Auditdienst Rijk
*Ministerie van Financiën*

# Onderzoeksrapport
# Beheer Verwijzingsportaal Bankgegevens

definitief

# Colofon

| | |
|---|---|
| Titel | Onderzoeksrapport Beheer Verwijzingsportaal Bankgegevens |
| Uitgebracht aan | DG Ondermijning van het ministerie van Justitie en Veiligheid |
| Datum | 18 april 2023 |
| Versie | Definitief |
| Kenmerk | 2023-0000099513 |

*Inlichtingen*
**Auditdienst Rijk**
070-342 7700

# Inhoud

# Aanleiding opdracht

De Wet verwijzingsportaal bankgegevens is op 10 september 2020 in werking getreden. Met deze wet wordt het voor banken en andere betaaldienstverleners die rekeningen aanbieden met een Nederlands IBAN identificatienummer en banken die kluizen verhuren in Nederland, verplicht om aan te sluiten op het Verwijzingsportaal Bankgegevens (VB).

Het Besluit verwijzingsportaal bankgegevens bevat o.a. nadere regels over de gegevens die via het VB worden ontsloten, de technische eisen waaraan het systeem en de aansluiting daarop moeten voldoen, de partijen die bevoegd zijn om het VB te gebruiken en uit te voeren audits.

Over uit te voeren audits zegt het Besluit verwijzingsportaal bankgegevens het volgende (artikel 5 lid 3 en lid 4):

> 3. Er wordt tweejaarlijks een audit gedaan naar de goede uitvoering van dit besluit, waarbij ten minste de volgende onderwerpen worden behandeld:
> a. de werking van het verwijzingsportaal bankgegevens;
> b. de kwaliteit van de vorderingen, verzoeken en verstrekkingen van gegevens.
>
> 4. In afwijking van het derde lid, wordt de audit de eerste vijf jaar na inwerkingtreding van dit besluit jaarlijks gedaan.

Om invulling te geven aan deze bepaling heeft directoraat-generaal Ondermijning (DGO) van het ministerie van Justitie en Veiligheid (JenV) aan de Auditdienst Rijk (ADR) gevraagd onderzoek te doen naar het beheer van het VB door de Justitiële Informatiedienst (Justid).

# Managementsamenvatting

In het Besluit verwijzingsportaal bankgegevens is bepaald dat jaarlijks een audit moet worden uitgevoerd naar de werking van het Verwijzingsportaal Bankgegevens (VB) en de kwaliteit van vorderingen en verstrekkingen.
Het directoraat-generaal Ondermijning van het ministerie van Justitie en Veiligheid, de eigenaar van het VB, heeft de Auditdienst Rijk (ADR) gevraagd om onderzoek te doen om daarmee invulling te geven aan de bepaling in het besluit. De ADR heeft daarvoor twee onderzoeken uitgewerkt; een onderzoek naar het beheer van het VB door Justid (een agentschap van het ministerie van Justitie en Veiligheid) en een onderzoek naar het gebruik van het VB door de FIOD. Dit rapport bevat de uitkomsten van het onderzoek naar het beheer van het VB dat binnen Justid wordt uitgevoerd door de afdeling Justid Opsporing.

### Justid Opsporing heeft veel aandacht besteed aan de inrichting van het beheer van het VB

In ons onderzoek hebben we vastgesteld dat Justid Opsporing er veel aan heeft gedaan om het beheer van het VB in te richten. Het incidentproces is georganiseerd voor het VB en stelt Justid in staat om incidenten tijdig af te handelen. Het wijzigingsproces is ingericht waardoor Justid Opsporing wijzigingen op een beheerste manier kan uitvoeren.
Om een ongestoorde werking van het VB te waarborgen heeft Justid daarnaast een groot aantal maatregelen getroffen. Bijvoorbeeld op het gebied van beheer van de configuratie, monitoring van componenten, beheer van toegangsrechten, versleuteling van gegevens en voorzieningen voor calamiteiten. Het logboek van de via het VB uitgevoerde bevragingen is operationeel en gelogde gegevens worden na de bewaartermijn verwijderd.

### Er zijn vier bevindingen die direct de aandacht vragen van Justid Opsporing

1) Justid Opsporing maakt bij het beheer van het VB gebruik van diensten van drie IT-dienstverleners. Op dit moment is er te weinig zicht op de beheertaken die door de IT-dienstverleners worden uitgevoerd. Er ontbreken afspraken over de beveiligingsmaatregelen die door de IT-dienstverleners moeten worden getroffen en het toezicht op beveiligingsmaatregelen is niet ingericht.
2) De voorziening om verdachte gebeurtenissen te signaleren is nog niet af. De onderbouwing voor gemaakte keuzes ontbreekt, geplande activiteiten voor de verdere inrichting staan nog open en de toegezegde externe toetsing is niet uitgevoerd.
3) Justid Opsporing voert beperkt testen uit van de voorzieningen voor calamiteiten. De uitgevoerde testen geven geen garantie dat het VB na een calamiteit tijdig in de volle breedte beschikbaar is.
4) Het traject om aantoonbaar te voldoen aan de Baseline Informatiebeveiliging Overheid (BIO) staat nog aan het begin. Het is onduidelijk wanneer Justid Opsporing de invoering van de BIO voor het VB volledig heeft afgerond.

