



Auditdienst Rijk
Ministerie van Financiën

Assurancerapport

Wpg hercontrole Belastingdienst (directies MKB,
P en GO excl. BEH)

Definitief

Colofon

Titel	Assurancerapport Wpg hercontrole Belastingdienst (directies MKB, P en GO excl. BEH)
Uitgebracht aan	Persoonsgegevens
Datum	22 februari 2024
Kenmerk	2024-0000173687

Inlichtingen
Auditdienst Rijk

Persoonsgegevens

Inhoud

1	Inleiding—4	
1.1	Aanleiding—4	
1.2	Context—4	
2	Oordeel en bevindingen hercontrole—6	
2.1	Oordelen en bevindingen hercontrole—6	
2.1.1	Directies MKB en P hebben op een aantal onderwerpen verbeteringen gerealiseerd echter nog niet op alle onderwerpen zijn verbeteringen in gang gezet.—6	
2.2	Bevindingen per onderwerp—7	
2.2.1	Reikwijdte (1)—7	
2.2.2	Doelbinding (2)—8	
2.2.3	Juistheid en volledigheid politiegegevens (4)—8	
2.2.4	Autorisaties en toegang tot politiegegevens (10)—8	
2.2.5	Onderscheid tussen verschillende categorieën van betrokkenen (12)—9	
2.2.6	Geheimhoudingsplicht (14)—9	
2.2.7	Uitvoering van de dagelijkse politietaak (16)—9	
2.2.8	Ondersteunende taken (19)—9	
2.2.9	Bewaartermijnen, verwijderen en vernietigen (20)—9	
2.2.10	Melding datalekken (30)—9	
3	Verantwoording onderzoek—10	
3.1	Werkzaamheden en afbakening—10	
3.1.1	Object van onderzoek en afbakening—10	
3.1.2	Criteria/normenkader—10	
3.2	Gehanteerde Standaard—11	
3.3	Verspreiding rapport—11	
4	Ondertekening—12	
	Bijlage Managementreactie	Persoonsgegevens —13

1 Inleiding

1.1 Aanleiding

De Wet politiegegevens (Wpg) is sinds 2007 van toepassing verklaard op de verwerking van persoonsgegevens die in het kader van de politietaak worden verwerkt. Naar aanleiding van de implementatie in 2019 van de Richtlijn gegevensbescherming politie & justitie, is de Wpg aangepast. Een van de aanpassingen betrof de reikwijdte van de Wet, waardoor de gegevensverwerking door boa's onder de Wpg is komen te vallen. Een en ander is uitgewerkt in het Besluit politiegegevens buitengewoon opsporingsambtenaar (Bpg boa). Vanaf 2019 vallen daarom de verwerkingen van politiegegevens door buitengewoon opsporingsambtenaren (boa's) in het kader van hun opsporingstaak onder de Wpg. De Wpg is daarmee van toepassing op de verwerking van politiegegevens door boa's die werkzaam zijn bij de directies GO, MKB en P van de Belastingdienst.

De Wpg schrijft voor dat de verwerkingsverantwoordelijke de naleving van de regels gesteld in de Wpg controleert door middel van periodieke audits, zowel intern als extern. De verwerkingsverantwoordelijke is verplicht om elk jaar een interne Wpg-audit uit te voeren en elke 4 jaar een externe Wpg-audit (hierna Privacy audit). De eerste Privacy audit moest echter twee jaar na inwerkingtreding worden uitgevoerd. Het resultaat van de Privacy audit moet worden gedeeld met de Autoriteit Persoonsgegevens (AP) als de bij wet aangestelde toezichthouder in Nederland.

De Wpg bepaalt dat de eerste Privacy audit twee jaar na inwerkingtreding moet worden uitgevoerd. De auditverplichting is met ingang van 01-01-2019 van kracht geworden voor (de werkgevers van) boa's. In juni 2023 is door de Auditdienst Rijk (ADR) de eerste Privacy audit uitgevoerd (kenmerk 2023-0000150445). De resultaten van deze audit zijn door de directies Midden- en Kleinbedrijf (MKB), Particulieren (P) en Grote Ondernemingen (GO) (excl. BEH) van de Belastingdienst gedeeld met de AP. De rapportage leidde tot een groot aantal bevindingen die middels een verbetertraject door de directies MKB, P, GO (excl. BEH) zijn opgepakt.

