Belastingdienst

Privacy Impact Assessment: Databank Auto

Toetsmodel Rijksdienst in NOREA format

22 december 2014

Omschrijving:

De Databank Auto is een web-based applicatie waarbij diverse gegevens (o.a. externe camerabeelden, ANPR-informatie en CJIB-boetes) in één systeem worden getoond. De applicatie wordt door geautoriseerde medewerkers gebruikt voor het toezicht op de autobelastingen (MRB, BPM, BZM en privégebruik auto/PGA).

#	Vraag	Antwoord	Aanbeveling?[1]

I	**Basisinformatie: type persoonsgegevens, type verwerking en noodzaak/ gegevensminimalisering**		
I.1	Wilt u als verantwoordelijke persoonsgegevens gaan gebruiken voor de verwerking die u voorziet? Zo ja, van welk type?	Ja. Het betreft de verwerking van o.a. parkeergegevens, externe camerabeelden, ANPR-informatie en CJIB-boetes als contra-informatie voor de heffing van de zogenoemde autobelastingen (zie voor een overzicht van alle gegevens Bijlage 1: Overzicht bronbestanden Databank Auto). Het Landelijk Coördinatiepunt Auto (LCA), als onderdeel van de Belastingdienst, verzorgt de coördinatie van de verwerking van de onderhavige persoonsgegevens. Voor deze verwerking wordt gebruik gemaakt van de Databank Auto (de databank) die via een web-based applicatie kan worden geraadpleegd. Deze databank is in de loop der jaren ontwikkeld en wordt beheerd binnen LCA. Deze PIA is met name gericht op de inrichting en het gebruik van deze databank. Naast het individueel bevragen van de databank door geautoriseerde medewerkers kunnen ook zogenoemde query-verzoeken worden gedaan.[2] De query-verzoeken lopen via de Landelijke Toezicht Organisatie (LTO is een onderdeel van de Belastingdienst) en bij elk verzoek staat centraal welke datavelden bevraagd worden en waarom deze velden noodzakelijk zijn voor het gestelde doel. Verzoeken voor autodata kunnen middels een intakeformulier worden ingediend bij de LTO-Business Analysis postbus. Dit intakeformulier kan via de postbus worden opgevraagd. Tevens worden daarbij de leveringscriteria toegezonden. Deze leveringscriteria zijn samengesteld i.s.m. met een privacy deskundige/beleidsmedewerker privacy van de LTO. Na registratie in de RIT (Rapportages intensief toezicht) tool en de aanmaak van een dossier t.b.v. archivering, worden de verzoeken verder beoordeeld.	Nee

[1] Zie voor een geprioriteerd overzicht van alle mogelijke risico's en aanbevelingen pagina 25 en 26 van dit document.
[2] Een query is huiselijk gezegd een bevraging van de databank aan de hand van een bepaalde set parameters.

2058012 00001

		Aspecten zijn; is er een formele opdrachtgever, heeft het verzoek met toezicht te maken, is er sprake van een project, worden gegevens eventueel aan derden geleverd, is er een wettelijke basis voor de levering aan derden en is er een doelbinding. Dit betreft een eerste beoordeling. De verzoeken worden nogmaals door LCA beoordeeld. LCA behandelt de query aanvraag en zorgt voor de uitlevering van de gevraagde gegevens. LCA heeft de brondata ter beschikking en is eigenaar hiervan en hebben meer zicht op en kennis van de soorten aanvragers. De gegevensdumps komen via drie routes binnen: 1. LTO 2. Belastingdienst/Centrale Administratie (B/CA) - Centrale Informatievoorziening (CIV) 3. Intern (bijvoorbeeld gegevens uit de Workflow Privégebruik Auto, PGA) Alle dataoverdrachten tussen LCA en LTO worden vastgelegd. De in de onderhavige databank verwerkte persoonsgegevens zijn in een overzicht weergegeven en kunnen verder gespecificeerd worden in de datavelden "onder de motorkap".[3] De verwerkte persoonsgegevens zijn onderverdeeld in de volgende 5 categorieën: 1. Voertuiggegevens 2. Contra-Informatie (extern) 3. Contra-Informatie (intern) 4. Basis gegevens 5. Productiegegevens	
I.2a	Is het de bedoeling om gegevens over de financiële of economische situatie van	Er worden financieel-economische gegevens van betrokkene verwerkt. Het niet de bedoeling om te stigmatiseren of uit te sluiten maar de databank is als toezichtinstrument wel een middel waarmee men invulling geeft aan	Nee.

[3] Het overzicht is als bijlage bij deze PIA beschikbaar en uitsluitend voor intern gebruik. Omdat in het overzicht strategische controle-informatie wordt weergegeven, mag de bijlage niet worden gepubliceerd of extern worden gebruikt.

	betrokkenen, of andere gegevens die kunnen leiden tot stigmatisering of uitsluiting te verwerken?	het risicoselectiebeleid. Je ontkomt er dan niet aan dat je risicogroepen selecteert en daarmee mogelijk stigmatiseert. Het uitgangspunt is overigens het object (de auto) i.p.v. het subject.	
I.2b	Is het de bedoeling om gegevens over kwetsbare groepen of personen te verwerken?	Het is niet de bedoeling dat gegevens over kwetsbare groepen of personen worden verwerkt, maar het is niet uit te sluiten dat er gegevens van kwetsbare groepen en personen worden verwerkt.	Nee.
I.2c	Is het de bedoeling gebruikersnamen, wachtwoorden en andere inloggegevens te verwerken?	Nee	Nee.
I.2d	Is het de bedoeling om uniek identificerende gegevens, zoals biometrische gegevens, te verwerken?	Nee Er zullen geen uniek identificerende gegevens worden verwerkt.	Nee.
I.2e	Is het de bedoeling om het BSN-nummer, of een ander persoonsgebonden nummer te verwerken?	Ja. Voor de toezichtstaak van de Belastingdienst (uitvoering publiekrechtelijke taak art. 8 letter e Wbp) is het gebruik van het BSN noodzakelijk en overigens ook wettelijk voorgeschreven.[4]	Nee.
I.3	Kan van elk van de onder vraag I.1 en vraag I.2 opgevoerde typen persoonsgegevens worden	Zie het overzicht met de vijf onderscheiden categorieën persoonsgegevens (Bijlage 1). In het overzicht wordt aangegeven welke gegevens van belang zijn en voor welk doel.	Ja. Momenteel wordt er nagedacht over een eventuele opschoning

