Auditdienst Rijk
Ministerie van Financiën

> Retouradres Postbus 20201 2500 EE Den Haag

Belastingdienst/ FIOD
Algemeen Directeur - [redacted]
Croeselaan 14
3521 CA Utrecht

[redacted]@belastingdienst.nl

Auditdienst Rijk

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

Inlichtingen
[redacted]

T [redacted]
[redacted]@minfin.nl
www.minfin.nl

Ons kenmerk
2022-0000043986

Uw brief (kenmerk)

Bijlagen
1

Datum	15 februari 2022
Betreft	Onderzoeksrapport Audit Wet Politiegegevens FIOD

Bijgaand doe ik u het onderzoeksrapport "Audit wet politiegegevens FIOD" met kenmerk 2022-0000044306 toekomen.

De Managementreactie is als bijlage toegevoegd aan het rapport.

Als Auditdienst Rijk hechten wij veel waarde aan opdrachtgevers tevredenheid. Daarom zijn wij benieuwd hoe u de toegevoegde waarde van het onderzoek en de betrokkenheid van het projectteam heeft ervaren middels onderstaande link naar een korte vragenlijst. Het invullen duurt circa twee minuten. Uw mening stellen wij zeer op prijs en zullen die vertrouwelijk behandelen. Onze dank dat u daar de tijd voor wil nemen.

Naar de vragenlijst

Mocht het klikken niet werken dan kan u deze link kopiëren naar uw internetbrowser:
https://www.adronderzoek.nl/index.php/162795?lang=nl

Met vriendelijke groeten,

[redacted]
Accountdirecteur Fin/EZK/LNV Auditdienst Rijk

Auditdienst Rijk
Ministerie van Financiën

Assurancerapport
Wet Politiegegevens FIOD

Definitief

Colofon

Titel	Wet Politiegegevens FIOD
Uitgebracht aan	[redacted] algemeen directeur FIOD
Datum	09-02-2022
Kenmerk	2022-0000044306

Inlichtingen
Auditdienst Rijk
[redacted]

Inhoud

Aanleiding opdracht

De Fiscale Inlichtingen- en Opsporingsdienst (FIOD) is de opsporingsdienst van de Belastingdienst. De organisatie richt zich specifiek op het opsporen en bestrijden van fiscale en financiële fraude, waaronder witwassen en corruptie en zet zich in voor een financieel veilig Nederland. De FIOD is naast ISZW-DO, NVWA-IOD en ILT-IOD, een van de vier bijzondere opsporingsdiensten die Nederland telt.

De Wet Politiegegevens (Wpg) is van toepassing verklaard op de verwerking van persoonsgegevens die in het kader van de politietaak worden verwerkt. De Wpg is, middels het Besluit politiegegevens bijzondere opsporingsdiensten, ook van toepassing op de verwerking van politiegegevens door de FIOD.

De Wpg schrijft voor dat de verantwoordelijke de naleving van de regels gesteld in de Wpg doet controleren door middel van een audit. Conform artikel 6:5 van het Besluit Politiegegevens (Bpg) dient deze privacy audit eenmaal in de vier jaar te worden uitgevoerd. De audit heeft betrekking op de wijze waarop het verwerken van politiegegevens is georganiseerd, de maatregelen en procedures die daarop van toepassing zijn, de controle en toezicht en de werking van deze maatregelen en procedures[1].

Door de FIOD is aan de Auditdienst Rijk (ADR) gevraagd de audit over de periode 2016 – 2019 uit te voeren.

Deze assurance-opdracht is door de Auditdienst Rijk (ADR) uitgevoerd in opdracht van , algemeen directeur FIOD.

Doel onderzoek

Het doel van dit assurance-onderzoek is om een beperkte mate van zekerheid te geven of aan de bepalingen van de wet op adequate wijze uitvoering is gegeven[2]. Op basis van dit onderzoek geeft de ADR een oordeel over:

a. de opzet en het bestaan van maatregelen en procedures die in de borging van de wettelijke eisen moeten voorzien;
b. de werking van de getroffen maatregelen en procedures.

Concreet betekent dit het beantwoorden van de vraag of in voldoende mate is geborgd dat voldaan wordt aan wetsartikelen van de Wpg die betrekking hebben op de hoofdgebieden:

- Algemene bepalingen (art. 3-7);
- Verwerking van politiegegevens (art. 8-15);
- Verstrekking van politiegegevens (art. 16-24);
- Rechten van betrokkenen (art. 25-31);
- Controle en toezicht (art. 32-34, art. 36).

Afbakening

De privacy audit heeft betrekking op de artikelen van de Wpg die van toepassing[3] zijn op de FIOD bij de verwerking[4] van politiegegevens in het kader van uitvoering van zijn wettelijke taak, zoals vastgelegd in artikel 3 Wet op de BOD'en. Het onderzoek richt zich op de beheersingsmaatregelen in de processen en de systemen

[1] Besluit Politiegegevens, artikel 6:5, lid 2.
[2] Zie ook Regeling periodieke audit politiegegevens
[3] Zie Besluit politiegegevens bijzondere opsporingsdiensten.
4 Elke bewerking of elk geheel van bewerkingen met betrekking tot politiegegevens of een geheel van politiegegevens, al dan niet uitgevoerd op geautomatiseerde wijze, zoals het verzamelen, vastleggen, ordenen, structureren, opslaan, bijwerken of wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiden of op andere wijze ter beschikking stellen, samenbrengen, met elkaar in verband brengen, afschermen of vernietigen van politiegegevens.

die gebruikt worden bij de uitvoering van opsporingsonderzoeken en de vastlegging van persoonsgegevens hierbij.

De beoordeling van de opzet, bestaan en werking omvat de maatregelen en procedures die in de borging van de wettelijke eisen uit hoofde van de Wpg moeten voorzien. Het bestaan is beoordeeld, voor zover mogelijk[5], op de procedures, werkwijze en vastleggingen met als peildatum 31 december 2019. De werking van procedures en maatregelen is, voor zover mogelijk, beoordeeld over de periode 01-01-2019 tot en met 31-12-2019. De werking van de controle en toezicht (art. 32-34) is, voor zover mogelijk, beoordeeld over de periode 1-1-2016 tot en met 31-12-2019. Dit betreft bijvoorbeeld de uitvoering van interne audits en de toezichtswerkzaamheden (inclusief opstellen jaarverslag) van de privacyfunctionaris.

Onafhankelijkheid en kwaliteitsbeheersing

Wij hebben de vereisten van het Reglement Gedragscode ('Code of Ethics') van de Nederlandse Orde van Register EDP-Auditors (NOREA) nageleefd, welke is gebaseerd op de fundamentele beginselen van integriteit, objectiviteit, deskundigheid en zorgvuldigheid, geheimhouding en professioneel gedrag.
Wij hebben de vereisten uit het Handboek Auditing Rijksoverheid (HARo) nageleefd, inclusief de daarin vastgelegd systeem van kwaliteitscontrole.

Deze opdracht is uitgevoerd volgens de Richtlijn voor assurance-opdrachten door IT-auditors (NOREA Richtlijn 3000D). Een assurance-opdracht om te rapporteren over de opzet, het bestaan en de werking van beheersmaatregelen omvat het uitvoeren van werkzaamheden ter verkrijging van assurance-informatie. Deze opdracht is gericht op het verkrijgen van een beperkte mate van zekerheid.

Leeswijzer

In het volgende hoofdstuk is de hoofdboodschap (oordeel) van dit onderzoek opgenomen. Tevens is een totaaloverzicht opgenomen van de bevindingen en geconstateerde restrisico's. In het overzicht tevens opgenomen het paragraafnummer van de onderbouwing zoals uitgewerkt in hoofdstuk 1.

In hoofdstuk 1 zijn de algemene bevindingen opgenomen. In hoofdstuk 2 zijn bevindingen opgenomen met betrekking tot de implementatie van de per 01-01-2019 ingegaan nieuwe wetsartikelen van de Wpg. In hoofdstuk 3 zijn enkele aanbevelingen opgenomen ter verbetering van de naleving. Hoofdstuk 4 en 5 betreffen de verantwoording van het onderzoek en de ondertekening van het rapport. In de bijlage is de managementreactie en de legenda van dit onderzoek opgenomen.

5 Zie 6.1 voor mogelijke beperkingen die opgeleverd worden voor het onderzoek. Daarnaast is het mogelijk dat niet alle situaties zich voordoen in de selectie, bijvoorbeeld het verwerken van bijzondere gegevens.

Stelsel van beheersmaatregelen beter geborgd ten opzichte van vorige controle, enkele verbeteracties nog in uitvoering

Conclusie met beperking
Wij hebben bij de FIOD onderzocht of aan de bepalingen van de Wet politiegegevens op adequate wijze uitvoering is gegeven. Op grond van onze werkzaamheden en de verkregen informatie is ons niets gebleken op grond waarvan wij zouden moeten concluderen dat het stelsel van maatregelen en procedures in alle van materieel belang zijnde aspecten niet effectief is in opzet, bestaan en werking. Dit *uitgezonderd* de aspecten die hierna zijn beschreven in paragraaf 'De basis voor de conclusie met beperking'.

Ons oordeel is gevormd op basis van de aangelegenheden die in dit assurance-rapport uiteengezet zijn. Het hierbij gehanteerde normenkader, gebaseerd op de artikelen in de wet, omvat de door de FIOD te nemen maatregelen. De specifieke, getoetste beheersingsmaatregelen en de aard en resultaten van die toetsingen zijn opgenomen in Tabel 1 – overzicht conclusie per norm en hoofdstuk 1 waarin een beschrijving van de bevindingen is opgenomen.

De basis voor de conclusie met beperking
Wij hebben vastgesteld dat een aantal maatregelen niet (volledig) opgezet, bestaan en/of effectief werken. Voor een overzicht van de afwijkingen wordt verwezen naar Tabel 1: Overzicht conclusie per norm (oranje of rood in tabel 1). Voor de volledigheid zijn de onderwerpen die afdoende zijn opgezet, geïmplementeerd en effectief werken ook vermeld (groen in tabel 1).

Wel is gebleken dat het volledig kunnen voldoen aan de Wpg eisen mede afhankelijk is van maatregelen die buiten de FIOD dienen te worden genomen. Tekortkomingen op deze vlakken hebben mede geleid tot het geformuleerde oordeel.

In paragrafen 1.1 tot en met 1.7 van hoofdstuk 1 hebben wij een samenvatting weergegeven van de belangrijkste bevindingen.

De externe Wpg audit vindt plaats in een vierjaarlijkse cyclus. De controleperiode voor dit assurance onderzoek is 2016 t/m 2019. De werking van procedures en maatregelen is, voor zover mogelijk, beoordeeld over de periode 01-01-2019 tot en met 31-12-2019. Uitvoering van dit onderzoek is gestart in 2020, maar vanwege COVID-19 moest het onderzoek tijdelijk worden uitgesteld. Uit ons onderzoek blijkt dat de FIOD in en na de controleperiode verbetermaatregelen heeft geïmplementeerd op basis van, onder andere, uitgevoerde interne audits. Dit betreft bijvoorbeeld het opstellen van een procedure voor samenwerkingsverbanden, het verder implementeren van risicomanagement en verbeteringen op informatiebeveiliging.

Scope onderzoek
Het onderzoek richt zich alleen op de procedures en maatregelen die de FIOD moet treffen voor naleving van de Wpg-eisen. De ADR heeft geen onderzoek verricht naar door derden aan de FIOD geleverde faciliteiten, voor zover de verantwoordelijkheid is belegd bij een andere overheidsorganisatie dan de FIOD. In dergelijke gevallen is wel gekeken naar de gemaakte afspraken tussen de partijen en de regie vanuit de FIOD gericht op de realisatie van de afspraken.

Inherente beperkingen onderzoek
De conclusie is verder onderworpen aan de inherente beperkingen die in paragraaf 6.1 van dit assurance-rapport zijn genoemd. Ons oordeel is gevormd op basis van de bevindingen die in deze rapportage zijn opgenomen. Het hierbij gehanteerde normenkader, gebaseerd op de artikelen in de wet, omvat de door de FIOD te nemen maatregelen.

Zoals eerder is aangegeven is het onderzoek oorspronkelijk opgestart begin 2020. Omdat het onderzoek deels op locatie moest worden uitgevoerd is het onderzoek uitgesteld vanwege COVID-19. In september 2020 is het onderzoek wederom opgestart en vanwege de nieuwe lock-down weer uitgesteld. In overleg met de algemeen directeur FIOD is het onderzoek begin 2021 weer opgestart. Hierbij zijn afspraken gemaakt met betrekking tot de werkzaamheden op locatie om het onderzoek zo veilig mogelijk uit te voeren. Een van de afspraken was het beperken van de interviews en waarnemingen op locatie tot het hoogstnoodzakelijk om een assurance onderzoek uit te voeren. In deze rapportage wordt daarom een beperkte mate van zekerheid gegeven. De werkzaamheden die bij een opdracht met een beperkte mate van zekerheid zijn uitgevoerd zijn geringer in omvang dan voor opdrachten tot het verkrijgen van een redelijke mate van zekerheid. Wij vinden dat de door ons verkregen assurance informatie voldoende en geschikt is als basis voor ons oordeel.

