden als ten aanzien van de AIVD is vermeld: de aard van de persoonsgegevens. In het uitzonderlijke individuele geval waarin mogelijk fiscale informatie verstrekt wordt, zal een ontheffing van de geheimhoudingsplicht worden aangevraagd.

Voor gegevens van toeslagen geldt dat deze ingevolge artikel 2:5 van de Awb mogen worden verstrekt, indien uit de taak van het bestuursorgaan de noodzaak tot mededeling voortvloeit. Hiervan is sprake in het onderhavige geval, waar mededeling nodig is voor het

veilig houden van de infrastructuur die van vitaal belang is voor het uitvoeren van de primaire taken van de Belastingdienst.

Ingevolge artikel 1:33 van de Algemene douanewet kan de Douane informatie verstrekken in de daar opgesomde gevallen.

5. **Zijn alle stappen van de verwerking in de zin van soorten gegevens en uitwisselingen, in kaart gebracht of te brengen, zodanig dat daardoor voor de betrokkenen inzichtelijk is bij wie, waarom en hoe de persoonsgegevens worden verwerkt?**

Als het gaat om betrokkenen binnen de Belastingdienst dan zal de centrale ondernemingsraad van de Belastingdienst worden geconsulteerd en gevraagd worden om in te stemmen met deelname aan het NDN. Verder zal worden onderzocht of de Internet Gedragscode moet worden aangepast zodat het NDN een plaats krijgt in de gedragscode. De gedragscode geldt voor alle medewerkers van de Belastingdienst.

Aanbeveling 3:
Informeer en consulteer de medezeggenschap over deelname aan de NDN.

Aanbeveling 4:
Pas de 'Internet gedragscode' waar nodig aan.

Onderzocht wordt of het vermelden van deelname aan het NDN op de webpagina van de Belastingdienst volstaat om aan de personen die via het internet met [medewerkers van] de Belastingdienst communiceren kenbaar te maken dat het inkomende en het uitgaande netwerkverkeer wordt gemonitord in het kader van NDN. De deelname zal dan vermeld worden op www.belastingdienst.nl/security.

In individuele gevallen kan de uitzondering van artikel 43, letter b en e, van de Wbp van toepassing zijn. Daarbij moet opsporing in het licht van detectie worden gezien. Het NDN kan vermoedelijke strafbare feiten detecteren.

Aanbeveling 5:
Pas de tekst op www.belastingdienst.nl/security waar nodig aan.

6. **Zijn er beleid en procedures voorzien voor het creëren en bijhouden van een verzameling van de persoonsgegevens die u wilt gaan gebruiken? Zo ja, hoe vaak en door wie zal de verwerking worden gecontroleerd? Omvat de verzameling een verwerking die namens u wordt uitgevoerd (bijvoorbeeld door een onderaannemer)?**

Ja. De AdR zal controleren en er wordt een plan-do-check-act-cyclus doorlopen op basis van het Handboek Beveiliging Belastingdienst (HBB). De pilot NDN wordt ook gecontroleerd door de AdR. Er zijn geen bewerkers in de zin van de Wbp.

Aanbeveling 6:
Verstrek een controleopdracht aan de AdR om periodiek de naleving van de Wbp en met name de beveiliging conform artikel 13 van de Wbp te controleren.

7. Is er sprake van overdracht van persoonsgegevens naar een (overheids)instantie buiten de EU/EER? Heeft dit land een niveau van gegevensbescherming dat als passend is beoordeeld door een besluit van de Europese Commissie of de Minister van Veiligheid en Justitie? Worden daarbij alle of een gedeelte van de persoonsgegevens doorgegeven?
Nee. De Belastingdienst zal bij het NCSC en de AIVD kenbaar maken dat de persoonsgegevens die afkomstig zijn uit de infrastructuur van de Belastingdienst niet zonder voorafgaande toestemming mogen worden gedeeld met andere organisaties in binnenland en buitenland.

Aanbeveling 7:
Neem op in het afsprakendocument dat de doelbinding uit de Wbp moet worden nageleefd en dat de persoonsgegevens niet zonder voorafgaande toestemming van de Belastingdienst mogen worden verwerkt voor andere doeleinden. Ze mogen dus ook niet verder worden verstrekt zonder medeweten en toestemming van de Belastingdienst.

IV. Beveiliging en bewaring/vernietiging

1. **Is het beleid met betrekking tot gegevensbeveiliging binnen uw organisatie op orde? Zo ja, wie/welke afdeling(en) is/zijn binnen de organisatie verantwoordelijk voor het opstellen, implementeren en handhaven hiervan? Is dit beleid specifiek gericht op gegevensbescherming en gegevensbeveiliging?**

Ja. Verantwoordelijk voor het opstellen van beleid is het directoraat-generaal Belastingdienst. In het Handboek Beveiliging Belastingdienst (HBB) is dit beleid vertaald in concrete acties en stappen om de informatiebeveiliging daadwerkelijk te realiseren. In het HBB deel B staat bijvoorbeeld (*B.1.4. Beleid op informatie-uitwisseling)* dat maatregelen getroffen moeten worden voor detectie. Hier wordt tevens genoemd dat automatische controle plaatsvindt op virussen, trojans en andere malware. B/CIE past dit beleid toe. Voor implementatie van het beleid is het lijnmanagement verantwoordelijk. De leden van het managementteam van de Belastingdienst in de rol van / en van zijn verantwoordelijke voor de naleving van het informatiebeveiligingsbeleid. De en de houden toezicht op de naleving van dit beleid.
Ongeveer 70% van al het e-mailverkeer tussen de Belastingdienst en het internet is versleuteld. Dan zijn de (persoons)gegevens niet zichtbaar voor de AIVD en het NCSC. Het netwerkverkeer tussen medewerkers van de Belastingdienst onderling gaat niet langs de sensoren. Op dit interne netwerkverkeer hebben de AIVD en het NCSC geen zicht. Wanneer een medewerker van de Belastingdienst een website bezoekt die beveiligd is met 'https' zijn de (persoons)gegevens niet zichtbaar voor de AIVD en het NCSC.

2. **Indien (een deel van) de verwerking bij een bewerker plaatsvindt, hoe draagt u zorg voor de gegevensbeveiliging, en het toezicht daarop, bij die bewerker?**

Er zijn geen bewerkers.

3. **Welke technische en organisatorische beveiligingsmaatregelen zijn getroffen ter voorkoming van niet-geautoriseerde of onrechtmatige verwerking/misbruik van (a)**

gegevens die in een geautomatiseerd format staan (bv. wachtwoord-bescherming, versleuteling, encryptie) en (b) gegevens die handmatig zijn opgetekend bv. sloten op kasten)? Is er een hoger beschermingsniveau om gevoelige persoonsgegevens te beveiligen?

De gegevens staan in het datacenter van B/CIE. De Belastingdienst hanteert voor de beveiliging van zijn datacenter zijn eigen normenkader zoals verwoord in het eerder genoemde HBB. Dit handboek is een afgeleide van de ISO27001 en ISO27002 standaard, de BIR en de VIR-BI.

De AIVD en het NCSC zullen voor het uitwisselen van informatie met betrekking tot een match aansluiten bij de reeds bestaande procedures van B/CIE. B/CIE handelt zelf de incidentmelding af, waar nodig met hulp van de AIVD en het NCSC. In het geval van een mogelijke integriteitsschending treedt de procedure voor integriteitsschendingen in werking. Hiervoor heeft de Belastingdienst een eigen procedure ingericht.

De AIVD heeft ingevolge artikel 15 van de Wiv 2002 de wettelijke plicht om zorg te dragen voor de geheimhouding van gegevens en bronnen van gegevens. Het uitlezen van een 'match' met een IOC gebeurt op afstand via een beveiligde (encryptie) verbinding. Indien blijkt dat de overige deelnemers van het NDN gebaat zullen zijn bij het delen van een resultaat van een deelnemer, dan zal hieromtrent overleg plaatsvinden met de Belastingdienst.

Daar waar de AIVD en het NCSC gegevens verwerken, omdat zij een match met bijbehorende informatie (pakketje) te bewerken krijgen, zijn afspraken gemaakt welke personen betrokken zijn bij deze werkzaamheden, wat zij mogen, hoe lang deze informatie bewaard blijft. De controle hierop gebeurt door de AdR en de Commissie van Toezicht betreffende de Inlichtingen- en Veiligheidsdiensten (CTIVD).

De medewerkers van het SOC hebben toegang tot de persoonsgegevens. De persoonsgegevens kunnen in het kader van NDN na tussenkomst van het SOC ook door derden worden ingezien. De AIVD heeft inzage in de persoonsgegevens op basis de Wiv 2002. Binnen het NCSC zullen de medewerkers van het 'Monitoring en Response'-team inzage hebben en binnen de AIVD de AIVD-analisten. Zowel voor de AIVD als het NCSC geldt het dat de betrokken medewerkers een geldige AIVD A-Screening hebben.

Aanbeveling 8:
De autorisatieprofielen zullen regelmatig moeten worden gecontroleerd op actualiteit en de AdR zal de naleving van het beleid hieromtrent moeten toetsen. Dit is onderdeel van de controle op de beveiliging van de verwerking.

4. **Welke procedures bestaan er in geval van inbreuken op beveiligingsvoorschriften, en voor het detecteren ervan? Is er een calamiteitenplan om het gevolg van een onvoorziene gebeurtenis waarbij persoonsgegevens worden blootgesteld aan onrechtmatige verwerking of verlies van persoonsgegevens af te handelen?**

In het geval van datalekken geldt de gangbare procedure (standaard incidentproces). Wanneer het loket melden datalekken operationeel is, zal de Belastingdienst hiervan gebruik maken.

5. **Hoe lang worden de persoonsgegevens bewaard? Geldt dezelfde bewaartermijn voor elk van de typen van verzamelde persoonsgegevens? Is het project onderworpen aan enige wettelijke/sectorale eisen met betrekking tot bewaring?**

De persoonsgegevens (zie I.1) worden 30 dagen bewaard. Deze termijn is overigens instelbaar. Na de 30 dagen worden de persoonsgegevens automatisch verwijderd. Er loopt elk kwartier een proces dat de data ouder dan 30 dagen onomkeerbaar verwijderd. Bij een melding (zie I.2c) kan dit langer zijn. Dan worden gegevens bewaard zo lang het onderzoek loopt. Wanneer het een strafrechtelijk onderzoek betreft, zullen hierover afspraken worden gemaakt met de betrokken Officier van Justitie.

6. **Op welke beleidsmatige en technische gronden is deze termijn van bewaring vereist?**

De termijn van 30 dagen is een initiële waarde. Gedurende het gebruik van NDN kan deze waarde naar beneden of naar boven worden aangepast. Er zal continue worden bijgehouden wat de juiste waarde is van deze parameter.

7. **Welke maatregelen zijn voorzien om de persoonsgegevens na afloop van de bewaartermijn te vernietigen? Worden alle persoonsgegevens, inclusief log-gegevens, vernietigd? Is er controle op de vernietiging, en door wie?**

De AIVD-sensor wordt er op ingesteld dat de gegevens na 30 dagen automatisch worden gewist. Gegevens staan op de harddisk van de detector en kunnen ook eerder dan na 30 dagen worden gewist. AdR wordt gevraagd toe te zien op vernietiging van de nog aanwezige persoonsgegevens in de sensor van het NCSC. Meldingen in de sensor van het NCSC gaan ook gelogd worden in een event monitoring systeem van B/CIE.

Aanbeveling 1:
Maak een plan van aanpak (of afsprakendocument) tussen B/CIE, NCSC en AIVD met duidelijke proces- en beheersafspraken.

V. Transparantie en rechten van betrokkene

1. **Is het doel van het verwerken van de gegevens bij de betrokkenen bekend of kan het bekend gemaakt worden? Wat is de procedure om betrokkenen indien nodig te informeren over het doel van de verwerking van hun persoonsgegevens?**

Ja, de Belastingdienst heeft in de 'Gedragscode voor internet' van 16 augustus 2013 in artikel 2.1 bekend gemaakt aan zijn medewerkers dat alle communicatiestromen worden gescand en gelogd. Wellicht is hier een toevoeging nodig dat het controleren van het netwerkverkeer ook in het kader van NDN plaatsvindt. Onderzocht wordt of het vermelden van deelname aan het NDN op www.belastingdienst.nl volstaat om aan de personen die via het internet communiceren met de Belastingdienst medewerkers kenbaar te maken dat het netwerkverkeer van en naar deze personen wordt bijgehouden in het kader van NDN. Plaatsing zal dan plaatsvinden op de pagina www.belastingdienst.nl/security.

Aanbeveling 9
Pas de tekst op de website zo nodig aan.

2. **Indien u de persoonsgegevens direct van de betrokkenen verkrijgt, hoe stelt u hen van uw identiteit en het doel van de verwerking op de hoogte vóór het moment van verwerking?**

Niet van toepassing.