Door de directies MKB, P, en GO (excl. BEH) van Belastingdienst is aan de ADR gevraagd om de uitkomsten van het verbetertraject voor de geselecteerde bevindingen te beoordelen. Het uitvoeren van deze hercontrole is een wettelijke verplichting waarbij de verwerkingsverantwoordelijke een afschrift van de (her)controlesresultaten aan de AP dient te zenden.

De directies MKB, P en GO (excl. BEH) van de Belastingdienst zijn verantwoordelijk voor de opzet en het bestaan van de aanvullende beheersingsmaatregelen om alsnog te kunnen voldoen aan de bij of krachtens de Wpg bepaalde normen. Om voortgang daarvan te controleren, schrijft de Wpg een hercontrole voor binnen een jaar na de initiële externe Privacy audit. Omdat de AP vasthoudt aan de in de Wpg oorspronkelijk gestelde termijnen, dient de hercontrole eind 2023 plaats te vinden en daarmee voor de betrokken directies binnen een half jaar na de initiële Privacy audit, die 27 juni 2023 was opgeleverd door de ADR. De AP heeft de uitvoeringsorganisaties en daarmee de Belastingdienst de gelegenheid gegeven om het definitieve rapport van de hercontrole voor 1 maart 2024 in te dienen bij de AP.

1.2 Context

De Belastingdienst staat onder gezag van het Ministerie van Financiën en is verantwoordelijk voor het heffen en innen van rijksbelastingen, en andere bij of

krachtens de wet opgedragen taken (art. 2 Uitvoeringsregeling Belastingdienst 2003). De Belastingdienst is onderverdeeld in verschillende directies, waaronder GO, P en MKB. De Wpg en het bijbehorende Bpg-boa zorgen voor een evenwicht tussen de belangen die met de politietaak gemoeid zijn en de bescherming van de privacy van de burger.

Voor de boa's gelden verschillende toezichtsdomeinen. De boa's bij GO, P en MKB zijn aangesteld op het domein V, Werk, Inkomen en Zorg. Er is onderscheid tussen bestuursrechtelijke en strafrechtelijke handhaving bij de Belastingdienst. Eerstgenoemde valt onder de Algemene verordening gegevensbescherming (AVG) en daarmee buiten scope van dit onderzoek. Voor deze hercontrole zullen wij ons richten op processen en procedures die betrekking hebben op de verwerkingsactiviteiten die onder het regime van de Wpg vallen.

Bij de uitvoering van de verbeterpunten door MKB, P en GO (excl. BEH), zoals opgesteld in het verbeterrapport naar aanleiding van de initiële Privacy audit door de ADR, is na een interne analyse door GO, naar voren gekomen dat de boa's werkzaam binnen de directie GO, buiten het Bureau Economische Handhaving (BEH) geen boa-werkzaamheden binnen de directie GO verrichten die onder het regime van de Wpg vallen. Dit is vastgelegd in de notitie: "Analyse Boa activiteiten Grote Ondernemingen in relatie tot de Wet Politie Gegevens" d.d. 18 oktober 2023.

Gevolg hiervan is dat de directie GO bij nader inzien ook niet gehouden is om de in het verbeterrapport opgenomen maatregelen te treffen binnen de directie GO. GO doorloopt voor BEH een eigen Wpg-verbetertraject gebaseerd op de zelfstandige Privacy audit van de ADR bij BEH en de daarnaast daarbij behorende en separaat bij BEH uitgevoerde Hercontrole Wpg. Gevolg hiervan is dat de ADR zich bij de onderhavige hercontrole alleen richt op de beoordeling van de verbeteringen binnen de directies MKB en P.

2 Oordeel en bevindingen hercontrole

2.1 Oordelen en bevindingen hercontrole

2.1.1 Directies MKB en P hebben op een aantal onderwerpen verbeteringen gerealiseerd echter nog niet op alle onderwerpen zijn verbeteringen in gang gezet.

