

# GEGEVENSBESCHERMINGSEFFECTBEOORDELING RIJKSDIENST (PIA)

## Verwijzingsportaal Bankgegevens

### A. Beschrijving algemene kenmerken gegevensverwerkingen

#### 1. Voorstel

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

##### *Verwijzingsportaal Bankgegevens*

Het Verwijzingsportaal Bankgegevens (hierna: VB) is een technische voorziening die het mogelijk maakt om identificerende bankgegevens van natuurlijke en rechtspersonen, en identificerende gegevens behorend bij financiële producten op basis van de huidige bevoegdheden van de opsporingsambtenaar, de FIU-Nederland en van de Belastingdienst geautomatiseerd, real-time op te vragen en voor banken en andere betaaldienstverleners die rekeningen en/of kluizen aanbieden<sup>1</sup> om ze geautomatiseerd te verstrekken. Doel van het VB is het betrouwbaar, snel, juist, volledig en efficiënt, digitaal opvragen en verstrekken van deze gegevens op een uniforme wijze bij alle in Nederland gevestigde banken, ten behoeve van het voorkomen en opsporen van fraude en andere vormen van criminaliteit. Door de komst van het VB verandert de wijze van verstrekking.

Het VB beoogt de gegevensverstrekking zo efficiënt mogelijk te effectueren en beoogt de wettelijke bevoegdheden gegevens op te vragen en te vorderen niet in te perken of te verruimen. Het VB verandert ook niet de gegevens die worden verstrekt of de doeleinden waarvoor dit gebeurt<sup>2</sup>. Zie voor het proces ook Aanwijzing opsporingsbevoegdheden, paragraaf 2:10. Dit betekent niet dat er met de komst van het VB niets zal veranderen. Om het opvragen, vorderen en verstrekken van gegevens via het VB zo efficiënt en gericht mogelijk te laten verlopen, voorziet het wetsvoorstel in een wettelijke grondslag voor het gebruik van het BSN door banken ten behoeve van het koppelen van een verzoek aan de gegevens uit de klantadministratie. Daarnaast komt door de automatische koppeling van een verzoek aan gegevens uit de klantadministratie van de bank de menselijke controle aan de kant van de bank, die in het huidige proces aan de verstrekking van gegevens vooraf gaat, te vervallen. Deze wijzigingen komen in deze PIA aan bod, evenals de maatregelen die worden genomen om de daarmee gepaard gaande risico's te beperken.

Er zijn drie opvraagmogelijkheden via het VB:

1. Op basis van persoons- en/of adresgegevens wordt informatie opgevraagd.
2. Op basis van een product, wordt informatie opgevraagd (productnummer en zo mogelijk soort product).
3. Rekeningnummerverificatie.

In paragraaf 3 wordt verder ingegaan op het verwerkingsproces en de grondslagen hiervoor.

Deze PIA heeft betrekking op het wetsvoorstel ter Wijziging van de Wet op het financieel toezicht in verband met het via een centraal systeem geautomatiseerd verstrekken van identificerende gegevens door banken en betaaldienstverleners (Wet verwijzingsportaal bankgegevens). In dit document wordt op verschillende plaatsen verwezen naar een pilot. In deze pilot wordt het systeem VB getest met een aantal (groot)banken. De resultaten van de genoemde pilot kunnen ervoor zorgen dat zowel het systeem als de afspraken over het gebruik van het systeem worden aangepast. Zo nodig zal deze PIA dienovereenkomstig worden geactualiseerd.

##### *Aangesloten partijen*

De volgende partijen nemen deel aan het VB:

<sup>1</sup> In de rest van dit document wordt voor de leesbaarheid enkel banken genoemd. Hiermee wordt steeds bedoeld banken en andere betaaldienstverleners die rekeningen en/of kluizen aanbieden.

<sup>2</sup> Het proces 1BRN kent door de komst van het VB wel een nieuw proces.

- Nationale Politie (hierna: NP)
- Openbaar Ministerie (hierna: OM)
- De Koninklijke Marechaussee (KMar)
- De Rijksrecherche
- Bijzondere Opsporingsdiensten:
  - de Fiscale Inlichtingen- en Opsporingsdienst (hierna: FIOD);
  - de Inlichtingen- en Opsporingsdienst van de Nederlandse Voedsel- en Warenautoriteit (hierna: NVWA-IOD);
  - de directie Opsporing van de Inspectie Sociale Zaken en Werkgelegenheid (hierna: Inspectie SZW);
  - de Inlichtingen- en Opsporingsdienst van de Inspectie Leefomgeving en Transport (hierna: ILT/IOD)<sup>3</sup>
- de Belastingdienst: Belastingdienst(BD-heffing), Douane (heffing), BD(inning), Douane (inning) BD(Toeslagen/ heffing) en BD(Toeslagen/ inning)
- FIU Nederland
- banken die betaalrekeningen met een Nederlands IBAN-nummer en/of kluizen aanbieden

Deze partijen zijn betrokken bij het opstellen van deze PIA. Omdat de betrokkenen, cliënten en gemachtigden van wie gegevens kunnen worden opgevraagd via het VB geen afgebakende groep zijn, is ervoor gekozen om hen de gelegenheid te bieden te reageren op het wetsvoorstel en het ontwerp voor de algemene maatregel van bestuur door middel van een internetconsultatie. Daarbij hebben verschillende partijen gereageerd die zich sterk maken voor de bescherming van persoonsgegevens.

*Bijzonderheden m.b.t. het VB en de geldende wetgeving en privacyregimes*

Op de verwerking van persoonsgegevens door deze organisaties zijn verschillende wettelijke regimes van toepassing (zie verder bij paragraaf 3 en 4), afhankelijk van de partij van wie gegevens afkomstig zijn. Enkele van deze regimes zullen tussen het moment van opstellen van de PIA en het moment van inwerkingtreding van de wetgeving waarmee het gebruik van het VB wordt voorgeschreven, wijzigen omdat nieuwe wetgeving inwerking treedt. Dit betreffen de volgende regimes:

1. De Wet politiegegevens en het Besluit politiegegevens (en Besluit politiegegevens bijzondere opsporingsdiensten) zijn van toepassing op de gegevensverwerking door de opsporingsinstanties. Deze wet en dit besluit wijzigen naar verwachting in de loop van 2018 omdat de Richtlijn gegevensbescherming opsporing en vervolging hierin wordt geïmplementeerd (implementatiedeadline 6 mei 2018).
2. Een aantal bepalingen uit de Wet politiegegevens is van overeenkomstige toepassing op de gegevensverwerking door de FIU-Nederland (art. 14 lid 3 Wwft). Ook deze bepalingen zullen wijzigen na de implementatie van de richtlijn.
3. Vanaf 25 mei 2018 is de Algemene Verordening Gegevensbescherming (AVG) en de uitvoeringswet AVG van toepassing op de verwerking van persoonsgegevens door de Belastingdienst<sup>4</sup> en de banken.

In dit document zal daarom waar nodig worden verwezen naar de bepalingen uit de oude en de nieuwe bepalingen in verschillende wetten. Voor het systeem betekent dit dat aan eisen uit verschillende wetten moet worden voldaan.

<sup>3</sup> In de rest van dit document wordt voor de leesbaarheid steeds opsporingsinstanties gebruikt indien het om alle volgende instanties gaat: NP, KMar, de Rijksrecherche en de bijzondere opsporingsdiensten.

<sup>4</sup> FIOD uitgezonderd.

## 2. Persoonsgegevens

Geef alle categorieën van persoonsgegevens die worden verwerkt. Geef per categorie van betrokkene aan welke persoonsgegevens van hen verwerkt worden. Deel deze persoonsgegevens in onder de typen: gewoon, bijzonder, strafrechtelijk en wettelijk identificatienummer.

Het VB wordt gebruikt voor het opvragen van identificerende gegevens van klanten bij banken (opsporingsdiensten) en voor rekeningverificatie (Belastingdienst) voor zover hiertoe een wettelijk voorschrift bestaat (zie ook de tekst bij vraag 4 en 14 m.b.t. omschrijving doel van het VB). Dit zijn twee verschillende processen waarvoor verschillende persoonsgegevens kunnen worden verwerkt. De persoonsgegevens kunnen betrekking hebben op de rekeninghouder(s), maar ook op de gemachtigde(n)<sup>5</sup>. Daarnaast worden via het verwijzingsportaal administratieve kenmerken verstrekt over het productbezit van een persoon, te weten de productsoort, de status van het product en de rol van de betrokkene (cliënt of gemachtigde). In lijn met de terminologie van artikel 126nc van het Wetboek van Strafvordering worden ook deze gegevens in het portaal en het wetsvoorstel aangeduid als 'identificerende gegevens'.

Welke gegevens een aangesloten overheidsinstantie in een concreet geval kan opvragen of vorderen hangt af van de wettelijke grondslag die daartoe wordt ingezet. Overheidsinstanties kunnen in het VB alleen de gegevens opvragen of vorderen waar ze op grond van de hen toekomende bevoegdheden toe gerechtigd zijn. De volgende identificerende gegevens zullen via het portaal beschikbaar zijn:

- in geval van een natuurlijk persoon: naam, tenaamstelling van de rekening, de kluis of het financiële product, adres, woonplaats, postadres, geboortedatum, en administratieve kenmerken (is het product actief of beëindigd, is de betreffende persoon zelf cliënt of gemachtigde);
- in geval van een rechtspersoon: naam, tenaamstelling van de rekening, de kluis of het financiële product, adres, vestigingsplaats, postadres, nummer van inschrijving bij de Kamer van Koophandel en administratieve kenmerken.

Voor het opvragen van deze gegevens via het portaal worden dezelfde identificerende gegevens verwerkt. Daarnaast kan hiervoor het BSN worden gebruikt.

Tenslotte worden bij het gebruik van het portaal persoonsgegevens geregistreerd ten behoeve van de controle op het gebruik van het portaal. Dit zijn gegevens van de opsporingsambtenaar die van het portaal gebruik maakt. Het betreft de volgende gegevens:

- Naam
- Organisatienaam opsporingsdienst

*Toelichting type persoonsgegevens:*

*Nb! Aard gegevens bepalend voor type bevraging.*

Bovenstaande gegevens moeten afhankelijk van de aard van de vragende instantie worden ingedeeld naar categorie/type, en het doel waarvoor de gegevens zullen worden verwerkt. Ook kan de aard van de gegevens bepalend zijn voor het wettelijk kader, de risico's die de gegevensverwerking met zich brengt en de maatregelen die moeten worden genomen om deze risico's te beperken. Het gaat met name om de vraag of de Wpg wel of niet van toepassing is, en of er sprake is van bijzondere persoonsgegevens of een nummer waar de Wabb op van toepassing is/was.

De aard van de gegevens op het moment van verwerking door de vragende partij is als volgt:

---

<sup>5</sup> Met gemachtigde wordt gevolmachtigde bedoeld. Gevolmachtigde is in dit kader de natuurlijke persoon die van de bankklant een volmacht heeft gekregen om in naam van de klant over de rekening te kunnen beschikken.

- Alle persoonsgegevens die door een van de opsporingsdiensten worden verwerkt in een strafrechtelijke vordering zijn politiegegevens in de zin van artikel 1 onder a Wpg;
- Er worden door de Belastingdienst geen bijzondere of strafrechtelijke gegevens in de zin van artikel 9 en 10 AVG verwerkt. Dit betekent dat alleen gewone persoonsgegevens worden verwerkt. Het BSN is een uniek identificerend nummer en hiervoor geldt dat er extra eisen aan de verwerking worden gesteld<sup>6</sup>.
- Een deel van de Wet politiegegevens is van overeenkomstige toepassing verklaard op de verwerking van persoonsgegevens uit ongebruikelijke transacties door de FIU-Nederland (art. 14 lid 3 Wwft), dit betreffen ook de vragen die door de FIU-Nederland worden gesteld via het verwijzingsportaal bankgegevens.

Voor de gegevens die door de banken worden verwerkt geldt het volgende: in een vordering staat op basis van welke bevoegdheid bij een bank informatie wordt opgevraagd. Indien het gaat om een strafvorderlijke bevoegdheid, moeten de gegevens uit de vordering als strafrechtelijke persoonsgegevens worden gezien. Het zijn immers gegevens over mogelijke betrokkenheid bij strafbare feiten. Daarnaast wordt een uniek identificerend nummer verwerkt bij het ontvangen en beantwoorden van vragen van de Belastingdienst, het BSN<sup>7</sup>. De overige gegevens die voor de beantwoording van vragen van de Belastingdienst worden verwerkt, zijn gewone persoonsgegevens. De gegevens uit vragen van de FIU-Nederland kunnen als anderszins gevoelige gegevens worden gekenmerkt omdat deze zicht kunnen geven op de financiële situatie van de betrokkene (betrokkenheid bij een ongebruikelijke transactie).

### 3. Gegevensverwerkingen

Geef alle voorgenomen gegevensverwerkingen weer.