3. **Indien u de persoonsgegevens via een andere (overheids)organisatie verkrijgt, hoe zullen de betrokkenen van uw identiteit en het doel van de verwerking op de hoogte worden gesteld op het moment van verwerking?**

Niet van toepassing.

4. **Indien u toestemming tot verwerking van persoonsgegevens aan de betrokkene vraagt (opt-in), kan de betrokkene deze toestemming dan op een later tijdstip weer intrekken (opt-out)? Bij een weigering toestemming te geven, of bij een dergelijke intrekking, wat is dan de implicatie voor de betrokkene?**

Niet van toepassing.

5. **Via welke procedure hebben betrokkenen de mogelijkheid zich tot de verantwoordelijke te wenden met het verzoek hen mede te delen of hun persoonsgegevens worden verwerkt? Hoe worden derden, die mogelijk bedenkingen hebben tegen een dergelijke mededeling, in de gelegenheid gesteld hun zienswijze te geven?**

Informatie over de verwerking van persoonsgegevens door de Belastingdienst is te vinden op www.rijksoverheid.nl en www.belastingdienst.nl.[1]

6. **Hoe kan een verzoek van een betrokkene tot verbetering, aanvulling, verwijdering of afscherming van persoonsgegevens in behandeling worden genomen?**

Informatie over de behandeling van een verzoek tot verbetering, aanvulling, verwijdering of afscherming van persoonsgegevens door de Belastingdienst is te vinden op www.rijksoverheid.nl en op www.belastingdienst.nl.[2]

[1] http://download.belastingdienst.nl/belastingdienst/docs/belastingdienst_wet_bescherming_persoonsgegevens_al5331z2pl.pdf
[2] http://www.rijksoverheid.nl/ministeries/fin/organisatie/meldingenregister

Samenvatting van de eerder gesignaleerde risico's en aanbevelingen

In het kader van de aansluiting van de Belastingdienst op NDN is deze Privacy Impact Assessment (PIA) uitgevoerd. Daarbij zijn voornoemde rijksbrede PIA en de daaruit voortvloeiende risico's als startpunt gebruikt. Hierna zullen de oorspronkelijke risico's uit de eerdere PIA worden samengevat. Er zijn aanbevelingen in de tekst gedaan waar dat nodig is. Deze aanbevelingen zullen zijn gericht op het mitigeren van mogelijke Wbp-risico's. Kortheidshalve wordt hieronder verwezen naar de tekst in de PIA.

1. Het moet duidelijk zijn welke bevoegdheden de AIVD heeft vanuit de WIV.
   Zie onder I.1 en III.3.
2. Wie de verantwoordelijke is voor de onderhavige verwerkingen van persoonsgegevens moet duidelijk zijn.
   Zie onder I.1 en III.1.
3. Als er bewerkers zijn dan moeten solide overeenkomsten worden gesloten.
   Er zijn geen bewerkers. Het is een samenwerking tussen verantwoordelijken. Zie onder andere III.3.
4. Er moet meer aandacht komen voor de transparantie over deze verwerkingen.
   Zie onder III.5, V.5 en V.6.
5. Er moet duidelijker worden welke rechten betrokkenen hebben.
   Zie onder V.5 en V.6.
6. De aard van de persoonsgegevens moet duidelijker naar voren komen.
   Zie onder I.1.
7. De noodzaak van (aansluiting bij) NDN moet voldoende worden aangetoond.
   De noodzaak wordt duidelijk gemaakt in de inleiding en onder I.1.
8. Het beveiligingsbeleid moet worden nageleefd en hier moet controle op zijn.
   Zie onder I.5, II.5 en II.6, III.1 en III.6 en IV.
9. Doelbinding moet gewaarborgd zijn zodat function-creep geen kans krijgt.
   Zie onder II.5 en II.6.
10. De toezichtrol van [redacted] of het Cbp mag worden benoemd.
    Zie onder II.4.

Belastingdienst

memo

Beantwoording vragen MT-BD d.d. 27-10-2014

Belastingdienst/CIE
Security Operations Center

Laan van Westenenk 490-492
7334 DS Apeldoorn
Postbus 9050
7300 GM Apeldoorn

Datum
29-01-2015

Versienummer
1

Auteur

Kopie aan

Bijlagen
Geen

Afgelopen maandag d.d. 27 oktober 2014 is de aansluiting van de Belastingdienst op het Nationaal Detectie Netwerk besproken. Vanuit het MT-BD zijn er een aantal aanvullende vragen. Verder zijn er door [redacted] een aantal vragen gesteld.

Doel van deze memo is het antwoord geven op de gestelde vragen.

Vragen MT-BD:
Privacy-aspecten: wie is betrokken geweest bij het opstellen vh memo, voorbeelden:

1. Vraag: [redacted]?
   Antwoord: [redacted] *is betrokken geweest bij de totstandkoming van de PIA. En heeft de PIA verder aangescherpt. Daarna is de PIA nog door* [redacted] *beoordeeld. Haar op- en aanmerkingen zijn verwerkt.*
2. Vraag: [redacted] van DG/Bel, zij is betrokken bij bredere beweging over gegevensuitwisseling [[redacted] heeft haar al benaderd].
   Antwoord: [redacted] *heeft inmiddels input geleverd op de PIA. Haar input is verwerkt in de PIA.*
3. Vraag: Is het integraal genoeg bekeken/aangevlogen.
   Antwoord: Zowel van het oogpunt van privacy, techniek en personele consequenties is er naar het NDN gekeken. Privacy en personele consequenties maken deel uit van de PIA. Voor de techniek zal er een ontwerp door B/CIE worden gemaakt. Het gaat hier alleen over de aansluiting van de Belastingdienst op het NDN. Dus niet het ontwerp van het NDN.

Communicatie:

1. Vraag: Wat als bekend wordt dat AIVD alle uitgaande mail van de BD leest communicatie richting medewerkers.
   Antwoord: Ten eerste de AIVD kan de mail tussen Belastingdienst medewerkers onderling niet lezen. Dit omdat deze mailstromen niet door de sensoren heen gaat. Verder is ongeveer 70% van het uitgaande en inkomende mailverkeer versleuteld. Dit betekent dat de AIVD deze mailstromen niet kan inzien. De Belastingdienst biedt aan een ieder die met de Belastingdienst mail wil uitwisselen versleutelde mail aan. Het is aan de externe partij, zowel in de rol als verzender of ontvanger om de mail aan de Belastingdienst te versleutelen. Tevens is er in het verleden aan gedragscode opgesteld voor Internet gebruik waar in staat dat alle verkeersstromen worden gelogd en gescanned.

Diversen:

1. Vraag: kosten aan verbonden [antwoord [redacted]: nauwelijks].
   Antwoord: De Belastingdienst draagt alleen de kosten van housing en menskracht (ontwerp en exploitatie). De investeringen worden door het NCSC en de AIVD gedragen.
2. Vraag: waarom vooral op uitgaande stromen [antwoord [redacted]: ivm analyse]
   Antwoord: De Indicators of Compromise (IOC) die worden gebruikt binnen het NDN zijn vooral van toepassing op externe IP adressen en dreigingen.
3. Vraag: wat is voordeel [dreigingsanalyse/spionage].

Antwoord: Vanuit het NDN krijgt de Belastingdienst andere dreigingsinformatie die zij niet vanuit de commerciële systemen die al binnen de Belastingdienst in gebruik zijn.

4. Vraag: waarom geen relatie naar fraude [gaat om gedachte, waar dubbelt dit vraagstuk met andere discussies,
   Antwoord: De informatie die uit het NDN komt kan worden gebruikt binnen het fraudeonderzoek. Echter daar is het initieel niet voor bedoeld. Onderzoek zal moeten uitwijzen of het NDN ook voor fraudeonderzoek kan worden gebruikt.
5. Vraag: tav van fraude zal het vermoedelijk niet proportioneel zijn gegevens te gebruiken voor andere doelen dan waarvoor verzamelt].
   Antwoord: Klopt. Proportionaliteit zal onderdeel van het onderzoek moeten zijn.

Vragen :

1. Vraag: Uit het stuk wordt niet helemaal helder hoe de detectie in zijn werk gaat. Wie signaleert nu primair (AIVD, NCSC of BD zelf) en wie doet het vervolg (idem)? Absolute helderheid daaromtrent is van belang om goed te kunnen bepalen wie verantwoordelijke en bewerker is in de zin van de Wbp. Daar worden nu wel uitspraken over gedaan, maar ik heb daar een ander idee bij (mi. zijn AIVD en NCSC sowieso verantwoordelijke, geen bewerker).
   Antwoord: Deze vraag is beantwoord in de nieuwe versie van de PIA.

2. Vraag: Vervolgvraag is wat voor het NCSC de basis is om persoonsgegevens te verwerken. Voor de AIVD is dit wel helder, daarvoor is een expliciete wettelijke basis aanwezig. De NCSC hangt echter onder de NCTV, die alleen berust op een (verouderde) instellingsregeling van de Minister van Justitie. Dat is een organisatieregeling, geen formeelwettelijke grondslag voor gegevensverwerking (zoals de Wbp vereist). Tegen hetzelfde hiaat in juridische basis lopen we ook steeds op bij Logius als beheerder van MijnOverheid. Mi. zou hier nog goed naar gekeken moeten worden voor we gegevens gaan leveren aan het NDN, omdat we anders alsnog het risico lopen van gegevensuitwisseling in strijd met de wet.
   Antwoord: Deze vraag is beantwoord in de nieuwe versie van de PIA.

3. Vraag: Ook niet duidelijk is wat precies met de signaleringen gebeurt in het vervolgtraject, en in welk mate dan nog persoonsgegevens worden verwerkt. De waarde van het netwerk lijkt mij het delen van de signalen, zodat andere organisaties op de hoogte zijn van dreigingen en maatregelen kunnen nemen om schade te voorkomen. Dat impliceert dat ook met andere dan de in de stukken genoemde organisaties informatie wordt uitgewisseld (de stukken zijn hier niet duidelijk over). Zijn daar persoonsgegevens bij, en wat is dan de basis voor uitwisseling?
   Antwoord: De Belastingdienst bepaald of de signaleringen met derden mogen worden gedeeld. Dit is beschreven in de PIA.

4. Vraag: Er wordt gesproken over controle/periodieke toetsing door de ADR, maar niet duidelijk wordt waar de ADR aan toetst (is er een concrete lijst met gegevens die worden uitgewisseld, aan de hand waarvan de ADR kan controleren of bij de detecties binnen de gestelde kaders is gebleven?).

Antwoord: In de PIA is deze vraag benoemd. Dit is een van de aanbevelingen die benoemd is in de PIA.

5. Vraag: Er wordt gesproken over de noodzaak om een ontheffing van de geheimhoudingsplicht ex 67 Awr te verstrekken aan het NCSC. Is dat al in gang gezet?
   Antwoord: In de PIA is opgenomen op welke wettelijke basis informatie met het NCSC mag worden gedeeld.

6. Vraag: PIA en opleggers zijn niet eenduidig in de scope van de detectie (alleen verkeer vanuit de BD, of alle verkeer van en naar de BD) en over de verantwoordelijkheid voor beheer van de sensoren (bij AIVD of geheel bij de BD?).
   Antwoord: Alleen het netwerkverkeer vanuit de vier netwerken (WiFi-Gasten, WiFi-BYOD, WiFi-Intern en Belastingdienst interne netwerk) wordt gebruikt binnen het NDN. Het netwerkverkeer tussen de belastingplichtige en de fiscale systemen van de Belastingdienst worden NIET gebruikt binnen het NDN. Hiervoor is een maatregel getroffen. Verder is de PIA op dit punt aangescherpt.

7. Vraag: Verder heb ik nog wat detailopmerkingen bij mn. de PIA. Ik denk dat het goed zou zijn om nog een slag op de stukken te maken, iig. voor ze naar de COR gaan. In deze vorm zullen ze waarschijnlijk tot veel vragen over de gevolgen voor BD-medewerkers leiden.
   Antwoord: De PIA is op deze punten aangescherpt nav een discussie tussen [ ] *en* [ ].

Meldingenformulier als bedoeld in de Regeling Wet bescherming persoonsgegevens ministerie van Financiën

Datum: **2015-01-26**

1. Welke naam heeft het gegevensbestand?

   Het gaat niet om een gegevensbestand. De melding heeft betrekking op de deelname van de Belastingdienst aan het Nationaal Detectie Netwerk

2. Waarvoor worden de gegevens verzameld en gebruikt
   (de doelen van het gegevensbestand)?

   Het doel van het NDN is om te komen tot een netwerk van samenwerkende publieke en private organisaties uit de kritieke infrastructuur. Het netwerk wordt ondersteund en gefaciliteerd door de AIVD, MIVD en het NCSC. Binnen het netwerk worden detectieactiviteiten uitgevoerd naar digitale dreigingen op basis van hoogwaardige dreigings- en incidenteninformatie. Door als Belastingdienst deel te nemen aan het NDN zal de infrastructuur van de Belastingdienst weerbaarder worden tegen digitale aanvallen.