[4] Zie bijvoorbeeld de Wet algemene bepalingen burgerservicenummer

	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.	Van de externe contra-informatie worden momenteel de Externe Camera Beelden (ECB's) gefilterd op zakelijke kentekens. Dit betekent dat alleen de ECB's van zakelijke kentekens worden weergegeven in de databank. Dit filter geldt op dit moment nog niet voor de overige externe contra-informatie (CJIB-boetes en ANPR-beelden). Inspectie, controle en toezicht	van de databank. Daarbij wordt er gekeken welke gegevens eventueel niet meer noodzakelijk zijn voor de databank. Het is aan te raden om bij de beoordeling van de bestanden in de databank gebruik te maken van het overzicht in Bijlage 1. Per bestand moet bepaald worden of het bestand noodzakelijk is voor het toezicht op de autobelastingen.
I.4	Kan als het gaat om gevoelige persoonsgegevens hetzelfde beleidseffect of technisch	Nee. Er worden gegevens verwerkt (zie antwoord op vraag 2a) die als gevoelig kunnen worden gekwalificeerd en die noodzakelijk zijn voor de controle van de juistheid en de volledigheid van de belastingheffing.	Nee.

	resultaat worden bereikt op een van de volgende wijzen: (a) door (gecombineerd) gebruik van normale persoonsgegevens, (b) door gebruik van geanonimiseerde of gepseudonimiseerde gegevens?		
I.5	In welk breder wettelijk, beleidsmatig of technisch kader wordt het voorziene 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?	De databank van het LCA is een instrument dat past binnen het toezicht beleid van de Belastingdienst met handhavingsregie via de LTO. De databank is al enkele jaren operationeel en er is nog niet eerder een PIA uitgevoerd voor deze databank. Deze PIA kan worden gezien als een tussentijdse uitvoeringstoets op de naleving van de Wbp. Het instrument PIA is relatief nieuw ten opzichte van de bedrijfsprocessen van de Belastingdienst en daarom niet eerder toegepast.	Nee.

II	**Doelbinding, koppeling, kwaliteit en profilering**		

II.1	Hebt u het/de specifieke doel(en) waarvoor u de persoonsgegevens gaat verwerken in detail vastgesteld? Geldt hiervoor één en hetzelfde specifieke doel?	Ja. De databank is tot stand gekomen n.a.v. overleg en bewuste besluitvorming binnen de Belastingdienst. Door voortschrijdend inzicht kan het nut van deze databank anders beoordeeld worden in de toekomst. Doel 1 was het oorspronkelijk doel. Doelen 2, 3, 4 en 5 zijn een resultante van het eerste doel en deze gevolg-doelen zijn verenigbaar met het eerste doel. Zie tevens ook Bijlage 2 voor het protocol waarin is aangegeven welke voertuigpassagegegevens fiscaal relevant zijn. Doel 1: Alle relevante (externe en interne) contra-informatie tonen in één systeem ten behoeve van het integrale toezicht op de autobelastingen (PGA, BPM, MRB en BZM) voor de Belastingdienst/Belastingen (blauw in jargon) Doel 2: Risicovinding autobelastingen Doel 3: Bestuurlijke informatie (BI); verantwoordingsinformatie en stuurinformatie Doel 4: Contra-informatie voor de andere bedrijfsonderdelen van de Belastingdienst (groen en rood in jargon) Doel 5: Administratieve controle en boekenonderzoeken; de voorbereiding. Er zit een TOP-knop in de databank. Daarmee kan men de scherminhoud exporteren naar een ander formaat (Excel, PDF, Word, etc.). Daarmee kan de informatie uit de databank worden gebruikt in andere applicaties die de Belastingdienst in haar toezichtproces gebruikt. Nu de Belastingdienst werkt met Digitale Werkruimte Belastingdienst (DWB) werkplekken waarbij tijd- en plaats onafhankelijk kan worden gewerkt, is deze knop wellicht niet meer nodig.	Ja. *Aanbevolen maatregel:* Onderzoek de noodzaak voor deze exporteer-knop in relatie tot de DWB-werkplekken waarmee iedere geautoriseerde medewerker op locatie (op plekken met beveiligde WiFi toegang) toegang heeft tot de databank.

II.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).	Nee. De persoonsgegevens werden altijd al gebruikt voor deze doelen maar waren niet eerder bijeen gebracht in één databank. De parkeergegevens zijn inmiddels uit de databank verwijderd en zullen dus niet gebruikt worden. De eerder opgevraagde parkeergegevens hebben overigens momenteel ook geen actualiteitswaarde meer, aangezien het gegevens zijn uit 2012. Het opvragen van parkeergegevens is recent aan de orde gekomen in een juridische procedure waarin is geoordeeld dat er bij het opvragen van de parkeergegevens geen strijd is met de Wbp. Citaat Persoonsgegevens uit de Beeldkant van 20 augustus: *"Nu zullen wij met inachtneming van het arrest de informatie binnen Special Auto alleen gaan benutten ter verifiëring van eigen fiscale vermoedens van niet juist gebruik van de zakelijke auto door verklaringhouders van 'geen privégebruik'. Van andere informatie wensen wij geen gebruik te maken noch toegang toe te hebben. Momenteel bouwen wij verder aan nieuwe filters om informatie gestuurd te handhaven."*	Nee.

[4] Function creep hoeft op zichzelf niet negatief te zijn. Het herbergt wel een risico van Wbp-schending in zich.