Hieronder volgt een beknopte omschrijving van de gegevensverwerking per processtap. Voor de gedetailleerde omschrijving wordt verwezen naar het referentieontwerp.

*Proces:*

0. Het gebruikte kanaal.

1. Identificeren gegevens

Er zijn zoals bij vraag 2 genoemd, twee soorten opvraagmogelijkheden:

- op basis van persoons- en/of adresgegevens (NAW): op basis van een combinatie van a) achternaam/organisatienaam en adres, b) achternaam en geboortedatum, c) adres, d) inschrijfnummer KvK (rechtspersoon);
- op basis van een product: op basis van een combinatie van a) soort product (VB-naam) en productnummer, b) alleen productnummer (NB! Dit kan alleen als een volledig nummer wordt ingevuld, een deel van het nummer is niet voldoende).

2. Fiatteren<sup>8</sup>

Het voornemen tot het doen van een vordering voor identificerende gegevens bij een bank wordt door de opsporingsambtenaar besproken met een hulpofficier van justitie en voor wat betreft de bijzondere opsporingsdiensten met een teamleider. De h(OvJ)/teamleider toetst het voornemen op basis van proportionaliteit en subsidiariteit (sprake van een misdrijf, noodzaak voor het opsporingsonderzoek, omvang en reikwijdte van bevraging én zijn er andere

<sup>6</sup> Het wetsvoorstel VB voorziet in een wettelijke grondslag voor BSN gebruik door banken ten behoeve van het koppelen van de vordering van identificerende gegevens aan de klant in het bestand van de bank.

<sup>7</sup> Het wetsvoorstel VB voorziet in een wettelijke grondslag voor BSN gebruik door banken ten behoeve van het koppelen van het verzoek tot het vorderen van identificerende gegevens aan het bestand van de klant.

<sup>8</sup> Zie hieronder het overzicht wettelijke grondslagen welke functionaris het fiat geeft voor een vordering.

opsporingsmogelijkheden om aan de benodigde informatie te komen). Als de hulpofficier/teamleider akkoord is met de inzet van de opsporingsbevoegdheid wordt de vordering opgemaakt (door een opsporingsambtenaar of de h(OvJ)/teamleider zelf). De opgemaakte vordering wordt door de hulpofficier/teamleider ondertekend. Een ondertekende vordering is het akkoord/het fiat van het voornemen door een opsporingsambtenaar om door middel van een opsporingsbevoegdheid de beschikking te krijgen over identificerende gegevens.

Onderzocht is het opnemen van een mogelijkheid tot flattering in het VB. Besloten is dit niet te doen, immers de vordering mag altijd worden uitgevoerd na de toets en de accordering door de hulpofficier/teamleider. De introductie van een dergelijke mogelijkheid zou daarnaast tot vertraging van het proces leiden (geen toegang VB op afstand). In het VB worden wel de namen van de hulpofficier/teamleider en van degene die de vordering in het VB heeft ingevoerd opgenomen/gelogd. Daarnaast moet de opsporingsambtenaar die gebruik maakt van het VB expliciet aangeven dat de hulpofficier/teamleider akkoord is met het indienen van de betreffende vordering, elke keer dat gebruik wordt gemaakt van het VB. Door middel van audits wordt achteraf gecontroleerd of deze processtappen correct worden doorlopen.

De ondertekende vordering wordt door de opsporingsambtenaar die het VB gebruikt, opgeslagen in het onderzoeksdossier. Overwogen is de ondertekende vordering ook te uploaden in het VB. Hier is niet voor gekozen omdat dit zou leiden tot extra verwerking van persoonsgegevens, immers zouden de vorderingen dan zowel door de opsporingsinstanties als het VB moeten worden bewaard. De gegevens die nodig zijn om te controleren of aan de vereisten van een vordering is voldaan, worden daarom door de opsporingsambtenaar overgenomen in het VB en met het verzoek aan de bank gestuurd.

### 3. Opvragen banken (geautomatiseerd)

In het portaal kunnen enkel geautoriseerde medewerkers van een vragende instantie gegevens opvragen of vorderen op basis van de aan deze medewerker toekomende bevoegdheden. Voordat wordt geselecteerd welke gegevens worden opgevraagd, moet de betreffende grondslag worden geselecteerd. Afhankelijk van de account van de betrokken medewerker en de geselecteerde grondslag, moet de medewerker vervolgens de nodige velden invullen. Dit betekent dat medewerkers van de FIU-Nederland bijvoorbeeld enkel op basis van de Wwft gegevens kunnen opvragen, dat de opsporingsambtenaren van de FIOD en de overige medewerkers van de Belastingdienst andere bevoegdheden kunnen selecteren, en dat opsporingsambtenaren van de politie de naam van de hulpofficier van justitie die een vordering heeft ondertekend invullen in het portaal terwijl opsporingsambtenaren van de FIOD de naam van een teamleider invullen.

Zowel bij het opvragen op basis van persoons- en/of NAW als bij het opvragen op basis van product geeft de opsporingsambtenaar altijd in de aanvraag mee: a) de wetsgrond (artikel) voor vordering. b) bij welke bank(en) de gegevens opgevraagd dienen te worden<sup>9</sup>. c) de periode waarover de gegevens gevraagd worden (wordt dit niet aangegeven dan worden alleen actieve producten opgevraagd). d) in geval fiat nodig is, kan opsporingsambtenaar de naam van de hulpofficier van justitie of teamleider die de vordering heeft ondertekend invullen. In geval van het opvragen op basis van product, wordt indien het IBAN wordt gebruikt de naam van de bank automatisch ingevuld. NB! Categorie a, b, c en d worden afgedwongen door het systeem. Zonder deze in te vullen kan de vordering niet verder. De opsporingsambtenaar vult ook de naam van de

---

<sup>9</sup> Een vordering op basis van artikel 126nc Strafvordering kan worden gericht aan een ieder die daarvoor redelijkerwijs in aanmerking komt. In de meeste gevallen zijn er aanwijzingen op basis waarvan een selectie van te bevragen instellingen kan worden gemaakt. Door de opsporingsambtenaar wordt daartoe eerst gekeken of via andere bronnen informatie kan worden verkregen op basis waarvan een gerichtere vraag kan worden gesteld. Er wordt een PV opgemaakt van het indienen van een vordering waarin wordt onderbouwd waarom degenen aan wie de vordering wordt gericht hiervoor redelijkerwijs in aanmerking komen. De (h)OvJ of teamleider toetst de vordering en kijkt hierbij onder meer naar de proportionaliteit en subsidiariteit. Pas nadat de vordering is goedgekeurd, wordt deze via het VB ingediend.

opsporingsorganisatie en zijn of haar e-mail adres in. Deze gegevens worden opgenomen het bericht naar de bank.

Het VB controleert of vordering correct (en conform wet/regelgeving) is ingevuld en geautoriseerd is en verstuurt de vordering aan banken. Deze toetsing betreft de vereisten voor een vordering: indien de nodige velden niet zijn gevuld, wordt het verzoek niet verstuurd. De toets op proportionaliteit en subsidiariteit is op het moment dat het VB wordt gebruikt reeds gedaan door de hulpofficier/teamleider. Het portaal is verder zo ingericht dat aan de eisen van de AVG en de Wpg wordt voldaan. Achteraf kan altijd worden gecontroleerd of aan alle vereisten is voldaan: door de bank middels de toegestuurde informatie of door de opsporingsinstanties op basis van de door de opsporingsambtenaar opgeslagen ondertekende vordering.

#### 4. Matching ID gegevens (geautomatiseerd)

Er zijn zoals bij vraag 2 genoemd, twee soorten opvraagmogelijkheden, tijdens de matching bij de bank controleert de bank automatisch de gestuurde gegevens. Hierbij wordt gevalideerd of de gegevens uit het verzoek exact matchen met de gegevens van een cliënt of gemachtigde uit de klantadministratie (geen fouttolerantie, met uitzondering van diakrieten). De volgende antwoorden zijn mogelijk:

- Matching op basis van persoons- en/of adresgegevens (NAW): a) er zijn meer dan 3 personen gevonden op basis van de vraag, dan levert bank geen gegevens maar maakt melding van het vinden van teveel personen. Vervolgactie opsporing: de aanvraag kan worden aangevuld. b) Indien bij de zoekvraag een periode is meegegeven, worden ook producten teruggegeven die in de opgegeven periode actief waren, maar inmiddels zijn afgesloten/beëindigd, voorzien van de mededeling/status: "beëindigd". c) Is de klantrelatie met de persoon beëindigd (geen lopende producten) dan wordt tevens de mededeling "beëindigde klant" teruggegeven. d) indien geen match dan wordt de melding "niet bekend" teruggegeven.
- Matching op basis van product: a) Het antwoord bevat alle productgegevens plus de klanten van en gemachtigden voor dat product. b) er wordt (optioneel) een specifiek type product gevraagd, dan wordt een persoon alleen geselecteerd als hij/zij klant dan wel gemachtigd is/was voor dat product. Het antwoord bevat de persoonsgegevens van de klant/gemachtigde (productnummer; en, in geval van een natuurlijk persoon: eerste voorletter, overige voorletter(s), voornaam, achternaam, voorvoegsel, woonadres (straatnaam, huisnummer, huisnummer toevoeging, postcode, plaatsnaam, land), postadres (straatnaam/huisnummer/huisnummer toevoeging of postbus, postcode, plaatsnaam, land), geboortedatum; en, in geval van een rechtspersoon: organisatiename, vestigingsadres (straatnaam, huisnummer, postcode, plaatsnaam, land) postadres (straatnaam/huisnummer of postbus, postcode, plaatsnaam, land), KvK-(vestigings)nummer) c) Is een periode opgegeven, dan wordt het product ook geleverd als het in die periode is beëindigd, tevens worden de in die periode beëindigde klanten en/of gemachtigden geleverd. Zijn deze gegevens niet beschikbaar dan meldt de bank dat. d) Is in de vraag ook het *soort product* opgenomen dan beperkt de bank zich tot dit soort product. De meegegeven productnaam is de voor het VB overeengekomen naam voor het product. De bank vertaalt dit naar de eigen productsoorten/-namen.

#### 5. Samenstellen antwoord

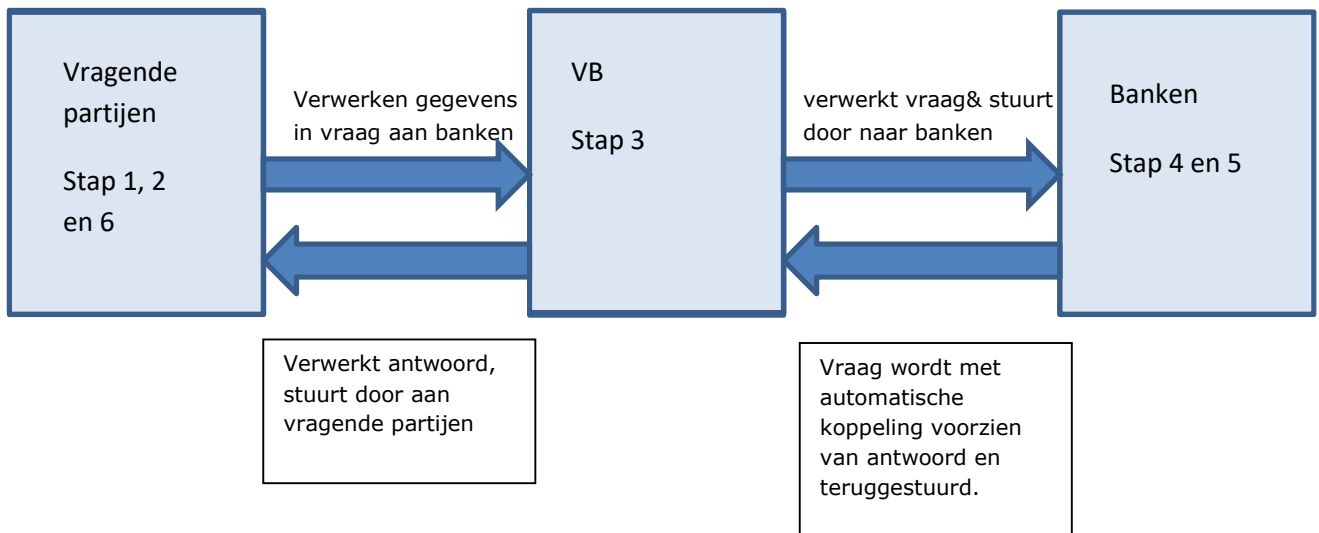
Een vraag wordt in één keer beantwoord, dat wil zeggen bij uitvraag aan meer dan één bank worden de antwoorden van de banken door het VB gebundeld tot één antwoord. Indien na de maximale beantwoordingstermijn (30 seconden) het antwoord nog niet volledig is (nog niet van alle banken binnen) dan wordt het onvolledige antwoord teruggegeven, met vermelding van welke bank(en) antwoord ontbreekt.