3. Over wie worden gegevens verwerkt en welke soorten van gegevens zijn dat?

   Er worden geen andere persoonsgegevens verwerkt binnen het NDN dan nu al worden verwerkt binnen de standaard Security Operations tooling die nu al wordt gebruikt. Er zijn nieuwe partijen waar persoonsgegevens aan worden verstrekt te weten het NCSC en de AIVD. Deze partijen gebruiken de persoonsgegevens voor hetzelfde doel als de Belastingdienst. De gegevens kunnen persoonsgegevens bevatten van Belastingdienst medewerkers en mogelijk ook belastingplichtigen wanneer de Belastingdienst medewerker met deze belastingplichtige een e-mail uitwisseling tot stand brengt. Echter ongeveer 70% van het e-mail verkeer is versleuteld waardoor de persoonsgegevens niet meer zichtbaar zijn. De typen persoonsgegevens die worden verwerkt, zijn variabel. Dit zal hieronder worden toegelicht.

   Al het digitale netwerkverkeer wordt getoetst aan de digitale patronen van digitale aanvallen. Dit is vergelijkbaar met netwerkcomponenten als firewalls, anti-spam en anti-malware oplossingen, zoals deze ook al worden gebruikt door B/CIE. Op het moment dat er een match is met een IOC die duidt op een digitale aanval, wordt hier een melding van gemaakt aan het SOC. Dit stukje netwerkverkeer wordt op de server, die bij B/CIE geplaatst is, voor een beperkte periode van 30 dagen opgeslagen. We kunnen hier spreken van pakketjes informatie rondom de match. Al het andere netwerkverkeer wordt niet opgeslagen. Uit welke persoonsgegevens het netwerkverkeer bestaat, wordt bepaald door de gegevens die er op het moment van de match over het netwerk gaan. Het is niet uit te sluiten dat het hierbij gaat om gebruikersnamen, wachtwoorden of inloggegevens.

4. Aan wie worden gegevens verstrekt?

Organisaties die persoonsgegevens gaan ontvangen zijn AIVD, NCSC. De persoonsgegevens kunnen in het kader van NDN ook, in het geval van het NCSC na overdracht door de Belastingdienst, door derden worden ingezien. Dit kan alleen wanneer de Belastingdienst daartoe toestemming voor heeft gegeven. De AIVD heeft inzage in de persoonsgegevens op basis de Wiv 2002. Verder zal de Belastingdienst bij het NCSC en de AIVD kenbaar maken dat de persoonsgegevens die afkomstig zijn uit de infrastructuur van de Belastingdienst niet zonder voorafgaande toestemming mogen worden gedeeld met andere organisaties in binnenland en buitenland.

5. Wie is de Wbp-beheerder van het gegevensbestand?

In het kader van de Wbp is Belastingdienst de verantwoordelijke voor de aansluiting van de Belastingdienst op het NDN; de Belastingdienst/Centrum voor infrastructuur en exploitatie (B/CIE) is de beheerder. Het SOC voert de werkzaamheden feitelijk uit.

6. Zijn er bewerkers ingeschakeld i.o.v. de verantwoordelijke?

Nee, er zijn geen bewerkers in de zin van de Wbp.

7. Eventuele bijzonderheden

Geen bijzonderheden

8. Wie is de contactpersoon voor vragen of het uitoefenen van rechten zoals kennisneming of correctie?

, **Security Operations Center – Belastingdienst/Centrum voor Infrastructuur en Exploitatie**

9. Wordt ten aanzien van de beveiliging van de gegevens voldaan aan het beveiligingsbeleid?

Ja. Verantwoordelijk voor het opstellen van beleid is het directoraat-generaal Belastingdienst. In het Handboek Beveiliging Belastingdienst (HBB) is dit beleid vertaald in concrete acties en stappen om de informatiebeveiliging daadwerkelijk te realiseren. In het HBB deel B staat bijvoorbeeld (*B.1.4. Beleid op informatie-uitwisseling)* dat maatregelen getroffen moeten worden voor detectie. Hier wordt tevens genoemd dat automatische controle plaatsvindt op virussen, trojans en andere malware. B/CIE past dit beleid toe. Voor implementatie van het beleid is het lijnmanagement verantwoordelijk. De leden van het managementteam van de Belastingdienst in de rol van / ( ) en van ( ) zijn verantwoordelijke voor de naleving van het informatiebeveiligingsbeleid. en de houden toezicht op de naleving van dit beleid.

10. Geeft u bij uw gegevensverwerking persoonsgegevens door naar een of meer landen buiten de Europese Unie?

Nee. De Belastingdienst zal bij het NCSC en de AIVD kenbaar maken dat de persoonsgegevens die afkomstig zijn uit de infrastructuur van de Belastingdienst niet zonder voorafgaande toestemming mogen worden gedeeld met andere organisaties in binnenland en buitenland.

Nationaal Detectie Netwerk (NDN)

Nederland digitaal veiliger door beter en sneller informatie over dreigingen en risico's te delen

Cyberincidenten die zich de afgelopen paar jaar hebben voorgedaan laten zien hoe kwetsbaar de Nederlandse samenleving is als gevolg van de steeds verder toenemende digitalisering. Het verhogen van de digitale weerbaarheid van Nederland is dus van groot belang. Naar aanleiding van de toezegging van minister Opstelten in de Tweede Kamer in 2012 en met de vaststelling van de tweede Nationale Cyber Security Strategie in 2013 is daarom besloten tot het uitwerken van een integrale aanpak van cyberdreigingen. Binnen deze aanpak wordt het Nationaal Detectie Netwerk (NDN) vormgegeven.

Wat is het?

Het NDN is een samenwerking voor het beter en sneller waarnemen van digitale gevaren en risico's. Door het delen van dreigingsinformatie kunnen partijen vanuit de eigen verantwoordelijkheid tijdig gepaste maatregelen nemen om mogelijke schade te beperken of voorkomen. Het NDN moet zorgen voor het beter en sneller waarnemen van digitale dreigingen en aanvallen. Zo werken we samen aan de digitale weerbaarheid van Nederland.

Twee sporen

Onder verantwoordelijkheid van het ministerie van Veiligheid en Justitie werken NCSC, AIVD, MIVD en het Directoraat-Generaal Organisatie en Bedrijfsvoering Rijk (BZK) samen in het NDN. Het NDN wordt verder versterkt met organisaties uit de vitale sectoren, ICT-dienstverleners, belangengroeperingen en verschillende publieke, private en publiek-private samenwerkingsverbanden. De inrichting van het NDN gebeurt langs twee sporen. Binnen de Rijksoverheid worden in 2014 ervaringen opgedaan middels een pilot. Hierbij is bijzonder aandacht voor de invloed op de privacy en medezeggenschap. Het andere spoor betreft de inrichting van het NDN met de private organisaties uit de vitale sectoren. In 2014 wordt gezamenlijk gewerkt aan het uitwerken van juridische en bestuurlijke vraagstukken, en onderwerpen op het gebied van techniek, informatie, proces en organisatie. De resultaten van beide sporen zorgen er voor dat er een samenwerkingsnetwerk ontstaat waarbinnen informatie over cyberdreigingen en risico's uitgewisseld kan worden.

Hoe werkt het?

De Nederlandse inlichtingen- en veiligheidsdiensten (AIVD/MIVD) en het Nationaal Cyber Security Centrum (NCSC) stellen informatie over dreigingen en aanvallen beschikbaar voor organisaties uit de Rijksoverheid, vitale sectoren en voor toeleveranciers van Defensie. Het NDN bestaat uit drie onderdelen.

1. Het verzamelen van dreigingsinformatie: NCSC en AIVD/MIVD verzamelen informatie over belangrijke, actuele dreigingen en vormen dit om tot bruikbare indicatoren. Ook andere deelnemende organisaties kunnen indicatoren inbrengen.
2. Informatie beschikbaar stellen: NCSC en AIVD/MIVD stellen indicatoren op gestandaardiseerde en geautomatiseerde wijze beschikbaar aan de deelnemers van het NDN. Deze kunnen vervolgens zelf vaststellen of ze te maken hebben met een digitale aanval en passende tegenmaatregelen nemen.
3. Terugkoppeling: door de informatie over verschillende aanvallen te combineren kan er een geanonimiseerd en rijker beeld worden opgeleverd voor alle deelnemers. Een aanval bij de een wordt hiermee een vroegtijdige waarschuwing voor de ander.

Planning

In 2013 zijn waarborgen voor privacy en medezeggenschap ingevoerd ter voorbereiding op de eerste overheidspilot. Daarnaast is begonnen met de voorbereidingen voor deelname van een Rijksbrede vertegenwoordiging in het NDN. Ook zijn in 2013 organisaties uit vitale sectoren geïnformeerd over het NDN initiatief. In 2014 wordt, samen met de vitale sectoren, een nadere invulling gegeven aan de voorwaarden voor samenwerking, en wordt toegewerkt naar een start van het NDN aan het eind van dit jaar. Hierbij worden ook dienstverleners en kennisorganisaties gevraagd te participeren en hun kennis en expertise in te zetten. In 2014 wordt de opbouwfase van het NDN afgerond. In de periode na 2014 wordt het NDN verder uitgebouwd binnen de Rijksoverheid en vitale sectoren.

Waarom meedoen?

Door deel te nemen aan het NDN werkt een organisatie mee aan de weerbaarheidsverhoging door vroegtijdige detectie. Immers, we hebben allemaal een rol in het digitaal veilig houden van Nederland. Daarnaast kan het NDN helpen voorkomen dat lokale uitbraken een sector overstijgende impact krijgen. Het NDN levert daarnaast een uniek, breed en gemeenschappelijk beeld van cyberdreigingen en incidenten in Nederland. Door te delen met zoveel mogelijk deelnemers, krijgen we een actuele en versterkte situational awareness van de BV Nederland.

Netwerken

Het NDN is onderdeel van de netwerkbenadering van het NCSC, waarbij intensieve samenwerking met publieke en private partners het uitgangspunt is. Naast het NDN wordt ook het Nationaal Respons Netwerk (NRN) en het Nationaal Expertise Netwerk Cybersecurity (NENCys) ingericht. Het NRN heeft als doel de gezamenlijke respons op cybersecurity-incidenten te versterken. Met NENCys wil het NCSC verschillende inhoudelijke expertises rond cybersecurity samenbrengen.

Contact

Heeft u vragen over het Nationaal Detectie Netwerk of een van de andere netwerkinitiatieven? Wij zijn bereikbaar via telefoon 070-888 7555 (tijdens kantooruren) of per e-mail: info@ncsc.nl.
Meer informatie over de digitale dreigingen en risico's in Nederland, vindt u ook op de websites van NCSC (www.ncsc.nl), AIVD (https://www.aivd.nl/onderwerpen/cyberdreiging/) en MIVD (http://www.defensie.nl/onderwerpen/cyber-security).

Belastingdienst

memo

Managementrapportage Belastingdienst 2015

Apeldoorn
Afdeling B/CA UCA

Tiberdreef 12 t/m 24
3561 GG UTRECHT

Postbus 9799
3506 GT Utrecht

Datum
13 februari 2015

Versienummer
1.0

Auteur

Bijlagen
1

Aan: CFO's Belastingdienst

Bij dezen biedt [ ] u de 'Managementrapportage Belastingdienst'-MRB - versie 1.0 aan. De verschijningsfrequentie is maandelijks. In hoofdstuk 1 zijn de aandachtspunten opgenomen.

Graag legt de [ ] aan het MT-Belastingdienst en aan [ ] van de bedrijfsonderdelen de volgende vragen voor:

1. Herkent u zich in de aandachtspunten, genoemd in hoofdstuk 1?
2. Zijn er andere onderwerpen die aandacht zouden moeten krijgen?
3. Zijn er punten die vragen om nader onderzoek?

De MRB zal op het MT-Belastingdienst van 16 februari 2015 worden geagendeerd.