### Wij zien verbetermogelijkheden voor onderdelen van het beheer

Het beleid van Justid en het ingerichte beheer sluiten niet helemaal op elkaar aan. Voor onderdelen van het beheer is het beleid onvolledig of het bestaande beleid wordt niet (geheel) gevolgd. Dit hoeft niet opgelost te worden door het opstellen van omvangrijke beleidsdocumenten. Justid Opsporing kan er bij onderdelen van het beheer voor kiezen om de huidige inrichting tot beleid op te waarderen.
In het wijzigingsproces bij Justid Opsporing kan de risico-afweging en traceerbaarheid verbeteren door beslissingen in twee stappen te nemen.
Het toezicht op privacy en informatiebeveiliging van het VB zijn alleen in opzet geregeld. Er is geen toezicht op het voldoen aan de BIO en het voldoen aan de bepalingen over beveiliging in verwerkersafspraken.
Bij het proces dat Justid Opsporing heeft ingericht voor het afhandelen van wijzigingen, kan de rol van de Information Security Officer verduidelijkt worden.

# Context

## Het Verwijzingsportaal Bankgegevens

Doel van het Verwijzingsportaal Bankgegevens (VB) is het betrouwbaar, snel, veilig, juist, volledig, efficiënt en uniform opvragen van gegevens bij in Nederland gevestigde financiële dienstverleners door bevoegde autoriteiten.

Het VB ondersteunt twee typen bevragingen:
1. Opvragen van identificerende gegevens bij financiële dienstverleners;
2. Rekeningnummerverificatie.

*Opvragen van identificerende gegevens bij financiële dienstverleners*

Voordat de bevraging van een bank of een betaaldienstverlener via het VB mag plaatsvinden, moet de geautoriseerde opsporingsambtenaar (hierna bevrager) beschikken over een vordering die is opgesteld door de (hulp) officier van justitie of teamleider. Bevraging via het VB zonder vordering is niet toegestaan.

Een bevraging via het VB start met het invoeren van gegevens van de vordering, de periode waarover moet worden gezocht en de entiteit (een persoon of een onderneming).
Een bevrager kan de vraag via het VB afhankelijk van de zoekcriteria richten aan één of meerdere banken. Ook is het mogelijk om alle banken te bevragen.

Het VB zet de bevraging door naar de geselecteerde bank(en). Elke geselecteerde bank of betaaldienstverlener geeft geautomatiseerd de gevraagde gegevens uit de klantenadministratie terug aan het VB. Het VB zet de gegevens vervolgens door naar de bevrager. Als de bank of betaaldienstverlener na vergelijking van de gegevens in de bevraging en de klantenadministratie geen gegevens aantreft, wordt deze informatie aan de bevrager teruggegeven.

Het VB bewaart de ontvangen gegevens niet. Het VB bewaart wel metagegevens van uitgevoerde bevragingen die nodig zijn voor audit en logging van het gebruik van het VB. Deze metagegevens worden in het VB vijf jaar bewaard en daarna verwijderd.

*Rekeningnummerverificatie*

Naast het interactieve deel van het VB voor het opvragen van identificerende gegevens door een bevrager biedt het VB ook de mogelijkheid voor rekening-nummerverificatie. Hiervoor is een systeem van de Belastingdienst gekoppeld aan het VB om te verifiëren of een opgegeven rekening toebehoort aan een specifieke natuurlijk persoon.

## Wie mag het VB gebruiken?

In het besluit VB is bepaald dat de volgende bevoegde autoriteiten gebruik mogen maken van het VB voor het opvragen van gegevens:

1. Opsporingsambtenaren die werkzaam zijn bij de Nationale Politie, het openbaar ministerie, de Koninklijke Marechaussee, de Rijksrecherche, de Fiscale Inlichtingen- en Opsporingsdienst, de Inlichtingen- en Opsporingsdienst van de Nederlandse Voedsel- en Warenautoriteit, de directie Opsporing van de Inspectie Sociale Zaken en Werkgelegenheid of de Inlichtingen- en Opsporingsdienst van de Inspectie Leefomgeving en Transport;
2. De officier van justitie;
3. De Financial Intelligence Unit-Nederland;

4. De Belastingdienst (de inspecteur, de ontvanger en de Belastingdienst/ Toeslagen).

### Het beheer van het VB is belegd bij Justid

Het VB wordt beheerd door Justid, een agentschap van JenV. Justid voert de volgende beheertaken uit:

- Applicatiebeheer – het proces om software en databases te onderhouden en aan te passen aan nieuwe omstandigheden. Hieronder vallen het incidentbeheer, het wijzigingenbeheer en het beheer van toegangsrechten;
- Technisch beheer - het operationeel houden, onderhouden en vernieuwen van de technische infrastructuur (netwerken, apparatuur). Hieronder vallen de monitoring van de infrastructuur en de koppelingen met alle banken, de beveiliging van de infrastructuur en het beheer van alle technische componenten.

Bij Justid is het beheer belegd bij de afdeling Opsporing/Informatiepunt Bijzondere Opsporingsonderzoeken (hierna Justid Opsporing) in Den Haag.

Justid Opsporing neemt diensten af van drie IT-dienstverleners die onderdelen van de infrastructuur van het VB beheren:



### Voor wie is dit rapport?

Dit rapport is opgesteld voor de opdrachtgever voor het onderzoek, de plaatsvervangend directeur-generaal van DGO. Met dit rapport wordt DGO in staat gesteld om de Tweede Kamer te informeren over de resultaten van uitgevoerde audits.

# Leeswijzer

In hoofdstuk 1 gaan we in op alle onderdelen van het beheer van het VB waaraan Justid Opsporing aandacht heeft besteed.
Daarna zoomen we in hoofdstuk 2 in op vier bevindingen die direct de aandacht vragen van Justid Opsporing.
We sluiten de weergave van bevindingen af in hoofdstuk 3 met verbetermogelijkheden die wij zien in het beheer door Justid Opsporing.

Daarna volgt in hoofdstuk 4 een toelichting op het door ons uitgevoerde onderzoek.