#### 6. Opnemen in dossier

De opsporingsambtenaar maakt een PV op, download vanuit het VB een PDF-document en een xml-bestand waarin de vraag en de antwoorden zijn opgenomen en archiveert het PV samen met het PDF-document en/of het xml-bestand in het onderzoeksdossier. Het vraagnummer is hiermee

altijd in het dossier opgenomen. Met dit nummer wordt het verband over de hele opvraagketen heen (opsporingsdossier – VB – bank) geborgd, bijvoorbeeld ten behoeve van een audit. Indien het antwoord volledig is, dat wil zeggen van alle bevroegde banken is binnengekomen en daarvan een digitaal document is aangemaakt, bewaart het VB de (inhoudelijke) vraag- & antwoordberichten vijf minuten. Daarna worden deze automatisch verwijderd. De meta-/logging-gegevens worden periodiek na de vastgestelde bewaartermijn verwijderd.

*Schematisch weergegeven*



*Overzicht wettelijke grondslagen en bevoegdheden voor opvragen identificerende gegevens via het VB<sup>10</sup>*

<i>artikel</i>	<i>Geautoriseerde partij</i>	<i>functionaris/rol</i>	<i>voorwaarde</i>
Wetboek van Strafvordering (WvSv), artikel <ul style="list-style-type: none"> <li>• 126nc (opsporing)</li> <li>• 126uc (bestrijding georganiseerde misdaad)</li> <li>• 126zk (terrorismedreiging)</li> </ul>	opsporing, zie noot (1)	opsporingsambtenaar, hulpofficier van justitie	akkoord van hulpofficier van Justitie (politie) of teamleider (BOD), de geautoriseerde partijen
<ul style="list-style-type: none"> <li>• 126a (bij een Strafrechtelijk Financieel Onderzoek)</li> </ul>	opsporing	opsporingsambtenaar, hulpofficier van justitie	machtiging van rechter-commissaris
<ul style="list-style-type: none"> <li>• 126ii (verkennend onderzoek terrorisme)</li> </ul>	opsporing	officier van justitie	
<ul style="list-style-type: none"> <li>• 577bb (executieonderzoek)</li> </ul>	opsporing	opsporingsambtenaar, hulpofficier van justitie	bevel van de officier van justitie

<sup>10</sup> Uit: VB-PSA v20170105

Wet Economische delicten (Wed) • art 19 (economisch delict)	opsporing	opsporingsambtenaar, hulpofficier van justitie, teamleider	akkoord van hulpofficier <sup>11</sup> van Justitie (politie) of teamleider (BOD)
Algemene wet inzake rijksbelastingen (AWR) • art 53, eerste lid, onderdeel a	toezicht: Belastingdienst(BD-heffing), Douane (heffing) (zie noot 2)	inspecteur	
Invorderingswet (IW) • art 62	toezicht: BD(inning), Douane (inning)	ontvanger, BD-systemen, zie noot (2)	
Invorderingswet (IW) • art 62bis (1BRN)	toezicht: BD(inning), Douane (inning)	ontvanger, BD-systemen, zie noot (2)	
Algemene wet inkomensafhankelijke regelingen (Awir) • art 38, incl. uitvoeringsbesluit art 1a/1b	toezicht BD(Toeslagen/ heffing), BD(Toeslagen/ inning), zie noot (3)	BD-systemen, zie noot (2)	
Wet ter voorkoming van witwassen en financieren van terrorisme (Wwft) • art 17	FIU	onderzoeker	akkoord teamleider, (plv) hoofd)

*Toelichting op overzicht wettelijke grondslagen:*

(1) Met 'opsporing' worden de opsporingsinstanties bedoeld.) Met 'toezicht' wordt bedoeld de Belastingdienst. Het betreft Belastingdienst(BD-heffing), Douane (heffing), BD(inning), Douane (inning) BD(Toeslagen/ heffing) en BD(Toeslagen/ inning).

(2) De Belastingdienst controleert in het kader van 1BRN het geregistreerde/te registreren rekeningnummer. Registratie kan plaatsvinden door de burger zelf via portalen van de belastingdienst, of door een belastingdienstmedewerker naar aanleiding van door burger opgestuurde formulieren. De registratie door burger gaat met de volgende systemen:  
- app Zorgtoeslag  
- portalen: 'Toeslagen' en 'Mijn BelastingDienst'

Ook in het kader van de InkomensHeffing (IH), Zorgverzekeringswet (ZVW) en Toeslagen kan het rekeningnummer worden gecontroleerd. Ten behoeve van de taken op dit gebied kunnen tevens identificerende gegevens worden opgevraagd.

(3) Met ingang van 1-1-2019 worden de invorderingsbepalingen uit de Algemene wet inkomensafhankelijke regelingen gehaald en ondergebracht in de Invorderingswet 1990 (wetsvoorstel BP2017). Vanaf dat moment zijn art. 62 (algemeen) en 62bis (1BRN) ook van toepassing op de invordering van toeslagen.

#### 4. Verwerkingsdoeleinden

Beschrijf de doeleinden van de voorgenomen gegevensverwerkingen (dwz: de gegevens zijn verkregen op grond van art ..)

<sup>11</sup> Hoewel niet beschreven in de Aanwijzing bijzondere opsporingsbevoegdheden, komt het juist voor dat het verzoek om inzage door de (h)OvJ/teamleider wordt gedaan.



Doel van het VB is door het bieden van een technische infrastructuur ondersteunen van het betrouwbaar, snel, juist, volledig en efficiënt, *geautomatiseerd* opvragen en verstrekken van een beperkte set identificerende (bankrekening)gegevens en identificerende gegevens behorend bij financiële producten op een uniforme wijze bij alle in Nederland gevestigde banken, ten behoeve van het verschaffen van een indicatie voor eventueel verder onderzoek of nadere controle in het kader van het voorkomen en opsporen van fraude en andere vormen van criminaliteit.

Het VB wordt gebruikt voor:

1. het opvragen van identificerende gegevens van klanten bij banken door opsporingsdiensten;
2. rekeningverificatie door de Belastingdienst, voor zover hiertoe een wettelijk voorschrift bestaat.

Dit zijn twee verschillende processen waarvoor verschillende persoonsgegevens kunnen worden verwerkt.

Op basis van de resultaten kan (bij verdenking van een misdrijf) verder onderzoek worden gedaan, of op basis van afwijkende resultaten (zoals bij de check voor 1BRN) kan nadere controle worden ingesteld. De gegevens leveren informatie die nodig is voor de (verdere) uitoefening van bevoegdheden van de vragende partij, waaronder het opvragen van inhoudelijke bankgegevens (daaronder begrepen de saldo- en transactie-informatie). Met behulp van het rekeningnummer kan namelijk onder meer de financiële situatie van een verdachte in kaart worden gebracht, kan worden onderzocht wie bij een ongebruikelijke transactie betrokken is en kan de Belastingdienst bepalen of een rekeningnummer geschikt is voor het innen en uitbetalen van belastinggelden. De banken zijn bij wet verplicht te voldoen aan een verzoek of vordering op grond van de wet.<sup>12</sup>

Het doel van de gegevensverwerking binnen het VB is afgeleid van het doel van de gegevensverwerking door de vragende partijen, het VB is immers verwerker voor de vragende partijen. Het doel van de verwerking via het VB, is het bevragen, vorderen en ontvangen van identificerende gegevens bij banken efficiënter en effectiever te laten verlopen. Door de komst van het VB verandert de wijze van verstrekking; het VB beoogt de gegevensverwerking zo efficiënt mogelijk te effectueren en beoogt de wettelijke bevoegdheden niet in te perken of te verruimen. Het VB verandert ook niet de gegevens die worden verstrekt of de doeleinden waarvoor dit gebeurt. De persoons- en zaakgegevens die in het portaal worden getoond c.q. verwerkt, zijn niet anders dan de gegevens die thans schriftelijk worden verstrekt. Dit is enkel anders voor het BSN: dit zal naast de eerder genoemde doeleinden worden verwerkt voor het specifieke doel van het mogelijk maken van een unieke koppeling tussen een verzoek of vordering en de gegevens van de betrokkene in de klantadministratie.

Met de komst van het VB worden binnen het VB ook persoonsgegevens verwerkt van degenen die binnen het VB gegevens hebben verwerkt en van degenen die een vordering of vraag via het VB hebben ingediend (metadata). Het doel van deze gegevensverwerking is het achteraf kunnen traceren van de verwerkingen binnen het VB. Deze gegevens worden gebruikt ten behoeve van periodieke audits (die vanuit het beheer van het VB worden uitgevoerd, de inhoud en frequentie worden gedurende de pilot vastgesteld, dwz Q1 2018)<sup>13</sup>.

Per organisatie worden de gegevens gevorderd en verkregen ten behoeve van de volgende doeleinden:

#### *Nationale Politie en Openbaar Ministerie*

Ten behoeve van de opsporing en vervolging van misdrijven kunnen de politie en het Openbaar Ministerie bij banken identificerende gegevens opvragen. De politie doet dit op grond van artikel 3 van de Politiewet 2012<sup>14</sup>. De informatie die wordt verstrekt naar aanleiding van een vordering kan bijvoorbeeld inzichtelijk maken wie rekeninghouder is en dus verantwoordelijk is voor een bepaalde transactie. Ook kan het zicht geven op de rekeningen die door een verdachte worden gebruikt. Op basis van deze informatie kan vervolgens een gerichte vordering worden gestuurd waarin bijvoorbeeld om transactiegegevens wordt gevraagd. Deze doeleinden kennen hun

<sup>12</sup> Mits de vordering geldig/correct is.

<sup>13</sup> Deze wordt in gezamenlijkheid ingericht, zodat bv ook rechtmatigheid vordering achteraf wordt gecheckt. Het is een audit vanuit de beheerspartij van het portaal.

<sup>14</sup> De politie heeft tot taak in ondergeschiktheid aan het bevoegd gezag en in overeenstemming met de geldende rechtsregels te zorgen voor de daadwerkelijke handhaving van de rechtsorde en het verlenen van hulp aan hen die deze behoeven.

grondslagen in de volgende artikelen: art 126nc, art 126uc, art 126zk, art 126a, art 126ii, art 577bb WvSv.

#### *Rijksrecherche en KMar*

Evenals de politie, kunnen de Rijksrecherche en de KMar identificerende gegevens vorderen in het kader van de opsporing van misdrijven waar zij mee zijn belast. De KMar doet dit op grond van artikel 4 van de Politiewet 2012. De Rijksrecherche doet dit op grond van artikel 49 van de Politiewet 2012. Deze doeleinden kennen hun grondslagen in de volgende artikelen: art 126nc, art 126uc, art 126zk, art 126a, art 126ii, art 577bb WvSv, en art 19 Wed.

#### *Bijzondere Opsporingsdiensten (FIOD, NVWA-IOD, ILT-IOD, ISZW-DO)*

De bijzondere opsporingsdiensten kunnen in het kader van de opsporing van misdrijven op een specifiek terrein waarmee ze zijn belast (zoals strafrechtelijk onderzoek naar alle strafbare feiten, en de tenuitvoerlegging van strafbeschikkingen en veroordelende vonnissen of arresten) op dezelfde wijze als de politie identificerende gegevens vorderen, zij doen dit ingevolge artikel 3 Wet op de bijzondere opsporingsdiensten (Wet BOD). Deze doeleinden kennen hun grondslagen in de volgende artikelen: art 126nc, art 126uc, art 126zk, art 126a, art 126ii, art 577bb WvSv, en art 19 Wed.

#### *Financial Intelligence Unit (FIU-Nederland)*

De FIU-Nederland kan met het oog op het voorkomen en opsporen van misdrijven (specifiek witwassen en financieren van terrorisme, art. 13 Wwft) identificerende gegevens opvragen bij banken die bij de FIU-Nederland een melding hebben gedaan van een ongebruikelijke transactie, ofwel op basis van intelligence afkomstig van een buitenlands meldpunt/FIU met een vergelijkbare taak, of op basis van eigen intelligence (art. 17 Wwft). Het doel van de vraag is het in kaart brengen van financiële netwerken en andere verbanden in relatie tot gemelde transacties/financial intelligence, overeenkomstig artikel 13 van de Wet ter voorkoming van witwassen en financieren van terrorisme.

#### *Belastingdienst*

De Belastingdienst (Heffing, Inning, Toeslagen/Heffing, Toeslagen/inning en Douane) verwerkt identificerende gegevens ten behoeve van de belastingheffing en -inning, toezicht en voor 1BRN. Via het VB kan worden gecontroleerd of het door de betrokkene opgegeven rekeningnummer juist is en kunnen identificerende gegevens worden opgevraagd (art. 53, eerste lid, onderdeel a, AWR, artt. 62 en 62bis Invorderingswet<sup>15</sup> en art. 38 Awir). Dit met het doel om onder meer zorg te dragen dat uitbetaald wordt op, dan wel geïncasseerd wordt van, het juiste rekeningnummer. Ten behoeve van 1BRN kan enkel worden geverifieerd of het rekeningnummer voor de uitbetaling van inkomstenbelasting en voor de uitbetaling van voorschotten en tegemoetkomingen klopt.