Wij hebben de beheersingsmaatregelen (normen), welke bij de initiële Privacy audit zijn beoordeeld als 'voldoet deels' of 'voldoet niet' én waarvan de -directies hebben aangegeven verbeteringen te hebben gerealiseerd van materieel belang, opnieuw beoordeeld. Naar ons oordeel zijn de beheersingsmaatregelen om te voorzien in de borging van de wettelijke eisen met betrekking tot de verwerking van politiegegevens door boa's van de betreffende directies (nog) niet op al deze 10 auditpunten afdoende wijze opgezet en ingericht (bestaan).

Wanneer in het licht van de gehele eerder uitgevoerde audit wordt gekeken, is te zien dat het opgestelde verbeterplan voor het wegwerken van tekortkomingen heeft geleid tot verbeteringen, maar dat deze nog niet allemaal zijn opgelost.

Bij de onderwerpen waar de directies MKB en P van de Belastingdienst wel al mee aan slag zijn gegaan (10 auditpunten die ook in de opdrachtbevestiging voor de hercontrole zijn vermeld, namelijk nr. 1, 2, 4, 10, 12, 14, 16, 19, 20, 30), zijn in opzet (grote) stappen gezet maar mist het nog, in een aantal gevallen, een verdere uitwerking en inrichting in het bestaan alsmede de controle hierop. Voor een aantal onderzochte normen hebben wij het bestaan dan ook nog niet kunnen vaststellen. De resultaten per onderwerp uit de hercontrole worden verder toegelicht in paragraaf 2.2.

Bij sommige onderwerpen waar tekortkomingen zijn geconstateerd tijdens de initiële Privacy audit, zijn door de directies aangegeven dat er nog geen verbeteringen zijn gestart van materieel belang. Deze onderwerpen zijn geen onderdeel van deze hercontrole en zijn in onderstaande tabel weergegeven als 'Niet Onderzocht' (NO). Voor deze onderwerpen blijven de bevindingen van de initiële Privacy audit staan.

Onderwerpen		IA			HC	
		O	B	W	O	B
1.	Reikwijdte					
2.	Doelbinding					
3.	Noodzakelijkheid en rechtmatigheid, vermelding herkomst				NO	NO
4.	Juistheid en volledigheid politiegegevens					
5.	Onderscheid feiten en oordeel				NO	NO
6.	Gegevensbescherming door beveiliging en ontwerp				NO	NO
7.	Gegevensbescherming door standaardinstellingen				NO	NO
8.	Gegevensbeschermingseffectbeoordeling / DPIA				NO	NO
9.	Bijzondere categorieën van politiegegevens				NO	NO
10.	Autorisaties en toegang tot politiegegevens					
11.	Autorisaties: aanwijzen functionarissen				NO	NO
12.	Onderscheid tussen verschillende categorieën van betrokkenen					
13.	Verwerker en Verwerkersovereenkomst				NO	NO
14.	Geheimhoudingsplicht					

15.	Geautomatiseerde individuele besluitvorming					NO	NO
16.	Uitvoering van de dagelijkse politietaak						
17.	Ter beschikking stellen van politiegegevens binnen het WPG-domein					NO	NO
18.	Geautomatiseerd vergelijken en in combinatie zoeken					NO	NO
19.	Ondersteunende taken						
20.	Bewaarttermijnen, verwijderen en vernietigen						
21.	Verstrekking van politiegegevens aan anderen dan politie en KMar					NO	NO
22.	Doorgiften aan derde landen					NO	NO
23.	Verstrekking aan derden structureel voor samenwerkingsverbanden					NO	NO
24.	Rechtstreekse verstrekking					NO	NO
25.	Informatie aan de betrokkene, recht op inzage, rectificatie en verwijdering					NO	NO
26.	Register					NO	NO
27.	Documentatie					NO	NO
28.	Logging					NO	NO
29.	Audits					NO	NO
30.	Melding datalekken						
31.	Functionaris voor gegevensbescherming					NO	NO
32.	Privacyfunctionaris					NO	NO