In bijlage 1 is de reactie van Justid op het rapport opgenomen.

# 1 Justid Opsporing heeft veel aandacht besteed aan de inrichting van het beheer van het VB

## 1.1 VB is gefaseerd in gebruik genomen, openstaande punten na ingebruikname zijn afgehandeld

Het VB is gefaseerd in gebruik genomen. Er is gestart met een pilot met enkele banken en na verloop van tijd zijn alle banken aangesloten. De werkzaamheden voor Justid waren op dat moment nog niet afgerond, er waren nog openstaande punten. Justid Opsporing heeft daarvan een uitgebreide administratie bijgehouden. Daarin zien wij dat in 2021 alle openstaande punten van de invoering van het VB zijn afgehandeld. Daarmee is de invoering van het VB afgerond.

## 1.2 Het incidentproces voor het VB is georganiseerd

Justid Opsporing heeft het proces ingericht om incidenten rondom het VB af te handelen. Het incidentproces is beschreven, incidenten worden gedetailleerd vastgelegd en de tijdige afhandeling wordt bewaakt. Daarvoor zijn normen bepaald voor de tijd waarbinnen Justid Opsporing moet reageren op de melding van een incident en de tijd waarbinnen een incident hersteld moet zijn. Aan de communicatie met de melder van een incident wordt veel aandacht besteed.

Over aantallen incidenten en de afhandeling wordt maandelijks gerapporteerd aan het management van Justid Opsporing.

Wij hebben de afhandeling door Justid Opsporing geanalyseerd van een groot beveiligingsincident dat in 2021 wereldwijd bij een groot aantal organisaties opgetreden is[1]. Het incident is door het Nationaal Cyber Security Centrum (NCSC) geclassificeerd als ernstige kwetsbaarheid. Justid Opsporing heeft het incident binnen de afgesproken termijn afgehandeld.

## 1.3 Wijzigingen worden beheerst doorgevoerd

Justid Opsporing heeft een proces ingericht om wijzigingen aan het VB op een beheerste manier uit te voeren. Justid Opsporing gebruikt daarbij de methode Agile.

Wijzigingen worden gegroepeerd in zogenaamde sprints. Van ontwikkeling naar ingebruikname doorloopt iedere sprint een aantal stappen.
Bij wijzigingen waarbij het koppelvlak van het VB met bevragers en/of verstrekkers wijzigt, wordt door de projectgroep die de wijziging ontwikkelt een risico-afweging uitgevoerd. De goedkeuring van dergelijke wijzigingen vindt plaats in de coördinatiegroep/stuurgroep.
Justid Opsporing heeft een aantal voorzieningen om ongeautoriseerde wijzigingen te voorkomen of te detecteren. Zichtbaar is wie welke code heeft gewijzigd en er worden verschillende versies van code bewaard voor vergelijking. Alle wijzigingen doorlopen een reviewproces, waarbij een collega-ontwikkelaar de aangepaste code controleert.
Wijzigingen doorlopen ook een aantal testen voordat ze worden goedgekeurd en in gebruik genomen.

In ons onderzoek hebben wij het testtraject voorafgaand aan het in gebruik nemen van VB-versie 1.2 nader bekeken (de versie die op dit moment in gebruik is). In het

[1] Dit betreft een inc dent met Apache Log4j. Apache is een opensource webserver die veel wordt gebruikt door websites. Apache maakt gebruik van de tool Log4j om logbestanden aan te maken. In Log4j is een kwetsbaarheid gevonden waardoor wereldwijd veel organisaties een reparatie moesten uitvoeren. De reparatie bestond uit het installeren van een update waarmee de kwetsbaarheid kon worden opgelost.

testtraject is veel aandacht besteed aan het uitvoeren van verschillende testen om de correcte werking van VB versie 1.2 aan te tonen:

- Door een ketentest om de koppeling van het VB met alle aangesloten financiële dienstverleners te testen;
- Met gebruikersacceptatietesten waarin gebruikers van het VB testen of ze met het VB alle mogelijke varianten van bevragingen kunnen uitvoeren.

Een sterk onderdeel van de aanpak van VB versie 1.2 is de inzet van een kwaliteitsfunctionaris. Deze heeft in opdracht van DGO vastgesteld dat alle testen zijn uitgevoerd en heeft daarover gerapporteerd aan DGO.

## 1.4 Beheerprocessen zijn ingericht

Justid Opsporing heeft veel maatregelen getroffen om een ongestoorde werking van het VB te kunnen waarborgen. Daarbij is aandacht besteed aan diverse aspecten van het beheer die hieronder worden toegelicht.

- Justid Opsporing beschikt over een actueel overzicht van de voor het VB gebruikte configuratie d.w.z. de gebruikte hardware, besturingssystemen, gegevensopslag, programmatuur en tools voor het beheer.

- Justid Opsporing heeft maatregelen genomen om tijdig inzicht te verkrijgen in technische kwetsbaarheden. Justid voert daarvoor zelf scans uit en is aangesloten op de informatievoorziening van het NCSC.

- Justid Opsporing heeft met Niet openbaar op operationeel en tactisch niveau contact over het serviceniveau georganiseerd.

- Er zijn binnen Justid afspraken gemaakt over het beheer van de Justitie Berichten Service[2].

- Het beheer van accounts en toegangsrechten is geregeld. Dit betreft alleen het beheer van toegang voor beheerders. De toegang voor gebruikers van het VB wordt niet door Justid beheerd.

- Onderdelen van de logging en monitoring van het VB zijn beschreven. Informatiebeveiligingsincidenten en activiteiten van beheerders (inloggen, uitloggen, beheeractiviteiten, doorvoeren van wijzigingen) worden gelogd. We hebben vastgesteld dat montoring is ingericht voor delen van de configuratie.