II.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?	Ja. De databank wordt in de loop van haar bestaan gebruikt voor meerdere doeleinden. Daarmee ligt het gevaar van ongecontroleerde *function creep* op de loer (dat de persoonsgegevens voor andere doeleinden worden gebruikt dan oorspronkelijk bedoeld was). Daar zal extra aandacht voor moeten zijn bij het beheer van de databank.[5] Zie het antwoord bij vraag II.1. De daar genoemde doelen 2,3 en 4 zijn verenigbaar met doel 1. Nieuwe doelen of nog niet beschreven doelen zullen moeten worden getoetst aan de Wbp-eisen zoals de verenigbaarheid van het nieuwe doel met het oorspronkelijke doel. Als voorbeeld: de databank gebruiken voor integriteitsonderzoeken onder rijksambtenaren is niet toegestaan. Dat doel is niet verenigbaar met het oorspronkelijke doel.	Ja. *Aanbevolen maatregel:* Eventuele nieuwe doelen toetsen door middel van een PIA. Zo moet er bijvoorbeeld in de toekomst getoetst worden of een nieuw doel verenigbaar is met het oorspronkelijke doel.
II.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) de functionaris voor de gegevensbescherming, of (b) het	De verwerking van de persoonsgegevens in de databank is niet nieuw en is opgenomen in de meldingen (Verwerkingen van persoonsgegevens door de Belastingdienst en de FIOD, 30 augustus 2013) zoals gepubliceerd op de website van de Belastingdienst. De aard van de publiekrechtelijke taak van de Belastingdienst maakt dat de handhavings- en toezichtinstrumenten van de Belastingdienst slechts beperkt gepubliceerd kunnen worden. Hoewel de overheid in zijn algemeenheid transparantie nastreeft past de Belastingdienst terughoudendheid in haar publicaties.	Nee.

[4] Function creep hoeft op zichzelf niet negatief te zijn. Het herbergt wel een risico van Wbp-schending in zich.

	Cbp indien er geen FG is?		
II.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?	In de toekomst zal er nog een PIA moeten worden afgenomen om het gebruik van de persoonsgegevens in de databank te controleren.	Ja. *Aanbevolen maatregel:* Bij nieuwe doelen is het raadzaam het PIA-instrument te gebruiken als toetsing op de naleving van de Wbp.
II.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?	De toetsing van de kwaliteit van de processen rondom de databank is onvoldoende gestructureerd. In het beheer van de databank moet nadrukkelijk aandacht komen voor de toets op de naleving van de Wbp en het voldoen aan andere normen zoals beschreven in het Handboek beveiliging Belastingdienst (HBB) en de Baseline beveiliging rijk (BIR). Ook de richtsnoeren van het College bescherming persoonsgegevens (CBP) over de beveiliging van persoonsgegevens moeten worden nageleefd. Documenteren van de processen en de processtappen is een eerste zet. Het inwinnen en het beheer van de gegevens uit de databank zal op korte termijn een activiteit worden van B/CA (Centrale Informatievoorziening ,CIV/Inwinnen en Verstrekken van Gegevens, IVG). Binnen B/CA is veel expertise en er wordt standaard gewerkt met behulp van protocollen.	Ja. *Aanbevolen maatregel:* De informatiebeveiliging van de databank Auto moet geregeld worden conform het HBB, BIR en de Cbp richtsnoeren. De overdracht naar B/CA zo snel mogelijk realiseren.

II.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?	Ja. De databank wordt gebruikt voor risicoselectie. Deze risicoselectie houdt per definitie in dat groepen kentekens worden onderscheiden als meer of minder risicovol in de zin van onvolledige/onjuiste belastingopbrengsten. In die zin kun je spreken van profiling.	Ja. *Aanbevolen maatregel:* Indien er nieuwe risicoprofielen worden ontwikkeld moeten deze getoetst worden door middel van de PIA (zie de PIA van de Belastingdienst, het onderdeel profilering).
II.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?	Er worden persoonsgegevens aan elkaar gekoppeld en met elkaar vergeleken. De uitkomsten van het geautomatiseerde proces worden gebruikt om de toezichtcapaciteit gericht in te vullen. Er worden geen geautomatiseerde beslissingen genomen op louter digitale informatie uit de databank*. De databank voorziet in de mogelijkheid tot gerichte renseignering (bijvoorbeeld t.b.v. belastingcontroles) en risicoselectie en -analyse. *Opmerking: B/CA is eveneens een gebruiker van de databank en vergelijkt geautomatiseerd de signaleringen van geschorste/handelsvoorraad auto's (toezicht op MRB). Zie ook Bijlage 1.	Nee.
III	**Betrokken instanties/systemen**		

	en verantwoordelijkheid		
III.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?	Zie het overzicht van bronbestanden en ook het overzicht waarin wordt gepubliceerd welke overheidsinstanties het BSN mogen gebruiken.	Nee.
III.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?	Persoonsgegevens is de verantwoordelijke voor de databank.	Nee.

III.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?	Er wordt een register bijgehouden van alle verleende autorisaties waarin wordt vastgelegd per wanneer de autorisatie verleend is en met welk doel hij is aangevraagd. Een autorisatie wordt voor een jaar verleend. Jaarlijks zal worden getoetst of de autorisatie verlengd wordt. Mutaties worden verwerkt in het register. Indien er gedurende een periode van een half jaar geen gebruik is gemaakt van de autorisatie wordt deze door LCA beëindigd. Ten tijde van het uitvoeren van deze PIA zijn er 1715 autorisaties uitgegeven. Er wordt gewerkt met autorisatieprofielen en er vinden regelmatig updates plaats.	Ja. Het is noodzakelijk een adequaat autorisatieproces te hanteren. Er moet beschreven worden wie en waarom diegene autorisatie heeft gekregen. *Aanbevolen maatregel:* Beoordeel de huidige autorisatielijst en de autorisatieprofielen. Een belangrijke vraag is of iedereen slechts toegang krijgt tot de gegevens die noodzakelijk zijn voor zijn of haar werkzaamheden (niet meer dan nodig).
III.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. Voor alle mensen die werken met de databank geldt artikel 67 AWR onverkort.	Nee.
III.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?	Nee. Zie V.1. Zie ook het overzicht in Bijlage 1.	Nee

III.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)?	Het LCA heeft een algemeen beleid en nog geen expliciet beleid voor de databank. Het beleid voor de databank moet HBB conform worden geformuleerd waarbij de Richtsnoeren van CBP tot leidraad kunnen dienen.	Ja. *Aanbevolen maatregel:* Formuleer Wbp-conform beleid en procedures omtrent de databank
III.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.	Nee.