Opstellen verbeterrapport en hercontrole
De verwerkingsverantwoordelijke is, op grond van artikel 4 lid 1 van de Regeling periodieke audit politiegegevens, verplicht binnen drie maanden een verbeterrapport op te stellen waarin de maatregelen worden beschreven die getroffen zijn ter verbetering van de in de privacy audit geconstateerde tekortkomingen. Op grond van artikel 4 lid 3 kan de hercontrole door de interne auditors worden uitgevoerd.

Tabel 1: Overzicht conclusie per norm[6]

In de tabel hierna is per norm uit het gebruikte normenkader het oordeel per opzet, bestaan en werking opgenomen. De afweging is gemaakt op basis van de detailbevindingen die zijn afgestemd met de FIOD. Daarnaast is de inschatting van het restrisico opgenomen indien niet of deels is voldaan aan de norm. Zie bijlage 2 voor de legenda.

Nr. Norm	Nr. §	Onderwerp	Norm	Opzet	Bestaan	Werking	Restrisico L/M/H[7]
1	1.1.1	**Doelbinding**	Politiegegevens worden alleen verwerkt als dat nodig is voor de in de wet genoemde doeleinden. Geborgd is dat bij het verwerken van politiegegevens altijd sprake is van doelbinding en dat de gegevens niet op een met die doeleinden onverenigbare wijze worden verwerkt.				-
2	1.1.2	**Noodzakelijkheid en rechtmatigheid**	De verzameling en verwerking van politiegegevens is toegespitst op een gespecificeerd doel met een wettelijke grondslag. Er wordt geborgd dat de persoonsgegevens daartoe toereikend, ter zake dienend en beperkt zijn tot wat noodzakelijk is (niet bovenmatig) en dat de herkomst van gegevens voor artikel 9, 10 en 12 verwerkingen wordt vermeld.				**L**
3	1.1.2	**Juistheid en volledigheid**	De verwerkingsverantwoordelijke heeft controles op de kwaliteit ingericht ten behoeve van de borging van de juistheid en nauwkeurigheid van persoonsgegevens.				**M**
4	1.1.3	**Bijzondere categorieën van persoonsgegevens**	Er vindt geen verwerking van bijzondere categorieën van politiegegevens, tenzij: - Dat nodig is voor het doel van de verwerking. - In aanvulling is op de verwerking van andere politiegegevens betreffende de persoon - De gegevens afdoende zijn beveiligd.				**L**
7	1.1.4	**Autorisaties: aanwijzen functionarissen**	Er is een actueel lijst van, door de verantwoordelijke aangewezen, bevoegde functionarissen.				-
9	1.1.5	**Reikwijdte**	De verwerkings-verantwoordelijke heeft verwerkingen van politiegegevens binnen de organisatie geïdentificeerd en gedocumenteerd.				**L**
10	1.1.6	**Gegevensbescherming door beveiliging**	Er is (aantoonbaar) een risicoanalyse uitgevoerd waaruit het risiconiveau blijkt en identificeert, evalueert en mitigeert systematisch en periodiek factoren die het beschermen van politiegegevens tegen ongeoorloofde of onrechtmatige verwerking en tegen opzettelijk verlies, vernietiging of beschadiging in gevaar brengen en past de maatregelen hierop aan.				**M**
	1.1.7		De organisatie heeft gegevensbeschermingsbeleid en procedures ontwikkeld en vastgesteld. De verwerkingsverantwoordelijke heeft de maatregelen die nodig zijn om het risico te beperken (passende technische en organisatorische maatregelen) aantoonbaar geïmplementeerd.				**M**
11	1.1.8	**Verwerkers en verwerkersovereenkomst**	Met verwerkers zijn de taken en afspraken schriftelijk vastgesteld en vastgelegd in een (toereikende) overeenkomst of andere rechtshandeling.				**M**
			De verwerker stelt de verwerkingsverantwoordelijke alle informatie ter beschikking die nodig is om aantoonbaar te maken dat aan de verplichtingen in de verwerkersovereenkomst worden nageleefd.				

[6] Zie legenda in bijlage 2
[7] Laag, Middel of Hoog restrisico

Nr. Norm	Nr. §	Onderwerp	Norm	Opzet	Bestaan	Werking	Restrisico L/M/H[8]
12	1.1.9	**Geheimhoudingsplicht**	Er is geborgd dat de ambtenaar van politie of de persoon aan wie politiegegevens ter beschikking zijn gesteld formeel bekend is met de plicht tot geheimhouding en de consequenties bij schending van deze plicht.				-
16	1.1.10	**Autorisaties en Toegang tot politiegegevens**	Er is een systeem van autorisaties dat voldoet aan de vereisten van zorgvuldigheid en evenredigheid. Dit houdt in dat: De verantwoordelijke heeft die personen die vanuit hun functie en de wet toegang mogen hebben tot bepaalde politiegegevens geautoriseerd voor alleen die gegevens (need-to-know). (Inclusief voor toezicht en controle, en technische werkzaamheden)				-
	1.1.11		Er is een proces voor het toewijzen, wijzigen en intrekken van autorisaties ten behoeve van de toegang tot politiegegevens.				**M**
	1.1.12		Er vindt periodiek controle plaats van de autorisaties.				
17	1.2.1	**Uitvoering van de dagelijkse politietaak**	Geborgd is dat art. 8 politiegegevens één jaar na de datum van de eerste verwerking zodanig worden opgeslagen (achter een schot worden geplaatst) dat ze alleen nog beschikbaar komen voor verdere verwerking op basis van de vergelijking van gegevens (hit-no-hit basis).				-
18	1.2.2	**Geautomatiseerd vergelijken en in combinatie zoeken**	Geborgd is dat gegevens alleen geautomatiseerd worden vergeleken met andere politiegegevens of met andere dan politiegegevens binnen de richtlijnen gesteld in art. 11.				**M**
			Geborgd is dat gegevens alleen in combinatie met elkaar worden verwerkt binnen de richtlijnen gesteld in art. 11.4.				
			Er is geborgd dat de ambtenaren die geautoriseerde zijn voor het geautomatiseerd vergelijken en in combinatie zoeken over voldoende kennis en vaardigheden beschikken.				
19	1.2.3	**Ondersteunende taken**	Geborgd is dat voor de verwerkingen bedoeld in art. 13.1, 13.2 en 13.2 Wpg, van tevoren is voldaan de schriftelijke vereisten (13.4 Wpg en 6:2 Bpg).				**M**
20	1.2.4	**Ter Beschikking stellen (voor verdere verwerking)**	Geborgd is dat de verdere verwerking van artikel 9 en 10 gegevens alleen plaats vindt na toestemming van de daartoe bevoegde functionaris.				-
			Geborgd is dat de ter beschikking stellen van politiegegevens aan bevoegde autoriteiten in andere lidstaten van de Europese Unie of aan organen en instanties belast met de taken, bedoeld in artikel 1, onderdeel a conform de richtlijnen gesteld in de wet plaatsvindt.				

[8] Laag, Middel of Hoog restrisico

Nr. Norm	Nr. §	Onderwerp	Norm	Opzet	Bestaan	Werking	Restrisico L/M/H[9]
21	1.2.5	**Bewaartermijnen, verwijderen en vernietigen**	Politiegegevens worden niet langer bewaard dan de minimale tijd die nodig is, zoals vereist door de toepasselijke wet- en regelgeving, of voor de doeleinden waarvoor deze zijn verwerkt. De verwerkingsverantwoordelijke voorziet in voldoende warborgen om te bewerkstelligen dat de gegevens conform de wet worden gecontroleerd, verwijderd en vernietigd.				L
			Geborgd is dat Politiegegevens na verwijdering maximaal vijf jaar worden bewaard. Indien van cultureel of historisch belang kan worden afgezien van vernietiging van de gegevens. Er wordt dan aan de bewaareisen voldaan.				
			Verwijderde gegevens worden alleen in bijzondere gevallen en indien voldaan wordt aan de vereisten gesteld in de wet ter beschikking gesteld voor hernieuwde verwerking.				
22	1.3.1	**Verstrekking van politiegegevens aan anderen dan politie en Koninklijke marechaussee**	Geborgd is dat politiegegevens alleen worden verstrekt aan personen of instanties buiten het politiedomein, voor zover dit noodzakelijk is voor de doeleinden zoals deze in de Wet politiegegevens en het Besluit politiegegevens zijn genoemd.				M
	1.3.1		Geborgd is dat wanneer gegevens verstrekt worden er wordt voldaan aan de documentatieplicht (conform 6:4 Bpg). Indien vereist is tevens de overeenstemming met het bevoegd gezag vastgelegd.				
	1.3.2		Bij verstrekkingen is geborgd dat de ontvangende partij wordt gewezen op zijn geheimhoudingsplicht.				
	1.3.3		De juistheid, volledigheid, actualiteit en betrouwbaarheid van politiegegevens bij verstrekking wordt, voor zover mogelijk, gecontroleerd en inzichtelijk gemaakt voor de ontvangende partij. Er is een procedure voor het onverwijld in kennis stellen van de ontvanger van politiegegevens indien geconstateerd wordt dat onjuiste politiegegevens zijn verstrekt of dat politiegegevens op onrechtmatig wijze zijn verstrekt.				
23	1.3.1	**Doorgiften aan derde landen**	De doorgifte van gegevens aan derde landen wordt vastgelegd (documentatieplicht).				-
24	1.3.4	**Verstrekking aan derden structureel voor samenwerkingsverbanden**	De verantwoordelijke heeft inzicht in de samenwerkingsverbanden waarbij politiegegevens worden verstrekt.				M
			'In de beslissing voor het verstrekken van politiegegevens ten behoeve van een samenwerkingsverband wordt vastgelegd: o Ten behoeve van welk zwaarwegend algemeen belang de verstrekking noodzakelijk is, o Ten behoeve van welk samenwerkingsverband de politiegegevens worden verstrekt, o Het doel waartoe dit is opgericht, o Welke gegevens worden verstrekt, o De voorwaarden onder welke de gegevens worden verstrekt en o Aan welke personen of instanties de gegevens worden verstrekt.				
			De daadwerkelijke verstrekking van gegevens wordt vastgelegd.				

[9] Laag, Middel of Hoog restrisico

Nr. Norm	Nr. §	Onderwerp	Norm	Opzet	Bestaan	Werking	Restrisico L/M/H[10]
25	1.3.5	**Rechtstreekse verstrekking**	Indien er rechtstreekse verstrekkingen zijn deze rechtmatig (art. 23.1, 23.2, 23.3), wordt voldaan aan de beveiligingseisen, en vinden (art. 23.3) allen plaats aan de aangewezen persoon(en).				-
26	1.4	**Recht op inzage, rectificatie en verwijdering**	Verzoeken tot inzage, rectificatie, vernietiging van betrokkenen wordt tijdig en adequaat afgehandeld. Dit houdt o.a. in dat de organisatie borgt dat bij een verzoek tot inzage (art 25.1) of rectificatie (art 28.1) de betrokkene zonder onnodige vertraging in kennis wordt gesteld van de ontvangst van het verzoek, de termijn voor uitsluitsel en de mogelijkheid een klacht in te dienen bij de AP.				-
			Een weigering gevolg te geven aan het verzoek conform art. 24a.4 is onderbouwd. Elke weigering of beperking van de inzage wordt aan de betrokkene toegelicht, met vermelding van de feitelijke of juridische gronden die aan het besluit ten grondslag liggen				-
28	1.5	**Documentatie[11]**	De verwerkingsverantwoordelijke borgt een volledige en toegankelijke schriftelijke vastlegging (documentatieplicht) van de onderdelen genoemd in art. 32 lid 1. De bedoelde politiegegevens worden conform art. 32 lid 4 bewaard.				-
			De schriftelijke melding van een gemeenschappelijke verwerking van politiegegevens aan de AP is geborgd.				-
30	1.6.1	**Audits**	Er wordt uitvoering gegeven aan de eisen zoals gesteld in de Regeling Periodieke Audit politiegegevens.				**L**
31	1.6.2	**Privacyfunctionaris**	De verantwoordelijke heeft een privacyfunctionaris (PF) benoemt en verleent de PF toegang tot de politiegegevens die onder zijn beheer worden verwerkt.				-
	1.6.3		Toezicht op verwerking van politiegegevens: De PF ziet namens de verwerkingsverantwoordelijke toe op de verwerking van politiegegevens overeenkomstig het bij of krachtens de wet bepaalde.				**M**
	1.6.4		Bijhouden schriftelijke vastlegging: De PF houdt hiertoe een overzicht bij van de schriftelijke vastlegging van: o Doelen van het rechercheonderzoek (art. 9) o Verstrekkingen o Feitelijke of juridische redenen die ten grondslag liggen aan een afwijzing				
	1.6.5		Jaarverslag PF: De privacyfunctionaris stelt jaarlijks een verslag op van haar bevindingen.				-

[10] Laag, Middel of Hoog restrisico

[11] Voor 'Documentatie' is geen rest risico inschatting gemaakt. Dit is al bij de betreffende onderwerpen (doelbinding, verstrekkingen enz.) meegewogen.