- Bij een aantal relevante onderdelen van de infrastructuur, wachtwoorden, verbindingen en dataopslag, wordt versleuteling (encryptie) toegepast.

- Er is een handleiding opgesteld voor back-ups en er is een herstelplan bij een eventuele uitwijk. Voorzieningen voor calamiteiten zoals het maken van back-ups en een uitwijkomgeving zijn ingericht. Deze worden beperkt getest.

## 1.5 Het logboek van bevragingen via het VB is ingericht

Het VB bewaart in een logbestand informatie over alle uitgevoerde bevragingen. De lay-out van dat bestand is bepaald tijdens het ontwikkelproces. Justid geeft aan dat een juridische klankbordgroep betrokken is geweest bij het bepalen van de gegevens die per bevraging worden bewaard. Als uitgangspunt is gehanteerd dat er met het logbestand een audittrail is van uitgevoerde bevragingen.

Wij hebben onderzocht welke bewaartermijn wordt gehanteerd voor het logbestand. Gegevens over een bevraging behoren gedurende een termijn van vijf jaar te worden bewaard in het logbestand. Daarna moeten de gegevens gewist worden. Wij hebben vastgesteld dat de bewaartermijn ingesteld is op vijf jaar.

[2] Het VB maakt gebruik van de Justitie Berichten Service JUBES die wordt beheerd door de afdeling Verbindingen en Veiligheid van Justid.

# 2 Vier bevindingen vragen direct aandacht van Justid Opsporing

## 2.1 Er is te weinig zicht op de dienstverlening door IT-dienstverlener

Justid Opsporing neemt diensten af van de IT-dienstverleners Niet openbaar Niet openbaar (zie *Context - Het beheer van het VB is belegd bij Justid*). Justid heeft niet bepaald welke beveiligingsmaatregelen met welke IT-dienstverlener overeengekomen moeten zijn. Het contract met de Justitiële ICT Organisatie vermeldt dat de BIO van toepassing is. De contracten met Niet openbaar zijn minder specifiek over de beveiligingsmaatregelen die van toepassing zijn. Het passende beveiligingsniveau is in deze contracten niet beschreven. De beveiligingseisen bij de Niet openbaar zijn door de Niet openbaar zelf bepaald.

De drie IT-dienstverleners rapporteren niet periodiek aan Justid Opsporing over het geleverde serviceniveau, de getroffen beveiligingsmaatregelen en de mate waarin wordt voldaan aan de BIO. Het is de keuze van Justid Opsporing dat de IT-dienstverleners alleen rapporteren in het geval van incidenten.

Justid Opsporing heeft niet volledig in beeld welke toeleveranciers deze drie IT-dienstverlener hebben en welke afspraken door de drie IT-dienstverlener zijn gemaakt met hun toeleveranciers over te treffen beveiligingsmaatregelen.

Justid Opsporing voert geen periodieke (bijv. jaarlijkse) evaluatie uit van de dienstverlening door IT-dienstverleners waarbij wordt vastgesteld in hoeverre de IT-dienstverleners voldoen aan beveiligingseisen van Justid Opsporing.

## 2.2 De voorziening voor het detecteren van oneigenlijke toegang of oneigenlijk gebruik van het VB is niet af

Justid Opsporing heeft voor het VB een systeem voor Security Information & Event Management (SIEM) ingericht. Een SIEM is een voorziening waarmee continu informatie uit computersystemen wordt verzameld en geanalyseerd. Het doel hiervan is om verdachte gebeurtenissen op het gebied van informatieveiligheid te ontdekken. De SIEM die Justid Opsporing heeft ingericht, is in onze ogen niet af. Over de huidige voorziening hebben wij de volgende opmerkingen:

- De SIEM signaleert op dit moment twee gebeurtenissen die een indicatie kunnen zijn van afwijkend gebruik van toegangsrechten voor beheer en afwijkende wijziging van gegevens. Er ontbreekt een risico-inschatting op basis waarvan deze twee gebeurtenissen zijn geselecteerd.
- Er zijn (sinds 2020) openstaande punten rondom de SIEM die niet zijn opgepakt. Het gaat hierbij om:
    - De afhandeling van de signalen van de SIEM;
    - Afstemming over de gekozen instellingen van de SIEM met bij het VB betrokken partijen;
    - De koppeling van de SIEM aan andere systemen van Justid.
- In 2018 is in de stuurgroep VB toegezegd dat er een externe toetsing van de SIEM zou plaatsvinden. Deze toetsing is niet uitgevoerd.

## 2.3 Het is onzeker of voorzieningen voor calamiteiten volledig en tijdig herstel van het VB mogelijk maken

Het beheerteam heeft een aantal voorzieningen voor calamiteiten ingericht. Er wordt dagelijks een back-up gemaakt van de systeeminstellingen. Het logboek van de bevragingen (logfile) wordt elk uur gekopieerd en veilig gesteld en er is een uitwijkomgeving beschikbaar bij het uitvallen van het huidige VB.

De voorzieningen voor calamiteiten worden periodiek getest. Deze testen hebben een beperkte scope.

Er wordt niet getest of een reserve-kopie in zijn geheel teruggezet kan worden vanaf een back-up tape die wordt teruggehaald van de bewaarlocatie. Er wordt vervolgens niet getest of het terugzetten van de reserve-kopie vanaf een back-up tape een werkend VB oplevert.