IV	Beveiliging en bewaring/vernietiging		
IV.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 ?	De gegevensbeveiliging van de databank is nog niet voldoende ingeregeld binnen het LCA.	Ja. *Aanbevolen maatregel:* Conformeer de handelswijzen bij het LCA aan het HBB (en daarmee impliciet aan de BIR en de beveiligingsrichtsnoeren van het CBP).
IV.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 wordt een bewerker ingehuurd die de schil en de workflow managementsystemen heeft gebouwd. ode bewerker ontwikkelt thuis en het testen gebeurt door de gebruikers van de (ver)nieuw(d)e functionaliteit. De bewerker heeft wel een geheimhoudingsverklaring getekend en er is een overeenkomst. Dit contract is er al jaren. De bewerker kan terecht op een Belastingdienst PC en doet ook nog wel andere klussen bij LCA op offertebasis.	Ja. *Aanbevolen maatregel:* Zorg voor een adequate bewerkersovereenkomst met de bewerker en gebruik daarvoor het Arvodimodel. Zorg voor een adequate beveiliging van de persoonsgegevens als de bewerker daar toegang toe heeft.
IV.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	Autorisatie via user ID en login en het loggen van het inloggen.	Ja. *Aanbevolen maatregel:* Zie de aanbeveling van vraag IV.1.

	(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?		
IV.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?	Zie aanbeveling bij IV.1. De procedures moeten conform HBB geregeld worden. De server waar de databank op draait staat nu nog in Almelo en gaat naar B/CA in Apeldoorn. Analyse, ontwikkeling, productie omgeving bijvoorbeeld worden nu gescheiden. Hier is een schema van gemaakt (zie Bijlage 3).	Ja. *Aanbevolen maatregel:* Zie de aanbeveling van vraag IV.1.
IV.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?	Momenteel wordt er door het LCA nagedacht over nieuwe bewaartermijnen van contra-informatie. Het idee is om alle contra-informatie welke ten behoeve van de processen van LCA wordt gebruikt via een filter binnen te halen. Dat betekent dat die gegevens die we als LCA niet via een filter inlezen niet langer beschikbaar hoeven te blijven voor ons toezicht proces en per direct kunnen worden vernietigd. Deze vernietiging wordt uitgevoerd door de beheerder, BCA/IVG. Uiteraard kan gebruik door andere partijen binnen de Belastingdienst langer bewaren noodzakelijk maken. Contra-informatie die door LCA wordt ingewonnen via het filter zal worden aangewend ten behoeve van toezicht. Dit toezicht omvat een proces	Nee.

		inclusief bezwaar en beroep. De toezichtwensen worden afgestemd met de overige segmenten en zullen bepalend worden voor het inwinnen van contra informatie. Het inwinnen van contra informatie sluit daarmee aan op het toezicht dat door de Belastingdienst wordt uitgeoefend. Vervolgens zal een keer per jaar zal worden getoetst welke contra-informatie daadwerkelijk in toezicht is gebruikt. Informatie die (nog) niet is aangewend wordt vernietigd. Informatie die in toezicht is gebruikt en waarvan het toezichtproces is afgerond zullen eveneens worden vernietigd. Contra informatie waarvan het toezicht proces nog niet is afgerond (bezwaar en beroep) zal nog beschikbaar blijven. De rest van de persoonsgegevens wordt bewaard volgens de normale bewaar/archief afspraken. Conform bestaande wet- en regelgeving (archiefwet).	
IV.6	Op welke beleidsmatige en technische gronden is deze termijn van bewaring vereist?	Toezichteisen en aangiftetermijnen, navorderings- en naheffing aanslagtermijnen en bezwaarprocedures bepalen de lengte van bewaartermijnen.	Nee.
IV.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 vernietiging van de gegevens wordt uitgevoerd door de beheerder, BCA/IVG. Het kan voorkomen dat medewerkers contra-informatie op een eigen computer bewaren omdat dat nodig is geweest voor het uitvoeren van bepaalde bewerkingen. Ook al is deze informatie alleen voor die medewerker benaderbaar, het is ongewenst dat deze informatie bewaard blijft buiten de afspraken om. Jaarlijks zullen alle medewerkers per mail worden bevraagd te bevestigen dat alle contra informatie welke niet meer in (fiscale) productie is, door hen verwijderd is uit kasten, laden en computerbestanden. Er is dan slechts één plaats waar dergelijke informatie voorhanden is en dat is de databank . Deze procedure wordt vastgelegd en per medewerker wordt bijgehouden dat er geschoond is.	Nee.

V	**Transparantie en rechten van betrokkenen**		
V.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?	Zie de meldingen "*Verwerkingen van persoonsgegevens door de Belastingdienst en de FIOD*". Hier wordt een beschrijving gegeven van de persoonsgegevens die door de Belastingdienst verwerkt worden. Hieronder vallen ook de persoonsgegevens die in de databank gebruikt worden. Omdat het bij de onderhavige verwerkingen gaat om strategische informatie van de Belastingdienst kan niet alles in detail worden gepubliceerd. In zijn algemeenheid zijn betrokkenen op de hoogte van de controle en selectiemethodieken van de Belastingdienst.	Nee.
V.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.	Nee.
V.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?	Via de op de website van de Belastingdienst gepubliceerde meldingen en de brochure in algemene zin maar niet in expliciete zin.	Nee.

V.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.	Nee
V.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?	Er wordt gebruik gemaakt van de standaard Belastingdienstoplossingen. Zie ook de folder: De Belastingdienst en de Wet bescherming persoonsgegevens (Wbp). Hier wordt ook vermeld dat men recht heeft op inzage en correctie.	Nee.
V.6	Hoe kan een verzoek van een betrokkene tot verbetering, aanvulling, verwijdering of afscherming van persoonsgegevens in behandeling worden genomen?	Via de folder en via Persoonsgegevens komt het verzoek terecht in de functionele postbus Persoonsgegevens	Nee.