#### *Banken*

Het doel voor het verstrekken van de gevraagde informatie is het voldoen aan de wettelijke verplichting gegevens te verstrekken.

## **5. Betrokken partijen**

Benoem welke organisaties betrokken zijn bij welke gegevensverwerkingen. Deel deze organisaties per gegevensverwerking in onder de rollen: verwerkingsverantwoordelijke, verwerker, verstrekker en ontvanger. Benoem tevens welke functionarissen binnen deze organisaties toegang krijgen tot welke persoonsgegevens.

**De volgende partijen zijn betrokken bij de gegevensverwerking:**

<sup>15</sup> De douane doet dat via artikel 62 van de Invorderingswet 1990 en de douane inspecteur via artikel 53 AWR. De Douane maakt **geen** gebruik van artikel 62bis IW (ziet alleen op Inkomstenbelasting en toeslagen). Dit zijn dezelfde artikelen die de ontvanger en inspecteur gebruiken bij de invordering en heffing van rijksbelastingen, e.d.

*Vragende partijen (verwerkingsverantwoordelijke, verstrekker en ontvanger)*

- Nationale Politie
- Openbaar Ministerie
- Bijzondere Opsporingsdiensten (FIOD, NVWA-IOD, ILT-IOD, ISZW-DO)
- FIU-Nederland
- Belastingdienst

*Verwerkende partij*

De Minister van Justitie en veiligheid (Justid-IBO) in de rol van verwerker, namens de vragende partijen, die verwerkingsverantwoordelijke zijn voor de verwerkte gegevens.

*Verstrekende partijen (verstrekker en ontvanger)*

Banken, te beginnen met:

- Rabobank
- Volksbank
- ING
- ABN-AMRO
- Bunq
- Overige banken die aan de aansluitcriteria voldoen

**Toelichting**

Verzenden verzoek of vordering om informatie:

Het verwijzingsportaal bankgegevens is een centrale voorziening waarlangs vragen van de respectievelijke bevragende organisaties bij de banken worden uitgezet conform de reeds bestaande en ongewijzigde wettelijke bevoegdheden. De bevragende organisaties zijn elk afzonderlijk verwerkingsverantwoordelijke voor het verzenden van hun verzoek of vordering om informatie aan het verwijzingsportaal bankgegevens. De gegevens die in het verwijzingsportaal bankgegevens worden opgeslagen (voor ongeveer drie minuten) vallen onder de verwerkingsverantwoordelijkheid van de bevragende organisatie. Hieronder een overzicht:

<b>Bevragende organisatie</b>	<b>Verwerkingsverantwoordelijke</b>
Nationale Politie	de korpschef (artikel 22 Richtlijn (EU) 2016/680 en artikel 1, aanhef en onderdeel f, onder 1°, en artikel 6c Wet politiegegevens)
OM	niet van toepassing, want doet zelf geen bevragingen
Koninklijke Marechaussee	de minister van Defensie (artikel 22 Richtlijn(EU) 2016/680 en artikel 1, aanhef en onderdeel f, onder 3°, Wet politiegegevens)
Rijksrecherche	het College van procureurs-generaal (artikel 22 Richtlijn (EU) 2016/680 en artikel 1, aanhef en onderdeel f, onder 2°, en artikel 6c Wet politiegegevens)
Fiscale Inlichtingen- en Opsporingsdienst	Directeur FIOD (artikel 22 Richtlijn (EU) 2016/680)
Inlichtingen- en Opsporingsdienst van de Nederlandse Voedsel- en Warenautoriteit	Directeur NVWA-IOD (artikel 22 Richtlijn (EU) 2016/680)
Directie Opsporing van de Inspectie Sociale Zaken en Werkgelegenheid	Directeur Opsporing (artikel 22 Richtlijn (EU) 2016/680)
Inlichtingen- en Opsporingsdienst van de Inspectie Leefomgeving en Transport	De minister van Infrastructuur en Waterstaat (artikel 22 Richtlijn (EU) 2016/680)
Belastingdienst	DG Belastingdienst namens de minister van Financiën
FIU-Nederland	Voor verwerking gegevens betreffende ongebruikelijke transacties: het hoofd FIU namens de minister van Justitie & Veiligheid (artikel 12, derde lid, Wwft) Voor verwerking gegevens betreffende verdachte transacties: de korpschef (artikel 22 Richtlijn (EU) 2016/680 en artikel 1, aanhef en onderdeel f, onder 1°, en artikel 6c Wet politiegegevens)

De Justitiële Informatiedienst (Justid), vallend onder de verantwoordelijkheid van de minister van Justitie en Veiligheid, is verwerker voor deze partijen (zie hieronder).

Ontvangst verzoek of vordering en verstrekking door banken en andere betaaldienstverleners:

Banken kijken vervolgens in hun eigen klantsystemen of de gevraagde persoonsgegevens bij hen bekend zijn. Als dat het geval is worden de resultaten via het verwijzingsportaal bankgegevens naar de bevragende organisaties gestuurd. De verstreckende partijen (banken en andere betaaldienstverleners) zijn steeds verwerkingsverantwoordelijke als het gaat om de ontvangst van het verzoek of de vordering van het verwijzingsportaal en het naar aanleiding daarvan verstrekken van gegevens aan het verwijzingsportaal. Vanaf het moment dat de vraag via het verwijzingsportaal bankgegevens bij het koppelvlak van de bank is aangekomen en de bank gegevens verwerkt waarmee de vraag kan worden beantwoord, is de bank verwerkingsverantwoordelijke. Dit koppelvlak, waarmee de bank op het verwijzingsportaal bankgegevens wordt aangesloten, wordt onder verantwoordelijkheid van de bank ontwikkeld. Verzoeken en vorderingen worden via het koppelvlak automatisch gekoppeld aan de gegevens uit de klantadministratie van de bank. Indien de bank over gegevens van de betrokkene beschikt, worden deze automatisch verstuurd. Dit betekent dat de bank als verwerkingsverantwoordelijke enkel achteraf kan controleren of het proces goed is verlopen. Daarom is het portaal zo ingericht dat enkel verzoeken en vorderingen die aan alle vereisten voldoen, aan de bank kunnen worden gestuurd. Daarnaast wordt, in overleg met de banken, een auditproces vormgegeven waarmee onder andere wordt getoetst of alle processtappen juist worden doorlopen. Banken krijgen periodiek inzage in de uitkomst van de audit.

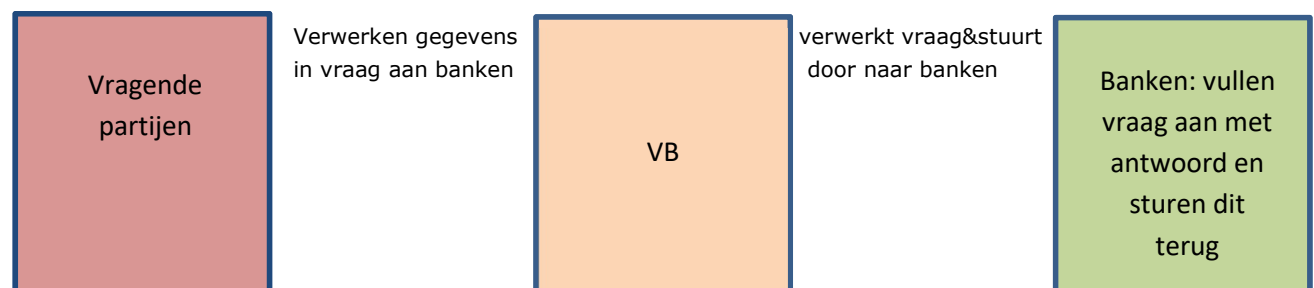
De bank stuurt (persoons)gegevens als antwoord op een zoekopdracht naar het verwijzingsportaal bankgegevens. Vanaf het moment dat deze gegevens worden ontvangen door het verwijzingsportaal bankgegevens, is de bevragende organisatie ten aanzien van de persoonsgegevens die zijn opgenomen in de vordering of het verzoek verwerkingsverantwoordelijke, dus ook verantwoordelijk voor de verdere verwerking van deze gegevens in de eigen systemen.

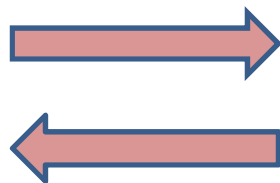
Loggingsgegevens:

Ten aanzien van de loggingsgegevens die door het verwijzingsportaal bankgegevens worden bewaard, is de minister van Justitie en Veiligheid verwerkingsverantwoordelijke. Deze gegevens worden beheerd door Justid-IBO.

Beheer verwijzingsportaal bankgegevens:

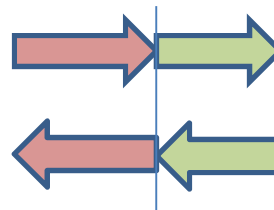
Het beheer van het verwijzingsportaal bankgegevens wordt uitgevoerd door de Justitiële Informatiedienst, met instemming van de minister van Justitie en Veiligheid (Justid in de rol van systeembeheerder, en derhalve verwerker in de zin van artikel 4, onderdeel 8, van de AVG, en verwerker in de zin van artikel 1, onderdeel i, van de Wet politiegegevens). Het verwijzingsportaal wordt beheerd door de Justitiële Informatiedienst, afdeling IBO (Justid-IBO). Aangezien Justid-IBO onder verantwoordelijkheid valt van de minister van Justitie en Veiligheid en er geen sprake is van een gezagsverhouding tussen ministeries onderling, maakt Justid-IBO per aangesloten partij (bevragende organisatie) verwerkersafspraken over onder meer de rechten en plichten van de verschillende partijen ten aanzien van de gegevens, het melden van een datalek, het toegang geven van personen tot het verwijzingsportaal bankgegevens binnen Justid (medewerkers hebben alleen in zeer uitzonderlijke gevallen volgens vastgestelde procedures toegang tot persoonsgegevens), uitvoeren van audits en feitelijke werkplekken van beheerders. Justid-IBO heeft kortom de rol om de gegevens technisch te verbinden en bij de in beheer name de taken uit te voeren die zijn opgenomen in de verwerkersafspraken.





Verwerkt antwoord,  
stuurt door aan  
vragende partijen

Bewaart  
metagegevens



Vullen vraag aan met  
antwoord en sturen  
dit terug

#### Koppelvlak bank

- (verwerkings)verantwoordelijke gegevensverwerking is vragende partij, regime Wpg, Wjsg of AVG
- (verwerkings)verantwoordelijke gegevensverwerking is bank, regime AVG
- verwerker voor vragende partij, privacyregime vragende partij: regime Wpg, Wjsg of Wbp (AVG), daarnaast namens de minister van Justitie en Veiligheid verwerkingsverantwoordelijke ten aanzien van metagegevens, regime AVG

#### Welke gegevens per organisatie

In onderstaand overzicht wordt aangegeven per soort vraag (opvragen identificerende gegevens door opsporingsdiensten of FIU-Nederland; rekeningverificatie door Belastingdienst) welke informatie door wie aan wie wordt verstrekt.

Vorderende/ opvragende partij	Vordering/ Opvraging	Combinatie gegevens in vordering/opvraging VB naar bank. Het uitgangspunt is dat de optionele velden – indien bekend - ook worden gevuld.	Antwoord bank naar VB
<b>Vorderen/opvragen identificerende gegevens door opsporingsdiensten, Belastingdienst of FIU-Nederland</b>			
Opsporings- diensten, FIU  Belasting- dienst (met uitzondering van 1BRN)	Op basis van NAW	<i>Vorderen/opvragen op achternaam en adres</i>	Het antwoord bevat de identificerende gegevens, plus alle producten <sup>17</sup> waarvoor de betrokken natuurlijk persoon rekeninghouder dan wel gemachtigde is of was, die in Nederland worden aangeboden door de banken.
		<i>Vorderen/opvragen op achternaam en postcode en huisnummer</i>	Identificerende gegevens natuurlijk persoon (indien beschikbaar bij de bank): - Actieve klant ja/nee - Eerste voorletter - Overige voorletter(s) - Voornaam - Achternaam - Voorvoegsel - Woonadres (straatnaam, huisnummer, huisnummer toevoeging, postcode, plaatsnaam, land) - Postadres (straatnaam/huisnummer/huisnumme

<sup>16</sup> Het wetsvoorstel VB voorziet in een wettelijke grondslag voor BSN gebruik door banken ten behoeve van het koppelen van de vordering van identificerende gegevens aan de klant in het bestand van de bank. Voor inwerkingtreding van dit wetsvoorstel wordt het BSN niet in een vordering of verzoek opgenomen.

<sup>17</sup> De definitie komt aan de orde in AMVB.