1 Risico’s naleving procedures en maatregelen, FIOD werkt aan verbeteringen.

1.1 Risico’s naleving algemene bepalingen geconstateerd

In paragraaf 1.1 zijn de voornaamste bevindingen opgenomen over de maatregelen die moeten borgen dat aan de algemene bepalingen, namelijk Wpg artikelen 1 t/m 7, van de wet wordt voldaan.

In het algemeen geldt dat er veel documentatie beschikbaar is. Er zijn procedures beschikbaar op de intranetpagina van de FIOD en deze worden periodiek bijgewerkt. Wel blijkt uit de interviews en eigen waarneming dat door de hoeveelheid informatie de juiste informatie niet altijd makkelijk vindbaar is en door de opbouw ervan niet alle aspecten van de Wpg worden afgedekt. Wat ons betreft is er inspanning benodigd op het nader, in onderlinge samenhang, comprimeren en organiseren van de documentatie als geheel. Voor dit onderzoek is uitgegaan van de vastgelegde procedures van de FIOD zoals die geldig waren tijdens de controleperiode.

1.1.1 Vastlegging doel onderzoek voldoende geborgd

In procedures is de opzet van (tijdig) vastlegging doelbinding en de verantwoordelijkheid hiervoor vastgelegd. Daarnaast bevat Summ-IT een aantal controls om dit proces te ondersteunen.

Wij hebben de toepassing van de maatregelen vastgesteld met behulp van waarneming ter plaatse van vastleggingen in Summ-IT. Daarbij is vastgesteld dat het doel wordt vastgelegd. Door de FIOD is tevens aangegeven dat per onderzoek wordt gecontroleerd op een tijdige vastlegging van het doel. Geconstateerd is op basis van ontvangen documentatie dat in de controleperiode door de interne audit controle is uitgevoerd op art. 9 doelbinding.

Voor art. 10 is op basis van ontvangen documentatie en interviews geconstateerd dat conform de richtlijnen controle wordt uitgevoerd door de CI-Officier op doelbinding.

1.1.2 Aandacht nodig voor structureel toepassen maatregelen borgen kwaliteit van gegevens

In verschillende documenten is de opzet voor borgen van de kwaliteit (noodzakelijkheid & rechtmatigheid, juistheid & volledigheid) opgenomen. Er is voor art. 9 aandacht nodig voor het nader comprimeren en op elkaar afstemmen van de documentatie. Daarnaast blijkt uit bestudering van de ontvangen documentatie dat voor art. 9 een aantal aspecten niet volledig of duidelijk vastgelegd is. Dit betreft bijvoorbeeld de maatregelen om te borgen dat de herkomst van gegevens wordt vastgelegd, de borging van de controles op de kwaliteit van politiegegevens en maatregelen borging kwaliteit van gegevens bij de werkzaamheden van de digi-recherche en internet recherche. Deels worden deze tekortkomingen in de opzet gemitigeerd door richtlijnen gesteld in de Wetboek van Strafvordering. Daarnaast is in interviews aangegeven dat in de praktijk beheersmaatregelen van toepassing zijn om de kwaliteit te borgen zoals het tegenlezen van processenverbalen.

Wij hebben de toepassing van de in interviews beschreven beheersmaatregelen gecontroleerd aan de hand van interviews en een deelwaarneming ter plaatse in Summ-IT. Daarbij is vastgesteld dat niet alle beheersmaatregelen structureel worden toegepast, zoals de technische maatregelen voor tegenlezen in Summ-IT. Door bijvoorbeeld het aanmaken van een onderzoek als eenmanszaak in plaats van meersmanszaken of het pas opnemen van een document in Summ-IT wanneer het definitief worden de controls in Summ-IT omzeild.

De geconstateerde afwijkingen kunnen een risico vormen voor de noodzakelijkheid, juistheid en volledigheid van gegevens en daarmee een risico vormen voor de naleving van de Wpg. Er zijn wel maatregelen inherent aan het rechercheproces om de risico's in de werking te mitigeren en de kwaliteit toch te borgen. Dit betreft de controle op de kwaliteit door de officier van justitie en rechter-commissaris.

Uit interviews, ontvangen documentatie en een lijncontrole bij TCI blijkt dat bij TCI een controlesysteem is ingericht en dat de CI-Officier de vereiste controles uitvoert.

1.1.3 Aandacht nodig voor opzet verwerken bijzondere categorieën van persoonsgegevens

In opzet is geen informatie aangetroffen met betrekking tot de werkwijze bij het verwerken van bijzondere gegevens. In Summ-IT is het mogelijk om aan te vinken dat gevoelige dan wel bijzondere gegevens worden verwerkt.

Uit interviews blijkt dat bij art. 9 onderzoeken het zelden noodzakelijk is om bijzondere gegevens te verwerken. Uit bestudering van de vastlegging van de controle uitgevoerd door de CI-officier van art. 12 verzamelde gegevens blijkt dat de (rechtmatige) verwerking van bijzondere gegevens onderwerp van controle is. Uit uitgevoerde waarnemingen in Summ-IT is niet gebleken dat er bijzondere gegevens zijn verwerkt. Hierdoor hebben wij geen controle kunnen uitvoeren op de juiste verwerking van bijzondere gegevens.

1.1.4 Bevoegde functionarissen zijn aangewezen

In het vastgestelde en gepubliceerde Ondermandaatbesluit Wet politiegegevens Belastingdienst/FIOD is aangegeven aan wie bevoegdheden behorende bij de bevoegd functionaris Wpg worden toegekend. Er is een overzicht van wie als bevoegd functionaris is aangewezen.

1.1.5 Reikwijdte is grotendeels inzichtelijk en vastgelegd

Om te kunnen bewaken wie toegang heeft tot welke gegevens, hoe lang gegevens bewaard worden enzovoort, is het van belang dat er een volledig inzicht is van de verwerkingen en de systemen alsmede de inrichting van het beheer ervan. De opzet hiervoor is vastgelegd in het Domeinarchitectuur FIOD waarin processen, applicaties en technologie in onderlinge samenhang zijn beschreven. In het Domeinarchitectuur zijn de belangrijkste applicaties benoemd. Met uitzondering van het deel Digitaal Rechercheren geeft het Domeinarchitectuur een beeld van het applicatielandschap FIOD.

1.1.6 Informatiebeveiliging: FIOD heeft aandacht voor mitigeren risico's en is bezig met implementatie risicomanagement alsmede borgen realisatie verbetermaatregelen.

Er is geen opzet ontvangen waaruit blijkt op welke wijze de FIOD uitvoering geeft aan het risicomanagement. Uit de domeinarchitectuur blijkt dat de Belastingdienst gestart is met een programma Risicomanagement. Een koppeling tussen het programma en het inrichten van risicomanagement voor informatiebeveiliging is nog een aandachtspunt.

Het uitvoeren van een risicoanalyse, alsmede het periodiek actualiseren ervan, is bij de FIOD nog in ontwikkeling. In 2019 zijn de Te Beschermen Belangen (TBB) van het ministerie van Financiën geactualiseerd en vastgesteld naar aanleiding van onderzoeken waaruit bleek dat de lijst met TBB'en niet meer actueel was. Hierdoor bestaat het risico dat in de controleperiode niet de juiste beveiligingsmaatregelen zijn gedefinieerd en geïmplementeerd. Uit de ontvangen documentatie blijkt dat in 2019 de TBB'en zorgvuldig zijn afgewogen en waar nodig verbetermaatregelen zijn gesteld.

Uit verschillende onderzoeken blijkt dat de FIOD meerdere maatregelen heeft genomen om de beveiliging te verbeteren. N.a.v. ADR onderzoeken, pentesten en door de beveiligingsfunctionaris uitgevoerde controles zijn verbetermaatregelen gedefinieerd. Er is een risicoregister opgesteld, waarin de resultaten van beveiligingsaudits naar zowel informatiebeveiliging als fysieke beveiliging, waaronder bevindingen met een hoog risico, zijn opgenomen. Uit het risicoregister blijkt niet duidelijk voor alle bevindingen wat de status is van het risico (en te nemen maatregelen). Uit verschillende onderzoeken en uit het risicoregister blijkt dat de FIOD meerdere maatregelen heeft genomen om de beveiliging te verbeteren. Echter blijkt hieruit ook dat enkele risicos al langere tijd openstaan.

1.1.7 *Beveiligingsbeleid grotendeels aanwezig, afspraken nodig voor logging & monitoring*

Het beveiligingsbeleid wordt gevormd door de rijksregelgeving samen met de referentiearchitectuur Integrale Beveiliging en het beveiligingsbeleid (IBB) van de Belastingdienst. Daarnaast wordt de procedure toegang gebouwen FIOD, geactualiseerde beleid met betrekking tot plaats onafhankelijk werken en het Normenkader Beveiliging Rijkskantoren (NKBR) 2.0 voor fysieke beveiliging door de FIOD gehanteerd. Er is nog geen uitwerking van het beleid voor de FIOD voor logging en voor monitoring door Security Operations Center (SOC). Afspraken hieromtrent met de IV-leverancier(s) ontbreken.

Wij hebben de toepassing van de beschreven maatregelen vastgesteld op basis van een door de ADR in 2019 uitgevoerd onderzoek dat uitgevoerd is op basis van normen uit de Baseline Informatiebeveiliging Overheid (BIO). Op basis van dit onderzoek en aanvullende interviews is geconstateerd dat voor een groot deel van de onderzochte normen, zoals bijvoorbeeld wijzigingsbeheer en logische toegangsbeveiliging, geen of niet risicovolle afwijkingen zijn geconstateerd. Tevens is geconstateerd dat er verbeteringen zijn getroffen, zoals het terugdringen en verbeteren van het beheer van samenwerkingsgebieden.
Er zijn enkele normen waar afwijkingen wel zijn geconstateerd, maar waarvoor inmiddels verbetermaatregelen zijn genomen. Dit betreft bevindingen met betrekking tot screening van personeel en fysieke beveiliging. Tevens zijn er enkele normen waarbij afwijkingen zijn geconstateerd die nog verbetering nodig hebben. Dit betreft bevindingen met betrekking tot logging en monitoring. Bij eventuele gebeurtenissen bestaat hiermee het risico dat niet kan worden nagegaan welke persoonsgegevens wanneer en door wie in Summ-IT zijn verwerkt. Ook bestaat het risico dat eventuele inbreuken op de beveiliging niet tijdig worden geconstateerd. Tevens bestaat het risico dat er onrechtmatig toegang wordt verkregen tot politiegegevens. De geconstateerde afwijkingen hebben de aandacht van de FIOD. Een deel van de geconstateerde tekortkomingen (tekortkomingen logging Summ-IT) ligt buiten de invloedsfeer van de FIOD.

Door de FIOD is aangegeven dat er viermaandelijks wordt gerapporteerd over risico’s en maatregelen. Uit de ontvangen documentatie blijkt niet dat in de controleperiode de rapportage volledig is (op basis van bijvoorbeeld een risicoregister en/of de audits). Hiermee bestaat het risico dat de (tijdige) realisatie van verbeteringen niet wordt bewaakt en dat informatie aan management onvolledig is. Uit ontvangen documentatie blijkt wel dat de FIOD hun pdca-cyclus nader aan het verbeteren is.

1.1.8 *Aandacht nodig voor afspraken met verwerkers*

Met betrekking tot de opzet is er geen documentatie ontvangen over wie verantwoordelijk is voor het opstellen van de verwerkersafspraken. In interviews is aangegeven verwerkersafspraken maken de verantwoordelijkheid is van de (gemandateerde) verwerkingsverantwoordelijke.