Bijlage 1: Overzicht bronbestanden Databank Auto

Bestand	Bron	Omschrijving inhoud	Frequentie	Categorieën gegevens	Feitelijk doel van de gegevens
H099 Nieuw	CIV	Bestaat uit meederde deelbestanden bevat alle informatie wagenpark NL uit HSB	maand	1: Voertuiggegevens	Dit is het kentekenregister (van auto's die op naam staan). Dit is nodig voor de query's. Het zijn alle auto's, dus niet alleen zakelijke auto's (HSB, houderschapsbelasting).
CJIB	CJIB/BCA	Alle verkeersboetes van de zakelijke auto's	maand	2: Contra-Informatie (extern)	Vastlegging van plaats en tijd (waar en wanneer reed een voertuig). Het betreft hier alle wegen. Deze waarnemingen kunnen worden gebruikt voor het toezicht privégebruik auto (IH, LH, Vpb en OB.) en de omzetverantwoording (IH, Vpb en OB). Tevens worden deze gegevens gebruikt voor het toezicht op de motorrijtuigenbelasting (MRB) en de belasting zware motorrijtuigen (BZM) én de wettelijke teurgmelding i.h.k.v. stelsel van basisregisters.
ECB	KLPD/CIE	Externe Camera Beelden	wekelijks	2: Contra-Informatie (extern)	Vastlegging van plaats en tijd (waar en wanneer reed een voertuig). Het betreft hier alle wegen. Deze waarnemingen kunnen worden gebruikt voor het toezicht privégebruik auto (IH, LH, Vpb en OB.) en de omzetverantwoording (IH, Vpb en OB). Tevens worden deze gegevens gebruikt voor het toezicht op de motorrijtuigenbelasting (MRB) en de belasting zware motorrijtuigen (BZM) én de wettelijke teurgmelding i.h.k.v. stelsel van basisregisters.
ANPR	BCA	Ongefilterde camerabeelden van onze eigen ANPR camera voeruigen	maand	3: Contra-Informatie (intern)	Vastlegging van plaats en tijd (waar en wanneer reed een voertuig). Het betreft hier alle wegen. Deze waarnemingen kunnen worden gebruikt voor het toezicht privégebruik auto (IH, LH, Vpb en OB.) en de omzetverantwoording (IH, Vpb en OB). Tevens worden deze gegevens gebruikt voor het toezicht op de motorrijtuigenbelasting (MRB) en de belasting zware motorrijtuigen (BZM) én de wettelijke teurgmelding i.h.k.v. stelsel van basisregisters.
ANPR GPS	LCA	Door middel van speciaal van externe partij aangkochte software de GPS codering omgezet in herkenbare straat en plaats namen	maand	2: Contra-Informatie (extern)	Hulpbestand voor ANPR (dit is software).
FLG	LTO	Loongegevens wernemers NL	maand	3: Contra-Informatie (intern)	PGA: Nodig om te achterhalen of iemand wel of niet bijtelt (ook de code voor de reden niet bijtellen). Afvragen of toezicht PGA ook moet zien wat iemand verdient. BPM: Inkomen van iemand nodig om te bepalen waar iemand woont (woonplaatsbeginsel).
Polis	UWV/BCA	Loongegevens NL specifiek raking auto	maand	2: Contra-Informatie (intern)	Alleen loongegevens die met auto te maken hebben. Nodig in toezicht.
BVR	LTO	Is kopie van BVR dump wat voor IT/IVT gebruikt word	maand	4: Basis gegevens	Nodig om de populatie te bepalen voor query's.
PGA Kentekenkaart	LCA	Dump uit LOTUS PGA systeem die alle kentekens bevat gebruikt de Verklaringhouders	2 wekelijks	5: Productiegegevens	Kentekens van verklaringhouders. Nodig om te achterhalen wie de verklaringhouders PGA zijn. Gebruikt in toezicht PGA.
PGA Naheffing	Real-Time	Alle door PGA opgelegde naheffingen (Rechtstreekse koppeling met produktie systeem)		5: Productiegegevens	Om een beeld te krijgen of mensen al eerder zijn naageheven.
PGA Verklaringhouders	LCA	Dump uit LOTUS PGA systeem die alle Verklaringhouders bevat	2 wekelijks	5: Productiegegevens	Kentekens van verklaringhouders. Nodig om te achterhalen wie de verklaringhouders PGA zijn. Gebruikt in toezicht PGA.
PGA Mutaties	LCA	Dump uit LOTUS PGA systeem die alle mutaties op Verklaringhouders	2 wekelijks	5: Productiegegevens	Nodig om te weten wat er veranderd is bij verklaringhouders (bijv nieuw kenteken).

Aanhangwagens	BCA	Op aanvraag verstrekt bestand van caravans en aanhangwagens	afroep	1: Voertuiggegevens	Staat alleen op de analyse server om een query te maken. Het bestand wordt ook gebruikt voor andere disciplines bij de Belastingdienst, zoals o.a. de FIOD. Bestand komt regulier bij de B/CA binnen en wordt op verzoek aan het LCA verstrekt.
Lease	BCA	Wisselend periodieke opleverings van bestanden die via BCA portaal door leasmaatschappijen worden ingestuurd		1: Voertuiggegevens	Is niet betrouwbaar, omdat we niet van alle leasemaatschapijnen de gegevens krijgen. Inhoudelijk is de data ook onjuist. Leasegegevens worden getoets. Ze worden alleen gebruikt als ze vallide zijn. De gegevens worden in toezicht PGA gebruikt.
H053	CIV	Alle zakelijke kentekens	maand	1: Voertuiggegevens	Om te bepalen wat de zakelijke kentekens zijn (mogelijk in de toekomst overbodig omdat het ook met HSB zou kunnen). H053 is een query om de voertuigegevens aan de RSIN nummers met een economische activiteit toe te voegen
UR1900A1	CIV	Alle ondernemers	maand	4: Basis gegevens	Om het wagenpark van een bedrijf in kaart te kunnen brengen (query). Ook nodig voor toezicht in het land (vullen van het TOP dossier).
UZGB Verklaringhouders	LCA	Dump uit LOTUS UZGB systeem die alle Verklaringhouders bevat	maand	5: Productiegegevens	Nodig om te achterhalen wie de verklaringhouders UZGB zijn. Gebruikt in toezicht UZGB
UZGB FIS	BOB/LCA	Door Fissers middels een app verzameld foto materiaal	afroep	3: Contra-Informatie (intern)	Mogelijk gebruikt voor UZGB toezicht.
RTL	RDW/BCA	Bevat alle verleggingen van de aansprakelijkheid op een kenteken	afroep	1: Voertuiggegevens	Verlegde aansprakelijkheid (APK, MRB, verzekering). De auto is eigenlijk van iemand anders (voorbeeld: betaal nu 50%, de rest over 2 jaar. Dan is het bedrijf nog officeel eigenaar en jij nog niet). Doel voor PGA: om te achterhalen wie de auto gebruikt. Dit wordt niet regulier opgevraagd bij de RDW. Is 1 of 2x opgevraagd i.h.k.v. een pilot.
APK	RDW/BCA	Bevat alle gegevens over de Alemene Periodiek Autokeuring van alle kentekens	afroep	2: Contra-Informatie (extern)	Plaats, tijd, keuringsstation en kilometerstand. Gebruikt in toezicht. Zakelijk voor PGA. Niet zakelijk nodig voor MRB (bijv schorsers). Wordt niet meer ververst. Hiervoor is een reguliere applicatie door de RDW ontwikkeld. Afspraak: 1x per week maximaal 20 kentekens uitvragen.
CNV	Oost	Alle afgesloten Belastingdiens Convenanten	maand	4: Basis gegevens	Nodig om te zien of het een convenant post is (zowel query als door medewerkers).
GOA	Oost	Alle openstaande belastingschulden	wekelijks	3: Contra-Informatie (intern)	Toezicht BPM (bepaling woonplaats).
Toeslagen	LTO	Overzicht van de toeslagen per BSN	afroep	2: Contra-Informatie (intern)	Toezicht BPM (bepaling woonplaats). Meest uitgebreide profiel kan dit zien. Het staat erin, maar de vraag is of het nog gebruikt wordt.
UZGB Workflow	Real-Time	Rechtreekse koppeling met het kantoorproces van de UZGB		5: Productiegegevens	Deze informatie is nodig om te zien of mensen in toezicht zitten en welke brieven ze hebben gehad.
PGA Workflow	Real-Time	Rechtreekse koppeling met het kantoorproces van de PGA		5: Productiegegevens	Deze informatie is nodig om te zien of mensen in toezicht zitten en welke brieven ze hebben gehad.