	<ul style="list-style-type: none"> <li>- Huisnummer</li> <li>- Land</li> <li>- Periode</li> </ul>	<ul style="list-style-type: none"> <li>r toevoeging of postbus, postcode, plaatsnaam, land)</li> <li>- Geboortedatum</li> </ul>
	<ul style="list-style-type: none"> <li>- Eerste voorletter</li> <li>- Overige voorletter(s)</li> <li>- Voornaam</li> <li>- Voorvoegsel</li> <li>- Geboortedatum</li> <li>- Straatnaam</li> <li>- Huisnummer toevoeging</li> <li>- Plaatsnaam</li> <li>- BSN<sup>18</sup></li> </ul>	<ul style="list-style-type: none"> <li>Product(en):</li> <li>- Productnummer</li> <li>- Productsoort</li> <li>- Rol van natuurlijk persoon (rekeninghouder/gemachtigde)</li> <li>- Contractpartij</li> </ul>
	<p><i>Vorderen/opvragen op achternaam en geboortedatum</i></p> <ul style="list-style-type: none"> <li>- Achternaam</li> <li>- Geboortedatum</li> <li>- Periode</li> <li>- Eerste voorletter</li> <li>- Overige voorletter(s)</li> <li>- Voornaam</li> <li>- Voorvoegsel</li> <li>- Straatnaam</li> <li>- Huisnummer</li> <li>- Huisnummer toevoeging</li> <li>- Postcode</li> <li>- Plaatsnaam</li> <li>- Land</li> <li>- BSN<sup>19</sup></li> </ul>	
	<p><i>Vorderen/opvragen op organisatiernaam en adres</i></p> <ul style="list-style-type: none"> <li>- Organisatiernaam</li> <li>- Straatnaam</li> <li>- Huisnummer</li> <li>- Plaatsnaam</li> <li>- Land</li> <li>- Periode</li> </ul> <ul style="list-style-type: none"> <li>- KvK-(vestigings)nummer</li> <li>- Postcode</li> <li>- Huisnummer toevoeging</li> </ul>	<p>Het antwoord bevat de identificerende gegevens, plus alle producten<sup>20</sup> waarvoor de betrokken natuurlijk persoon rekeninghouder dan wel gemachtigde is of was, die in Nederland worden aangeboden door de banken.</p> <p>Identificerende gegevens rechtspersoon (indien beschikbaar bij de bank):</p> <ul style="list-style-type: none"> <li>- Actieve klant ja/nee</li> <li>- Organisatiernaam</li> <li>- Vestigingsadres (straatnaam, huisnummer, postcode, plaatsnaam, land)</li> <li>- Postadres (straatnaam/huisnummer of postbus, postcode, plaatsnaam, land)</li> <li>- kvK-(vestigings)nummer</li> </ul>
	<p><i>Vorderen/opvragen op organisatiernaam en postcode en huisnummer</i></p> <ul style="list-style-type: none"> <li>- Organisatiernaam</li> <li>- Postcode</li> <li>- Huisnummer</li> <li>- Land</li> <li>- Periode</li> </ul> <ul style="list-style-type: none"> <li>- KvK-(vestigings)nummer</li> <li>- Straatnaam</li> </ul>	<ul style="list-style-type: none"> <li>Product(en):</li> <li>- Productnummer</li> <li>- Productsoort</li> </ul>

<sup>18</sup> Het wetsvoorstel VB voorziet in een wettelijke grondslag voor BSN gebruik door banken ten behoeve van het koppelen van het verzoek tot het vorderen van identificerende gegevens aan het bestand van de klant. Voor inwerkingtreding van dit wetsvoorstel wordt het BSN niet in een vordering of verzoek opgenomen.

<sup>19</sup> Het wetsvoorstel VB voorziet in een wettelijke grondslag voor BSN gebruik door banken ten behoeve van het koppelen van het verzoek tot het vorderen van identificerende gegevens aan het bestand van de klant. Voor inwerkingtreding van dit wetsvoorstel wordt het BSN niet in een vordering of verzoek opgenomen.

<sup>20</sup> De definitie komt aan de orde in AMVB.

		<ul style="list-style-type: none"> <li>- Huisnummer toevoeging</li> <li>- Plaatsnaam</li> </ul>	<ul style="list-style-type: none"> <li>- Rol van rechtspersoon (rekeninghouder/gemachtigde)</li> <li>- Contractpartij</li> </ul>
		<p><i>Vorderen/opvragen op KvK-(vestigings)nummer</i></p> <ul style="list-style-type: none"> <li>- KvK-(vestigings)nummer</li> <li>- Periode</li> </ul>	
		<ul style="list-style-type: none"> <li>- Organisatiename</li> <li>- Straatnaam</li> <li>- Huisnummer</li> <li>- Huisnummer toevoeging</li> <li>- Postcode</li> <li>- Plaatsnaam</li> <li>- Land</li> </ul>	
		<p><i>Vorderen/opvragen op adres</i></p> <ul style="list-style-type: none"> <li>- Straatnaam</li> <li>- Huisnummer</li> <li>- Plaatsnaam</li> <li>- Land</li> <li>- Periode</li> </ul>	Het antwoord bevat de identificerende gegevens, plus alle producten waarvoor de betrokken natuurlijke perso(o)n(en) en/of rechtsperso(o)nen rekeninghouder dan wel gemachtigde is/zijn of was/waren, die in Nederland worden aangeboden door de banken.
		<ul style="list-style-type: none"> <li>- Postcode</li> <li>- Huisnummer toevoeging</li> </ul>	
		<p><i>Vorderen/opvragen op postcode en huisnummer</i></p> <ul style="list-style-type: none"> <li>- Postcode</li> <li>- Huisnummer</li> <li>- Land</li> <li>- Periode</li> </ul>	De identificerende gegevens en de productgegevens in het antwoord van de bank met betrekking tot natuurlijke personen en rechtspersonen zijn hierboven vermeld.
		<ul style="list-style-type: none"> <li>- Straatnaam</li> <li>- Plaatsnaam</li> <li>- Huisnummer toevoeging</li> </ul>	
	Op basis van product	<p><i>Vorderen/opvragen op productnummer</i></p> <ul style="list-style-type: none"> <li>- Productnummer</li> <li>- Periode</li> </ul>	<p>Het antwoord bevat de productgegevens en de identificerende gegevens van de rekeninghouders en gemachtigden (natuurlijke perso(o)n(en) en/of rechtsperso(o)nen van betreffende product(en), die in Nederland worden aangeboden door de banken.</p> <p>Product(en):</p> <ul style="list-style-type: none"> <li>- Productnummer</li> <li>- Productsoort</li> <li>- Contractpartij</li> <li>-</li> </ul> <p>Identificerende gegevens natuurlijk perso(o)nen (indien beschikbaar bij de bank):</p> <ul style="list-style-type: none"> <li>- Actieve klant ja/nee</li> <li>- Eerste voorletter</li> <li>- Overige voorletter(s)</li> <li>- Voornaam</li> <li>- Achternaam</li> <li>- Voorvoegsel</li> <li>- Woonadres (straatnaam, huisnummer, huisnummer)</li> </ul>
		<ul style="list-style-type: none"> <li>- Productsoort</li> </ul>	

		<p>toevoeging, postcode, plaatsnaam, land)</p> <ul style="list-style-type: none"> <li>- Postadres (straatnaam/huisnummer/huisnummer toevoeging of postbus, postcode, plaatsnaam, land)</li> <li>- Geboortedatum</li> </ul> <p>Identificerende gegevens rechtspersoon (indien beschikbaar bij de bank):</p> <ul style="list-style-type: none"> <li>- Actieve klant ja/nee</li> <li>- Organisatienaam</li> <li>- Vestigingsadres (straatnaam, huisnummer, postcode, plaatsnaam, land)</li> <li>- Postadres (straatnaam/huisnummer of postbus, postcode, plaatsnaam, land)</li> <li>- kvK-(vestigings)nummer</li> </ul>
Metadata bij vorderingen/opvragingen	<p>De volgende metadata worden door het VB meegegeven naar de bank(en):</p> <ul style="list-style-type: none"> <li>- Wetsgrond</li> <li>- Vraagnummer (uniek)</li> <li>- VB-identificatienummer bank</li> <li>- Organisatienaam opsporingsdienst</li> <li>- Naam opsporingsambtenaar</li> <li>- E-mail adres opsporingsambtenaar</li> <li>- Datum/tijd geregistreerd</li> <li>- Vraagtype (product, NAW)</li> </ul>	<p>De volgende metadata worden door de bank meegegeven naar het VB:</p> <ul style="list-style-type: none"> <li>- Vraagnummer (uniek)</li> <li>- VB-identificatienummer bank</li> </ul>
<b>Rekeningverificatie (1BRN)</b>		
Belastingdienst	<p><i>1BRN</i></p> <p>Verplicht:</p> <ul style="list-style-type: none"> <li>- BSN<sup>21</sup></li> <li>- IBAN</li> </ul>	<p>Het antwoord bevat de productgegevens en de identificerende gegevens van een natuurlijke persoon behorende bij het productnummer, die in Nederland worden aangeboden door de banken.</p> <p>Product:</p> <ul style="list-style-type: none"> <li>- Tenaamstelling</li> <li>- Actieve rekening ja/nee</li> <li>- Betaalrekening ja/nee</li> <li>- Postadres (straatnaam/huisnummer of postbus, postcode, plaatsnaam, land)</li> </ul> <p>Identificerende gegevens natuurlijk persoon (indien beschikbaar bij de bank):</p> <ul style="list-style-type: none"> <li>- Eerste voorletter</li> <li>- Overige voorletter(s)</li> <li>- Voornaam</li> <li>- Achternaam</li> <li>- Voorvoegsel</li> <li>- Geboortedatum</li> </ul>

<sup>21</sup> Het wetsvoorstel VB voorziet in een wettelijke grondslag voor BSN gebruik door banken ten behoeve van het koppelen van het verzoek tot het vorderen van identificerende gegevens aan het bestand van de klant. Voor inwerkingtreding van dit wetsvoorstel wordt het BSN niet in een vordering of verzoek opgenomen.



Metadata bij 1BRN	De volgende metadata worden door het VB meegegeven naar de bank(en): - Wetsgrond - Vraagnummer (uniek) - VB-identificatienummer bank - Datum/tijd geregistreerd - Vraagtype (1BRN)	De volgende metadata worden door de bank meegegeven naar het VB: - Vraagnummer (uniek) - VB-identificatienummer bank

## 6. Belangen bij de gegevensverwerking

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

Het belang van de verwerkingsverantwoordelijke bij de verwerking van gegevens via het VB is dat het gedeelte van het vorderingsproces dat in het VB geautomatiseerd verloopt efficiënter wordt: doordat sneller en effectiever informatie kan worden opgevraagd (digitaal en bij verschillende banken tegelijkertijd, en door de inrichting van het systeem is, is het bevragsingsproces sneller, de informatie vollediger, betrouwbaarder en juister) kunnen strafbare feiten beter worden voorkomen of opgespoord, en kan de Belastingdienst onjuiste inningen en uitbetalingen van bedragen voorkomen.

Het belang van de banken is gelegen een soortgelijke reden, die leidt tot een vermindering van de werklast: doordat geautomatiseerd informatie kan worden verstrekt hoeven banken vorderingen niet meer handmatig te beantwoorden. Dat vergt minder capaciteit.

Daar komt bij dat het vertrouwen van de samenleving in zowel de opsporingsdiensten en de FIU-Nederland, als in de banken zal toenemen indien sneller en efficiënter onderzoek wordt gedaan, verdachte transacties en verdenkingen van strafbare feiten (zoals witwassen, fraude en oplichting) en naar de juistheid van rekeningnummers. Het VB draagt daarnaast bij aan het bereiken van de specifieke doelstelling van de aangesloten organisaties.

Doordat het proces wordt geautomatiseerd kunnen menselijke fouten in het vorderingsproces eerder worden opgemerkt en worden voorkomen. Dit betreft bijvoorbeeld een onjuist overgenomen naam in een vordering. Indien in het systeem een niet-bestaande combinatie van gegevens voorkomt, zal dit niet tot een match leiden.

## 7. Verwerkingslocaties

Benoem in welke landen de voorgenomen gegevensverwerkingen plaatsvinden.

De gegevensverwerking binnen het VB vindt plaats in Nederland, bij het Ministerie van Justitie en Veiligheid. Het systeem wordt geplaatst bij de Justitiële Informatiedienst, bij IBO<sup>22</sup>. Deze organisatie is onderdeel van het Ministerie van Justitie en Veiligheid, maar treedt hier op in de rol van beheerder, en derhalve verwerker, en heeft dus een onafhankelijke rol (opdrachtnemer ten aanzien van beheer).

Ten aanzien van de deelnemers geldt het volgende:

1. Alleen de hierboven genoemde overheidsorganisaties gevestigd in Nederland hebben toegang tot het portaal (het gaat om feitelijke vestiging i.v.m. waarborg veiligheidsvoorschriften).

Overheidsinstanties in overzeese gebiedsdelen dienen dit op te lossen via een in Nederland gevestigd gedeelte van de organisatie.