FIOD betrekt IT-diensten (exploitatie, beheer) van de Politie IV-organisatie, NFI, Doc-Direkt en Belastingdienst/CIE. Er is een SLA en een DAP opgesteld tussen de Politie IV-organisatie en de FIOD. Uit de ontvangen SLA en DAP blijkt dat te leveren diensten zijn vastgelegd, maar niet dat alle vereiste elementen zijn opgenomen. Voor NFI en Doc-Direkt blijkt niet uit ontvangen documentatie dat er afspraken zijn vastgelegd. Hiermee bestaat het risico dat niet alle benodigde (beveiligings)maatregelen worden uitgevoerd. Tevens bestaat het risico dat aan de FIOD niet alle benodigde informatie ten behoeve van verantwoordingsplicht beschikbaar wordt gesteld. Door de FIOD is tijdens hoor/wederhoor aangegeven dat er een verwerkersafspraak voor Doc-Direkt door het MT is geaccordeerd in aug 2021.

Omdat de afspraken niet zijn vastgelegd, en daarom niet voldoende duidelijk zijn, hebben wij de werking ervan niet kunnen controleren.

1.1.9 *Ambtenaren van FIOD zijn bekend met geheimhoudingsplicht*

De opzet van de borging van de geheimhoudingsplicht is in richtlijnen vastgelegd.

Uit interviews blijkt dat FIOD-medewerkers worden beëdigd bij vaste aanstelling en als opsporingsambtenaar. Hierbij wordt gewezen op de geheimhoudingsplicht. Daarnaast worden medewerkers die Wpg-informatie verwerken gescreend door de AIVD. In de controleperiode is een inhaalslag gemaakt om alle medewerkers te laten screenen. De screening zal periodiek herhaald worden.

1.1.10 *Zorgvuldigheid en evenredigheid systeem bepalen autorisaties ingericht*

De opzet voor het systeem voor het bepalen van toe te kennen autorisaties is vastgelegd in procedures en toegekende verantwoordelijkheden.

Er is een profielenmatrix, waarin per categorie medewerker de toe te kennen rollen per applicatie zijn opgenomen, en een autorisatiematrix voor Summ-IT waarin de rollen en autorisatieniveaus per categorie medewerker zijn opgenomen. Uit ontvangen documentatie en uit interviews is tevens vastgesteld dat de rollen periodiek worden besproken in een formeel overleg en dat op basis van besluitvorming de matrices worden aangepast.

1.1.11 *Toegang tot politiegegevens middels autorisatieproces in opzet vastgelegd, controles op juistheid autorisatie kunnen onvoldoende worden uitgevoerd*

De procesopzet voor autorisaties blijkt uit vastgestelde procedures voor autorisaties voor de verwerking van gegevens in systemen en een werkinstructie instroom, doorstroom en uitstroom van medewerkers. De procesopzet voldoet aan de eisen uit de wet.

Wij hebben de toepassing van de maatregelen vastgesteld op basis van de eerder door de ADR uitgevoerd onderzoek en interviews. Hieruit blijkt dat het autorisatieproces (toekennen, intrekken, wijzigen) voor de basis autorisaties conform de procedures worden uitgevoerd. Naast de basis autorisaties worden autorisaties voor specifieke onderzoeksdossiers (Summ-IT en FD) toegekend door de projectleider voor de onderzoeken waarvoor hij verantwoordelijk voor is. Bij de controle ter plaatse en op basis van interviews zijn de volgende afwijkingen geconstateerd:

- Er worden meer medewerkers opgevoerd dan dat er daadwerkelijk actief zijn in de opsporing van het betreffend onderzoek. De aanpak hierbij kan per regio verschillen.
- Er wordt een hoger autorisatieniveau dan noodzakelijk voor de werkzaamheden binnen Summ-IT toegekend.
- De autorisaties op onderzoeken worden niet periodiek gecontroleerd door projectleiders.
- Medewerkers worden niet structureel gedeautoriseerd wanneer toegang tot het dossier / betreffend onderzoek niet meer nodig is.
- Bij het deautoriseren komt het voor dat een autorisatie van een medewerker geheel wordt verwijderd, in plaats van de autorisatie op ‘niet-actief’ te zetten. Hierdoor is het mogelijk dat niet meer te achterhalen is wie toegang heeft gehad tot gegevens of wat voor soort handelingen zijn uitgevoerd.

Door de afwijkingen bestaat de kans dat medewerkers meer rechten hebben dat noodzakelijk is voor de uitvoering van hun werkzaamheden. Ook is er een kans dat autorisaties niet worden ingetrokken als toegang niet langer noodzakelijk is. Een mitigerende maatregel is dat bij vertrek van een medewerker bij de FIOD de basis autorisatie voor Summ-IT geautomatiseerd wordt ingetrokken. Het restrisico beperkt zich daardoor tot FIOD-medewerkers die, ook bij functiewijzigingen, mogelijk meer toegang dan noodzakelijk hebben tot gegevens. Aanvullend risico is dat er geen logging is op autorisaties of handelingen waardoor bij incidenten het moeilijker wordt te achterhalen wie eventueel toegang heeft gehad tot de gegevens en wanneer.

1.1.12 *Interne controles op autorisaties worden uitgevoerd, maar door beperkingen Summ-IT niet volledig*

Het periodiek uitvoeren van controles op autorisaties is vastgelegd in het interne controle jaarplan (ICP). Hiermee wordt in opzet voldaan aan de Baseline Informatiebeveiliging Overheid (BIO).

Uit bestudering van ontvangen documentatie blijkt dat de controle op de basis autorisaties, zoals toegekend middels IMS, worden uitgevoerd zoals vastgesteld in het ICP door team Kwaliteitszorg.

Daarnaast blijkt uit interviews dat er nog geen structurele controle uitgevoerd wordt op de autorisaties binnen individuele rechercheonderzoeken. Oorzaak hiervan is dat er binnen Summ-IT geen historie wordt bijgehouden van toegekende en ingetrokken autorisaties binnen een onderzoek. Daarnaast geldt voor het FD dat de FIOD nog bezig is om het autorisatieproces verder te automatiseren. De huidige inrichting is niet toereikend om jaarlijks automatische controles op deze autorisaties uit te kunnen voeren. Hiermee bestaat het risico dat medewerkers onbevoegd toegang hebben tot gegevens.

1.2 Proces verwijderen en vernietigen verbeterd; risico's geconstateerd bij artikel 11 en 13 verwerkingen

In deze paragraaf zijn de voornaamste bevindingen opgenomen over de maatregelen die moeten borgen dat aan de Wpg-artikelen 8 t/m 15 met betrekking tot de verwerking van gegevens wordt voldaan.

1.2.1 *Verwerken art. 8 gegevens in opzet verbeterd*

Bij de FIOD beperkt de art. 8 verwerking zich tot het verwerken van binnengekomen meldingen en signalen. De procesopzet is beschreven in de instructie verwerken en vastlegging van tips en meldingen art 8 en een instructie voor het achter schot zetten (afschermen) van art. 8 gegevens. Hiermee voldoet de opzet aan de eisen uit art. 8. Door de beperkte verwerking van art. 8 gegevens is alleen de opzet van art 8 onderzocht.

1.2.2 *Geautomatiseerd vergelijken en in combinatie verwerken opzet niet vastgelegd*

Er is geen opzet aangetroffen voor de borging van het geautomatiseerd vergelijken en het in combinatie zoeken (art. 11 verwerkingen) conform de gestelde richtlijnen. Dit met uitzondering van het handboek voor de TCI (ten behoeve van art. 10 verwerkingen). Omdat de opzet van de maatregelen niet beschikbaar is, hebben wij niet kunnen vaststellen dat de in de praktijk toegepaste maatregelen in overeenstemming zijn met de beoogde inrichting van de maatregelen voor het geautomatiseerd vergelijken en het in combinatie zoeken.

Op basis van interviews en de procedure 'autorisaties voor de verwerking van gegevens in systemen' is geconstateerd dat de autorisaties voor art. 11 handelingen ruimer zijn toebedeeld dan in het Bpg is gesteld. Een aandachtspunt dat ook in eerdere audits is geconstateerd. Er is gekozen voor deze werkwijze omdat, volgens de FIOD, het risico beperkt is. Op basis van 'een hit' dient namelijk alsnog toestemming te worden gevraagd van de Bevoegd Functionaris. Dit is echter wel afhankelijk van het juist hanteren van coderingen en de juiste autorisaties van medewerkers.

Art. 11 verwerkingen kunnen vergaande gevolgen hebben voor betrokkenen. Een dergelijke verwerking van politiegegevens is daarom door de wetgever verbonden aan een aantal criteria om de rechtmatigheid en zorgvuldigheid van de verwerking te borgen. Er zijn wel mitigerende maatregelen. Bij alle geïnterviewden is bekend dat voor het gebruik van gegevens afkomstig uit een andere onderzoek toestemming nodig is van, minimaal, de Bevoegd Functionaris. Daarnaast geeft de ruimer toebedeelde autorisaties alleen toegang tot onderzoeken van de FIOD.

1.2.3 *Art. 13 verwerking geprotocolleerd, aandacht nodig voor toezicht op naleving*

De procesopzet is beschreven in de instructie 'Documenteren verwerkingen Wpg FIOD art. 13'. Wij hebben deze bestudeerd en vastgesteld dat de opzet aan de eisen gesteld in de Wpg art.13 voldoet.

Wij hebben de toepassing van de vastgestelde maatregelen gecontroleerd op basis van de ontvangen documentatie. Aangegeven is dat de FIOD één art. 13 verwerking heeft (thema corruptie ten behoeve van de Anti Corruptie Centre (ACC)). Het vastgestelde protocol hiervoor voldoet aan de eisen gesteld in de wet.

Op basis van interviews is vastgesteld dat de maatregelen ter controle op de naleving echter niet wordt toegepast.

1.2.4 Ter Beschikking stellen (voor verdere verwerking) ingericht

De procesopzet is vastgelegd in een werkinstructie en het Handboek TCI. Wij hebben deze bestudeerd en vastgesteld dat de maatregelen voldoen aan de eisen gesteld aan ter beschikking stellingen.

Omdat een ter beschikking stelling van art. 9 politiegegevens wordt vastgelegd in het algemeen journaal kon geen overzicht van ter beschikking stellingen worden verkregen en kon dus maar beperkt onderzoek worden uitgevoerd naar bestaan en werking. Op basis van interviews en een deelwaarneming in Summ-IT zijn geen afwijkingen geconstateerd van de vastgestelde maatregelen.

1.2.5 Verbeterslag proces verwijderen en vernietigen van politiegegevens uitgevoerd

De opzet voor het verwijderen en vernietigen van politiegegevens is vastgelegd in verschillende documenten. In opzet is het proces van verwijderen en vernietigen voldoende geborgd.

In 2018 is de FIOD begonnen de achterstand in het verwijderen en vernietigen van gegevens in IDR in te halen. In interviews is aangegeven dat de achterstand in het verwijderen en vernietigen van art. 9 is ingehaald.

Wij hebben de toepassing van de beschreven maatregelen gecontroleerd op basis van interviews, ontvangen documenten en een deelwaarneming ter plaatse. Hierbij is geconstateerd dat de maatregelen nu grotendeels conform het verbeterd proces worden toegepast. Er wordt gebruik gemaakt van PSF om de termijnen te bewaken. De aantoonbaarheid van de uitvoering van de vernietiging van gegevens bij bijzondere activiteiten zoals OSINT werkzaamheden kan verbeterd worden. Tevens is aangegeven dat het verkrijgen van afloopberichten (de trigger voor het verwijderproces) van het OM nog niet helemaal goed loopt, hoewel beter dan voorheen.

Wij hebben op basis van interviews, de rapportage van de CI-officier en een lijncontrole ter plaatse geconstateerd dat de maatregelen voor verwijderen worden uitgevoerd.

Omdat in de controleperiode de FIOD nog bezig was met het realiseren van het verbeterproces, bestaat er een klein risico dat in de controleperiode gegevens die verwijderd hadden moeten zijn, nog beschikbaar waren voor onderzoeken.

1.3 Aandacht nodig voor eenduidige vastlegging verstrekkingen en beheer samenwerkingsverbanden

In deze paragraaf zijn de voornaamste bevindingen opgenomen over de maatregelen die moeten borgen dat aan artikelen met betrekking tot de verstrekking van politiegegevens (Wpg art. 16 t/m 24) wordt voldaan.

1.3.1 Toereikende instructies voor verstrekken en doorgifte aanwezig, risico door afwijking vastlegging

In opzet heeft de FIOD verschillende documenten, handreikingen en instructies opgesteld als handvatten voor het verstrekken van politiegegevens evenals het documenteren van verstrekkingen. Wij hebben deze bestudeerd en vastgesteld dat de opzet toereikend is om de processen te beheersen. De handreiking evenals de verstrekkingenwijzer zijn wel toe aan actualisering. In de procesopzet is vastgelegd verstrekkingen in de verstrekkingenmodule van Summ-IT vastgelegd dienen te worden.