Er wordt niet getest of het VB na installatie op de uitwijkomgeving in de volle breedte, met alle bevragers en alle banken, functioneert. Er wordt niet bepaald hoeveel tijd het volledige herstel kost en niet vastgesteld of de benodigde tijd voor herstel past bij de verwachtingen van DGO (een maximale hersteltijd van 48 uur). Daarmee is het onzeker of met de huidige voorzieningen, na een calamiteit tijdig een volledig werkend VB gerealiseerd kan worden.

## 2.4 Invoering van de BIO binnen Justid Opsporing staat nog aan het begin; het tijdspad voor invoering van de hele BIO is onduidelijk

Met de BIO is een set van maatregelen op het gebied van informatiebeveiliging samengesteld die van toepassing is voor de rijksoverheid. De BIO is ook van toepassing voor Justid.

Door het inrichten van het beheer van het VB heeft Justid Opsporing impliciet ook delen van de BIO ingevoerd. Een eenduidige relatie tussen de BIO en huidige inrichting van het beheer van het VB is daarbij niet gelegd.

Voor de invoering van de BIO onderscheidt Justid Opsporing 250 beheers-maatregelen. In maart 2022 is een plan van aanpak opgesteld waarin de aanpak wordt beschreven om de eerste 42 (van de 250 onderscheiden) BIO-maatregelen te implementeren. Dat houdt in dat de opzet van elke BIO-maatregel is bepaald en dat de werking (aantoonbaar) is vastgesteld.
Justid Opsporing gaf tijdens het onderzoek de volgende status weer van de uitvoering van het plan:

- 8 maatregelen zijn gereed;
- 14 maatregelen zijn in uitvoering.

Het tijdspad voor de invoering van alle BIO-maatregelen binnen Justid Opsporing is in het huidige plan niet uitgewerkt.

Wij hebben niet geanalyseerd wat de aanleiding is dat Justid Opsporing vier jaar na de vaststelling van de BIO bezig is met de opzet en werking van de eerste 42 (van 250 onderscheiden) BIO-maatregelen.

# 3 Wij zien verbetermogelijkheden voor onderdelen van het beheer

## 3.1 Beleid van Justid en praktische inrichting van het beheer sluiten niet altijd op elkaar aan

Justid of Justid Opsporing heeft voor een aantal aspecten van het beheer uitgangspunten (beleid) geformuleerd. In ons onderzoek hebben wij vastgesteld dat de relatie tussen het beleid en de praktische inrichting drie vormen kent:

1. Er is onvolledig beleid van Justid of Justid Opsporing, er ontbreken onderdelen of onderdelen zijn onduidelijk. We zien dit bij beleid voor accountbeheer, patchbeleid, monitoringactiviteiten en bewaartermijnen van logging-gegevens.
2. Er is beleid van Justid of Justid Opsporing, maar dat beleid wordt niet of niet geheel gevolgd. Hiervan is sprake binnen accountbeheer bij de rol van de leidinggevende bij het toekennen en beoordelen van accounts en speciale bevoegdheden. We zien dit ook bij onderdelen van het loggingbeleid: bij de keuze welke gebeurtenissen worden gelogd, de inhoud van logregels, de afscherming van loginformatie en controle van logging.
3. Er is beleid dat wordt gevolgd voor het VB. Dit heeft betrekking op het wachtwoordbeleid.

Onze suggestie is om beleid van Justid of Justid Opsporing en de praktische inrichting beter op elkaar aan te sluiten. Dat wil niet zeggen dat er omvangrijke beleidsdocumenten opgesteld moeten worden. Justid Opsporing kan ook vaststellen dat de huidige opzet en inrichting van onderdelen van het beheer voldoet en dat daarmee het beleid bepaald is.

## 3.2 Besluitvorming over wijzigingen in twee stappen kan de risico-afweging en traceerbaarheid verbeteren

De "grote" wijzigingen aan het VB doorlopen een goedkeuringsproces waarbij DGO betrokken is. Ons valt op dat er bij wijzigingen waarover Justid Opsporing zelf beslist (de "kleine" wijzigingen) op een informele manier besluitvorming plaatsvindt of plaatsgevonden heeft:

- Bij het doorvoeren van wijzigingen van configuratie-items in de CMDB is er geen goedkeuring door de verantwoordelijke teamleider.
- Vraag- & antwoordberichten werden in het VB tijdelijk opgeslagen. In de huidige versie van het VB (1.2) is deze tijdelijke opslag komen te vervallen. Het is onduidelijk hoe de besluitvorming hierover gegaan is. Er is geen formele besluitvorming terug te vinden over de verwijdering van de tijdelijke opslag.
- Voor wijzigingen die niet van invloed zijn op de koppelvlakken van het VB met bevragers en verstrekkers vindt de goedkeuring plaats door de Product Owner[3] van Justid Opsporing. Daarbij vindt geen zichtbare risico-afweging plaats.

Besluitvorming in twee stappen is bij de hier gegeven voorbeelden te overwegen:

1. Voorbereiding door de Product Owner of beheerder;
2. Akkoord geven door de manager van Justid Opsporing of de teamleider.

Dit kan de risico-afweging verbeteren en de traceerbaarheid vergroten zodat op een later moment zichtbaar is wie heeft er besloten, op basis van welke informatie.

## 3.3 Toezicht is in opzet geregeld maar beperkt ingericht

*Verantwoordelijkheden voor informatiebeveiliging zijn belegd*

[3] De Product Owner vertaalt de wensen van de eigenaar in de door een ontwikkelteam te ontwikkelen functionaliteit, bewaakt de voortgang van de ontwikkeling en de invoering van nieuwe funct onaliteit

Justid heeft het beleid voor informatiebeveiliging uitgewerkt in een Beveiligingsbeleidsplan. Voor Justid Opsporing is dit verder gedetailleerd uitgewerkt in een Integraal beveiligingsplan. In beide beleidsstukken is de verantwoordelijkheid voor het blijven voldoen aan geldende kaders voor informatiebeveiliging uitgewerkt.