Correctiestaat PGA	Real-Time	Web-based opvoertool van terugmeldingen van landelijke PGA onderzoeken		5: Productiegegevens	Deze informatie is nodig om te zien wie een correctie PGA heeft gekregen. Ook nodig voor BI.
PGAS	Real-Time	Web-based opvoertool van renseigneringen gemaakt door onze FIS medewerkers		3: Contra-Informatie (intern)	Zichtwaarnemingen. Tijd en plaats signaleringen. Toezicht PGA/UZGB.
SURF	download	Dump van alle in SURF aanwezige onderzoeken	afroep	3: Contra-Informatie (intern)	Waarnemingen door bijvoorbeeld Fissers. Toezicht PGA/UZGB.
AxiTaxi	Real-Time	Web-based opvoertool van AxiTaxi renseigneringen		3: Contra-Informatie (intern)	Wordt gebruikt door het project Axi Taxi. Waarnemingen.
BPM Workflow	Real-Time	Rechtreekse koppeling met het kantoorproces van de BPM		5: Productiegegevens	Je kan hiermee zien welke posten in behandeling zijn.
ABD	UCI (Douane)	excel en access in SG, maandelijkse levering;	maand	5: Productiegegevens	Brongegeven voor het dashboard BPM (BI en stuurinformatie). Je kan in detail doorklikken. Niet te zien in klandbeeld auto (beperkte autorisatie). Samen BPMT vormt dit het dashboard.
BPMT	ZuidWest	restitutie BPM	maand	5: Productiegegevens	Brongegeven voor het dashboard BPM (BI en stuurinformatie). Je kan in detail doorklikken. Niet te zien in klandbeeld auto (beperkte autorisatie). Samen ABD vormt dit het dashboard.
Buitenlandse militairen	Persoonsgegevens		aanvraag	1: Voertuiggegevens	Niet meer gebruikt. Zit nu in HSB. Zitten niet in HSB maar eventueel in HSB accent, afhankelijk van de al dan niet van toepassing zijnde privilege
NL militairen	Persoonsgegevens		aanvraag	1: Voertuiggegevens	Niet gebruikt en hebben we ook niet.
BN GN kentekens	Persoonsgegevens		wekelijks	1: Voertuiggegevens	Niet meer gebruikt. Dit zit niet meer in HSB maar in HSB accent
HSB Accent	BCA	MRB buitenlandse kentekens	maand	1: Voertuiggegevens	HSB Accent wordt door het LCA maar beperkt gebruikt. Het is alleen nodig om te kijken of er op een buitenlands kenteken MRB wordt betaald en om die kentekens vervolgens uit te sluiten voor toezicht.
CJIB Buitenland	BCA	Verkeersboetes op buitenlandse kentekens	maand	2: Contra-Informatie (extern)	Vastlegging van plaats en tijd (waar reed iemand). Gaat om buitenlandse kentekens.
M016AA10	CIV	Alle zware vrachtauto's	maand	1: Voertuiggegevens	Toezicht BZM. Worden niet in klantbeeld getoont. Wordt gebruikt voor de vaststelling of een ECB waarneming al dan niet van toepassing is voor een BZM plichtig voertuig.

UR1940A1	CIV	Alle werkgevers van NL	maand	4: Basis gegevens	De werkgevers worden gekoppeld aan loongegevens. Wij tonen de naam en adresgegevens van de werkgever. Verschil met de BVR gegevens is dat hier ook historie in zit.
KC_GENNO27.csv	ATK+	Volgende velden worden in databank auto opgenomen: Klantcoördinator, VIPindicator (posten uit MZGO)		4: Basis gegevens	Nodig om af te schermen (VIP). KC'er nodig om te weten met wie er contact opgenomen moet worden.
ENT.DBF	IKB	Volgende velden worden in databank auto opgenomen: Aandachtcategorie, Zwaartecategorie, Risicoklasse		4: Basis gegevens	Comfortinformatie. Verwacht compliant gedrag voor de komende 6 maanden.

Bijlage 2: Protocol m.b.t. fiscale relevantie voertuigpassagegegevens

Belastingdienst

Belastingdienst

Protocol behorend bij het Convenant Belastingdienst-Politie inzake medegebruik van de ANPR-camera's van de Politie

Versie 1.00

Datum 18-12-2014
Auteur Persoonsgegevens

Protocol behorend bij het Convenant Belastingdienst-Politie
inzake medegebruik van de ANPR-camera's van de Politie

1.1 Doelstelling van dit protocol

Dit protocol geeft aan hoe de Belastingdienst concreet omgaat met voertuigpassagegegevens. Die gegevens worden uitsluitend gebruik als deze fiscaal relevant zijn. Dit houdt in dat de Belastingdienst deze gegevens slechts gebruikt ten behoeve van het toezicht op de juiste naleving van de belastingplicht en bij de heffing en inning van belastingen. Alleen voertuigpassagegegevens die fiscaal relevant zijn worden opgenomen in de databank auto.