Belastingdienst

2015

Managementrapportage Belastingdienst

januari

Belastingdienst

B/CA-UCA

Inhoudsopgave

1.0 Aandachtspunten ... 2
1.1 Algemeen overzicht ... 2
1.2 Aandachtspunten ... 2
2.0 Geldstromen belastingmiddelen en toeslagen ... 4
2.1 Belasting- en premieontvangsten ... 4
2.2 Toeslagen ... 6
3.0 Dienstverlening ... 7
3.1 Telefonie ... 7
3.2 Balie ... 8
3.3 Internet ... 8
4.0 Centrale concernprocessen ... 9
4.1 Volumes klant tot klantprocessen ... 9
4.2 Kwaliteit klant tot klantprocessen ... 11
5.0 Lokale kantoorprocessen ... 12
5.1 Bezwaarschriften ... 12
5.2 Klachten ... 13
6.0 Toezicht en opsporing ... 15
6.1 Belastingen ... 15
6.2 Douane ... 17
6.3 Toeslagen ... 17
6.4 FIOD ... 18
7.0 Incasso ... 19
7.1 Achterstand invordering ... 19
8.0 IV-aanbod ... 20
9.0 Personeel en organisatie ... 21
9.1 Formatie en bezetting ... 21
9.2 In- en uitstroom ... 21
9.3 Leidinggeven (functioneringsgesprekken) ... 22
9.4 Inzetbaarheid ... 22
10.0 Middelen ... 24

1910997 01746

1.0 Aandachtspunten

1.1 Algemeen overzicht

Proces overzicht	bedrijfs-onderdeel	resultaat	trend	*prognose*
Geldstromen belastingmiddelen				
belasting- en premieontvangsten		●	⇨	●
Dienstverlening				
telefonie		●	⇩	
waarvan SMART belafspraken				
internet		●	⇩	●
waarvan informatiesystemen (Douane)		●	⇧	●
waarvan internetdiensten en sites		●	⇩	●
Centrale concernprocessen				
volumes klant tot klant processen		●		
kwaliteit klant tot klant processen		●		
Lokale kantoorprocessen				
bezwaarschriften		●	⇩	●
klachten		●	⇧	
Toezicht en opsporing				
horizontaal toezicht	Belastingen	●	⇨	●
actuele handhavingsvormen	Belastingen	●	⇨	●
horizontaal toezicht	Douane	●	⇨	●
actuele handhavingsvormen	Douane	●	⇨	●
verdeling opsporingscapaciteit	Fiod	●	⇨	●
processen-verbaal	Fiod	●	⇨	●
Incasso				
betalingsachterstand		●	⇨	●
Personeel en organisatie				
functioneringsgesprekken		●	⇨	
ziekteverzuim		●	⇩	●
Middelen				
budget/ uitgaven				
inhuur/ uitzendkrachten		●	⇨	●
⇧ = *positieve ontwikkeling in de realisatie*				

1.2 Aandachtspunten

Bij het opstellen van de rapportage zijn nog niet bij alle pi's definitieve normen of maandplanningen bekend. Dit vanwege het nog grotendeels niet vastgesteld zijn van de stuurcontracten. De genoemde normen zijn indicatief.

1.2.1 Dienstverlening

Bereikbaarheid (grafiek 3.1)

Het geplande aantal calls is afgedaan. Hierbij is een bereikbaarheid gerealiseerd van 79,3%. Dat is nagenoeg de beoogde ondergrens. De BelTel stuurt als gevolg van de financiële situatie zo scherp mogelijk op het realiseren van de geplande calls binnen de norm. De planning is dermate scherp dat er binnen de poolomvang weinig tot geen ruimte is om plotselinge pieken volledig op te vangen. In januari is zo scherp gestuurd dat de financiële besteding zelfs iets lager uitkwam dan gepland. Daarnaast moet worden meegenomen dat de bereikbaarheid negatief wordt beïnvloedt door bellers die binnen het menuproces ophangen. Sinds bellers in het menu hun BSN-nummer moeten intoetsen stijgt het aantal afgebroken gesprekken van ca. 3% naar ca. 8%.

Beschikbaarheid internetdiensten en sites (tabel 3.2)

In januari was de beschikbaarheid van het persoonlijk domein 97,9%. Oorzaken zijn verstoringen bij een netwerkaanpassing en bij het plaatsen van nieuwe hardware. Daarnaast was er een verstoring in de infrastructuur waarvan de oorzaak nog niet is gevonden. Er vindt onderzoek plaats onder regie van

1.2.2 Centrale concernprocessen

Openstaande of aangehouden uitbetalingen wegens rekeningnummer

Per januari 2015 is de tenaamstellingsverplichting voor de omzetbelasting in het kader van de 'een-bankrekeningmaatregel' vervallen. De eenbankrekeningmaatregel geldt dan uitsluitend nog voor de inkomstenbelasting en toeslagen. Voor de openstaande of aangehouden uitbetalingen wegens rekeningnummer is een nieuwe opzet van de tabel en grafiek voorgesteld. Vanaf de februari-rapportage zullen de nieuwe tabellen en grafieken weer worden opgenomen.

1.2.3 Lokale kantoorprocessen

Bezwaar – afdoeningsresultaat (grafiek 5.1)

De norm is aangepast naar 90-95%. Het cumulatieve percentage van het concern is 84,1%. De score wordt met name veroorzaakt door Belastingen en B/CA. Bij Belastingen is de maandscore 82,5% en bij B/CA 85,9%.

Bezwaar – voorraad (tabel 5.1)

Belastingen

De voorraad groeit met 6000 verder door naar 140.000 posten. Met een Awb-percentage van 75,3% betekent het dat er nu bijna 35.000 bezwaren 'te oud' zijn.

Toeslagen

Bij Toeslagen stabiliseert de voorraad op bijna 31.000 en daalt de Awb-houdbaarheid naar 87%. Ingekomen bezwaren worden in veel gevallen verdaagd. UCA adviseert om terughoudend gebruik te maken van het verruimde gebruik van beslistermijnen en de burger snel duidelijkheid te bieden waar ze in financiële zin aan toe zijn.

Klachten – voorraad (tabel 5.3)

De totale geschatte voorraad is ongeveer 1300 klachten. In het systeem staan aantallen die niet betrouwbaar worden geacht. Aan een oplossing wordt gewerkt.

1.2.4 Toezicht en opsporing (Douane)

EU controles

De score is 40%. Bij drie van de zeven verordeningen is niet voldaan aan de opnameverplichting. Een uitgebreide procesanalyse naar de oorzaak vindt bij Douane momenteel plaats.

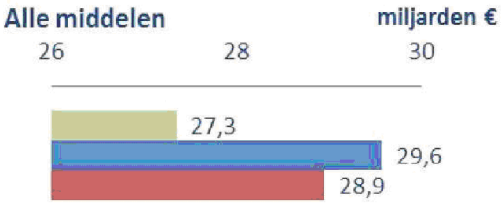
2.0 Geldstromen belastingmiddelen en toeslagen

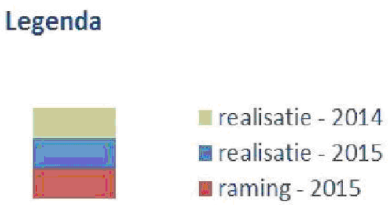
2.1 Belasting- en premieontvangsten

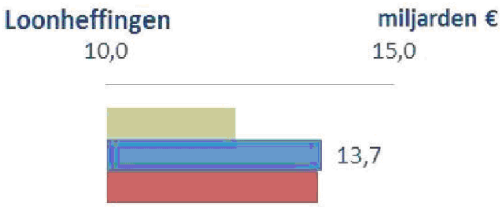
Grafiek 2.1 Belastingen en premies - gebruikte ramingen (jaartotalen)

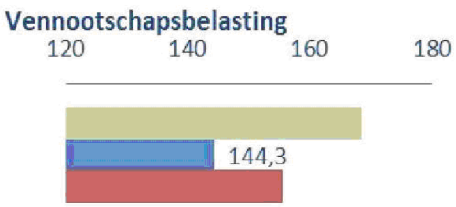


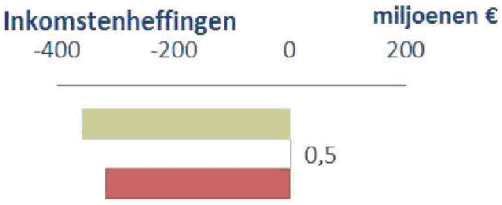
Grafiek 2.2 Belastingen en premies - realisatie (cumulatief)

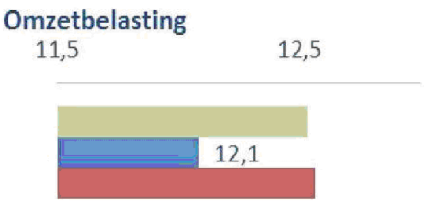


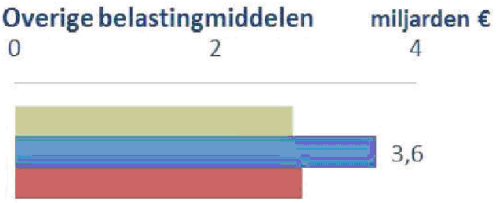












Tabel 2.1

Verschil realisatie 2015	verschil t.o.v. raming		verschil t.o.v. realisatie 2014	
	€	%	€	%
Loonheffingen	58,5	0,4%	1495,5	12,2%
Vennootschapsbelasting	-11,2	7,2%	-24,2	14,4%
Inkomstenheffingen	318,1	100,1%	357,8	100,1%
Omzetbelasting	-479,6	3,8%	-447,0	3,6%
Overige belastingmiddelen	738,4	25,7%	844,6	30,6%

bedragen x € 1 miljoen

Grafiek 2.3 Belastingen en premies - cumulatief verschil per middel



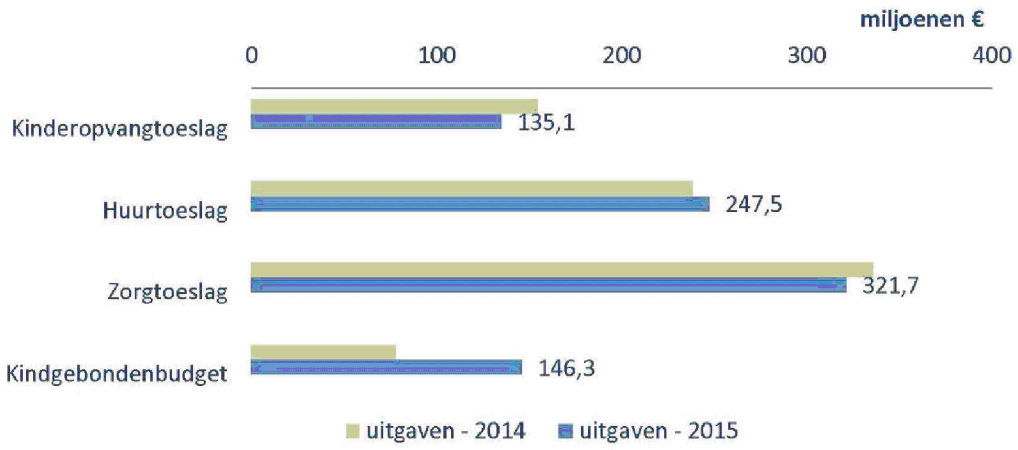
Omzetbelasting en loonbelasting
De ontvangsten in januari zijn altijd hoger dan gemiddeld, vanwege de kwartaalaangiften OB over eind 2014. Vooral op de laatste dagen van de maand zijn de ontvangsten hoog. De laatste betaaldag van januari viel in het weekend, waardoor er meer betalingen in de eerste dagen van februari (te laat) binnenkomen. De bijschrijvingen op de eerste twee werkdagen in februari zijn € 301 miljoen hoger dan normaal. De grootste verschillen treden op bij de omzetbelasting en de loonheffingen (beide € 115 miljoen). Echter, voor de omzetbelasting verklaart dat niet het hele verschil tussen opbrengst en raming. Er is nog onvoldoende cijfermateriaal beschikbaar om daar nu een uitspraak over te kunnen doen.

Inkomensheffing
De ontvangsten en uitgaven voor de inkomensheffing houden elkaar in januari in evenwicht: de realisatie is (afgerond in miljoenen) € 0. De hoge realisatie heeft vermoedelijk te maken met een extra december-productie van Belastingen van 800.000 posten en massaal corrigeren; 195.000 posten.

Overige belastingmiddelen
De realisatie voor de accijnzen was € 296 miljoen hoger dan de prognose. De grootste afwijkingen doen zich voor bij de tabaksaccijns (€ 197 miljoen hoger) en de brandstofaccijns (€ 121 miljoen hoger). Verder is de realisatie voor de dividendbelasting € 338 miljoen hoger.