Het toezicht op het voldoen aan de BIO is binnen Justid Opsporing belegd bij de Information Security Officer (ISO) die daarover verantwoording afgelegd aan de Chief Information Security Officer (CISO) van Justid.

Justid Opsporing geeft aan dat enkele onderdelen uit het Beveiligingsbeleidsplan niet zijn ingericht: interne audit en de jaarlijkse self-assessment BIO-maatregelen door alle afdelingen van Justid.

*Toezicht op informatiebeveiliging ontbreekt*

Er is voor het VB geen periodieke controle ingericht op naleving van het beleid over informatiebeveiliging en alle maatregelen die zijn opgenomen in de BIO.

*Verantwoordelijkheden voor privacy zijn in beeld*

De verantwoordelijkheden binnen Justid voor het opstellen en uitvoeren van het privacy-beleid zijn beschreven. Volgens het privacy-beleidskader is de privacy officer de interne toezichthouder en adviseur.

*Er is toezicht op de PIA, toezicht op verwerkersafspraken ontbreekt*

Volgens het privacy-beleid dient een Plan-Do-Check-Act-Cyclus (PDCA-cyclus) ingeregeld te worden voor o.a. Privacy Impact Assessments (PIA's) en verwerkersafspraken.

Justid heeft de PDCA-cyclus voor PIA's ingericht door voor elke nieuwe (risicovolle) verwerking een PIA uit te voeren, de PIA elke drie jaar te reviewen en een check te doen bij iedere grotere wijziging. De huidige PIA voor het VB is in 2018 opgesteld. De privacy-officer geeft aan dat de PIA die door het project VB2[4] is opgeleverd, wordt gebruikt voor de actualisatie van de PIA van Justid.

Voor verwerkersafspraken zien wij dat een PDCA-cyclus niet is ingericht. Dit leiden wij af uit de huidige verwerkersafspraken over het VB tussen Justid en de gebruikers van het VB. Daarin geeft de directeur van Justid aan:

1. dat verwerking plaats vindt op infrastructuur die voldoet aan de BIR[5] (de voorloper van de BIO);
2. dat toegang, verwerking en opslag plaatsvindt conform de maatregelen behorend bij het standaardniveau van de BIR;
3. dat Justid de verwerkingsverantwoordelijke voldoende zicht geeft in het geboden beveiligingsniveau en de overeengekomen getroffen beveiligingsmaatregelen.

Er wordt niet gecontroleerd of de bepalingen in de verwerkersafspraken nog voldoen en of deze bepalingen in verwerkersafspraken door Justid kunnen worden nagekomen. Gezien de stand van zaken van de invoering van de BIO binnen Justid Opsporing (zie *2.4 Invoering van de BIO binnen Justid Opsporing staat nog aan het begin; het tijdspad voor invoering van de hele BIO is onduidelijk*) is dat laatste niet het geval.

[4] Project VB2 ontwikkelt een nieuwe versie van het VB waarmee ook saldo- en transactie-gegevens kunnen worden opgevraagd.

[5] Baseline Informatiebeveiliging Rijksdienst; op 1-1-2019 vervangen door de BIO.

### 3.4 De rol van de ISO in het wijzigingstraject kan verduidelijkt worden

Uit interviews met medewerkers van Justid Opsporing blijkt dat er onduidelijkheid is over de rol die de ISO heeft binnen het wijzigingsproces. Dit heeft betrekking op twee aspecten:

- Door de ISO beoordelen of testplannen voldoende ingaan op beveiliging;
- Goedkeuring door de ISO binnen het wijzigingsproces.

# 4 Verantwoording onderzoek

## 4.1 Werkzaamheden en afbakening

*Werkzaamheden*
De opdrachtbevestiging voor het onderzoek VB (d.d. 5 oktober 2022; kenmerk 2022-0000244988) is op 12 oktober 2022 goedgekeurd door de plaatsvervangend directeur-generaal van DGO, drs. M.C. van Tuyll.

De opdracht bestaat uit twee deelonderzoeken, een deelonderzoek bij Justid en een deelonderzoek bij de FIOD. Dit rapport focust zich op Justid en geeft antwoord op de onderzoeksvraag *Welke bevindingen heeft de ADR over het door Justid uitgevoerde beheer van het VB?*

In het deelonderzoek Justid zijn de volgende onderdelen van het beheer van het VB onderzocht:
1. Governance van privacy en informatiebeveiliging;
2. Contractmanagement;
3. Incidentbeheer;
4. Ingebruikname;
5. Wijzigingenbeheer;
6. Logische toegangsbeveiliging;
7. Beveiliging van IT-infrastructuur en data;
8. Operationeel beheer: Logging en monitoring;
9. Back-up, restore en uitwijk;
10. Opschonen en vernietigen.

In het onderzoek is gebruik gemaakt van het Toetsingskader Beheer Verwijzingsportaal Banken - 1.0 - 24-8-2022. Daarin zijn voor bovenstaande onderdelen in totaal 43 te toetsen beheersmaatregelen opgenomen.

Het onderzoek is uitgevoerd in de periode oktober 2022 – januari 2023. Tijdens het onderzoek is regelmatig afgestemd met contactpersonen bij DGO en Justid.

Het onderzoek is gestart met een analyse van de documentatie die per onderzochte beheersmaatregel is aangeleverd. Vervolgens zijn interviews gehouden met medewerkers van Justid die ons per onderzochte beheersmaatregel van relevante informatie konden voorzien. Daarnaast zijn er waarnemingen gedaan van instellingen in het VB en waarnemingen in de systemen die Justid Opsporing gebruikt bij het beheer van het VB.