Toelichting gebruikte kleuren:

	Voldoet aan de beheersingsmaatregel (norm)
	Voldoet deels aan de beheersingsmaatregel (norm)
	Voldoet niet aan de beheersingsmaatregel (norm)
	Niet onderzocht (NO) of niet van toepassing (NVT)

Toelichting gebruikte afkortingen:

IA: Initiële Controle
 HC: Hercontrole
 O: Opzet
 B: Bestaan
 W: Werking
 NO: Niet onderzocht

2.2 Bevindingen per onderwerp

2.2.1 Reikwijdte (1)

Mede naar aanleiding van de resultaten uit de initiële Privacy audit, is vanuit het Wpg projectteam, verschillende boa-teams en vaktechnische coördinatoren geïnventariseerd welke verwerkingsactiviteiten met politiegegevens plaatsvinden. Er is geconcludeerd dat bij de directies MKB en P enkel sprake is van zogenaamde 'artikel 8 Wpg' verwerkingen. Deze verwerkingsactiviteit is gedocumenteerd middels een verwerkingsformulier, maar is nog niet opgenomen in het Wpg verwerkingsregister.

Door de directie MKB zijn procedures opgesteld voor de inrichting van een tijdelijke beveiligde digitale omgeving voor de registratie van AVG en Wpg-documenten (met politiegegevens). Verschillende werkprocessen zijn uitgeschreven, weliswaar nog niet allemaal met dezelfde diepgang en op hetzelfde niveau. Naar deze (uitgeschreven) werkprocessen wordt in een later stadium verwezen bij de entry in het register alsmede de soort gegevens die worden verwerkt. Het verwerken van het bsn vereist hierbij extra aandacht. Voor vastleggen van de verwerkingsactiviteiten van politiegegevens is gezamenlijk het formulier verwerken Wpg gegevens boa ontworpen. Elke directie is verantwoordelijk voor het gebruik en het toetsen daarvan. Aangegeven is dat deze werkwijze ook van toepassing is bij de directie P.

Met het beschrijven van deze verwerkingsactiviteiten van politiegegevens worden (onder meer) de doeleinden en de categorieën van betrokken vastgelegd. De inventarisatie van de verwerkingen en de opzet van de procesbeschrijving hebben geleid tot de beoordeling dat de werkzaamheden in het weegproces geheel vallen onder het regime van de AVG.

De directie MKB en P hebben het voornemen de controle op de werkinstructies en de opslag van de politiegegevens periodiek te gaan uitvoeren. Echter ontbreekt de entry in het register de verwerkingsactiviteiten.

Vandaar dat wij voor opzet en voor bestaan de kleur oranje hebben toegekend bij de hercontrole. Dit houdt in dat in opzet en bestaan deels aan de gestelde eis in de norm is voldaan.

2.2.2 *Doelbinding (2)*

Door middel van het verwerkingsformulier is het doel (en de grondslag) vastgelegd voor de medewerkers van MKB en P. Het ontbreekt echter aan een koppeling met de entry in het register van verwerkingsactiviteiten. Op welke manier controle wordt gehouden op de vastlegging van de doeleinden is tevens niet beschreven. Aangegeven is dat de controle op de vastlegging van het doeleinde per verwerking samen zou moeten vallen met de controle op uitgegeven autorisaties waarvan beschreven is dat de eerste controle uiterlijk 1 maart 2024 zou moeten plaatsvinden en de tweede controle uiterlijk oktober 2024. De directies zijn voornemens om daarna jaarlijks op/rond oktober van het jaar deze controle te herhalen. Dit houdt in dat in opzet en bestaan deels aan de gestelde eis in de norm is voldaan.