2. Hetzelfde geldt voor de banken, alleen banken die op de Nederlandse markt producten aanbieden sluiten zich (verplicht) aan op het portaal en hebben hier dus toegang toe. Ten aanzien van evt. subverwerking van gegevens in derde landen zijn de banken zelf verantwoordelijk voor verwerking conform huidige werkwijze, maar verzoeken in het kader van dit portaal worden alleen uitgewisseld tussen de bank en het portaal. In het geval dat banken gebruik maken van datacenters in andere landen, zal dit met de komst van het VB dus niet veranderen. Informatie kan zo nodig in het datacenter worden opgehaald, maar dient via een in Nederland gevestigde bank te worden uitgewisseld. Vragen en vorderingen die banken via het VB ontvangen verlaten Nederland echter niet.

3. Informatie over producten die in Nederland zijn afgenomen kan via het VB worden opgevraagd, ongeacht het woon- of vestigingsland van de betrokkene.

## 8. Techniek van gegevensverwerking: geautomatiseerde besluitvorming, profilering en big data

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

Het VB is bedoeld voor het direct (real-time) opvragen van gegevens. Hierbij moet het portaal zoveel mogelijk aansluiten op bestaande informatiesystemen bij de vragende partijen. Hierdoor biedt het portaal koppelingsmogelijkheden.

Niet alle partijen hebben eigen applicaties waarop aangesloten kan worden. In die gevallen kunnen de (opsporings)ambtenaren rechtstreeks gebruik maken van VB. Bevoegde (opsporings)ambtenaren kunnen inloggen met de inloggegevens (gebruikersnaam en wachtwoord) die bij de geautoriseerde opsporingsambtenaar bekend zijn. Het VB toetst de inloggegevens bij de betrokken organisatie en valideert dat deze gebruiker toegang heeft tot het portaal. Gebruikersbeheer vindt plaats in de organisaties die het VB gebruiken. Hiertoe wordt federatieve authenticatie gebruikt.

Na het verkrijgen van toegang tot het portaal dient de (opsporings) ambtenaar bij elk verzoek de gebruikersvoorwaarden te accepteren. Alleen als deze expliciet geaccepteerd worden kan de gebruiker daarna een vordering indienen. Het VB voert een aantal toetsen uit, voordat de vraag van de (opsporings) ambtenaar wordt uitgezet bij de banken:

- Garanderen dat een (opsporings)ambtenaar alleen op basis van wettelijke artikelen kan vorderen (m.a.w. is geautoriseerd op grond waarvan de opsporingsambtenaar bevoegd is gegevens te vorderen);

<sup>22</sup> Het Ministerie van JenV maakt geen gebruik van een Cloud die wordt gehost in een land dat een onvoldoende beschermingsniveau biedt.

- Valideren of vraag conform de vastgestelde minimale zoekcriteria voldoet;
- Controleren of de bijbehorende vorderingsgegevens zijn ingevuld, inclusief fiattering dooreen hOvJ of teamleider;
- In het geval van het vorderen op basis van een IBAN-nummer: garanderen dat de vraag alleen naar de bank verzonden wordt die het IBAN-nummer heeft uitgegeven.

Er is geen sprake van geautomatiseerde besluitvorming, profilering of big data. Slechts indien en voorzover geconcludeerd zou kunnen worden dat enige verwerking binnen het VB toch geduid zou moeten worden als geautomatiseerde besluitvorming (artikel 22 lid 1 AVG), is deze geautomatiseerde besluitvorming toegestaan op grond van artikel 40 UAVG; de verwerking is noodzakelijk om te voldoen aan een wettelijke verplichting, zonder dat sprake is van profilering. Immers, voorzover sprake zou zijn van een geautomatiseerde besluitvorming, komt het besluit niet tot stand na (of: op basis van) een "verwerking van persoonsgegevens ter beoordeling van persoonlijke aspecten van een natuurlijk persoon, met name om kenmerken betreffende beroepsprestaties, economische situatie, gezondheid, persoonlijke voorkeuren of interesses, betrouwbaarheid of gedrag, locatie of verplaatsingen van de betrokkene te analyseren of te voorspellen." (Overweging 71 AVG). De bevestigingen in het VB zijn gericht op een specifiek natuurlijk persoon of rechtspersoon, een zoekopdracht zal een of enkele resultaten opleveren. De uitkomsten van de zoekvraag worden opgenomen in het onderzoeksdossier, waarmee een financieel rechercheur samen met andere bronnen tot een oordeel komt. Dit systeem sluit aan bij de bestaande wijze van financieel rechercheren en introduceert geen automatische besluitvorming.

De verwerking is noodzakelijk omdat reeds bij ontvangst van het verzoek door de bank is vastgesteld dat er sprake is van een wettelijke verplichting tot verstrekking van de gegevens, het VB controleert immers of aan de wettelijke vereisten voor verstrekking is voldaan (indien dit niet het geval is wordt het verzoek niet aan de bank verstuurd). De beslissing van de banken om gegevens te verstrekken wordt geautomatiseerd. Dit betekent dat de banken bij het gebruik van het VB niet per verstrekking voorafgaand goedkeuring geven. Om deze reden worden enkel vorderingen die voorafgaand zijn beoordeeld op proportionaliteit en subsidiariteit via het portaal ingediend, worden de ondertekende vorderingen bewaard in het onderzoeksdossier en wordt achteraf door middel van audits getoetst of alle processtappen juist zijn doorlopen. Banken zijn betrokken bij de ontwikkeling van het verwijzingsportaal en worden ook in de gelegenheid gesteld om input te leveren bij het inrichten van het auditsysteem. Daarnaast krijgen zij, periodiek, inzage in de uitkomst van de audit. Op deze manier kunnen banken voorafgaand aan de in gebruikname van het portaal controleren of het systeem aan alle vereisten voldoet en na ingebruikname van het portaal controleren of het in de praktijk ook juist wordt gebruikt. Het systeem wordt ontwikkeld binnen de kaders van de BIR en heeft een Departementaal Vertrouwelijke rubricering. Verder worden de NCSC webrichtlijnen toegepast op het VB. Het VB wordt onderworpen aan een penetratietest (zgn. PEN test) voordat deze in productie wordt genomen. Deze test wordt periodiek herhaald.

De banken zijn verantwoordelijk voor het beheersen van risico's in de eigen organisatie. Om te controleren of het systeem geschikt is voor gebruik, wordt ook aan de kant van de banken een penetratietest van het koppelvlak uitgevoerd waarvan de resultaten met het VB worden gedeeld voordat (echte) persoonsgegevens via het systeem aan de bank wordt gestuurd.

## 9. Juridisch en beleidsmatig kader

Benoem de wet- en regelgeving, met uitzondering van de AVG en de Richtlijn, en het beleid met mogelijke gevolgen voor de voorgenomen gegevensverwerkingen.

De volgende wettelijke bepalingen liggen ten grondslag aan het VB:

- Wetboek van Strafvordering (WvSv), artikel
- 126nc (opsporing)
  - 126uc (bestrijding georganiseerde misdaad)
  - 126zk (terrorismebestrijding)

- 126a (bij een Strafrechtelijk Financieel Onderzoek)
  - 126ii (verkennd onderzoek terrorisme)
  - 577bb (executieonderzoek)
- Wet economische delicten (Wed)
- art 19 (economisch delict)
- Algemene wet inzake rijksbelastingen (AWR)
- art 53, eerste lid, onderdeel a
- Invorderingswet (IW)
- art 62
  - art 62bis (1BRN)
- Algemene wet inkomensafhankelijke regelingen (Awir)
- art 38, incl. uitvoeringsbesluit art 1a/1b
- Wet ter voorkoming van witwassen en financieren van terrorisme (Wwft)
- art 17

Wet politiegegevens  
 Wet basisregistratie personen  
 Wet justitiële en strafvorderlijke gegevens  
 Archiefwet 1995.

Richtlijn (EU) 2018/843 van het Europees Parlement en de Raad van 30 mei 2018 tot wijziging van Richtlijn (EU) 2015/849 inzake de voorkoming van het gebruik van het financiële stelsel voor het witwassen van geld of terrorismefinanciering, en tot wijziging van de Richtlijnen 2009/138/EG en 2013/36/EU (PbEU 2018, L 156).

## 10. Bewaartermijnen

Bepaal en motiveer de bewaartermijnen van de persoonsgegevens aan de hand van de verwerkingsdoeleinden.

Er zijn verschillende bewaartermijnen van toepassing:

1. Het VB kent geen centrale opslag van persoonsgegevens van gevorderde of opgevraagde persoonsgegevens van klanten, deze worden na 5 minuten verwijderd. Het maakt gebruik van een centrale routeringsvoorziening. In het VB worden slechts metagegevens opgeslagen die betrekking hebben op de expliciete vraag van de desbetreffende opsporingsambtenaar, waaronder de aanduiding van de opsporingsambtenaar. De metagegevens bevatten de gegevens *over* de vragen en antwoordberichten. Deze gegevens dienen onder andere voor de besturing, zoals (zoals het koppelen van de antwoorden aan de vraag), de rapportages en de controle (audits). De bewaartermijn voor de metagegevens bedraagt 4 jaar.

2. De persoonsgegevens die in het berichtenverkeer worden verzonden, worden bewaard door de aangesloten partijen (opsporing, FIU-Nederland en Belastingdienst voor wat betreft de vraag, de banken voor wat betreft ontvangen /verwerken verzoek en banken wat betreft de levering en de opsporing ten aanzien het ontvangen). Het uitgangspunt ten aanzien van deze gegevensuitwisseling is dat hiervoor reeds bestaande bewaartermijnen worden gehanteerd en dat gegevens in ieder geval niet langer worden bewaard dan noodzakelijk is voor een correct en legitiem functionerend VB, conform het huidige proces. Voorafgaand en na afloop van de pilot zullen met de betrokken partijen aanvullende afspraken worden gemaakt over de bewaartermijnen, indien dit naar aanleiding van de uitkomsten van de pilot aanvulling behoeft.

## B. Beoordeling rechtmatigheid gegevensverwerkingen

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

### 11. Grondslag

Bepaal op welke rechtsgronden de gegevensverwerkingen worden gebaseerd.

De gegevensverwerking door de verschillende organisaties is gebaseerd op verschillende rechtsgronden:

Opsporingsdiensten:

- NP: art. 8,9 en 10 Wpg
- OM: art. 39b Wjsg
- De Kmar: art. 8,9 en 10 Wpg
- De Rijksrecherche: art. 8,9 en 10 Wpg

Bijzondere Opsporingsdiensten: art. 10 Besluit politiegegevens bijzondere opsporingsdiensten in combinatie met 8 en 9 Wpg (NB! wordt aangepast vanwege richtlijn implementatie)

- de FIOD
- NVWA-IOD
- Inspectie SZW
- ILT/IOD

FIU-Nederland: artikel 6:6 van het Besluit politiegegevens

Deze rechtsgronden betreffen in alle gevallen taken van algemeen belang die aan de betreffende organisaties zijn opgedragen: artikel. 6, lid 1, onder e, jo. artikel 6, derde lid, van de AVG

De Belastingdienst: artikel. 6, lid 1, onder e, jo. artikel 6, derde lid, van de AVG:  
voor: de Belastingdienst is de verwerking noodzakelijk voor de vervulling van een taak van algemeen belang die aan de Belastingdienst is opgedragen.

Naast de Wbp/AVG geldt voor de BD ook de geheimhoudingsplicht van artikel 67 AWR en IW. Deze geheimhoudingsplicht wordt in het geval van het gebruik van het VB na inwerkingtreding van het wetsvoorstel VB doorbroken voor de gegevens die noodzakelijk zijn om identificerende gegevens bij een bank op te vragen (NAW gegevens, IBAN en BSN), omdat wetgeving tot gegevensverstrekking verplicht en artikel 67, tweede lid, onderdeel a, AWR en IW voor die gevallen een uitzondering maakt.

Banken: De banken zijn verplicht te reageren op vorderingen en verzoeken om informatie die door opsporingsinstanties of Belastingdienst worden gedaan. De grondslag van deze verwerking volgt uit artikel 6, lid 1, onder c, jo. artikel 6, derde lid, van de AVG.

### 12. Bijzondere persoonsgegevens

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

De gegevens uit zoekopdrachten van opsporingsdiensten en de reactie daarop van banken zijn strafrechtelijke gegevens. Dit betekent dat door het portaal strafrechtelijke gegevens worden

verwerkt. Deze gegevens worden verwerkt door de opsporingsdiensten en de beheerder in opdracht van de opsporingsdiensten. Deze gegevens mogen op grond van artikel 6, lid 1 AVG, alleen worden verwerkt onder toezicht van de overheid of indien de verwerking is toegestaan bij wettelijke bepalingen die passende waarborgen voor de rechten en vrijheden van de betrokkenen bieden (art. 10 AVG). Op basis van artikel 33 lid 1 onder a UAVG mogen strafrechtelijke gegevens worden verwerkt, ook door private instellingen zoals banken, indien deze door de verwerkingsverantwoordelijke zijn verkregen krachtens de Wpg of de Wjsg. Het vorderen van gegevens is een strafvorderlijke bevoegdheid die wordt ingezet bij de opsporing en voorkoming van strafbare feiten. De gegevens die worden verwerkt ten behoeve van het vorderen, worden door de politie verwerkt binnen het regime van de Wpg. In dit geval is de verwerking van deze strafrechtelijke gegevens door de banken dus toegestaan.