Wij hebben de toepassing van de maatregelen vastgesteld op basis van interviews en een deelwaarneming van verstrekkingen. Daaruit is gebleken dat het proces deels afwijkt van de vastgestelde richtlijnen. Hoewel het proces verbeterd is ten opzichte van 2016, wordt de specifieke verstrekkingenmodule in Summ-IT nog steeds niet altijd gebruikt. Bij vastlegging buiten de module is niet geborgd dat alle vereiste elementen (documentatieplicht) worden vastgelegd.

Uit de controle is niet gebleken dat er onrechtmatige verstrekkingen hebben plaatsgevonden. Door de afwijking in de vastlegging is er echter geen volledig overzicht beschikbaar van alle verstrekkingen die zijn gedaan in de controleperiode. Risico hiervan is dat er geen effectief toezicht plaats kan vinden op alle verstrekkingen. Tevens bestaat het risico dat indien gegevens onjuist blijken te zijn dit niet kan worden gecommuniceerd aan eventuele ontvangers van de gegevens.

1.3.2 Geheimhoudingsplicht niet structureel toegevoegd aan verstrekking

De procesopzet voor het wijzen van de ontvangende partij op de geheimhoudingsplicht voldoet aan de gestelde eisen in art. 7, tweede lid, van de Wet politiegegevens.

Uit de onder paragraaf 1.3.1 genoemde controle is niet gebleken dat bij een verstrekking van art. 9 gegevens wordt voldaan aan het gestelde in de procesopzet. Er zijn wel mitigerende maatregelen. De meeste verstrekkingen vinden plaats aan partijen waarvoor andere (eigen) wetgeving geldt, bijvoorbeeld Toezichtswetgeving, waarvoor ook een geheimhoudingsplicht geldt. Door de FIOD is aangegeven tijdens hoor/wederhoor dat bij de Infodesk wel inmiddels verbetermaatregelen zijn getroffen hieromtrent.

1.3.3 Controle van kwaliteit van politiegegevens bij verstrekking in opzet niet vastgelegd

De procesopzet borgt niet de naleving van deze eisen. Er is niet vastgelegd hoe de controle op juistheid, volledigheid, actualiteit en betrouwbaarheid van politiegegevens die verstrekt worden is geborgd. Tevens is de opzet van de kennisgevingsplicht, indien geconstateerd wordt dat onjuiste politiegegevens zijn verstrekt of dat politiegegevens op onrechtmatig wijze zijn verstrekt, niet vastgelegd.

1.3.4 Afspraken samenwerkingsverbanden vastgelegd, tekortkomingen geconstateerd bij beheer ervan

Geconstateerd is dat in opzet het beheer van samenwerkingverbanden in de controleperiode niet volledig is geweest. Naar aanleiding van de interne audit 2019 (uitgevoerd in 2020) is een instructie opgesteld voor het beheer van samenwerkingsverbanden en per april 2021 gepubliceerd op intranet. Het verstrekken binnen samenwerkingsverbanden volgt het proces van verstrekkingen van de FIOD. Zie paragraaf 1.3.1. voor de opzet hiervan.

Op basis van de interne audit 2019 op de vastlegging van afgesloten samenwerkingsverbanden (SV's) met betrekking tot gegevensuitwisseling van Wpg-gegevens in het jaar 2019 blijkt dat er geen volledig centraal inzicht is in alle SV’s, geen volledig beeld van alle SV’s waarbij de FIOD betrokken is en geen volledig betrouwbaar centraal databestand aanwezig is van SV’s. Het ontbreekt daarnaast aan een bewakingsmechanisme op de verschillende termijnen van de SV’s. Naar aanleiding van deze constateringen is door de FIOD diverse acties in gang gezet, onder andere om SV's van met name convenanten te gaan verzamelen. Dit heeft geleid tot een overzicht van samenwerkingsverbanden. Hoewel centraal inzicht ontbrak zijn er voor meerdere samenwerkingsverbanden wel afspraken vastgelegd.

Met de geconstateerde tekortkomingen bestaat het risico dat er geen toezicht en controle is op de naleving van de beheersmaatregelen.

1.3.5 Rechtstreekse verstrekking

Door de FIOD is aangegeven dat er geen rechtstreekse verstrekkingen plaatsvinden. De ADR heeft derhalve geen controle hiernaar kunnen uitvoeren.

1.4 Rechten betrokkenen proces geborgd

De procesopzet is vastgelegd in de procesbeschrijving voor inzageverzoeken en voor rectificatieverzoeken. De opzet voldoet aan de eisen gesteld in de Wpg artikelen 25 t/m 31.

Wij hebben de toepassing van de beschreven maatregelen vastgesteld met behulp van een interview met de privacyfunctionaris en een controle van het register en behandelde verzoeken. Daarbij is vastgesteld dat de maatregelen worden toegepast zoals beschreven.

1.5 Documentatieplicht deels ingericht

De opzet is vastgelegd in een instructie voor de vastlegging van het documentatieplicht (protocolplicht) en het melden van gemeenschappelijke verwerkingen. Uit bestudering van de procesopzet is vastgesteld dat deze voldoet aan de eisen zoals gesteld in art. 32 Wpg en de aanvullende richtlijnen uit de Bpg.

De documentatieplicht geldt voor een aantal artikelen in de Wpg. Met betrekking tot de bevindingen op bestaan en werking documentatieplicht (protocolplicht) wordt verwezen naar de betreffende onderdelen:

- Paragraaf 1.1.1 voor vastleggen doel onderzoek
- Paragraaf 1.3.1 voor vastleggen van verstrekkingen
- Paragraaf 1.1.11 voor documenteren van toegekende autorisaties

Door de verschillen in werkwijze tussen de regio's en projectleiders is het mogelijk dat de benodigde documentatiegegevens (protocolgegevens) niet structureel en op een eenduidige wijze worden vastgelegd.

De FIOD heeft aangegeven dat er geen gemeenschappelijke verwerkingen actief waren in de controleperiode. Er is dan ook geen controle op bestaan en werking van gemeenschappelijke verwerkingen uitgevoerd.

1.6 Uitvoering wordt gegeven aan interne audits, aandacht nodig voor realisatie toezichtswerkzaamheden

In deze paragraaf zijn de voornaamste bevindingen opgenomen over de controle en toezicht van maatregelen zoals vastgelegd in de Wpg art. 33-34, art. 36 van de wet.

1.6.1 Interne audits zijn conform de richtlijnen uitgevoerd, aandacht nodig voor positie binnen organisatie

Er is een procesbeschrijving evaluatie toezicht auditverplichtingen. Wij hebben de procesopzet bestudeerd en vastgesteld dat deze grotendeels voldoet aan de eisen gesteld in art. 33 van de Wpg en de Regeling periodieke audit politiegegevens (RPAP). De procesopzet dient nog wel geactualiseerd te worden.

De positie van de interne audit staat onafhankelijk van de uitvoerende primaire teams en stafteams. Het cluster heeft wel taken gerelateerd aan de naleving van de Wpg zoals bijvoorbeeld het opstellen van procedures en beoordeling aanvragen autorisaties. Daarnaast blijkt uit ons onderzoek dat het uitvoeren van verbetermaatregelen afkomstig uit de interne audits en controles vaak belegd worden bij de audit medewerkers. Dit kan effect hebben op de objectiviteit en onafhankelijkheid van de interne auditors.

Wij hebben de toepassing van de opzet vastgesteld met behulp van interviews en ontvangen documentatie. Daarbij is vastgesteld dat er uitvoering wordt gegeven aan de maatregelen zoals beschreven.

1.6.2 *Privacyfunctionaris benoemd en toegang gegevens geborgd*

De FIOD heeft formeel een privacyfunctionaris benoemd en er is een formele taakomschrijving. De privacyfunctionaris heeft de autorisatie en daarmee toegang tot de politiegegevens voor het kunnen uitoefenen van de werkzaamheden. Hiermee voldoet de FIOD aan de wettelijke eisen.

1.6.3 *Uitvoering toezicht privacyfunctionaris niet navolgbaar*

In de documentatie is vastgelegd dat de privacyfunctionaris namens de verwerkingsverantwoordelijke toeziet op de verwerking van politiegegevens. Uit de documentatie blijkt niet op welke wijze hier uitvoering aan moet worden gegeven.

Er is geen documentatie ontvangen waaruit blijkt dat toezichtstaken zijn uitgevoerd. In interviews is aangegeven dat het werkterrein van de privacyfunctionaris vrij breed en de werkdruk hoog is. Aangegeven is dat verschillende medewerkers (in)direct betrokken zijn bij de (toezichts)werkzaamheden rondom privacy en bescherming van persoonsgegevens. De onderlinge afspraken hierover zijn nog niet vastgesteld. Aangegeven is dat dit een aandachtspunt is dat opgepakt gaat worden.

1.6.4 *Bijhouden schriftelijke vastlegging in opzet niet ingericht*

In opzet is vastgelegd dat de privacyfunctionaris toezicht houdt op de schriftelijke vastlegging van gegevens als bedoeld in art. 32 lid 1 Wpg. Er is in opzet geen documentatie ontvangen waaruit blijkt op welke wijze de privacyfunctionaris een overzicht bijhoudt van de betreffende schriftelijke vastlegging.

Door de verschillen in werkwijze tussen de regio’s en projectleiders worden de benodigde documentatiegegevens (protocolgegevens) niet structureel en op een eenduidige wijze vastgelegd. Het toezicht houden op signalen en meldingen wordt daardoor bemoeilijkt. Aangegeven is dat er stappen worden ondernomen om dergelijke risico’s te mitigeren.

1.6.5 *Jaarverslag privacyfunctionaris wordt opgesteld*

De privacyfunctionaris heeft een jaarverslag opgesteld over de jaren 2018 en 2019. Door de knelpunten met betrekking tot het bijhouden van een overzicht en toezicht houden op de schriftelijke vastlegging (documentatieplicht) wordt niet over deze elementen gerapporteerd.

1.7 PDCA-cyclus beter borgen voor structurele verbetering

Door de ADR is bij de controle op verschillende normen geconstateerd dat in de controle periode de pdca-cyclus gericht op de naleving van de Wpg niet volledig was. Uit ontvangen documentatie blijkt wel dat de FIOD in 2020 en 2021 verbeteringen heeft betroffen om de pdca-cyclus beter in te richten.

2 Concretisering benodigde maatregelen nieuwe wetsartikelen en bewaking implementatie wenselijk

Per 6 mei 2018 is de nieuwe Richtlijn Gegevensbescherming Politie en Justitie[12] van kracht geworden. De Richtlijn resulteert, onder andere, in een substantiële wijziging van de Wpg[13]. Dit betreft zowel wijzigingen aan bestaande artikelen, als nieuwe artikelen waaraan de organisatie moet voldoen. Deze nieuwe Wpg is in werking getreden per 1 januari 2019.

Tijdens dit onderzoek is op hoofdlijnen gekeken naar de manier waarop de organisatie bezig is de wijzigingen te implementeren. De naleving van de nieuwe wetsartikelen valt buiten de scope van dit onderzoek en is niet meegewogen in de eindbeoordeling.

Memo wijzigingen
Door de FIOD is een memo opgesteld over de belangrijkste inhoudelijke wijzigingen, de gevolgen hiervan voor de FIOD en de hierop te nemen acties. Voor meerdere nieuwe wetsartikelen geldt dat ze niet behandeld worden in het memo. Het is daardoor niet inzichtelijk op welke mate deze nieuwe eisen worden afgedekt door de bestaande maatregelen, en of nieuwe maatregelen nodig zijn. Dit betreft bijvoorbeeld geautomatiseerde individuele besluitvorming en onderscheid tussen feiten en oordeel.

Onderscheid verschillende categorieën van betrokkenen
Nog niet alle verwerkingssystemen kunnen het onderscheid tussen de verschillende categorieën van betrokkenen aanbrengen. Daarom heeft de FIOD bepaald dat aanpassingen nodig zijn binnen die verwerkingssystemen die dit onderscheid nog niet kunnen maken. Hiertoe moet onderzocht worden of en zo ja op welke wijze, binnen welke termijn én tegen welke kosten dit alsnog mogelijk is. Voor wat betreft Summ-IT was ten tijde van het onderzoek nog niet bekend of ten behoeve van dit nieuwe wetsartikel wijzigingen moeten worden aangebracht.

Gegevensbescherming door ontwerp
Met betrekking tot privacy by design is in het memo aangegeven dat gegevensbescherming 'ingebakken' moet worden in de processen en systemen (by design), waardoor gegevensbescherming in feite standaard op 'aan' staat (by default).
In het memo is geen analyse opgenomen in hoeverre de FIOD hieraan al voldoet en welke acties nodig zijn om dit te realiseren.