De hoofdlijnen van de bevindingen zijn op 5 december 2022 afgestemd met de manager van Justid Opsporing.
De resultaten van documentanalyse, interviews en waarnemingen en een samenvatting van de bevindingen zijn per getoetste beheersmaatregel vastgelegd in een toetsingsformulier. De toetsingsformulieren van alle getoetste beheers-maatregelen zijn op 8 december 2022 bij Justid teruggelegd voor een reactie. Waar nodig is daarna aanvullende informatie verwerkt.

Het concept rapport is op 8 februari 2023 teruggelegd bij de manager van Justid Opsporing voor een reactie. De manager van Justid Opsporing heeft op 1 maart 2023 een reactie gegeven die is besproken in een overleg tussen Justid Opsporing

en ADR op 9 maart 2023. In dat overleg is de afhandeling van de gemaakte opmerkingen afgestemd.
Het concept rapport is op 15 maart 2023 opgeleverd aan DGO voor een reactie. DGO heeft op 30 maart 2023 gereageerd. DGO en ADR hebben op 12 april 2023 de verwerking van opmerkingen van DGO over het rapport afgestemd.

*Afbakening*
Bij het deelonderzoek Justid is de volgende afbakening gehanteerd:
- De hierboven aangegeven beheerprocessen zijn onderzocht voor zover deze betrekking hebben op de door Justid Opsporing beheerde infrastructuur. Die is weergegeven op een door Justid Opsporing opgestelde infraplaat die is afgestemd tussen Justid Opsporing en de ADR;
- Justid Opsporing heeft beheerwerkzaamheden belegd bij drie IT-dienstverleners;Niet openbaar De uitbestede beheerwerkzaamheden vallen buiten de scope van dit onderzoek. De contracten met deze partijen vallen binnen de scope van het onderzoek en zijn meegenomen bij het onderdeel Contractmanagement;
- Justid - Niet openbaar beheert de Justitiële Berichten Service (JUBES) en levert diensten aan afnemers (waaronder Justid Opsporing) conform het basisniveau dienstverlening. De afspraken tussen Justid Opsporing en Justid Niet openbaa zijn meegenomen bij het onderdeel Contractmanagement;
- Justid maakt gebruik van diensten die worden geleverd door Niet openbaar De contracten met Niet openbaar zijn afgesloten door de Directie Informatievoorziening en Inkoop van J&V. Justid is hier niet verantwoordelijk voor. Deze contracten vallen buiten de scope van het onderzoek;
- Het toetsen van de opzet en het bestaan van beheersmaatregelen binnen deze tien beheerprocessen is een momentopname van de situatie op 1 oktober 2022. Daarmee kan geen uitspraak worden gedaan over de werking van beheers-maatregelen in een periode.

## 4.2 Gehanteerde standaard

Deze opdracht is uitgevoerd in overeenstemming met de Internationale Standaarden voor de Beroepsuitoefening van Internal Auditing. Dit onderzoek verschaft geen zekerheid in de vorm van een oordeel of conclusie, omdat het een onderzoeksopdracht betreft en geen controle-, beoordelings- of andere assurance-opdracht.

De opdracht is uitgevoerd conform de algemene uitgangspunten voor de uitoefening van de interne auditfunctie bij de rijksdienst. Daarbij hoort ook een stelsel van kwaliteitsborging. Een onderdeel daarvan is dat er een onafhankelijke kwaliteitstoetsing heeft plaatsgevonden op deze onderzoeksopdracht.

## 4.3 Verspreiding rapport

De opdrachtgever, de plaatsvervangend directeur-generaal van DGO, is eigenaar van dit rapport. Dit rapport is primair bestemd voor de opdrachtgever met wie wij deze opdracht zijn overeengekomen. Hoewel het rapport de context van het onderzoek zo goed mogelijk probeert te beschrijven, is het mogelijk dat iemand die de context niet (volledig) kent, de uitkomsten anders interpreteert dan bedoeld.

De ADR is de interne auditdienst van het Rijk. Dit rapport is primair bestemd voor de opdrachtgever met wie wij deze opdracht zijn overeengekomen. Voor openbaarmaking door het opdrachtgevende ministerie van door de ADR aan dit ministerie uitgebrachte rapporten gelden de voorschriften uit de Wet open overheid. De minister van Financiën stuurt elk halfjaar een overzicht van door de ADR uitgebrachte rapporten naar de Tweede Kamer.

# 5 Ondertekening

Den Haag, 18 april 2023

w/g

Projectleider
Auditdienst Rijk

# Bijlage 1: Reactie Justid

Justitiële Informatiedienst
*Ministerie van Justitie en Veiligheid*

> Retouradres Postbus 337 7600 AH Almelo

**Justitiële Informatiedienst**
Burgemeester Raveslootsingel 2
7607 GK Almelo
Postbus 337
7600 AH Almelo
www.justid.nl

**Contactpersoon**
Justid Opsporing

**Ons kenmerk**
Managementreactie Justid Opsporing 2023

*Bij beantwoording de datum en ons kenmerk vermelden. Wilt u slechts één zaak in uw brief behandelen.*

Datum 12 april 2023
Onderwerp Managementreactie Justid Opsporing auditrapport VB

Geachte heer/mevrouw,

De afdeling Opsporing van de Justitiële Informatiedienst (Justid) voert sinds september 2019 het beheer over het Verwijzingsportaal Bankgegevens (VB).

De Auditdienst Rijk (ADR) heeft in opdracht van DG Ondermijning (DGO) een onderzoek uitgevoerd naar het beheer van het VB door Justid Opsporing, met als peildatum oktober 2022.