De gegevens die door het VB worden verwerkt, worden verwerkt onder toezicht van de overheid. Dit betreft in eerste instantie de vragende instanties als verwerkingsverantwoordelijke. Daarnaast is Justid/IBO namens de minister van Justitie en Veiligheid de beheerder van het portaal. Het betreft geen register van strafrechtelijke veroordelingen.

Voor wat betreft de verwerking van het BSN, het wettelijk identificatienummer, geldt dat de vragende instanties als overheidsinstanties dit mogen gebruiken ten behoeve van de uitvoering van hun taak (art. 10 Wabb). De banken, als private partijen, mogen het BSN verwerken voor zover hier een wettelijke grondslag voor is. In het wetsvoorstel VB is een bepaling opgenomen waarin staat dat de banken het BSN mogen gebruiken voor het opvragen van gegevens uit de eigen administratie ten behoeve van de verstrekking van identificerende gegevens. Indien dit voorstel wordt aangenomen, betekent dit dat het BSN kan worden gebruikt ten behoeve van het koppelen van een verzoek aan de juiste informatie binnen het klantsysteem van de bank, het 'matchen'. Het gebruik van het BSN is noodzakelijk om gericht informatie uit de administratie van aangesloten partijen te kunnen opvragen ten behoeve van verstrekking via het VB. Hiervoor is gekozen in het kader van dataminimalisatie: naarmate gericht gezocht kan worden, worden de zoekresultaten specifiek. Indien wordt gezocht met gebruik van een uniek nummer, het BSN, is er maximaal kans op één uniek zoekresultaat. Dit betekent dat alleen gegevens van die betrokkene door de bank aan de vragende instantie wordt verstrekt. In het wetsvoorstel is uitdrukkelijk beschreven dat het BSN op grond van dit wetsvoorstel aan de kant van banken en betaalinstanties alleen mag worden gebruikt om identificerende gegevens geautomatiseerd in de eigen administratie op te zoeken ten behoeve van een vordering of verzoek op grond van het VB. Banken en betaaldienstverleners kunnen het BSN hiervoor alleen gebruiken als zij daarover al beschikken op grond van een andere wettelijk voorschrift.

### **13. Doelbinding**

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

De gegevens die door het VB worden verwerkt, worden verwerkt ten behoeve van het doel waarvoor deze door de bank aan de vragende instantie worden verstrekt<sup>23</sup>. Dit betreft de doeleinden zoals beschreven in het antwoord op vraag 4. Deze gegevens worden door het VB verwerkt ten behoeve van het versturen van de vraag en het antwoord aan de juiste instanties (routing). Dit ligt in het verlengde van het doel van de verwerking door de vragende instantie. De loggingsgegevens worden verwerkt voor de besturing, zoals (zoals het koppelen van de antwoorden aan de vraag), de rapportages en de controle (audits) op het systeem. Voor dit doel zijn de gegevens door de betrokkene (de vragende medewerker) ook verstrekt.

<sup>23</sup> De elektronische verwerking van de gegevens is dus verenigbaar met de oorspronkelijke doeleinden van de verwerking.

Voor de banken verschilt het nieuwe proces niet ten opzichte van het oude proces. Het doel van de verstrekking aan de vragende instanties komt niet overeen met het doel van de verstrekking van de gegevens door de klant aan de bank ( in het kader van een overeenkomst tussen bank en klant). De bank is echter wettelijk verplicht deze informatie te verstrekken indien deze wordt opgevraagd door de opsporingsinstanties (en de FIU-Nederland en Belastingdienst). Van dit wettelijk voorschrift zijn banken zich bewust en hebben dit ook opgenomen in hun privacy statements. Derhalve is verdere verwerking verenigbaar met het doel waarvoor de gegevens zijn verzameld.

De gegevens kunnen door de vragende instanties na ontvangst enkel worden gebruikt voor het doel waarvoor deze zijn opgevraagd (zie ook antwoord op vraag 4).

#### 14. Noodzaak en evenredigheid

Beoordeel of de voorgenomen gegevensverwerkingen noodzakelijk zijn voor het verwezenlijken van de verwerkingsdoeleinden. Ga hierbij in ieder geval in op proportionaliteit en subsidiariteit.

- a. Proportionaliteit: staat de inbreuk op de persoonlijke levenssfeer en de bescherming van de persoonsgegevens van de betrokkenen in evenredige verhouding tot de verwerkingsdoeleinden.
- b. Subsidiariteit: kunnen de verwerkingsdoeleinden in redelijkheid niet op een andere, voor de betrokkenen minder nadelige wijze, worden verwezenlijkt? Benoem hierbij de overwogen alternatieven.

De Europese Commissie heeft op 5 juli 2016 een voorstel gedaan voor een richtlijn tot wijziging van Richtlijn (EU) 2015/849 inzake de voorkoming van het gebruik van het financiële stelsel voor het witwassen van geld of terrorismefinanciering en tot wijziging van Richtlijn 2009/101/EG. Dit voorstel is inmiddels aangenomen. De richtlijn bevat onder meer de verplichting voor lidstaten te voorzien in automatische gecentraliseerde mechanismen, zoals centrale registers of centrale elektronische systemen voor gegevensontsluiting, die de tijdige identificatie mogelijk maken van natuurlijke of rechtspersonen die houder zijn van of zeggenschap hebben over betaalrekeningen en bankrekeningen die worden aangehouden door een kredietinstelling. Het VB is een dergelijk systeem.

Daarnaast, wordt in het kader van de Rijksbrede aanpak fraude *Financial intelligence* gebruikt om criminele geldstromen en vermogen in beeld te brengen om criminele feiten te achterhalen en criminele winsten af te pakken, ten behoeve van de ontmanteling van criminele organisaties. Hiertoe is een samenwerkingsverband opgericht tussen opsporingsdiensten en de financiële sector, maar de samenwerking tussen de financiële sector en opsporingsdiensten kan beter en eenvoudiger.

In reactie op Kamervragen na de uitzending van Zembla op 25-11-2015 over informatie-uitwisseling tussen banken en financieel rechercheurs, heeft de minister van Justitie en Veiligheid aangegeven dat er invulling wordt gegeven aan het verder verbeteren van het proces voor het opvragen van identificerende gegevens van banken in de vorm van een VB met rechtstreekse aansluiting op de Bijzondere Opsporingsbevoegdheden-kamer van het OM en de opsporingsinstanties. Door het gebruik van een VB worden aanzienlijke verbeteringen verwacht in effectiviteit en snelheid van de opsporing en tevens een kostenbesparing voor zowel overheidsdiensten als banken.

Doel van het VB is door het bieden van een technische infrastructuur ondersteunen van het betrouwbaar, snel, juist, volledig en efficiënt, *geautomatiseerd* opvragen en verstrekken van een beperkte set identificerende (bankrekening)gegevens en identificerende gegevens behorend bij financiële producten op een uniforme wijze bij alle in Nederland gevestigde banken, ten behoeve van het verschaffen van een indicatie voor eventueel verder onderzoek of nadere controle in het kader van het voorkomen en opsporen van fraude en andere vormen van criminaliteit.

Het doel van de gegevensverwerking binnen het VB is afgeleid van het doel van de gegevensverwerking door de vragende partijen, het VB is immers verwerker voor de vragende partijen. Het doel van de verwerking via het VB, is het bevragen, vorderen en ontvangen van identificerende gegevens bij banken efficiënter en effectiever te laten verlopen. Door de komst van het VB verandert de wijze van verstrekking; het VB beoogt de gegevensverwerking zo

efficiënt mogelijk te effectueren en beoogt de wettelijke bevoegdheden niet in te perken of te verruimen. Het VB verandert ook niet de gegevens die worden verstrekt of de doeleinden waarvoor dit gebeurt. De persoons- en zaakgegevens die in het portaal worden getoond c.q. verwerkt, zijn niet anders dan de gegevens die thans schriftelijk worden verstrekt. Dit is enkel anders voor het BSN: dit zal naast de eerder genoemde doeleinden worden verwerkt voor het specifieke doel van het mogelijk maken van een unieke koppeling tussen een verzoek of vordering en de gegevens van de betrokkene in de klantadministratie.

Vanwege het unieke karakter van het burgerservicenummer en het brede gebruik van het nummer binnen de overheid, zijn aan het gebruik van het burgerservicenummer door private partijen risico's verbonden voor de betrokkenen. In het onderhavige geval zijn deze risico's voor betrokkenen afgewogen tegen de risico's voor betrokkenen die bestaan als in het portaal geen burgerservicenummer zou worden gebruikt. De uitkomst hiervan is dat het gebruik van het burgerservicenummer meer risico's wegneemt dan dat het oplevert.

Het gebruik van het burgerservicenummer is noodzakelijk om gericht en snel informatie uit de administratie van aangesloten partijen te kunnen opvragen ten behoeve van verstrekking via het verwijzingsportaal. Voor het gebruik van het burgerservicenummer is gekozen in het kader van dataminimalisatie: naarmate gericht gezocht kan worden, worden de zoekresultaten specifiek. Indien wordt gezocht met gebruik van een uniek nummer, het burgerservicenummer, dat ook een beveiliging bevat tegen typefouten, is er maximaal kans op één uniek zoekresultaat. Dit betekent dat alleen gegevens van die betrokkene door de bank aan de vragende instantie worden verstrekt. In het wetsvoorstel is uitdrukkelijk beschreven dat het burgerservicenummer op grond van dit wetsvoorstel aan de kant van banken en betaalinstanties alleen mag worden gebruikt om identificerende gegevens geautomatiseerd in de eigen administratie op te zoeken ten behoeve van een vordering of verzoek op grond van het verwijzingsportaal bankgegevens. Banken en betaaldienstverleners kunnen het burgerservicenummer hiervoor alleen gebruiken als zij daarover al beschikken op grond van een andere wettelijk voorschrift.

Met de komst van het VB worden binnen het VB ook persoonsgegevens verwerkt van degenen die binnen het VB gegevens hebben verwerkt en van degenen die een vordering of vraag via het VB hebben ingediend (metadata). Het doel van deze gegevensverwerking is het achteraf kunnen traceren van de verwerkingen binnen het VB. Deze gegevens worden gebruikt ten behoeve van periodieke audits (die vanuit het beheer van het VB worden uitgevoerd, de inhoud en frequentie worden gedurende de pilot vastgesteld, dwz Q1 2018)<sup>24</sup>.

#### *Proportionaliteit*

Met de komst van het VB zullen persoonsgegevens van de betrokkene in plaats van direct van vragende instantie naar bank en andersom, door tussenkomst van het VB worden verstrekt. Dit betekent dat er een extra verwerking van persoonsgegevens aan het huidige proces wordt toegevoegd. Hier staat tegenover dat gegevens gericht kunnen worden opgevraagd en dat het niet meer noodzakelijk is dat verschillende personen zicht hebben op een verzoek dat bij een bank binnenkomt en gegevens die aan de vragende partijen worden verstrekt. In het systeem worden daarnaast verschillende maatregelen genomen om de inbreuk op de persoonlijke levenssfeer te beperken, zoals de zeer beperkte bewaartermijn (5 minuten) voor opgevraagde of gevorderde gegevens van de betrokkene in het portaal en het versleuteld versturen van gegevens. Hierdoor worden de gegevens van de betrokkene in het portaal enkel bewaard ten behoeve van de ontvangst van de gegevens door de vragende instanties (antwoorden downloaden binnen 5 minuten) en niet langer bewaard dan noodzakelijk voor dit doel. Deze gegevens zijn daarnaast niet toegankelijk voor derden die niet gerechtigd zijn deze in te zien.

Het doel van de verzoeken die via het VB worden ingediend is eveneens de rechtvaardiging voor de inbreuk op de persoonlijke levenssfeer van de betrokkene. Gegevens worden immers opgevraagd ten behoeve van het voorkomen en opsporen van fraude en andere vormen van criminaliteit en het opsporen van (criminele) vermogens en het opleggen van financiële maatregelen en sancties door de daarvoor bevoegde opsporingsdiensten, en het voorkomen van misbruik met toeslagen door de Belastingdienst. De kwaliteit en de volledigheid van de gegevens

---

<sup>24</sup> Deze wordt in gezamenlijkheid ingericht, zodat bv ook rechtmatigheid vordering achteraf wordt gecheckt. Het is een audit vanuit de beheerspartij van het portaal.



die worden verstrekt zal met de komst van het VB toenemen, hierdoor kunnen ook de aangesloten overheidsinstanties beter hun werkzaamheden uitvoeren. Dit kan echter alleen als de zij hier op basis van de huidige wetgeving bevoegd zijn identificerende gegevens op te vragen. De bevoegdheden worden met de komst van het systeem niet uitgebreid.