Verwerking Politiegegevens aantoonbaar in overeenstemming met Wpg
Met betrekking tot het treffen van passende technische en organisatorische maatregelen om aan te kunnen tonen dat de verwerking van politiegegevens wordt verricht in overeenstemming met wat bepaald is in de wet blijkt niet uit de ontvangen documentatie of een analyse is uitgevoerd in hoeverre de FIOD hieraan al voldoet en welke acties nog nodig zijn om dit te realiseren.

[12] RICHTLIJN (EU) 2016/680 VAN HET EUROPEES PARLEMENT EN DE RAAD van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens door bevoegde autoriteiten met het oog op de voorkoming, het onderzoek, de opsporing en de vervolging van strafbare feiten of de tenuitvoerlegging van straffen, en betreffende het vrije verkeer van die gegevens.
[13] Wet van 17 oktober 2018 tot wijziging van de Wet Politiegegevens ter implementatie van Europese regelgeving over de verwerking van persoonsgegevens met het oog op de voorkoming, het onderzoek, de opsporing en vervolging van strafbare feiten of de tenuitvoerlegging van straffen.

Gegevensbeschermingseffectbeoordeling (GEB)
De verplichting tot het uitvoeren van een gegevensbeschermingseffectbeoordeling (GEB) is een van de nieuwe vereisten opgenomen in de Wpg. Er zijn twee actiepunten gedefinieerd. Ten eerste dat de datacoördinator en senior privacyfunctionaris zorgen voor een procesbeschrijving. Ten tweede het aanpassen van het mandaatbesluit.

Aangegeven is dat er nog geen landelijke procedure is voor het opstellen van GEB's. Er wordt daarom zoveel mogelijk gewerkt conform de procedure voor de AVG. Met betrekking tot het aanpassen van het mandaatbesluit is aangegeven dat dit punt meermaals onder de aandacht is gebracht van het ministerie, maar hierop is nog geen actie ondernomen.

Door de privacyfunctionaris (PF) is aangegeven dat binnen de Belastingdienst gebruikt wordt gemaakt van de Will-Mogen-Kunnen toets (WMK-toets) om een analyse uit te voeren of bij een verwerking sprake is van een hoog risico en een GEB nodig is. Aangegeven is dat in 2019 een Wpg variant hiervan is opgesteld. Er is geen documentatie ontvangen waaruit blijkt dat voor alle verwerkingen van politiegegevens een analyse (WMK toets) is uitgevoerd. Er is geen overzicht ontvangen van welke GEB'en opgesteld moeten worden en de stand van zaken daarvan. In verschillende interviews is aangegeven dat de FIOD bezig is met een GEB voor Hansken en voor FCI-net. Tevens is aangegeven dat er ook een aantal oude GEB’en zijn, echter dat deze (nog) niet zijn geactualiseerd.

Er is geen proces aangetroffen dat borgt dat GEB’en actueel worden gehouden (bijv. bij ontwikkelingen die effect kunnen hebben op gelopen risico's) of die borgt dat een toetsing wordt uitgevoerd of de verwerking overeenkomstig de GEB wordt uitgevoerd.

Melding datalekken
De FIOD dient de procedure van DG-Belastingdienst te hanteren voor de behandeling van privacy gerelateerde incidenten en inperking van de gevolgen. Procedures worden via intranet met de medewerkers van de FIOD gedeeld evenals via periodieke nieuwsberichten. Er wordt een register bijgehouden van geconstateerde datalekken.

Doorgifte op basis van adequaatheidsbesluit of uitzonderingsgrond
In het memo is voor de doorgifte van gegevens (internationale gegevensuitwisseling) aangegeven dat ten aanzien van de uitwerking van de gestelde kaders nog onduidelijkheid bestaat. Onder leiding van J&V is een projectgroep geformeerd, waarin ook de FIOD is vertegenwoordigd, met als doel te komen tot een praktische handleiding voor de doorgifte van gegevens.

Er is een tijdelijke instructie voor de politie, de Koninklijke Marechaussee en de Bijzondere Opsporingsdiensten opgesteld voor de doorgifte in afzonderlijke gevallen opgesteld in afwachting van de te nemen besluiten.

Informatie aan de betrokkene
De Belastingdienst heeft een privacyverklaring opgesteld waarin aan burgers informatie wordt verschaft over de verwerking van persoonsgegevens.

Register
Als actie is vastgesteld dat alle verwerkingen van politiegegevens in een register opgenomen moeten worden. De vastlegging van de verwerkingen zal in hetzelfde register worden vastgelegd als de AVG-verwerkingen. Aangegeven is dat het register momenteel nog in opbouw is. Er zijn nog enkele onduidelijkheden over de wijze van vulling van het verwerkingenregister. Hierbij is de FIOD afhankelijk van DG-Bel. De FIOD is in overleg met de FG om te kijken met welke diepgang het register gevuld dient te worden. Wel is er aan aantal conceptmeldingen opgenomen. Tevens is aangegeven dat nog niet duidelijk is hoe het vaststellingstraject dient te lopen.

Functionaris voor gegevensbescherming
Voor de FIOD is er sinds medio 2020 een (plaatsvervangend) FG aangesteld die toezicht dient te houden op het naleven van de Wpg. Er moet nog afstemming plaatsvinden met de privacyfunctionaris met betrekking tot de verdeling van taken

en verantwoordelijkheden. Gezien de impact van de ontvlechting bij de Belastingdienst kan het nog enige tijd duren voordat de (p)FG concreet zal beginnen aan zijn toezichts- en adviesrol.

3 Aanbevelingen voor het zorgdragen van compliancy met de Wpg

Naar aanleiding van dit onderzoek wordt aanbevolen verbetermaatregelen door te voeren voor die normen waarvan het restrisico Middel tot Hoog is. In het algemeen geldt dat er veel documentatie beschikbaar is, waardoor de juiste informatie niet altijd makkelijk is te vinden en of deze duidelijk is. Aanbevolen wordt de opzet toegankelijker te maken door het te comprimeren en beter te ordenen.

Op basis van de bevindingen stellen wij de onderstaande verbetermaatregelen voor.

Paragraaf	**Aanbeveling**
1.1.2	*Aanbevolen wordt zorg te dragen dat de controlemaatregelen die zorg moeten dragen voor de kwaliteit van de politiegegevens structureel en aantoonbaar worden toegepast.*
1.1.6	*Draag zorg voor een volledig risico-register en het bijhouden van de stand van zaken van verbetermaatregelen. Tevens wordt aanbevolen het risicomanagement verder te implementeren en te borgen binnen de organisatie waarbij voldoende aandacht is voor IB en de Rijksregelgeving daaromtrent. Ook wordt aanbevolen te onderzoeken of GRC-tooling uitkomst kan bieden om dit proces beter te borgen.*
1.1.7	*Borg dat de realisatie van verbetermaatregelen wordt bewaakt en dat periodiek over de realisatie wordt gerapporteerd.*
1.1.7	*Draag zorg voor nadere uitwerking van het beleid met betrekking tot loggen en het bewaren van logbestanden in richtlijnen en procedures voor de FIOD. Tevens wordt aanbevolen beleid op monitoring van beveiligingsmaatregelen op te stellen en afspraken over de uitvoering hiervan vast te leggen.*
1.1.8	*Aanbevolen wordt in kaart te brengen welke verwerkersafspraken nog vastgelegd moeten worden en om zorg te dragen voor een procedure voor het vastleggen en actueel houden van de afspraken.*
1.2.2	*Leg de procedures voor art. 11 verwerkingen die de FIOD hanteert vast inclusief de maatregelen die gehanteerd worden om de afwijkingen van de richtlijnen te mitigeren.*
1.2.3	*Aanbevolen wordt uitvoering te geven aan de toezichtswerkzaamheden zoals vastgelegd in de protocollering van de art. 13 verwerking van de ACC.*
1.6.1	*Draag zorg voor de borging van de onafhankelijke rol van de interne auditors door zorg te dragen dat invoering van verbeteringen worden belegd bij de primair verantwoordelijke functionaris.*
1.7	*Draag zorg voor een centrale overzicht van te nemen verbetermaatregelen, alsmede een proces voor het borgen en bewaken van de realisatie van de maatregelen.*
2	*Aanbevolen wordt zorg te dragen voor een nadere analyse van nog benodigde acties om de wijzigingen in de Wpg volledig te implementeren. Bijvoorbeeld het borgen van privacy by design & privacy by default bij ontwikkelen en beheer van processen en systemen.*

4 Verantwoording onderzoek

4.1 Werkzaamheden en afbakening

Het doel van dit assurance-onderzoek is om een beperkte mate van zekerheid te geven of aan de bepalingen van de wet op adequate wijze uitvoering is gegeven. Hiertoe hebben wij werkzaamheden uitgevoerd om de opzet, het bestaan en de werking vast te stellen van de beheersingsmaatregelen die de FIOD heeft getroffen te toetsen aan het normenkader.

Het normenkader is gebaseerd op de in de Wpg, de Bpg en de RPAP[14] gestelde eisen.

Dit onderzoek bestond uit de volgende werkzaamheden:

- Review werkzaamheden interne auditors: we hebben een review uitgevoerd van de interne audits.
- Interviews met de privacyfunctionarissen, functioneel beheer, teamleiders, projectleiders, beveiligingsfunctionaris en interne auditors. De interviews zijn vastgelegd en afgestemd met de betreffende functionarissen.
- Documentanalyse: wij hebben documenten opgevraagd om inzicht te verkrijgen in de opzet, bestaan en/of werking van de beheersingsmaatregel. Dit betreft bijvoorbeeld procedures en rapportages van de PF, werkinstructies, screenshots uit Summ-IT, interne audit rapporten en jaarverslagen.
- Waarneming: wij hebben door middel van waarneming van de uitvoering van een beheersingsmaatregel beoordeeld of de beheersingsmaatregel wordt toegepast zoals beschreven. Hiervoor is een deelwaarneming gedaan van een aantal onderzoeken in Summ-IT.

Afbakening

De beoordeling van de opzet, bestaan en werking omvatte de maatregelen en procedures die in de borging van de wettelijke eisen van de Wpg moeten voorzien. Het bestaan is beoordeeld, voor zover mogelijk[15], aan de hand van procedures, werkwijze en vastleggingen op peildatum december 2019. De werking van procedures en maatregelen is, voor zover mogelijk, beoordeeld over de periode 01-01-2019 tot en met 31-12-2019. De werking van de controle en toezicht (art. 32-34) is, voor zover mogelijk, beoordeeld over de periode 1-1-2016 tot en met 31-12-2019. Dit betreft bijvoorbeeld de uitvoering van interne audits en de toezichtswerkzaamheden (inclusief opstellen jaarverslag) van de privacyfunctionaris.

Verbetermaatregelen en nieuwe proces die zijn opgestart en afgerond na 2019 zijn, voor zover relevant, aangegeven in dit rapport. Omdat de controle begrensd is tot periode 2016 t/m 2019, kan het voorkomen dat een verbetermaatregelen wel zijn benoemd, maar vanwege de begrenzing niet zijn meegewogen in de eindconclusie.

Het onderzoek richt zich alleen op de procedures en maatregelen van de FIOD zelf. De ADR heeft geen onderzoek verricht naar door derden aan de FIOD geleverde faciliteiten, voor zover de verantwoordelijkheid is belegd bij andere overheidsorganisaties. In dergelijke gevallen is wel gekeken naar de gemaakte

[14] Regeling periodieke audit politiegegevens geldend van 26-06-2019 t/m heden.
15 Het is mogelijk dat niet alle situaties zich voordoen in de selectie, bijvoorbeeld het verwerken van bijzondere gegevens.

afspraken tussen de partijen en de regie vanuit de FIOD gericht op de realisatie van de afspraken.

Per 6 mei 2018 is de nieuwe Richtlijn Gegevensbescherming Politie en Justitie[16] van kracht geworden. De Richtlijn heeft geresulteerd in een substantiële wijziging van de Wpg[17]. Dit betreft zowel wijzigingen van bestaande artikelen, als nieuwe artikelen waaraan de organisatie moet voldoen. Twee jaar na de inwerkingtreding van de (gewijzigde) wet gaat de externe auditverplichting in. Om een actueel beeld te kunnen geven aan belanghebbenden is tijdens dit onderzoek gekeken naar de manier waarop de organisatie bezig is de wijzigingen te implementeren (voor zover mogelijk, en op moment van de controle van toepassing), maar dit maakt geen onderdeel uit van het oordeel over de naleving van de wet in de controleperiode.

De algemeen directeur FIOD heeft op basis van zijn bevoegdheid op grond van artikel 2 lid 4 van de regeling periodieke audit politiegegevens aan de privacy auditor de **toegang te weigeren** tot de volgende verwerking: De registratie van de persoonsgegevens van de informanten van de TCI. Reden hiertoe is de grote risico's die de informanten lopen als hun identiteit bekend wordt.