2.2 Toeslagen

Grafiek 2.4 Toeslagen - cumulatief saldo uitgaven en ontvangsten

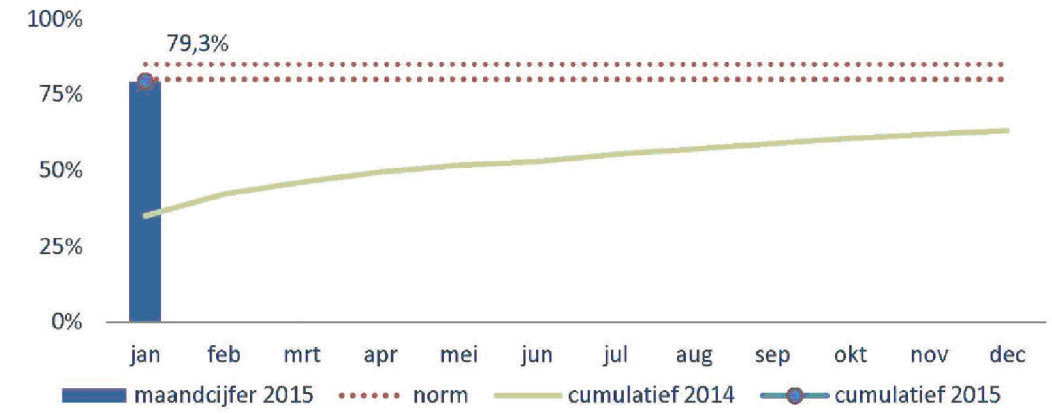


3.0 Dienstverlening

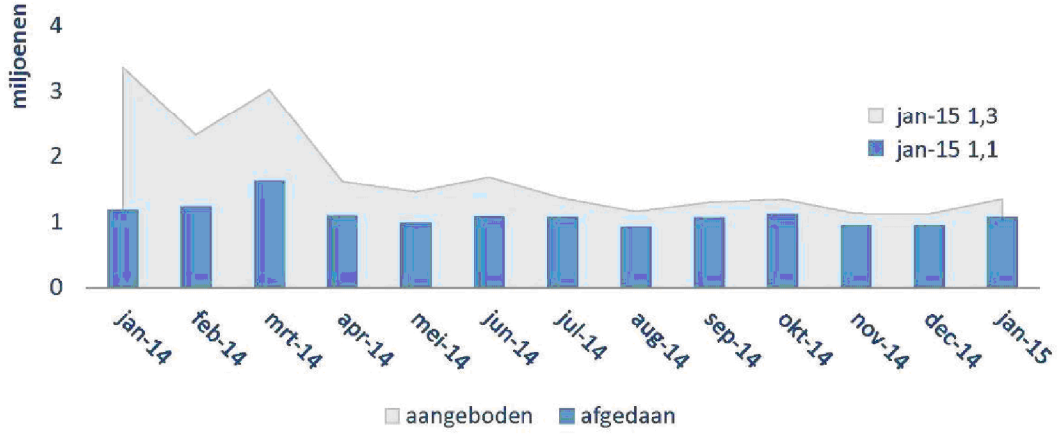
3.1 Telefonie

3.1.1 Bereikbaarheid

Grafiek 3.1 BelastingTelefoon - bereikbaarheid



Grafiek 3.2 BelastingTelefoon - afdoening en aanbod telefonie



3.1.2 Kwaliteit / tijdigheid telefonie

Tabel 3.1

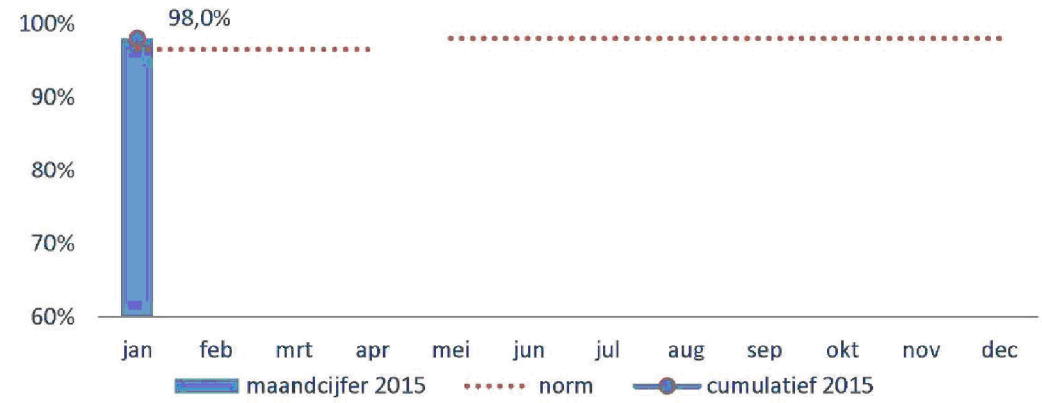
Kwaliteit / tijdigheid telefonie		
	norm	resultaat
Klanten die in één contact worden geholpen	90 - 95%	91,9%
Kwaliteit beantwoording fiscale vragen	80 - 85%	87,3%
Kwaliteit beantwoording status- en proces vragen	90 - 95%	91,4%
Tijdige reactie op complexe vragen < 2 dagen	85 - 90%	90,6%
Tijdige reactie op complexe vragen < 4 dagen	90 - 100%	94,1%
Tijdig afgehandelde (SMART) belafspraken*	95 - 100%	n.b.)*
)*Door een foutieve registratie in de nieuwe release van Lotus Notes is het cijfer niet betrouwbaar. Het probleem wordt onderzocht.		

3.2 Balie

Jaarindicator.

3.3 Internet

Grafiek 3.3 Douane - beschikbaarheid informatiesystemen



De eerste vier maanden is een norm van 96,5% vastgesteld. Vanaf mei geldt een norm van 98%.

Tabel 3.2

Beschikbaarheid internetdiensten en sites			
		resultaat	
	norm	maand	cumulatief
mijn.belastingdienst.nl	≥ 99,9%	97,91%	97,91%
belastingdienst.nl	≥ 99,9%	99,96%	99,96%
douane.nl	≥ 99,9%	99,96%	99,96%
toeslagen.nl	≥ 99,9%	99,96%	99,96%

4.0 Centrale concernprocessen

4.1 Volumes klant tot klantprocessen

4.1.1 Aanslagbelastingen

Tabel 4.1

Samenstelling voorraad aangiften ouder dan 15 maanden	totaal	wv > 15 mnd	%
Aangiften IH			
Belastingjaar 2012	509.094	340.996	67,0%
Belastingjaar 2011	25.439	18.740	73,7%
Belastingjaar 2010	5.199	945	18,2%
Belastingjaar 2009	4.988	232	4,7%
Belastingjaar 2008 en ouder	310	309	99,7%
Totaal IH	545.030	361.222	66,3%
Aangiften Vpb			
Belastingjaar 2012	41.716	10.400	24,9%
Belastingjaar 2011	8.896	7.923	89,1%
Belastingjaar 2010	651	602	92,5%
Belastingjaar 2009	378	356	94,2%
Belastingjaar 2008 en ouder	309	300	97,1%
Totaal Vpb	51.950	19.581	37,7%
Schenkbelasting			
Belastingjaar 2012	856	0	0%
Belastingjaar 2011	272	0	0%
Belastingjaar 2010	152	0	0%
Belastingjaar 2009	72	0	0%
Belastingjaar 2008 en ouder	218	0	0%
Totaal schenkbelasting	1.570	0	0%
Erfbelasting			
Belastingjaar 2012	838	456	54,4%
Belastingjaar 2011	187	143	76,5%
Belastingjaar 2010	42	28	66,7%
Belastingjaar 2009	30	26	86,7%
Belastingjaar 2008 en ouder	45	44	97,8%
Totaal erfbelasting	1.142	697	61,0%

Tabel 4.2

Nog te ontvangen aangiften IH 2012 en 2013	2012	2013
Nog te ontvangen aangiften	92.205	625.746
waarvan met uitstel	2.136	506.933
waarvan zonder uitstel	90.069	118.813

Tabel 4.3

Nog te ontvangen aangiften Vpb 2012 en 2013		
	2012	2013
Nog te ontvangen aangiften	31.206	221.954
waarvan met uitstel	3.787	172.363
waarvan zonder uitstel	27.419	49.591

4.1.2 Aangiftebelastingen

Tabel 4.4

Tijdig ontvangen aangiften OB en LH				
	te ontvangen	tijdig ontvangen	niet tijdig ontvangen	tijdig
Omzetbelasting	1.618.642	1.553.710	64.932	96,0%
Loonheffing	670.896	665.751	5.145	99,2%

Tabel 4.5

Op aangifte tijdig betaalde OB			
		aantal	bedrag
Ontvangen aangiften		n.b.	n.b.
Aangiften met een te betalen bedrag		n.b.	n.b.
waarvan tijdig betaald		n.b.	n.b.
waarvan niet tijdig betaald		n.b.	n.b.
waarvan naar aanslagselectie		n.b.	n.b.
Aangiften met een te ontvangen bedrag		n.b.	n.b.
Aangiften zonder een te betalen of terug te ontvangen bedrag		n.b.	-
Aangiften waarop tijdig is betaald	n.b.		
Bedrag tijdig betaald	n.b.		

bedragen x € 1 miljoen

De OB gegevens zijn deze maand niet beschikbaar omdat de BI bron niet volledig ververst was.

Tabel 4.6

Aandeel in procenten kasopbrengst omzetbelasting	
Primaire aangifteproces	n.b.
Vrijwillige verbeteringen (suppleties)	n.b.
Niet vrijwillige verbeteringen (repressief toezicht)	n.b.

De OB gegevens zijn deze maand niet beschikbaar omdat de BI bron niet volledig ververst was.

4.1.3 Toeslagen

Tabel 4.7

Definitief vastgestelde toeslagen	2011	2012	2013
Huurtoeslag			
Aantal voorlopige beschikkingen	1.377.393	1.379.133	1.431.591
Aantal eerste definitieve beschikkingen	1.251.115	1.316.022	1.256.429
Percentage definitief	90,8%	95,4%	87,8%
Zorgtoeslag			
Aantal voorlopige beschikkingen	6.034.162	5.999.187	5.984.397
Aantal eerste definitieve beschikkingen	5.995.297	5.824.977	5.307.006
Percentage definitief	99,4%	97,1%	88,7%
Kindgebondenbudget			
Aantal voorlopige beschikkingen	1.089.004	1.091.619	1.085.787
Aantal eerste definitieve beschikkingen	1.022.563	1.015.922	869.560
Percentage definitief	93,9%	93,1%	80,1%
Kinderopvangtoeslag			
Aantal voorlopige beschikkingen	575.188	560.641	540.337
Aantal eerste definitieve beschikkingen	537.032	469.895	351.891
Percentage definitief	93,4%	83,8%	65,1%
Totaal			
Aantal voorlopige beschikkingen	9.075.747	9.030.580	9.042.112
Aantal eerste definitieve beschikkingen	8.806.007	8.626.816	7.784.886
Percentage definitief	97,0%	95,5%	86,1%
Norm ultimo 2015	-	99,0%	98,0%

4.1.4 Openstaande of aangehouden uitbetalingen wegens rekeningnummer

De informatie is niet beschikbaar, zie H. 1.2.2.

4.2 Kwaliteit klant tot klantprocessen

Tabel 4.8

Outputcontrole			
B/CA	norm	resultaat	
		maand	cumulatief
Postzendingen zonder fouten	> 99%	98,6%	98,6%
Aantal gecontroleerde partijen		690	690
Aantal poststukken*		14,0	14,0

** aantal x 1 miljoen*

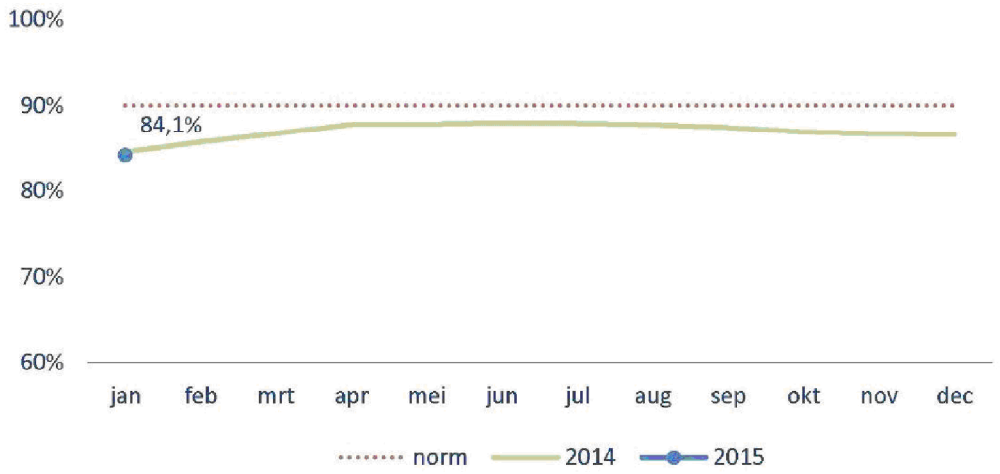
Tabel 4.9

Verstoringen in het massale proces		
	resultaat	
	maand	cumulatief
Aantal procesverstoringen	8	8