2.2.3 *Juistheid en volledigheid politiegegevens (4)*

Voor juistheid en volledigheid van de politiegegevens is recentelijk een procesbeschrijving opgesteld. In het verwerkingsformulier is beschreven dat de boa zorg dient te dragen dat de politiegegevens die worden verwerkt juist, volledig en actueel dienen te zijn. Als blijkt dat gegevens niet langer juist en compleet zijn, dan zullen deze onverwijld moeten worden gewijzigd of vernietigd. Op welke manier hier controle op wordt gehouden is echter niet beschreven. Aangegeven is dat de controle op juistheid en volledigheid samen zou moeten vallen met de controle op uitgegeven autorisaties waarvan beschreven is dat de eerste controle uiterlijk 1 maart 2024 zou moeten plaatsvinden en de tweede controle uiterlijk oktober 2024. De directies zijn voornemens om daarna jaarlijks op/rond oktober van het jaar deze controle te herhalen. Dit houdt in dat in opzet en bestaan deels aan de gestelde eis in de norm is voldaan.

2.2.4 *Autorisaties en toegang tot politiegegevens (10)*

Voor de uitgifte van autorisaties op de dossiers van de boa's wordt een Identity Management System (IMS) van de belastingdienst gebruikt. De specifieke autorisatiematrix en waarborgen ten aanzien van de autorisaties dienen voor de directies MKB en P beter beschreven te worden. Rapportages over de controle van het autorisatiebeheer zijn niet aangetroffen. Hiermee wordt in opzet voldaan en in het bestaan ten dele aan de norm voldaan.

Het werken met samenwerkingsgebieden op de Q:schijf voor de boa's is een tijdelijke oplossing. De autorisaties hierbinnen worden geregeld met autorisatiebeheer via IMS. Het beheer van autorisaties alsmede de manier waarop hier controle dient te worden gehouden is in opzet beschreven. Beschreven is dat de eerste controle uiterlijk 1 maart 2024 zou moeten plaatsvinden en de tweede controle uiterlijk oktober 2024. De directies zijn voornemens om daarna jaarlijks op/rond oktober van het jaar deze controle te herhalen.

- 2.2.5 *Onderscheid tussen verschillende categorieën van betrokkenen (12)*
Voor het onderscheid tussen verschillende categorieën van betrokkenen beschikken de directies MKB en P over een beschreven procedure waarbij onder andere gebruik gemaakt wordt van een formulier. In dit formulier wordt gevraagd om per zaak de verschillende categorieën van betrokkenen te benoemen. Wij hebben door middel van een bestaanscontrole vastgesteld dat de categorieën van betrokkenen worden vastgelegd. Dit houdt in dat in opzet en bestaan aan de norm wordt voldaan.
- 2.2.6 *Geheimhoudingsplicht (14)*
Het geformaliseerde uitgangspunt is dat boa's worden beëdigd. Hiermee wordt voldaan aan artikel 7 van de Wpg. Vastgesteld is dat boa's aktes aanwezig zijn. Dit houdt in dat in opzet en bestaan aan de norm wordt voldaan.
- 2.2.7 *Uitvoering van de dagelijkse politietaak (16)*
Na 1 jaar worden gegevens in een verder afgeschermd omgeving (achter schot) geplaatst. Dit is kort beschreven en uitgewerkt alsmede dat vervolgens deze gegevens gedurende 4 jaar alleen op basis van hit/no hit doorzocht mogen worden om te bezien of er verbanden zijn aan te tonen met andere verwerkingen. Daarnaast wordt voor het eerst in maart 2024 en vervolgens in oktober 2024 controle uitgevoerd. Deze zullen eerst handmatig worden uitgevoerd. Geautomatiseerd uitvoeren van de controle is een actie voor de lange termijn. Vandaar dat wij voor opzet en bestaan de kleur oranje hebben toegekend bij de hercontrole. Dit houdt in dat in opzet en bestaan deels aan de gestelde eis in de norm is voldaan.
- 2.2.8 *Ondersteunende taken (19)*
Naar aanleiding van de inventarisatie in samenwerking met vaktechnische coördinatoren is geconstateerd dat er geen artikel 13 verwerkingen plaatsvinden. Indien er in de toekomst wel artikel 13 gegevens verwerkt zullen worden, beschikken de directies over een beschreven protocol. Dit houdt in dat in opzet aan de gestelde eis in de norm is voldaan en voor bestaan is het hier niet van toepassing.
- 2.2.9 *Bewaartermijnen, verwijderen en vernietigen (20)*
Er zijn selectielijsten aanwezig en de bewaartermijnen zijn duidelijk vastgesteld in de Wpg. De boa wordt op de hoogte gesteld van de bewaartermijnen middels het formulier Wpg verwerking Boa MKB. De teamleider dient hierop controle uit te oefenen. Aangegeven is dat dit proces als zodanig nog niet formeel is beschreven. Wel wordt er verwezen naar een passage omtrent autorisaties waar staat beschreven dat de eerste controle plaatsvindt uiterlijk 1 maart 2024 en vervolgens uiterlijk oktober 2024 een tweede keer en daarna jaarlijks op/rond oktober van het jaar. Dit houdt in dat in opzet en bestaan deels aan de gestelde eis in de norm is voldaan.
- 2.2.10 *Melding datalekken (30)*
Meldingen van datalekken worden in het systeem Sharepoint opgeslagen. De toegang tot dit systeem is op basis van need to know ingericht. Er is een speciaal formulier ontworpen om datalekken te melden. Dit formulier wordt Belastingdienst breed toegepast. Eveneens kan in het formulier worden aangegeven of de melding betrekking heeft op het AVG- of Wpg-domein.
Het bestaan kunnen wij op dit moment niet vaststellen. Aangegeven is dat tot op heden geen meldingen van datalekken hebben plaatsgevonden die betrekking hebben op het Wpg-domein. Dit houdt in dat in opzet aan de gestelde eis in de norm is voldaan en voor bestaan is het hier niet van toepassing.