Justid Opsporing heeft kennisgenomen van het rapport 'Onderzoeksrapport Beheer Verwijzingsportaal Bankgegevens 15 maart 2023'.

Justid Opsporing herkent zich in de conclusie van het audit onderzoek die ADR heeft uitgevoerd. Dat geldt zowel voor dat Justid Opsporing veel aandacht en zorg besteedt aan de algemene inrichting van het beheer van het VB; denk hierbij aan een georganiseerd incidentproces dat Justid Opsporing in staat stelt om incidenten tijdig af te handelen, het wijzigingsproces dat zodanig is ingericht waardoor wijzigingen op een beheerste wijze worden uitgevoerd en zijn er een groot aantal maatregelen getroffen om een ongestoorde werking van het VB te kunnen waarborgen. Maar er zijn ook verbetermogelijkheden die aandacht vragen van Justid Opsporing. Dit betreft de volgende vier bevindingen:

1. **Er is te weinig zicht op de dienstverlening door IT-dienstverlener**
   Justid Opsporing maakt bij het beheer van het VB gebruik van diensten van drie IT-dienstverleners. Op dit moment is er te weinig zicht op de beheertaken die door de IT-dienstverleners worden uitgevoerd. Er ontbreken afspraken over de beveiligingsmaatregelen die door de IT-dienstverleners moeten worden getroffen en het toezicht op beveiligingsmaatregelen is niet ingericht.

*Reactie Justid Opsporing*

De IT-dienstverleners zijn gehouden aan overheidsbeleid op beveiliging (i.c. BIO). Dit is opgenomen in de dienstverleningsafspraken. De afspraken met de IT-dienstverleners bieden Justid de mogelijkheid rapportages uit te vragen en mee te werken aan audits op de naleving. Voor de evaluatie en mogelijke aanpassing van de afspraken zal een jaarlijks evaluatiemoment ingepland worden.

De configuratie van VB bevindt zich in de rekencentra in afgesloten segmenten die zonder begeleiding niet toegankelijk zijn voor beheerders van de IT-dienstverleners. Het dataverkeer is volledig versleuteld. De IT-dienstverleners hebben geen toegang tot de data of het systeem.

2. **De voorziening voor het detecteren van oneigenlijke toegang of oneigenlijk gebruik van het VB is niet af**

De voorziening om verdachte gebeurtenissen te signaleren is nog niet af. De onderbouwing voor gemaakte keuzes ontbreekt, geplande activiteiten voor de verdere inrichting staan nog open en de toegezegde externe toetsing is niet uitgevoerd.

*Reactie Justid Opsporing*

De voorziening is continu in ontwikkeling en zal de komende tijd door Justid Opsporing verder worden geprofessionaliseerd. Op de planning heeft Justid Opsporing 7 taken geplaatst op basis van BBN3-maatregelen en bedoeld om bedreigingen van API's te ondervangen.

3. **Het is onzeker of voorzieningen voor calamiteiten volledig en tijdig herstel van het VB mogelijk maken**

Justid Opsporing voert beperkt testen uit van de voorzieningen voor calamiteiten. De uitgevoerde testen geven geen garantie dat het VB na een calamiteit tijdig in de volle breedte beschikbaar is.

*Reactie Justid Opsporing*

Een uitwijktest is onderdeel geweest van de oplevering van de uitwijkomgeving aan de beheerorganisatie. De uitwijktest wordt jaarlijks herhaalt en is in 2022 succesvol getest. De uitwijktest nam in totaal minder dan 2 dagen in beslag binnen de gemaakte afspraken met de opdrachtgever.
De connectie met de financiële dienstverleners is belegd bij Justid Niet openbaar Niet openbaar en niet meegenomen met de uitwijktest van Justid Opsporing. Justid Niet openb. heeft een dubbel uitgevoerd platform. Beide platformen verwerken actief berichten. Een uitwijk test wordt periodiek uitgevoerd bij software patches en updates.

In de uitwijktest 2023 zullen we aandacht gaan besteden aan de aanbevelingen van ADR en een uitgebreider verslag maken van de keuzes en uitgevoerde acties.

4. **Invoering van de BIO binnen Justid Opsporing staat nog aan het begin; het tijdspad voor invoering van de hele BIO is onduidelijk**
Het is onduidelijk wanneer Justid Opsporing de invoering van de BIO voor het VB volledig heeft afgerond.

*Reactie Justid Opsporing*
Er is een nieuw Plan van Aanpak (PvA BIO) opgesteld door Afdeling Justid Opsporing en vastgesteld door de manager Justid Opsporing op 21 maart 2023. Van de 42 maatregelen in scope zijn er nu 9 gereed. In het PvA BIO is een planning opgenomen voor de 33 resterende maatregelen die naar verwachting dit jaar doorgevoerd zijn.

**Opvolging bevindingen**
Justid Opsporing heeft op basis van deze audit een bevindingen- en aanbevelingenmatrix opgesteld met de intentie om deze binnen een redelijke termijn op te volgen. Verder is er binnen Justid Opsporing een audit werkgroep waarin deze bevindingen- en aanbevelingenmatrix is opgenomen om de opvolging hiervan te stimuleren. De voortgang zal periodiek worden gerapporteerd aan de manager Justid Opsporing en uiteraard wordt ook de opdrachtgever DGO op de hoogte gehouden. Wij danken u wederom voor het audit onderzoek. Uw bevindingen en aanbevelingen hebben onze volledige aandacht.

Met vriendelijke groet,

Manager Opsporing

**Auditdienst Rijk**
Postbus 20201
2500 EE Den Haag
(070) 342 77 00