5.0 Lokale kantoorprocessen

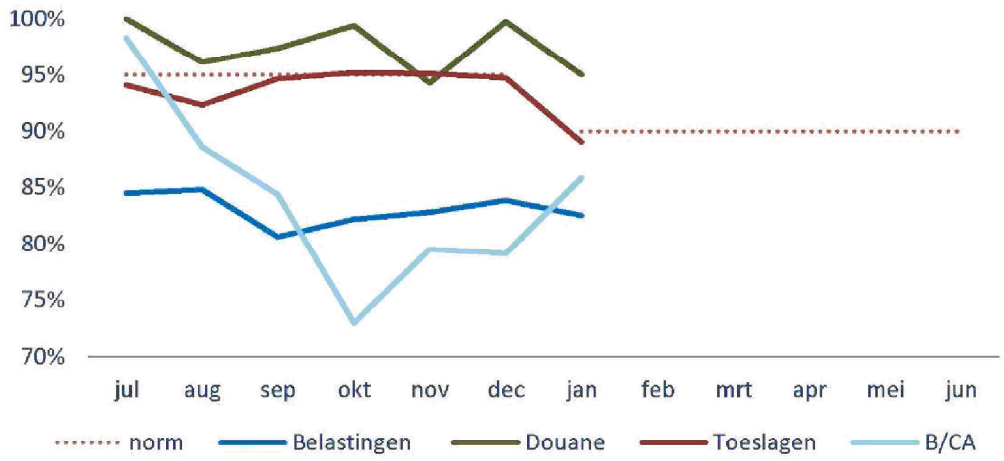
5.1 Bezwaarschriften

Grafiek 5.1 Bezwaarschriften - Awb-conform afgedaan (concern)



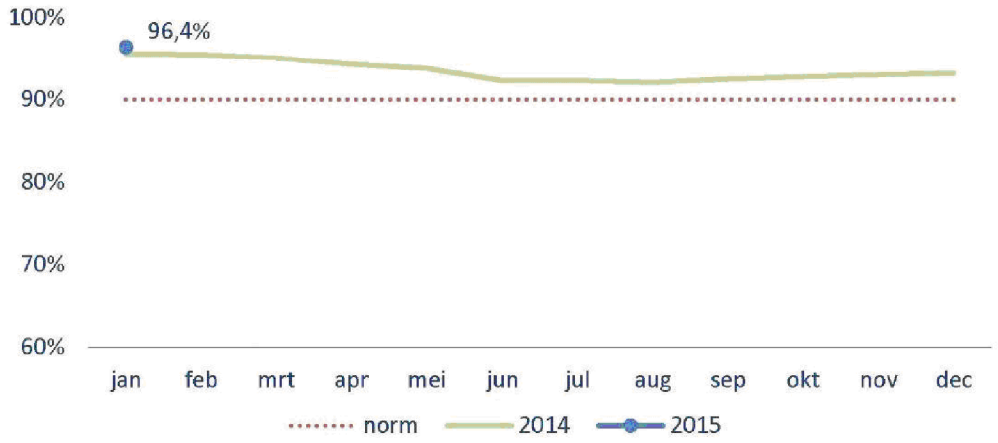
De realisatielijn 2015 sluit niet rechtstreeks aan op de lijn van 2014 omdat het cumulatieve cijfer opnieuw opgebouwd wordt. Verder is de PI-ondergrens aangepast van 95% naar 90%.

Grafiek 5.2 Bezwaarschriften - Awb-conform afgedaan



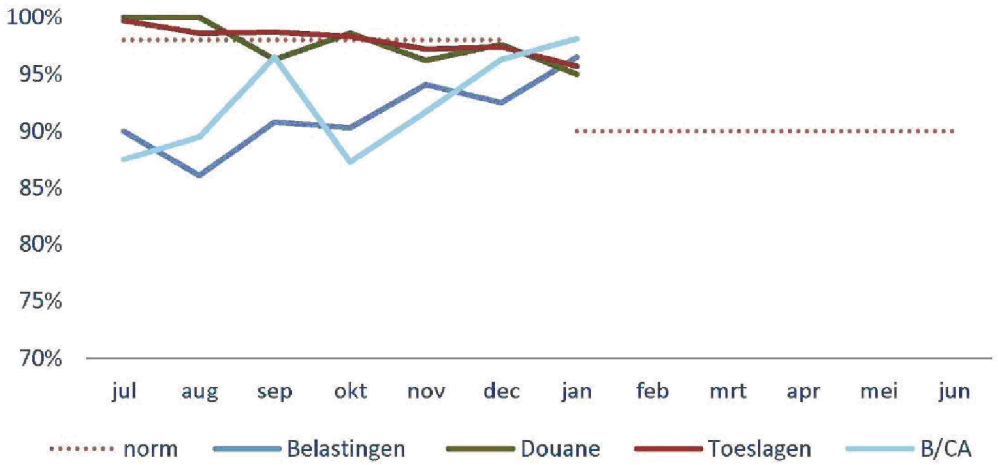
5.2 Klachten

Grafiek 5.3 Klachten - Awb-conform afgedaan (concern)



De realisatielijn 2015 sluit niet rechtstreeks aan op de lijn van 2014 omdat het cumulatieve cijfer opnieuw opgebouwd wordt. Verder is de PI-ondergrens aangepast van 98% naar 90%.

Grafiek 5.4 Klachten - Awb-conform afgedaan



Tabel 5.1

Ontwikkeling voorraad bezwaarschriften	voorraad				
	jaar -1	< Awb	actueel	< Awb	wijziging
Inkomensheffing	69.126	71%	60.530	76%	-12%
Vennootschapsbelasting	15.918	93%	12.113	80%	-24%
Omzetbelasting	12.248	80%	26.366	64%	115%
Loonheffingen	12.117	82%	24.076	94%	99%
Overig)[1]	5.917	70%	17.271	59%	192%
Belastingen	**115.326**	**76%**	**140.356**	**75%**	**22%**
Toeslagen	**21.391**	**96%**	**30.855**	**87%**	**44%**
Motorrijtuigenbelasting	**3.108**	-	**6.253**	-	**101%**
Douane	**1.411**	**93%**	**1.800**	**94%**	**28%**

- cijfer is niet beschikbaar

)[1] *Belastingen / Overig*

Belastingen stelt dat alleen de registratie van de vier hoofdmiddelen in GBV leidend is voor interne sturing. De gepresenteerde cijfers onder Overig hebben daardoor een beperkte waarde.

Tabel 5.2

Afhandeling klachten	norm	resultaat
Afgehandelde klachten binnen Awb-termijn	≥ 90%	96,4%
Klachten binnen 6 weken afgehandeld	> 85%	65,4%
Klachten binnen 7 dagen contact met klager opgenomen	> 75%	86,0%

Tabel 5.3

Voorraad klachten	voorraad				
	jaar-1	< Awb	actueel	< Awb	wijziging
Belastingen	470	72%	n.b.		
BelTel	31	100%	n.b.		
Toeslagen	371	100%	n.b.		
Douane	8	100%	n.b.		
B/CA	135	100%	n.b.		
Totaal Belastingdienst	**1015**	**87%**	**n.b.)***		

)* De totale geschatte voorraad is ongeveer 1300 klachten. In het systeem staan aantallen die niet betrouwbaar worden geacht. Aan een oplossing wordt gewerkt.

5.3 Aanvragen

Deze paragraaf is nog in ontwikkeling.

6.0 Toezicht en opsporing

6.1 Belastingen

6.1.1 Horizontaal toezicht

Tabel 6.1

Horizontaal toezicht			
	segment	norm	resultaat
Ondernemingen onder een horizontaal toezichtconvenant	MKB	75.000 - 100.000	110.115
Organisaties onder een horizontaal toezichtconvenant	GO	1.750 - 2.000	1.904
Gemeenten en provincies onder een horizontaal toezichtconvenant	GO	140 - 180	157
Organisaties met een actueel behandelplan	GO	70 - 80%	69,8%
Organisaties die adequaat werken aan opzet, bestaan en werking van de fiscale beheersing	GO	70 - 80%	81,3%
Organisaties, niet onder HT, waarbij passende toezichtsmaatregelen zijn uitgevoerd	GO	70 - 80%	69,8%

6.1.2 Actuele handhaving

Tabel 6.2

Actuele handhavingsvormen			
	segment	norm	resultaat
Tijdigheid aangiften: percentage bereikte belastingplichtigen na verzuim (OB)	MKB	50 - 60%	76,5%
Tijdigheid aangiften: percentage bereikte belastingplichtigen na verzuim (LH)	MKB	90 - 95%	88,9%
Tijdigheid aangiften: percentage bereikte belastingplichtigen na verzuim (IH niet-winst)	MKB	65 - 75%	n.b.

Tabel 6.3

Toezicht buiten - actueel					
	segment	2013	2014	jaar-1	resultaat
Actualiteitsbezoeken	MKB-GO	44.506	32.793	2.808	1.761

6.1.3 Samenwerking met andere organisaties

P.M.

1910997 01746

6.1.4 Repressieve behandeling

Tabel 6.4

Repressief toezicht	norm	resultaat
Behandelde aangiften IH (particulieren en MKB)	700.000 - 900.000	42.028
Behandelde aangiften Vpb	29.000 - 37.000	2.431

Tabel 6.5

Toezicht buiten - repressief		segment	2013	2014	jaar-1	resultaat
		MKB	38.945	37.339	n.b.	1.992
Aantal boekenonderzoeken		GO	1.716	940	n.b.	20
norm	*35.750 - 38.750*	*Totaal*	*40.661*	*38.279*	n.b.	2.012
		MKB	41,4%	40,7%	n.b.	n.b.
Correctiepercentage		GO	56,7%	46,6%	n.b.	55%

Tabel 6.6

Waardeonderzoeken	2013	2014	jaar -1	resultaat
Totaal aantal afgedaan	6.714	6.234	1.042	556
Aantal afgedaan excl. vaststellingsovereenkomsten	4.860	4.386	747	392
Aantal correcties	4.311	3.818	726	385
Correctiepercentage	89%	87%	97%	98%
Correctiebedrag*	1.184	1.174	240	640
Aantal gecontroleerde objecten	7.901	7.236	1.221	660

** x € 1 miljoen*

6.1.5 Effect handhaving op compliance

P.M.

6.2 Douane

6.2.1 Horizontaal toezicht

Tabel 6.7

Goederenstroom		
	norm	resultaat
Omvang gecertificeerd deel van de goederenstroom	> 85%	> 85%

6.2.2 Actuele handhaving

Tabel 6.8

Controles en uren toezicht					
	norm		maandplanning		resultaat
	min.	max.	min.	max.	
Controles op goederenstroom	360.000	400.000	30.000	33.400	30.934
Controles op passagiersvluchten	12.000	15.000	1.000	1.260	1.033
Aantal uren toezicht (excl. luchthaven)	430.000	470.000	35.800	39.200	41.118
Controles ambulant **buitengrens**	3.700	4.200	310	350	273)*
Controles ambulant **binnenland**	9.000	11.000	750	920	658

)* Door een verandering in de aansturing van dit proces geeft de bestuurlijke informatie (nog) geen betrouwbaar beeld.

6.2.3 Repressieve behandeling

Tabel 6.9

EU Douanecontroles		
	norm	resultaat
Nakoming van de door de EU voorgeschreven douanecontroles	100%	40%

6.2.4 Verbeterinitiatieven handhavingsregie

Tabel 6.10

Verbeterinitiatieven handhavingsregie			
	norm		
	jaar	periode	resultaat
Percentage jaarlijks getoetste AEO gecertificeerde bedrijven	75%	4%	3%

6.3 Toeslagen

6.3.1 Horizontaal toezicht

Tabel 6.11

Toezicht partnerovereenkomsten kinderopvangorganisaties	
	Aantal
Toezicht op convenantspartners	0

1910997 01746

6.3.2 Actuele handhaving

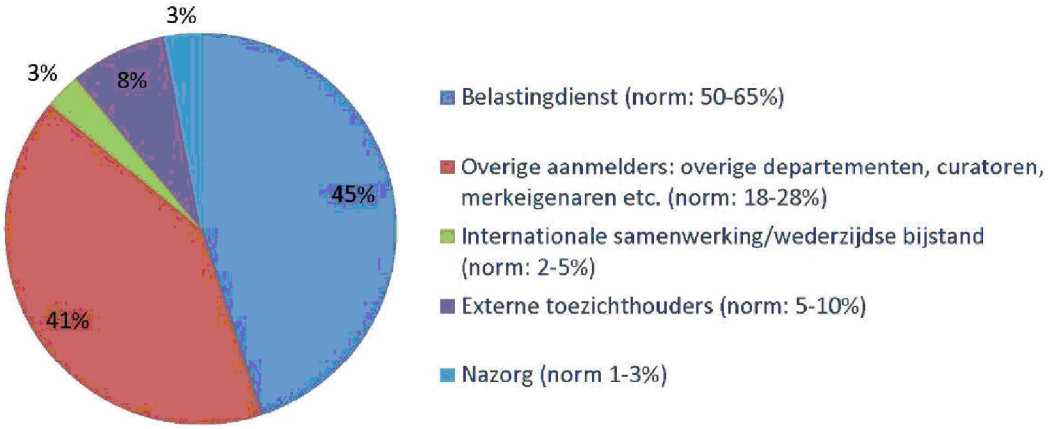
Tabel 6.12

Handmatig toezicht proces verstrekken toeslagen	vooraf	tijdens	na	totaal
Uitworp (op basis risicoregels)	3.277	7.656		10.933
Thematisch toezicht (objectgericht)	4.808	244	7.077	12.129
Intensief toezicht (subjectgericht)	2.387	458	989	3.834
Totaal	10.472	8.358	8.066	26.896