1.2 Grondslag voor dit protocol

Dit protocol is gebaseerd op artikel 3:3 van het Convenant Belastingdienst-Politie inzake medegebruik van de ANPR-camera's van de Politie.

2 Noodzaak van het gebruik van voertuigpassagegegevens

Het verwerken van voertuigpassagegegevens is nodig, omdat geen andere informatie beschikbaar is of kan worden verkregen waarmee het toezicht op de naleving van belastingwetgeving indien en voor zover motorrijtuigen fiscaal relevant zijn. Voertuigpassagegegevens worden gebruikt voor het toezicht op de naleving van de volgende belastingwetten:

- Wet op de loonbelasting 1964 (vanwege privé gebruik auto);
- Wet Inkomstenbelasting 2001 (o.a. vanwege privé gebruik auto);
- Wet op de belasting van personenauto's en motorrijwielen 1992;
- Wet op de motorrijtuigenbelasting 1994;
- Wet belasting zware motorrijtuigen (eurovignet);
- Wet op de omzetbelasting 1968;
- Wet op de vennootschapsbelasting 1969.

2.2 Concretisering van fiscale relevantie

De volgende voertuigpassagegegevens zijn fiscaal relevant:

- Voertuigpassagegegevens die betrekking hebben op motorrijtuigen die geleerd zijn aan een ondernemer in de zin van de Wet op de Omzetbelasting 1968, de Wet op de Inkomstenbelasting 2001 of de Wet op de Vennootschapsbelasting, dan wel een inhoudingsplichtige in de zin van de Wet op de Loonbelasting 1964. Deze gegevens zijn naar hun aard altijd fiscaal relevant.
- Voertuigpassagegegevens die betrekking hebben op zware vrachtwagens waarop de Wet belasting zware motorrijtuigen van toepassing is zijn naar hun aard ook altijd fiscaal relevant.
- Voertuigpassagegegevens die betrekking hebben op motorrijtuigen op naam van particulieren, niet-ondernemers, worden alleen verwerkt als daar een concrete aanleiding voor is. Zij zijn fiscaal relevant als ten aanzien van die motorrijtuigen sprake is van een aanwijzing dat een daarop betrekking hebbende verplichting op basis van de Wet op de motorrijtuigenbelasting 1994 of de Wet op de belasting van personenauto's en motorrijwielen 1992 niet is of wordt nageleefd.

4 Inzage- en correctierecht

Houders van voertuigen hebben het recht desgevraagd informatie te ontvangen van de Belastingdienst over de voertuigpassagegegevens die zijn opgeslagen in de databank, indien deze gegevens gerelateerd kunnen worden aan concrete navorderingsaanslagen, dan wel naheffingsaanslagen. Voor de overige opgeslagen gegevens geldt dat deze vallen onder de reikwijdte van artikel 43 sub d van de Wet bescherming persoonsgegevens.
De gegevens zullen worden gecorrigeerd of verwijderd als blijkt dat ze niet juist zijn.

Belastingdienst

Protocol behorend bij het Convenant Belastingdienst-Politie
inzake medegebruik van de ANPR-camera's van de Politie

Deze gegevens worden desgewenst overgelegd aan een belastingplichtige als er sprake is van een bezwaar- of beroepsprocedure waarin deze gegevens een rol spelen. In het kader van de vrije bewijsleer kan hij daarop reageren.

5. Verwijderen van voertuigpassagegegevens

De voertuigpassagegegevens die zijn opgenomen in de databank worden verwijderd nadat duidelijk is geworden dat de fiscale relevantie niet meer van toepassing is. Periodiek, maar minimaal eenmaal per jaar, wordt de databank geschoond.

6. Evaluatie

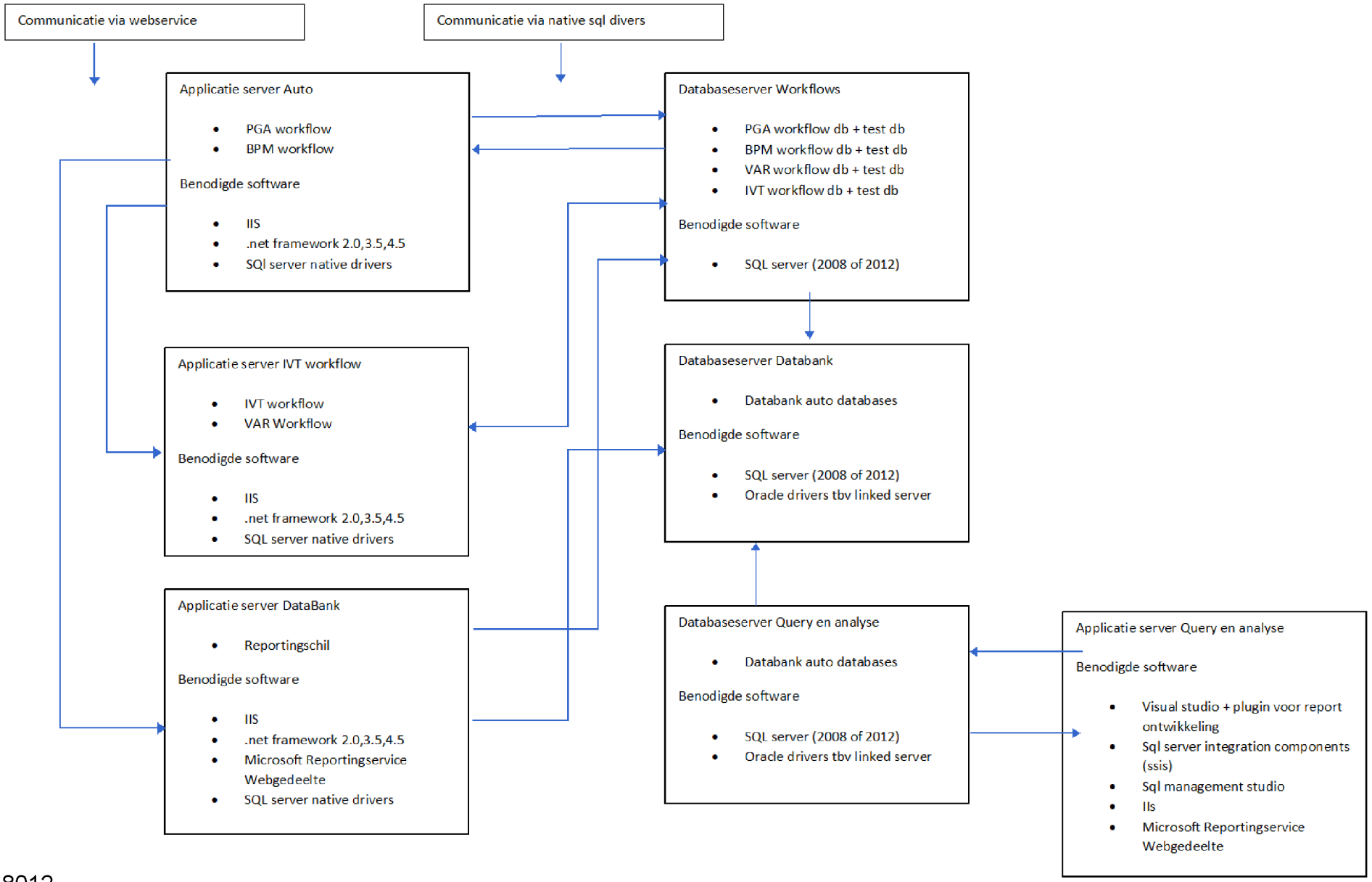
De Belastingdienst zal jaarlijks evalueren of het protocol voldoet aan zijn doelstellingen en aansluit bij de huidige en mogelijke toekomstige ontwikkelingen. Indien nodig past hij het protocol aan. Tevens zal bij deze evaluatie onderzocht worden of het filter moet worden aangepast in het licht van wetgeving, jurisprudentie en het te voeren toezicht.