De algemeen directeur FIOD heeft op basis van zijn bevoegdheid op grond van artikel 2 lid 4 van de RPAP aan de privacy auditor **beperkende voorwaarden** te verbinden aan de toegang tot de volgende verwerking: Politiegegevens beheerd door de TCI (artikel 10.1.a en artikel 12 en overige door de TCI beheerde politiegegevens).

- Beperkende voorwaarde: deze politiegegevens mogen alleen door medewerkers van het auditteam die een A-status hebben (A-screening AIVD) ingezien worden.
- Toelichting: het betreft zeer gevoelige gegevens met groot afbreukrisico en mogelijk gevaar voor betrokkenen waarover gegevens geregistreerd staan.

4.2 Gehanteerde Standaard

Deze opdracht is uitgevoerd volgens de Richtlijn voor assurance-opdrachten door IT-auditors (NOREA Richtlijn 3000D).

4.3 Verspreiding rapport

De opdrachtgever, Dhr N.S.T. Obbink, algemeen directeur FIOD, is eigenaar van dit rapport.

De ADR is de interne auditdienst van het Rijk. Dit rapport is primair bestemd voor de opdrachtgever met wie wij deze opdracht zijn overeengekomen. In de ministerraad is besloten dat het opdrachtgevende ministerie waarvoor de ADR een rapport heeft geschreven, het rapport binnen zes weken op de website van de rijksoverheid plaatst, tenzij daarvoor een uitzondering geldt. De minister van Financiën stuurt elk halfjaar een overzicht naar de Tweede Kamer met de titels van door de ADR uitgebrachte rapporten en plaatst dit overzicht op de website.

Conform artikel 33 lid 2 van de Wet politiegegevens dient de verantwoordelijke tevens een afschrift van de controleresultaten van de privacy audits aan het Autoriteit persoonsgegevens beschikbaar te stellen.

[16] RICHTLIJN (EU) 2016/680 VAN HET EUROPEES PARLEMENT EN DE RAAD van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens door bevoegde autoriteiten met het oog op de voorkoming, het onderzoek, de opsporing en de vervolging van strafbare feiten of de tenuitvoerlegging van straffen, en betreffende het vrije verkeer van die gegevens.
[17] Wet van 17 oktober 2018 tot wijziging van de Wet Politiegegevens ter implementatie van Europese regelgeving over de verwerking van persoonsgegevens met het oog op de voorkoming, het onderzoek, de opsporing en vervolging van strafbare feiten of de tenuitvoerlegging van straffen.

5 Ondertekening

Den Haag, 09 februari 2022

Projectleider
Auditdienst Rijk
Sector IT

6 Bijlage(n)

6.1 Bijlage 1: Managementreactie FIOD

De Auditdienst Rijk komt op basis van de privacy audit tot het oordeel dat de FIOD het stelsel van beheersmaatregelen beter heeft geborgd ten opzichte van de vorige controle maar dat nog verbeteracties nodig zijn.

De FIOD herkent zich in de geconstateerde tekortkomingen door de Audit Dienst Rijk (verder ADR). Hierbij wordt opgemerkt, dat de onderzochte periode enkele jaren achter ons ligt en bevindingen na deze periode werden opgelost.

In het op te stellen verbeterplan zal de FIOD de geconstateerde tekortkomingen opnemen en de daarbij behorende acties in de vorm van beheersmaatregelen gaan instellen. Bij enkele acties is de FIOD afhankelijk van beheersmaatregelen die buiten de organisatie dienen te worden genomen. Deze te nemen maatregelen liggen bij de externe beheerder van het systeem Summ-IT.

Een hercontrole zal worden uitgevoerd naar de door de FIOD ingestelde beheersmaatregelen in opzet, bestaan en werking.

6.2 Bijlage 2: Legenda en normenkader

Beoordeling
De privacy audit betreft een Assurance onderzoek op opzet, bestaan en werking. Er wordt dus een oordeel gegeven. Dit wordt gedaan door middel van een stoplichtenrapportage:

Aan de norm is voldaan	
Aan de norm is niet geheel (of niet aantoonbaar) voldaan.	
Aan de norm is niet (aantoonbaar) voldaan	
De maatregel kon niet gecontroleerd worden. Bijvoorbeeld indien de opzet niet voldoende duidelijk is, wordt het bestaan en de werking niet gecontroleerd.	
De norm is niet van toepassing of de maatregel is niet gecontroleerd tijdens het onderzoek. Tijdens het onderzoek kan het voor komen dat gekozen wordt om een norm niet te controleren.	

Weging op basis van key controls
Om tot een beoordeling te komen worden de bevindingen gewogen.
Bij afwijkingen van de norm (deels of onvoldoende effectief) is het restrisico beoordeeld (als laag, middel of hoog). Hierbij wordt bijvoorbeeld rekening gehouden met mitigerende maatregelen en de risico's voor de rechten van betrokkenen.
Binnen het normenkader zijn een key controls[18] gedefinieerd. De normen die als 'key control' zijn gedefinieerd betreffen aspecten die een groter risico kunnen vormen voor de rechten van betrokkenen indien er niet aan wordt voldaan. Bij het beoordelen van het restrisico wordt rekening gehouden indien een norm als key control is gedefinieerd. Afwijkingen van de norm, waarbij er een hoog restrisico resteert, kunnen leiden tot een afkeurende verklaring. Hetzelfde geldt als bij meerdere normen een gemiddeld restrisico resteert.

[18] Met ▲ aangeduid in normenkader

Normenkader

#	Titel	Verwijzing Artikel	Norm	Norm uitleg (opzet/bestaan/werking)		Key Control
Algemene Bepalingen						
1	**Doelbinding**	Art 3 lid 1, 3 en 4, 8.1, 9.1 en 9.2, 10.1 en 12.1	1.1	Politiegegevens worden alleen verwerkt als dat nodig is voor de in de wet genoemde doeleinden. Geborgd is dat bij het verwerken van politiegegevens altijd sprake is van doelbinding en dat de gegevens niet op een met die doeleinden onverenigbare wijze worden verwerkt.	-	
2	**Noodzakelijkheid & rechtmatigheid en Gegevensbescherming door standaardinstellingen** *Dat gegevens rechtmatig moeten zijn verkregen is onderdeel van de toetsing van politiewerk (WvSv). Dit onderdeel van de norm toetsen we niet.*	Art 3 lid 2 & 5 en Art 4b.1a	2.1	De verzameling en verwerking van politiegegevens is toegespitst op een gespecificeerd doel met een wettelijke grondslag. Er wordt geborgd dat de persoonsgegevens daartoe toereikend, ter zake dienend en beperkt zijn tot wat noodzakelijk is (niet bovenmatig) en dat de herkomst van gegevens voor artikel 9, 10 en 12 verwerkingen wordt vermeld.		
			2.2	Om te borgen dat alleen die politiegegevens worden verwerkt die noodzakelijk zijn voor elk specifiek doel van de verwerking heeft de verwerkingsverantwoordelijk passende technische en organisatorische maatregelen gedefinieerd en geïmplementeerd.		
3	**Juistheid en volledigheid politiegegevens**	Art 4, lid 1 en 4	3.1	De verwerkingsverantwoordelijke heeft controles op de kwaliteit ingericht ten behoeve van de borging van de juistheid en nauwkeurigheid van persoonsgegevens.		

4	**Bijzondere categorieën van politiegegevens**	Art 5	4.1	Er vindt geen verwerking van bijzondere categorieën van politiegegevens, tenzij: - Dat nodig is voor het doel van de verwerking. - In aanvulling is op de verwerking van andere politiegegevens betreffende de persoon - De gegevens afdoende zijn beveiligd.	-	**X**
5	**Geautomatiseerde individuele besluitvorming**	Art 7a, lid 1-3	5.1	Het verbod op het gebruik van profilering die leidt tot discriminatie van personen op grond van de bijzondere categorieën van politiegegevens (art 5) is bekend binnen de organisatie. Het verbod op profilering is onderwerp van de bewustwordingssessies binnen de organisatie.		
6	**Onderscheid feiten en oordeel**	Art 4.3	6.1	Er zijn maatregelen genomen om politiegegevens die op feiten zijn gebaseerd, voor zover mogelijk, te onderscheiden van politiegegevens die op een persoonlijk oordeel zijn gebaseerd.		
7	**Autorisaties: aanwijzen functionarissen**	Art 6.7	7.1	Er is een actueel lijst van, door de verantwoordelijke aangewezen, bevoegde functionarissen.		
8	**Onderscheid tussen verschillende categorieën van betrokkenen**	Art 6b	8.1	De verwerkingsverantwoordelijke heeft geborgd dat, voor zover mogelijk, duidelijk onderscheid wordt gemaakt in de verschillende categorieën van betrokkenen.		

Algemene Bepalingen: Bescherming van gegevens						
9	**Reikwijdte**	Art 2, lid 1 en 2	9.1	De verwerkingsverantwoordelijke heeft verwerkingen van politiegegevens binnen de organisatie geïdentificeerd en gedocumenteerd.		
10	**Gegevensbescherming door beveiliging en ontwerp**	Art 4a, lid 1-5	10.1	Er is (aantoonbaar) een risicoanalyse uitgevoerd waaruit het risiconiveau blijkt en identificeert, evalueert en mitigeert systematisch en periodiek factoren die het beschermen van politiegegevens tegen ongeoorloofde of onrechtmatige verwerking en tegen opzettelijk verlies, vernietiging of beschadiging in gevaar brengen en past de maatregelen hierop aan.		
			10.2	De organisatie heeft gegevensbeschermingsbeleid en procedures ontwikkeld en vastgesteld. De verwerkingsverantwoordelijke heeft de maatregelen die nodig zijn om het risico te beperken (passende technische en organisatorische maatregelen) aantoonbaar geïmplementeerd.		**X**
			10.3	Privacy by design wordt toegepast/geborgd (bijv. bij ontwikkelingen/ wijzigingen).		
			10.4	De verwerkingsverantwoordelijke kan aantonen dat de verwerking van politiegegevens wordt verricht in overeenstemming met wat bepaald is in de wet;		**X**
11	**Verwerker en Verwerkersovereenkomst**	Art 6c.1 en Art 6c, lid 2-5	11.1	Met verwerkers zijn de taken en afspraken schriftelijk vastgesteld en vastgelegd in een (toereikende) overeenkomst of andere rechtshandeling. Er zijn afspraken vastgesteld en vastgelegd m.b.t. de handelswijze bij een inbreuk op de beveiliging. *Wanneer de Verwerker een overheidsorganisatie betreft zijn verwerkersafspraken vastgelegd in een overeenkomst die minimaal de vereiste onderdelen bevatten die de wet voorschrijft.*		**X**

			11.2	Een andere partij is alleen ingeschakeld bij de uitvoering van de verwerking met toestemming van de verwerkingsverantwoordelijke. Aan deze andere verwerker (subverwerker) is bij een overeenkomst dezelfde verplichtingen inzake gegevensbescherming opgelegd.		
			11.3	De verwerker stelt de verwerkingsverantwoordelijke alle informatie ter beschikking die nodig is om aantoonbaar te maken dat aan de verplichtingen in de verwerkersovereenkomst worden nageleefd.		
12	**Geheimhoudingsplicht**	Art 7, lid 1-3	12.1	Er is geborgd dat de ambtenaar van politie of de persoon aan wie politiegegevens ter beschikking zijn gesteld formeel bekend is met de plicht tot geheimhouding en de consequenties bij schending van deze plicht.		
13	**Gegevensbeschermings-effectbeoordeling**	Art 4c, lid 1-3	13.1	Verwerkingen van politiegegevens zijn beoordeeld of ze een hoog risico voor de rechten en vrijheden van personen oplevert. De beoordeling is vastgelegd.		
			13.2	Indien een verwerking waarschijnlijk een hoog risico voor de rechten en vrijheden van personen oplevert wordt binnen de organisatie de risico's systematisch geïdentificeerd, beoordeeld en aangepakt door middel van een gegevensbeschermingseffectbeoordeling (GEB) die ten minste aan de eisen gesteld in de wet voldoet.		**X**
			13.3	De verwerkingsverantwoordelijke beoordeelt, indien nodig of wanneer sprake is van een verandering van het risico, of de verwerking in overeenstemming met de GEB wordt uitgevoerd en past de GEB zonodig aan.		
14	**Melding datalekken**	Art 33a lid 1-4 Art 33a lid 5-7	14.1	De organisatie detecteert en behandelt privacygerelateerde incidenten op gepaste wijze om de gevolgen te beperken en maatregelen te nemen om toekomstige inbreuken te voorkomen.		X
			14.2	De verantwoordelijkheden van de behandeling van datalekken zijn belegd in de organisatie, de daadwerkelijke uitvoering wordt beheerst, gedocumenteerd en geëvalueerd.		