6.4 FIOD

6.4.1 Opsporingsuren

Grafiek 6.1 Verdeling ingezette opsporingscapaciteit



6.4.2 Rechtelijke uitspraak/transactie

Tabel 6.13

Processen-verbaal	norm	resultaat
Processen-verbaal leidend tot veroordeling/transactie	82 - 85%	80%

6.4.3 Opbrengsten 'afpakken'

Tabel 6.14

Opbrengsten afpakken	norm	resultaat
Opbrengsten witwassen*	>25 mln	n.b.

bedragen x 1 € miljoen/ viermaandsinformatie

** betreft conservatoir beslag*

7.0 Incasso

7.1 Achterstand invordering

Tabel 7.1

Betalingsachterstand LH, OB, Vpb, IH, Zvw en HSB		norm	stand	
			jaar -1	actueel
PI totaal		2,5-3,0%	2,5%	2,4%
Totaal betalingsachterstand			4.560	4.615
Opbrengst laatste 12 maanden	192.841			
bedragen x € 1 miljoen				

Tabel 7.2

Openstaande vorderingen (LH, OB, Vpb, IH, Zvw en HSB) Belastingen	stand	
	jaar-1	actueel
Betalingsherinneringen	712	678
Uitstel bezwaar	3.174	3.333
Totaal invordering B/CA en Belastingen	4.560	4.615
bedragen x € 1 miljoen		

Tabel 7.3

Openstaande vorderingen Toeslagen	stand	
	jaar-1	actueel
Betalingsherinneringen	93	100
Betalingsregelingen	594	696
Uitstel bezwaar	210	245
Totaal invordering B/CA en Belastingen	207	248
bedragen x € 1 miljoen		

Tabel 7.4

Oninbaarlijdingen belastingen en premies	norm	stand	
		jaar-1	actueel
PI % oninbaarlijdingen*	**0,6-0,8%**	**0,64%**	**0,56%**
oninbaarlijdingen		1,37	1,28
kasopbrengsten		214,9	226,9
*bedragen x € 1 miljard, * twaalfmaands*			

8.0 IV-aanbod

Deze maand is de IV informatie nog niet beschikbaar.

9.0 Personeel en organisatie

9.1 Formatie en bezetting

Tabel 9.1

Verhouding bezetting en formatie							
	formatie				bezetting*		
	2015	2016	2017	2018	2014	**resultaat**	*prognose eind 2015*
Belastingen	n.n.b.				16.241	16.205	*n.n.b.*
Douane	n.n.b.				4.579	4.566	*n.n.b.*
Toeslagen	n.n.b.				815	852	*n.n.b.*
BelTel	n.n.b.				843	903	*n.n.b.*
FIOD	n.n.b.				1.290	1.293	*n.n.b.*
B/CA	n.n.b.				1.651	1.655	*n.n.b.*
DGBel	n.n.b.				289	245	*n.n.b.*
B/CFD	n.n.b.				1.239	1.242	*n.n.b.*
B/CKC	n.n.b.				622	600	*n.n.b.*
B/CAO	n.n.b.				1.472	1.470	*n.n.b.*
B/CIE	n.n.b.				977	981	*n.n.b.*
Totaal BD	**n.n.b.**				**30.015**	**30.011**	***n.n.b.***

**ambtelijk personeel*

9.2 In- en uitstroom

Tabel 9.2

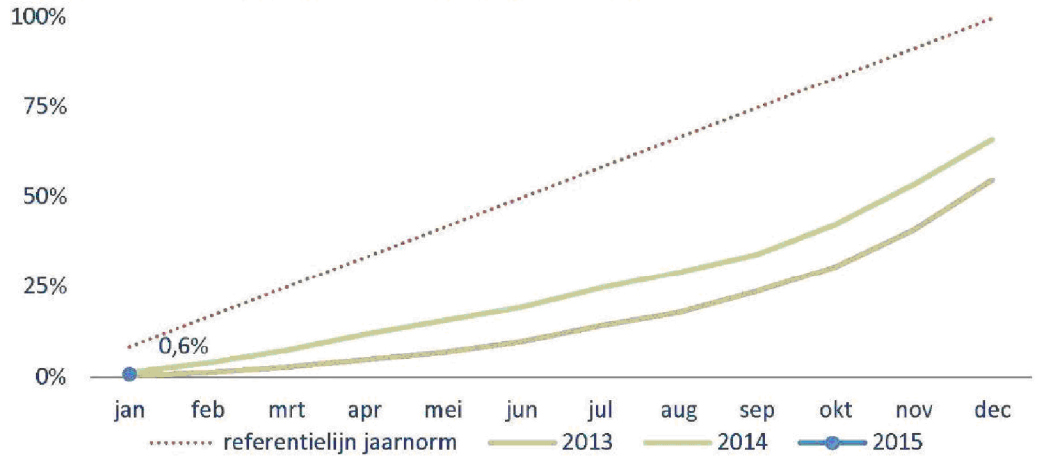
Mobiliteit*				
	in-/ uitstroom		doorstroom	
	in	uit	in	uit
Belastingen	34,9	68,9	11,0	12,2
Douane	12,9	20,4	3,7	8,6
Toeslagen	38,4	2,4	1,8	1,0
BelTel	2,3	4,7	66,5	4,0
FIOD	2,1	3,1	5,0	1,0
B/CA	9,4	8,3	7,9	4,9
DGBel	2,6	0,8	1,0	46,7
B/CFD	8,3	5,0	2,0	1,9
B/CKC	1,3	2,8	51,0	71,7
B/CAO	5,9	8,1	0,9	0,8
B/CIE	3,5	1,4	3,0	1,0
Totaal Belastingdienst	**121,6**	**125,9**	**153,8**	**153,8**

**ambtelijk personeel, fte's cumulatief*

1910997 01746

9.3 Leidinggeven (functioneringsgesprekken)

Grafiek 9.1 Leidinggeven - functioneringsgesprekken

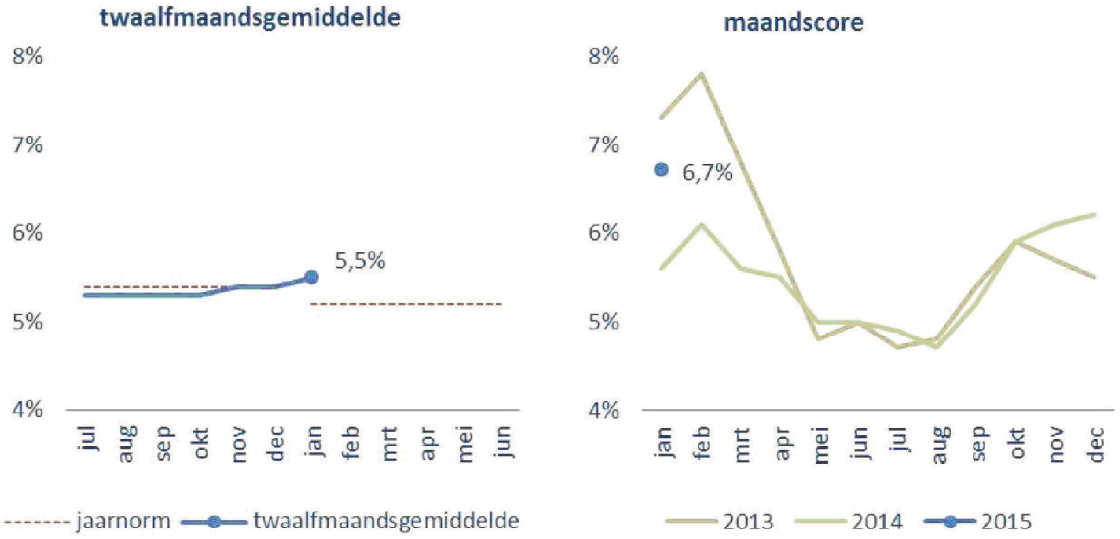


Bron: P-Direkt, onvolledige registratie

9.4 Inzetbaarheid

9.4.1 Ziekteverzuim

Grafiek 9.2 Ziekteverzuimpercentage



Tabel 9.3

Ziekteverzuim		
	norm	resultaat*
Belastingen	5,5%	5,8%
Douane	5,2%	5,9%
Toeslagen	5,5%	5,6%
BelTel	6,7%	6,2%
FIOD	3,8%	4,2%
B/CA	4,5%	4,4%
DGBel	3,2%	2,7%
B/CFD	4,9%	5,4%
B/CKC	4,8%	4,8%
B/CAO	4,5%	4,7%
B/CIE	4,7%	4,8%
Totaal Belastingdienst	**5,2%**	**5,5%**
**voortschrijdend twaalfmaandsgemiddelde*		

9.4.2 Meldingsfrequentie verzuim

Tabel 9.4

Meldingsfrequentie verzuim		
	norm	resultaat*
Meldingsfrequentie	≤ 1,2	1,0
**voortschrijdend twaalfmaandsgemiddelde*		

1910997 01746

10.0 Middelen

10.1 Uitgaven (apparaat)

Tabel 10.1

Percentage kasuitgaven personeel en materieel versus budget*		
	kasrealisatie t/m rapportagemaand*	*kasrealisatie trend**
Personeel	**24,9%**	***25,0%***
waarvan vast personeel	25,5%	*25,0%*
waarvan inhuur externen (incl. UZK)	20,0%	*25,0%*
Materieel	**18,5%**	***25,0%***
waarvan ICT-uitgaven	11,5%	*25,0%*
waarvan uitgaven Shared Services Organisatie (SSO)	10,5%	*25,0%*
waarvan overige materiële uitgaven	29,5%	*25,0%*
Totaal uitgaven	**23,1%**	***25,0%***
Totaal ontvangsten	10,9%	*25,0%*
Saldo	**23,2%**	***25,0%***

**1e viermaanden*

Tabel 10.2

Financieel beeld per bedrijfsonderdeel (op basis kosten)						
		budget*	*prognose**	afwijking prognose - budget	gem. maand-budget	realisatie
Belastingen	P	301.429	*309.835*	8.406	75.357	77.724
	M	13.348	*16.447*	3.099	3.337	8.239
	Totaal	**314.777**	***326.282***	**11.505**	**78.694**	**85.963**
Douane	P	81.815	*83.517*	1.702	20.454	21.432
	M	9.828	*21.689*	11.861	2.457	1.732
	Totaal	**91.643**	***105.206***	**13.563**	**22.911**	**23.164**
Toeslagen	P	22.917	*25.473*	2.556	5.729	6.388
	M	233	*233*	0	58	26
	Totaal	**23.150**	***25.706***	**2.556**	**5.788**	**6.414**
BelTel	P	34.020	*38.420*	4.400	8.505	7.480
	M	4.078	*4.078*	0	1.020	2.958
	Totaal	**38.098**	***42.498***	**4.400**	**9.525**	**10.438**
FIOD	P	26.533	*28.015*	1.482	6.633	7.129
	M	3.122	*3.086*	-36	781	879
	Totaal	**29.655**	***31.101***	**1.446**	**7.414**	**8.008**
B/CA	P	35.104	*35.104*	0	8.776	8.677
(incl. BD-brede uitgaven)	M	10.326	*10.326*	0	2.582	932
	Totaal	**45.430**	***45.430***	**0**	**11.358**	**9.609**
DGBel	P	6.066	*6.825*	759	1.517	2.021
(incl. BD-brede uitgaven)	M	15.579	*22.326*	6.747	3.895	7.926
	Totaal	**21.645**	***29.151***	**7.506**	**5.411**	**9.947**
B/CFD	P	28.756	*28.680*	-76	7.189	6.091
	M	100.259	*122.995*	22.736	25.065	8.531
	Totaal	**129.015**	***151.675***	**22.660**	**32.254**	**14.622**
B/CKC	P	13.102	*13.102*	0	3.276	3.395
	M	7.115	*7.115*	0	1.779	739
	Totaal	**20.217**	***20.217***	**0**	**5.054**	**4.134**
B/CAO	P	46.609	*50.152*	3.543	11.652	9.825
	M	10.450	*12.788*	2.338	2.613	3.251
	Totaal	**57.059**	***62.940***	**5.881**	**14.265**	**13.076**
B/CIE	P	27.137	*28.687*	1.550	6.784	6.811
(incl. BD-bescheiden)	M	56.692	*67.029*	10.337	14.173	10.834
	Totaal	**83.829**	***95.716***	**11.887**	**20.957**	**17.645**
Centrale kaders	P	1.942	*1.942*	0	486	0
	M	12.966	*12.966*	0	3.242	6
	Totaal	**14.908**	***14.908***	**0**	**3.727**	**6**
Totaal intern kader uitgaven		**869.426**	***950.830***	**81.404**	**217.357**	**203.026**
Totaal intern kader ontvangsten		**8.735**	***6.585***	**-2.150**	**2.184**	**1.288**
		860.691	***944.245***	**83.554**	**215.173**	**201.738**