Een gevolg van introductie van het systeem kan echter wel zijn dat doordat het proces eenvoudiger en sneller is, er meer vorderingen worden ingediend. Een vordering is immers onderdeel van een breder onderzoek. Hiermee wordt vaak informatie verkregen die leidt tot vervolgvragen. De inbreuk op de persoonlijke levenssfeer die per geval beperkt is, kan hierdoor wel voor een grotere groep betrokkenen spelen. Hierbij is van belang op te merken dat voor het indienen van een vordering steeds aan dezelfde vereisten moet zijn voldaan: dit kan niet in geval er geen sprake is van een verdenking van een misdrijf of als niet aan de voorwaarden van andere gronden voor het opvragen via het verwijzingsportaal bankgegevens is voldaan. In het kader van de opsporing van het misdrijf of het andere doel van het opvragen moet het vorderen van gegevens steeds proportioneel zijn en moeten lichtere bevoegdheden worden ingezet indien deze tot hetzelfde resultaat kunnen leiden (subsidiariteit).

Een ander gevolg van de introductie van het systeem is dat er ook gegevens zullen worden verstrekt van betrokkenen waar de vragende instanties uiteindelijk niet naar op zoek blijken te zijn. Dit is ook nu het geval: na ontvangst van informatie beoordeelt de opsporingsambtenaar welke gegevens voor het onderzoek wel en welke niet van belang zijn. Een verschil ten opzichte van het huidige vorderingsproces is dat er bij het gebruik van het VB geen persoonlijk contact meer is voorafgaand aan de verstrekking tussen de opsporingsambtenaar en de bank. In voorkomende gevallen waarin een vordering op dit moment gegevens van veel verschillende personen betreft, wordt vaak telefonisch besproken of de zoekvraag verder kan toegespitst, waardoor het aantal zoekresultaten wordt beperkt. Om te voorkomen dat bij gebruik van het VB wel gegevens van een grote groep personen worden verstrekt is afgesproken dat zoveel mogelijk beschikbare informatie wordt ingevoerd in het systeem, dat kan worden gematcht op basis van het BSN en dat enkel gegevens worden teruggestuurd indien een zoekvraag tot maximaal drie personen leidt. Dit laatste is alleen anders bij zoekvragen op basis van product. Deze kunnen wel tot meer personen leiden.

#### *Subsidiariteit*

Bij de ontwikkeling van het VB zijn verschillende mogelijkheden onderzocht om een dergelijk systeem in te richten. Mede met het oog op de mogelijke inbreuk op de persoonlijke levenssfeer van de betrokkene is in het uiteindelijke ontwerp gekozen voor een koppeling tussen de vragende instantie en de bank. Enkel indien er een bevoegdheid is informatie te vragen en de verstrekende instantie over informatie beschikt, worden gegevens van de bank via het VB aan de vragende instantie verstrekt.

Een van de alternatieven die is onderzocht betreft centrale databank met gegevens waaruit informatie wordt gehaald indien hier om wordt gevraagd. Een dergelijk systeem vergt een regelmatige overdracht van een bestand met alle klantgegevens van banken, zodat de gegevens die worden opgevraagd steeds actueel zijn. Hier is niet voor gekozen vanuit het oogpunt van dataminimalisatie: enkel de noodzakelijke informatie wordt verstrekt binnen de gekozen oplossing.

De vragende instanties kunnen niet vrij in de gegevens van de bank zoeken. Per ingediend verzoek moet worden onderbouwd op welke gronden de gegevens worden opgevraagd.

Hiermee is gekozen voor de oplossing die zo min mogelijk ingrijpt op de persoonlijke levenssfeer van de betrokkene.

## 15. Rechten van de betrokkenen

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

Ten aanzien van de huidige situatie/werkwijze verandert er met de komst van het VB niets met betrekking tot de rechten van betrokkene. Het systeem is immers slechts 'verwerker' dus beschikt zelf niet over additionele informatie of anderszins die de rechten van betrokkene zou kunnen beperken. Door het inrichten van het VB ontstaat wel meer inzicht in de verwerkingen bij het vorderen of verzoeken en het verstrekken van bankgegevens ten opzichte van de bestaande situatie. Doordat het VB bij wet is geregeld en er informatie over de werking van het VB, de aangesloten partijen en de manier waarop verstrekkingen via het portaal plaatsvinden openbaar beschikbaar zal zijn, neemt de transparantie van de manier van vorderen of verzoeken en verstrekken toe.

Wel verandert het privacyregime voordat het VB daadwerkelijk in gebruik wordt genomen. Met de komst van de AVG nemen de rechten van de betrokkene toe, betrokkenen moeten bijvoorbeeld altijd kunnen vragen welke persoonsgegevens van hem of haar worden verwerkt en verzoeken kunnen indienen deze aan te passen indien deze niet juist zijn.

De betrokkene kan bij de bank terecht voor een antwoord op de vraag over welke gegevens de bank van de betrokkene beschikt. De bank kan hier desgewenst informatie over geven en de gegevens zo nodig aanpassen. De betrokkene kan eveneens bij de bank informeren welke gegevens met anderen zijn gedeeld en voor welk doeleinde.

In uitzonderlijke gevallen kunnen deze rechten van betrokkene worden beperkt (art. 23 AVG), door middel van wettelijke bepalingen, op voorwaarde dat die beperking de wezenlijke inhoud van de grondrechten en fundamentele vrijheden onverlet laat en in een democratische samenleving een noodzakelijke en evenredige maatregel is ter waarborging van onder meer de voorkoming, het onderzoek, de opsporing en de vervolging van strafbare feiten of de tenuitvoerlegging van straffen. Artikel 126bb, vijfde lid, van het Wetboek van Strafvordering schrijft geheimhouding voor aan degene tot wie een vordering als bedoeld in artikel 126nc, 126uc en 126zk is gericht, in het belang van het onderzoek. Dit geldt eveneens voor vorderingen die op grond van 126a van het Wetboek van Strafvordering worden gedaan via het VB (art. 126a, vijfde lid). Achtergrond voor deze bepaling is dat het onderzoek kan worden belemmerd, indien de betrokkene hierover wordt geïnformeerd. In het geval een bankmedewerker twijfelt of geheimhouding in het belang van het onderzoek nog noodzakelijk is, bijvoorbeeld omdat het een vordering van enkele jaren geleden betreft of anderszins blijkt dat een onderzoek is afgerond en de betrokkene daarvan op de hoogte is, kan de bankmedewerker hierover contact opnemen met de opsporingsambtenaar.

Voor het voldoen aan verzoeken van de FIU-Nederland geldt om dezelfde reden een geheimhoudingsplicht (art. 23 lid 1 Wwft). Dit betekent dat indien de betrokkene aan de bank vraagt of deze informatie aan derden heeft verstrekt de bank hier geen antwoord op geeft voor zover het verstrekken van informatie aan de opsporingsinstanties of de FIU-Nederland betreft. Hiervoor geldt immers de genoemde geheimhoudingsplicht. Ook voor verstrekkingen aan de Belastingdienst geldt op grond van artikel 67 Awr en Invorderingswet 1990 een geheimhoudingsplicht voor de banken, zodat over de daadwerkelijke verstrekking via het portaal geen mededelingen gedaan kunnen worden.

Betrokkenen kunnen eveneens aan de vragende partijen vragen over welke informatie zij beschikken. Zij zullen dit verzoek toetsen aan de hand van de wettelijke kaders die van toepassing zijn.

Het VB is (behoudens ten aanzien van metagegevens) enkel verwerker van gegevens namens de vragende partijen. Betrokkenen die bij het VB een verzoek indienen gegevens in te zien die worden verwerkt, worden doorverwezen naar de relevante vragende partijen. Op de website van het VB wordt duidelijk beschreven welke gegevens door het VB voor welk doeleinde worden verwerkt.

### C. Beschrijving en beoordeling risico's voor de rechten en vrijheden betrokkene

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

#### 16. Risico's

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

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

De nieuwe gegevensverwerking binnen en ten behoeve van het functioneren van het VB draagt een aantal privacyrisico's in zich. Deze zijn beoordeeld in de context van de bestaande structuur. Dit betekent dat er enkel is gekeken naar de wijzigingen die het nieuwe systeem met zich brengt, systemen die reeds worden gebruikt zijn niet opnieuw beoordeeld. De risico's ten aanzien van de beveiliging kunnen zich op verschillende plekken voordoen:

- Tussen de vragende overheidspartijen en het VB (Haagse Mail Relay<sup>25</sup>)
- Tussen het VB en de bank (internet)
- Bij het VB (web-omgeving)

Hierbij is naast hetgeen eerder in dit document is genoemd van belang dat:

- Op de verwerking van gegevens een standaard set van beveiligingsnormen van toepassing is (o.a. BIR en NCSC-web richtlijn).
- Het rubriceringsniveau van de te verwerken data is vastgesteld op 'Departementaal Vertrouwelijk (DEP-Vertrouwelijk').
- Op de data die binnen het portaal verwerkt wordt, zijn de Wpg en de AVG van toepassing, afhankelijk van het regime dat van toepassing is op de vragende partij.
- Er (technische) aansluitvoorwaarden bepaald worden op basis waarvan een deelnemer mag aansluiten.

Het dreigingsbeeld kan per organisatie verschillen. Dit kan betekenen dat sommige risico's voor de ene organisatie meer impact en een hogere kans hebben dan voor een andere organisatie. Bij het beoordelen van het risico dat indringers van buiten toegang krijgen tot het systeem moet rekening worden gehouden met statelijke actoren en georganiseerde criminaliteit.

Er zijn 20 risico's geïdentificeerd die gecategoriseerd zijn in:

- legitimiteits-risico's, zoals het risico dat gegevens worden opgevraagd zonder dat aan alle formele vereisten voor die vordering is voldaan of het risico dat gegevens worden opgevraagd in situaties dat dit voor het onderzoek minder relevant is;
- privacy-risico's (waaronder mede wordt verstaan risico's voor de rechten en vrijheden van betrokkenen), zoals het risico dat gegevens van verkeerde personen worden verstrekt of dat te veel gegevens worden verstrekt, en
- informatiebeveiligings-risico's, zoals het risico dat personen die niet zijn geautoriseerd toch toegang krijgen tot het verwijzingsportaal.

Ten aanzien van deze categorieën is het risico op foutief handelen van een opsporingsambtenaar/bevoegde autoriteit of buitenstaander concreet gemaakt. Op basis van de beschreven (foutieve) handelingen is de impact beschreven en is ingeschat of deze impact groot, middel of klein is. Daarna is het rest risico beoordeeld op relevantie. Daar waar de rest risico's als "klein" worden beoordeeld, wordt het risico geaccepteerd.

<sup>25</sup> Dit is het informatienetwerk waar de overheidsdiensten gebruik van maken.

Dit overzicht is terug te vinden in de bijlage 'Risico Assessment 20171220'. Ook worden in dit overzicht de mitigerende maatregelen genoemd, deze worden inhoudelijk toegelicht in het antwoord op vraag 17.

## D. Beschrijving voorgenomen maatregelen

### 17. Maatregelen

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

De bescherming van persoonsgegevens is een belangrijke overweging geweest bij beslissingen over de inrichting van het verwijzingsportaal, zoals artikel 25 AVG ook voorschrijft. Voorbeelden zijn:

- dat geen database is ingericht maar een technische voorziening met een koppelvlak, zodat alleen de informatie die concreet wordt opgevraagd wordt verstrekt;
- dat minimaal een aantal velden ingevuld moet worden om via het VB te kunnen opvragen om te brede of onnauwkeurige uitvragen te voorkomen;
- dat naar aanleiding van een zoekvraag per bank maximaal drie personen in het antwoord worden opgenomen (met uitzondering van zoekvragen obv product, waar het er meer kunnen zijn).

Het uitgangspunt is verder dat er standaard een set van beveiligingsnormen van toepassing is (o.a. BIR en NCSC-web richtlijn). Zoals al in het antwoord op vraag 16 is omschreven, zijn voor de risico's die onacceptabel worden geacht maatregelen geformuleerd die tijdens het project geïmplementeerd zijn c.q. zullen worden. Het overzicht hiervan is terug te vinden in het 'Risico Assessment VB 20171220' dat genoemd wordt bij vraag 16.

De genoemde maatregelen in de risico assessment worden breed toegelicht in het document 'Generiek overzicht VB-maatregelen 20171220'.

*Toelichting maatregelenlijst (Generiek overzicht VB-maatregelen 20171220)*

Er is een set van 39 detail maatregelen ontwikkeld voor de eerder geïdentificeerde 19 impactgevoelige risico's (zie antwoord vraag 16) op gebied van legitimiteit, privacy en informatiebeveiliging waarvan er een relatief grote kans is dat het zich kan voordoen als er geen mitigerende maatregelen worden getroffen.

Van de maatregelen genoemd in de 'Risico Assessment VB 20171220' is in het document 'Generiek overzicht VB-maatregelen 20171220' het doel en de inhoud toegelicht en wordt in de kolom "Wat?" concreet aangegeven wat de maatregel na implementatie mitigeert.