			14.3	De melding van een datalek aan de AP vindt tijdig en volledig plaats.		
			14.4	Betrokkenen worden, indien vereist, tijdig en volledig in kennis gesteld van een inbreuk op de beveiliging als deze inbreuk waarschijnlijk een hoog risico voor hun rechten en vrijheden betekend.		X
Algemene bepalingen: alleen geautoriseerde medewerkers hebben toegang tot gegevens						
15	**Gegevensbescherming door standaardinstellingen**	Art 4b, lid 2	15.1	Er zijn passende technische en organisatorische maatregelen bepaald en geïmplementeerd zodat politiegegevens niet zonder tussenkomst van een natuurlijke persoon voor een onbeperkt aantal natuurlijke personen toegankelijk worden gemaakt.		
16	**Autorisaties en Toegang tot politiegegevens**	Art 6, lid 1-6 en 6a, lid 1-3	16.1	Er is een systeem van autorisaties dat voldoet aan de vereisten van zorgvuldigheid en evenredigheid. Dit houdt in dat: De verantwoordelijke heeft die personen die vanuit hun functie en de wet toegang mogen hebben tot bepaalde politiegegevens geautoriseerd voor alleen die gegevens (need-to-know). (Inclusief voor toezicht en controle, en technische werkzaamheden)		X
			16.2	Er is een proces voor het toewijzen, wijzigen en intrekken van autorisaties t.b.v. de toegang tot politiegegevens.		X
			16.3	Er vindt periodiek controle plaats van de autorisaties.		X
Verwerking van gegevens						
17	**Uitvoering van de dagelijkse politietaak**	Art 8	17.1	Geborgd is dat art 8 politiegegevens één jaar na de datum van de eerste verwerking zodanig worden opgeslagen (achter een schot worden geplaatst) dat ze alleen nog beschikbaar komen voor verdere verwerking op basis van de vergelijking van gegevens (hit-no-hit basis).		

18	**Geautomatiseerd vergelijken en in combinatie zoeken**	Art 11, lid 1, 2, 3 en 5 Art 11.4 Art 8.3	18.1	Geborgd is dat gegevens alleen geautomatiseerd worden vergeleken met andere politiegegevens of met andere dan politiegegevens binnen de richtlijnen gesteld in art 11.		**X**
			18.2	Geborgd is dat gegevens alleen in combinatie met elkaar worden verwerkt binnen de richtlijnen gesteld in art 11.4.		**X**
			18.3	Er is geborgd dat de ambtenaren die geautoriseerde zijn voor het geautomatiseerd vergelijken en in combinatie zoeken over voldoende kennis en vaardigheden beschikken.		**X**
19	**Ondersteunende taken**	Art 13, lid 1-4	19.1	Geborgd is dat voor de verwerkingen bedoeld in artikel 13.1, 13.2 en 13.2 Wpg, van tevoren is voldaan de schriftelijke vereisten (13.4 Wpg en 6:2 Bpg).		
20	**Ter Beschikking stellen (voor verdere verwerking)**	Art 4.1, 8.4, 9.3, 10.5, 12.2, 15, lid 1 en 2 en 15a lid 1 en 2	20.1	Geborgd is dat de verdere verwerking van artikel 9 en 10 gegevens alleen plaats vindt na toestemming (aantoonbaar) van de daartoe bevoegde functionaris.		
			20.2	Geborgd is dat de ter beschikking stellen van politiegegevens aan bevoegde autoriteiten in andere lidstaten van de Europese Unie of aan organen en instanties belast met de taken, bedoeld in artikel 1, onderdeel a conform de richtlijnen gesteld in de wet plaatsvindt.		

Verwerking van gegevens: gegevens worden niet langer bewaart dan noodzakelijk / toegestaan						
21	**Bewaartermijnen, verwijderen en vernietigen**	Art 4.2, 8.6, 9.4, 10.6, 12.6, 14 lid 1-4	21.1	Politiegegevens worden niet langer bewaard dan de minimale tijd die nodig is, zoals vereist door de toepasselijke wet- en regelgeving, of voor de doeleinden waarvoor deze zijn verwerkt. De verwerkingsverantwoordelijke voorziet in voldoende warborgen om te bewerkstelligen dat de gegevens conform de wet worden gecontroleerd, verwijderd en vernietigd.		x
			21.2	Geborgd is dat Politiegegevens na verwijdering maximaal vijf jaar worden bewaard. *Indien van cultureel of historisch belang kan worden afgezien van vernietiging van de gegevens. Er wordt dan aan de bewaareisen voldaan.*		
			21.3	Verwijderde gegevens worden alleen in bijzondere gevallen en indien voldaan wordt aan de vereisten gesteld in de wet ter beschikking gesteld voor hernieuwde verwerking.		
Verstrekking van gegevens						
22	**Verstrekking van politiegegevens aan anderen dan politie en Koninklijke marechaussee**	Art 16, 18, 19, 21 en 22 Art 7.1 (3) Art 4	22.1	Geborgd is dat politiegegevens alleen worden verstrekt aan personen of instanties buiten het politiedomein, voor zover dit noodzakelijk is voor de doeleinden zoals deze in de Wet politiegegevens en het Besluit politiegegevens zijn genoemd.		x
			22.2	Geborgd is dat wanneer gegevens verstrekt worden er wordt voldaan aan de documentatieplicht (conform 6:4 Bpg). Indien vereist is tevens de overeenstemming met het bevoegd gezag vastgelegd.		x
			22.3	Bij verstrekkingen is geborgd dat de ontvangende partij wordt gewezen op zijn geheimhoudingsplicht.		x

			22.4	De juistheid, volledigheid, actualiteit en betrouwbaarheid van politiegegevens bij verstrekking wordt, voor zover mogelijk, gecontroleerd en inzichtelijk gemaakt voor de ontvangende partij. Er is een procedure voor het onverwijld in kennis stellen van de ontvanger van politiegegevens indien geconstateerd wordt dat onjuiste politiegegevens zijn verstrekt of dat politiegegevens op onrechtmatig wijze zijn verstrekt.		
23	**Doorgiften aan derde landen**	Art 17a, lid 1–7	23.1	De doorgifte van gegevens aan verwerkingsverantwoordelijke in derde landen vindt alleen plaats indien er een adequaatheidsbesluit is van de Commissie van de Europese Unie of indien één van de uitzonderingsgronden zoals genoemd in de wet van toepassing is.		
			23.2	De doorgifte van gegevens aan derde landen wordt vastgelegd (documentatieplicht).		**X**
			23.3	Indien doorgifte plaatsvindt op basis van lid 2 onderdeel a of b, lid 3 of lid 5 is (aantoonbaar) voldaan aan de gestelde eisen in de wet.		
			23.4	Indien politiegegevens van een andere lidstaat afkomstig worden doorgegeven aan een derde landen is de toestemming van de verantwoordelijke autoriteit van dit lidstaat beschikbaar		

24	**Verstrekking aan derden structureel voor samenwerkingsverbanden**	Art 20, lid 1-2	24.1	De verantwoordelijke heeft inzicht in de samenwerkingsverbanden waarbij politiegegevens worden verstrekt.		
			24.2	In de beslissing voor het verstrekken van politiegegevens t.b.v. een samenwerkingsverband wordt vastgelegd: o Ten behoeve van welk zwaarwegend algemeen belang de verstrekking noodzakelijk is, o Ten behoeve van welk samenwerkingsverband de politiegegevens worden verstrekt, o Het doel waartoe dit is opgericht, o Welke gegevens worden verstrekt, o De voorwaarden onder welke de gegevens worden verstrekt en o Aan welke personen of instanties de gegevens worden verstrekt.		**X**
			24.3	De daadwerkelijke verstrekking van gegevens wordt vastgelegd.		
25	**Rechtstreekse verstrekking**	Art 23, lid 1-4	25.1	Indien er rechtstreekse verstrekkingen zijn deze rechtmatig (23.1, 23.2, 23.3), wordt voldaan aan de beveiligingseisen, en vinden (23.3) allen plaats aan de aangewezen persoon(en).		
	Rechten betrokkenen					
26	**Informatie aan de betrokkene, Recht op inzage, rectificatie en verwijdering**	Art 24a lid 1-4 en 24b lid 1-4 Art 25 lid 1-2, 26 lid 1–3, 27 lid 1–3, 28 lid 1–5	26.1	De verwerkingsverantwoordelijke biedt de betrokkene informatie over de verwerking van persoonsgegevens en doet dit beknopt, toegankelijk en duidelijk, zodat de betrokkene zijn rechten kan uitoefenen. De informatievoorziening voldoet aan de eisen gesteld in art 24b.1 en art 24b.2.		**X**
			26.2	Bij uitstel, beperking of achterwege laten van de verstrekking van informatie bedoeld in 24b.2 is de uitstel, beperking of achterwege laten alsmede de duur van deze maatregel onderbouwd.		

			26.3	Verzoeken tot inzage, rectificatie, vernietiging van betrokkenen wordt tijdig en adequaat afgehandeld. Dit houdt o.a. in dat de organisatie borgt dat bij een verzoek tot inzage (art 25.1) of rectificatie (art 28.1) de betrokkene zonder onnodige vertraging in kennis wordt gesteld van de ontvangst van het verzoek, de termijn voor uitsluitsel en de mogelijkheid een klacht in te dienen bij de AP.		X
			26.4	Een weigering gevolg te geven aan het verzoek conform art 24a.4 is onderbouwd. Elke weigering of beperking van de inzage wordt aan de betrokkene toegelicht, met vermelding van de feitelijke of juridische gronden die aan het besluit ten grondslag liggen.		
27	**Register**	Art 31d.1	27.1	De verwerkingsverantwoordelijke houdt een register bij van alle categorieën van verwerkingsactiviteiten die onder zijn verantwoordelijkheid plaatsvinden. Het register voldoet aan de eisen gesteld in de wet (lid 1a-j).		X
				Controle en Toezicht		
28	**Documentatie**	Art 32. lid 1-4	28.1	De verwerkingsverantwoordelijke borgt een volledige en toegankelijke schriftelijke vastlegging (documentatieplicht) van de onderdelen genoemd in art 32 lid 1. De bedoelde politiegegevens worden conform art 32 lid 4 bewaard.		X
			28.2	De schriftelijke melding van een gemeenschappelijke verwerking van politiegegevens aan de AP is geborgd.		
29	**Logging (1 en 2)**	Art 32a	29.1	De verwerkingsverantwoordelijke en de verwerker dragen zorg voor de logging van verwerkingen zoals opgenomen in art 32a lid 1 en gebruikt de logging uitsluitend ter controle van de rechtmatigheid van de gegevensverwerkingen, interne controles, ter waarborging van de integriteit en de beveiliging van politiegegevens en voor strafrechtelijke procedures. .		X
30	**Audits**	Art 33 lid 1-5	30.1	Er wordt uitvoering gegeven aan de eisen zoals gesteld in de Regeling Periodieke Audit politiegegevens.		X

31	**Privacyfunctionaris**	Art 34.1 Art 34.2	31.1	De verantwoordelijke heeft een privacyfunctionaris (PF) benoemt en verleent de PF toegang tot de politiegegevens die onder zijn beheer worden verwerkt.		**X**
			31.2	De PF ziet namens de verwerkingsverantwoordelijke toe op de verwerking van politiegegevens overeenkomstig het bij of krachtens de wet bepaalde.		**X**
			31.3	De PF houdt hiertoe een overzicht bij van de schriftelijke vastlegging van: o Doelen van het rechercheonderzoek (art 9) o Verstrekkingen o Feitelijke of juridische redenen die ten grondslag liggen aan een afwijzing o Inbreuk op de beveiliging van persoonsgegevens.		
			31.4	De privacyfunctionaris stelt jaarlijks een verslag op van zijn bevindingen.		
32	**Functionaris voor gegevensbescherming**	Art 36	32.1	Er is een functionaris voor gegevensbescherming aangesteld die toezicht houdt op: - het naleven van de WPG; - het beleid van de verwerkingsverantwoordelijke met betrekking tot de bescherming van persoonsgegevens; - de toewijzing van de autorisaties, bedoeld in artikel 6; - de bewustmaking en opleiding van de ambtenaren van politie betrokken bij de verwerking van politiegegevens; - de audits; - de uitvoering van de gegevensbeschermingseffectbeoordeling.		**X**
			32.2	De FG stelt jaarlijks een verslag op van zijn bevindingen en stelt het bekend aan de verwerkingsverantwoordelijke.		
33	**Algemeen (overkoepelend meerdere normen)**					

Auditdienst Rijk
Postbus 20201
2500 EE Den Haag