bedragen x € 1.000

**1e viermaanden*

Tabel 10.3

Financieel beeld externe inhuur per bedrijfsonderdeel (op basis kosten)					
		budget*	*prognose**	afwijking prognose - budget	realisatie
Belastingen	totaal inhuur	1.150	*4.500*	3.350	384
Douane	totaal inhuur	78	*78*	0	0
Toeslagen	totaal inhuur	10.600	*12.586*	1.986	3.063
BelTel	totaal inhuur	18.789	*21.289*	2.500	4.200
FIOD	totaal inhuur	0	*0*	0	2
B/CA	totaal inhuur	1.537	*1.537*	0	479
DGBel	totaal inhuur	0	*200*	200	0
B/CFD	totaal inhuur	2.697	*9.062*	6.365	420
B/CKC	totaal inhuur	600	*600*	0	28
B/CAO	totaal inhuur	13.557	*14.580*	1.023	1.803
B/CIE	totaal inhuur	6.072	*7.206*	1.134	1.497
Centraal kader	totaal inhuur	0	*0*	0	0
Totaal Belastingdienst	**totaal inhuur**	**55.080**	***71.638***	**16.558**	**11.876**

bedragen x € 1.000

**1e viermaanden*

Tabel 10.4

Realisatie/ prognose inhuur externen en uitzendkrachten		
	realisatie inhuur	*prognose inhuur**
Belastingen	0,5%	*1,5%*
Douane	0,0%	*0,1%*
Toeslagen	47,9%	*49,4%*
BelTel	56,1%	*55,4%*
FIOD	0,0%	*0,0%*
B/CA	5,5%	*4,4%*
DGBel	7,8%	*2,9%*
B/CFD	6,9%	*31,6%*
B/CKC	0,8%	*4,6%*
B/CAO	18,4%	*29,1%*
B/CIE	22,0%	*25,1%*
Centraal kader	0,0%	*0,0%*
Totaal Belastingdienst	**7,7%**	***11,0%***

**1e viermaanden*

Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

Datum
12 december 2014

Kenmerk
2014-0000668784

agenda

VERGADERING INTERDEPARTEMENTALE COMMISSIE BEDRIJFSVOERING RIJKSDIENST

Vergaderdatum en tijd	17 februari 2015 15.00-17.00
Vergaderplaats	Ministerie van BZK, Z01-36 IJsselzaal

1. Opening en Mededelingen **15.00-15.20**

a. Welkom aan nieuwe [redacted] SGO5
b. Vaststelling agenda ICBR-agenda 17 februari
c. Stand van zaken CAO Rijk, GOR Rijk, kabinetsreactie-Elias *(mondeling)*

2. Verslag ICBR 20 januari 2015 **15.20-15.25**

a. Ter vaststelling

3. Ter advisering SGO **15.25-16.00**

a. Transities binnen de bedrijfsvoering Rijk: omgaan met personele consequenties *(stuk: 3a)*
b. Voorstel voor structurele overboeking ICBR budget naar begroting BZK *(stuk: 3b)*

4. Ter besluitvorming **16.00-16.10**

a. Eindverantwoordingsrapportage Jaarplan ICBR 2014 *(stuk: 4a)*

5. Ter bespreking **16.00-16.40**

a. "BZ in vogelvlucht" (presentatie [redacted]) *(mondeling)*

6. Ter kennisname

a. Centrale bekostiging FMHaaglanden *(stuk: 6a)*

7. Rondvraag/sluiting **16.40-16.45**

Belastingdienst

B/CA

Contactpersoon

memo

Eén bankrekeningnummer

Datum
15 februari 2015

Inleiding

In het MT Belastingdienst van 9 februari is kort gesproken over één bankrekeningnummer (verder: 1BRN), mede naar aanleiding van een signaal dat vanuit het project 1BRN het plan zou bestaan om binnenkort brieven aan burgers te verzenden. Gezien de eerdere ervaringen met 1BRN is het nodig om het MT goed betrokken te houden bij de aanpak, zodanig dat er draagvlak is voor de acties die ondernomen worden. Op die manier kunnen we een goede afweging maken tussen enerzijds de aanpak om fraude tegen te gaan en anderzijds ervoor te zorgen dat de aanpak realistisch is over de uitvoeringsmogelijkheden (en eventuele publicitaire consequenties). Deze notitie beschrijft de resultaten van 1BRN tot op heden en maakt inzichtelijk hoe de aanpak er voor de komende periode uitziet.

Kader 1BRN

Per 1 december 2013 mag de Belastingdienst alleen bankrekeningnummers accepteren die op naam staan van degenen die recht hebben op uitbetaling van toeslagen, OB, IH en ZVW. Bij iedere opgaaf of verandering van het rekeningnummer wordt gecontroleerd of dit op naam van betreffende persoon of onderneming staat. De Belastingdienst maakt voor de validatie gebruik van de gegevens die hij van banken krijgt in het kader van de vooringevulde aangifte. Is deze geautomatiseerde validatie niet mogelijk, dan moet de belanghebbende bewijzen dat het nummer op naam staat. De belanghebbende ontvangt dan een verzoek tot verificatie.

De nieuwe wetgeving kende aanvankelijk een zogenoemde overgangsperiode tot 1 juli 2014. In het voorjaar van 2014 heeft de staatssecretaris besloten de zogenaamde overgangsperiode te verlengen tot 1 juli 2015. Hiermee kreeg de Belastingdienst extra tijd om het verificatieproces te verbeteren. Tot aan het einde van de overgangsperiode betaalt de Belastingdienst uit op het laatst bekende, niet-gevalideerde rekeningnummer. Bij de opgave van een nieuw rekeningnummer wordt het oude rekeningnummer automatisch geblokkeerd. Dit leidt er toe dat in die situaties waarin de Belastingdienst het opgegeven rekeningnummer niet geautomatiseerd kan valideren er vertragingen ontstaan in de uitbetalingen.

Startpositie januari 2014

In totaal zijn bij de Belastingdienst 14 miljoen burgers en ondernemers bekend voor de uitbetalingen van toeslagen, IH, ZVW en OB. Op 19 januari 2014 is de rekeningnummeradministratie van de Belastingdienst geconverteerd; de rekeningnummeradministratie is geverifieerd en omgezet ten behoeve van de uitvoering van de één bankrekeningnummermaatregel.

- Bij 11 miljoen burgers en ondernemers kon het geregistreerde rekeningnummer gevalideerd worden. Zij hebben niet te maken gekregen met de ingevoerde maatregel.
- Ongeveer 900.000 burgers en ondernemers hebben in het eerste kwartaal van 2014 een brief van de Belastingdienst ontvangen, waarin werd aangegeven dat de uitbetaling plaatsvindt op één van de op hun naam gestelde bankrekeningnummers.
- Ongeveer 600.000 burgers en ondernemers hebben met de invoering per 1 december 2013 met de maatregel te maken gekregen. Het betreft hier de opgaven van nieuwe rekeningnummers.
- Voor ongeveer 1,5 miljoen burgers en ondernemers kon de Belastingdienst de rekeningnummers nog niet valideren.

Procesverbeteringen

De kwaliteit van het verificatieproces is een belangrijke factor in de aanpak 1BRN. Om een indruk te geven: in 2014 kon de Belastingdienst 70% van de nieuwe of gewijzigde rekeningnummers geautomatiseerd valideren en in 30% leidde een opgave van een rekeningnummer tot een verzoek om verificatie.

Medio vorig jaar bleek dat het verificatieproces niet op korte termijn kon worden verbeterd via betere IV-ondersteuning, zoals het zichtbaar maken van bij de Belastingdienst bekende rekeningnummers in het portal of op het mogelijk maken van het uploaden van bewijsstukken naar het portal voor bij de Belastingdienst onbekende rekeningnummers. Om toch verbeteringen te kunnen doorvoeren, zijn vervolgens de volgende afspraken gemaakt:

- Rekeningnummers die niet geautomatiseerd gevalideerd kunnen worden, worden per medio november dagelijks gecontroleerd via de zogenaamde 'NAW navraagservice' van Equens (clearing house voor alle Nederlandse bankrekeningen). Het uitvalpercentage bij het verificatieproces is daarmee teruggedrongen van 30% tot 15%.
- Het mutatieproces wordt per 24 maart 2015 zodanig aangepast dat het oude rekeningnummer actief blijft tot dat het nieuwe rekeningnummer geverifieerd of afgewezen wordt (met een maximum van 45 dagen). Burgers die niet willen dat op het oude rekeningnummer betaald wordt, krijgen de mogelijkheid om betalingen te blokkeren totdat het nieuwe rekeningnummer geverifieerd is.

Waar staan we nu?

De omvang van de oorspronkelijke groep van 1,5 miljoen burgers en ondernemers waarvan op 19 januari 2014 geen rekeningnummer op naam bekend was, maar wel een ander rekeningnummer, is op dit moment nog ongeveer 700.000. De afname van dit aantal wordt veroorzaakt doordat het project 1BRN een aantal acties heeft kunnen uitvoeren:

- De tenaamstellingsverplichting voor de OB per 1 januari 2015 is afgeschaft;
- Rekeningnummers van overledenen zijn gedeactiveerd;
- Rekeningnummers van burgers, die geen verblijfplaats hebben, zijn gedeactiveerd;
- Rekeningnummers van burgers, die sinds 1 januari 2013 geen betalingen meer van de Belastingdienst hebben ontvangen, zijn gedeactiveerd;
- Burgers hebben hun rekeningnummer op eigen initiatief gewijzigd.

Omdat in november en december nog grote groepen burgers een éénmalige uitbetaling ontvangen in het kader van Toeslagen of IH is besloten verdere acties met betrekking tot deze burgers op te schorten tot in ieder geval na 1 januari 2015. De inzet is om deze burgers beheerst en gefaseerd aan een rekeningnummer te helpen die voldoet aan de tenaamstellingsverplichting.

Voorgestelde aanpak

De resterende groep van 700.000 burgers waarvan geen rekeningnummer op naam bekend is maar wel een ander rekeningnummer, zal de komende twee weken gesplitst en geanalyseerd worden. Hiermee bereiken we dat de groep naar verwachting wederom kleiner wordt. Wij stellen voor om de volgende acties uit te voeren:

- Overledenen: rekeningnummer deactiveren;
- VOW: recht op toeslagen stoppen en rekeningnummer deactiveren;
- Burgers die langer dan 18 maanden geen betalingen meer van de Belastingdienst hebben ontvangen: rekeningnummer deactiveren;
- Derden (zoals schuldhulpverlening e.d.): verifiëren van de onder andere met koepels gemaakte afspraken bij instellingen en vervolgens administreren;
- Buitenlandse rekeningen: apart zetten en analyseren vanwege verificatieproblematiek;
- Uitvoeren NAW-navraag check bij Equens voor overgebleven groep: indien positieve uitkomst dan rekeningnummer als gevalideerd registreren;
- Uitvoeren controles met andere bestanden en administraties: bij positieve uitkomst rekeningnummer aanbieden als door de Belastingdienst te gebruiken rekeningnummer.

De aanpak om eerst zoveel mogelijk controles te doen, zonder de burger te benaderen, is recent met een steekproef uitgeprobeerd. De steekproef is gedaan voor 60.000 burgers en heeft de bovenstaande categorieën daarbij als leidraad gehanteerd. Van de 60.000 zijn er - na opschoning - 39.000 rekeningnummers gecontroleerd via de NAW-navraag. Daarvan voldeden 29.000 aan de tenaamstellingsverplichting. De steekproef leverde dus een restgroep op van 10.000 rekeningnummers.

De uitkomsten van de analyse van de volledige groep van 700.000 en de voorgestelde acties per categorie moeten over twee weken zowel een betrouwbare indicatie afgeven van het aantal rekeningnummers dat nog geverifieerd moet worden als inzicht in de opbouw en karakteristieken van de restgroep. We kunnen dan tevens beoordelen of de gehanteerde einddatum van de overgangsperiode, 1 juli 2015, realistisch is. Het MT Belastingdienst zal in maart nader geïnformeerd worden.

Directoraat-Generaal
Belastingdienst

Datum
12 februari 2015

agenda Bezoek SZW P&I

Vergaderdatum en -tijd	16 februari 2015, 15.30 - 17.30 uur
Vergaderplaats	Snipzaal, Korte Voorhout 7, 2511 CW Den Haag

Agendapunten

15.30 – 16.15 uur **Uitvoeringstoets Nieuwe Stijl Belastingdienst**

16.15 –17.00 uur **Loonaangifteketen**

- koesteren van eigenaarschap van de keten
- taakverdeling bij toekomstige regelingen
- streven naar hechtere samenwerking tussen departementen en uitvoeringsorganisatie aangaande politieke en beleidswensen
- groeiende complexiteit.

17.00- 17.30 uur **WVTTK**