Aldus opgemaakt door de Belastingdienst/Centrale Administratie te Apeldoorn
en ondertekend op 18 december 2014.

Persoonsgegevens

2

Bijlage 3: Weergave architectuur nieuwe servers



Belastingdienst

Privacy Impact Assessment: Databank Auto

Overzicht van mogelijke risico's en aanbevelingen:

1. Informatiebeveiliging

Risico:
De gegevensbeveiliging van de databank is nog niet voldoende ingeregeld. In het beheer van de databank moet nadrukkelijk aandacht komen voor de toets op de naleving van de Wet bescherming persoonsgegevens (Wbp) en het voldoen aan (beveiligings)normen zoals beschreven in het Handboek Beveiliging Belastingdienst (HBB) en de Baseline Informatiebeveiliging Rijksdienst (BIR). Ook de richtsnoeren beveiliging van persoonsgegevens van het College bescherming persoonsgegevens (CBP) moeten worden nageleefd.

Aanbeveling:
De informatiebeveiliging van de databank Auto moet geregeld worden conform het HBB, BIR en de CBP richtsnoeren. Het inwinnen en het beheer van de gegevens uit de databank zal op korte termijn een activiteit worden van Belastingdienst/Centrale Administratie, B/CA (Unit Centrale Informatievoorziening, CIV/Unit Inwinnen en Verstrekken van Gegevens, IVG). Binnen B/CA is veel expertise en er wordt standaard gewerkt met behulp van protocollen. De overdracht naar B/CA zal zo snel mogelijk gerealiseerd moeten worden.

2. Bronbestanden

Risico:
In de databank zitten verscheiden bronbestanden (zie Bijlage 1 van het volledige PIA-document). Bij enkele bestanden is het de vraag of ze daadwerkelijk noodzakelijk zijn voor het toezicht op de autobelastingen.

Aanbeveling:
Momenteel wordt er nagedacht over een opschoning van de databank. Daarbij wordt er gekeken welke gegevens eventueel niet meer noodzakelijk zijn voor de databank. Het is aan te raden om bij de beoordeling van de bestanden in de databank gebruik te maken van het overzicht in Bijlage 1. Per bestand moet er beoordeeld worden of het bestand noodzakelijk is voor het toezicht op de autobelastingen.

3. Autorisaties

Risico:
Er wordt een register bijgehouden van alle verleende autorisaties waarin wordt vastgelegd per wanneer de autorisatie verleend is en met welk doel hij is aangevraagd. Ten tijde van het uitvoeren van deze PIA zijn er 1715 autorisaties uitgegeven. Verder wordt er gewerkt met autorisatieprofielen. De vraag is echter of de huidige autorisatieprofielen toereikend zijn.

Aanbeveling:
Het is noodzakelijk om een adequaat autorisatieproces te hanteren, dus de huidige autorisatielijst en de autorisatieprofielen moeten beoordeeld worden. Er moet getoetst worden of iedereen met een autorisatie enkel toegang heeft tot de gegevens die noodzakelijk zijn voor zijn of haar werkzaamheden (niet meer dan nodig).

4. Nieuwe doeleinden

Risico:
De databank wordt in de loop van haar bestaan gebruikt voor meerdere doeleinden. Daarmee ligt het gevaar van ongecontroleerde *function creep* op de loer (dat de persoonsgegevens voor andere doeleinden worden gebruikt dan oorspronkelijk bedoeld was). Daar zal extra aandacht voor moeten zijn bij het beheer van de databank.

Aanbeveling:
Eventuele nieuwe doelen moeten worden getoetst door middel van een PIA. Zo moet er bijvoorbeeld in de toekomst getoetst worden of een nieuw doel verenigbaar is met het oorspronkelijke doel. Tevens moeten eventuele nieuwe risicoprofielen getoetst worden door middel van de PIA (zie de PIA van de Belastingdienst, het onderdeel profilering).

5. Exporteer-knop

Risico:
Er zit een exporteer-knop in de databank. Daarmee kan men de scherminhoud exporteren naar een ander formaat (Excel, PDF, Word, etc.). Daarmee kan de informatie uit de databank worden gebruikt in andere applicaties die de Belastingdienst in haar toezichtproces gebruikt. Nu de Belastingdienst werkt met Digitale Werkruimte Belastingdienst (DWB) werkplekken waarbij tijd- en plaats onafhankelijk kan worden gewerkt, is deze knop wellicht niet meer nodig.

Aanbeveling:
Onderzoek de noodzaak voor deze exporteer-knop in relatie tot de DWB-werkplekken waarmee iedere geautoriseerde medewerker op locatie (op plekken met beveiligde WiFi-verbinding) toegang heeft tot de databank