3 Verantwoording onderzoek

3.1 Werkzaamheden en afbakening

3.1.1 Object van onderzoek en afbakening

Object van onderzoek

Het object van onderzoek van deze audit bestaat uit de beoordeling van de procedures en maatregelen die de betreffende directies hebben getroffen naar aanleiding van de geconstateerde tekortkomingen tijdens de initiële Privacy Audit. De betreffende directies hebben aangegeven op basis van de aanbevelingen per 1 december 2023 in opzet en bestaan verbetermaatregelen te hebben gerealiseerd op de onderwerpen:

1. Reikwijdte
2. Doelbinding
4. Juistheid en volledigheid politiegegevens
10. Autorisaties en toegang tot politiegegevens
12. Onderscheid verschillende categorieën van betrokkenen
14. Geheimhoudingsplicht
16. Uitvoering van de dagelijkse politietaak
19. Ondersteunende taken
20. Bewaartermijnen, verwijderen en vernietigen
30. Melding datalekken

Afbakening

De ADR geeft geen overall beeld over de mate waarin de organisatie voldoet aan de Wpg, enkel de bovengenoemde onderwerpen. De onderwerpen waar tijdens de initiële Privacy Audit wel tekortkomingen zijn geconstateerd maar waarvoor de betreffende directies niet hebben aangegeven dat verbetering is gerealiseerd, worden niet meegenomen in de scope van het onderzoek.

De ADR verricht geen onderzoek naar door derden aan de betreffende directies geleverde faciliteiten, voor zover de verantwoordelijkheid is belegd bij anderen dan de betreffende directies. In dergelijke gevallen wordt wel gekeken naar de gemaakte afspraken tussen de partijen en de regie vanuit de betreffende directies gericht op de realisatie van de afspraken.

3.1.2 Criteria/normenkader

Met de opdrachtgever is afgestemd dat het onderzoek wordt uitgevoerd aan de hand van het toetsingskader dat gebaseerd is op de in de Wpg en Bpg gestelde eisen evenals de NOREA Handreiking Privacy audit Wet politiegegevens (Wpg) voor Boa's. Het relevante deel van het toetsingskader is in bijlage 1 opgenomen.

De (generieke) algehele beheersingsdoelstelling voor de privacy audit Wpg voor boa's is het voorzien in de borging van de wettelijke eisen met betrekking tot de verwerking van politiegegevens door boa's. Hiertoe heeft de organisatie beheersingsmaatregelen getroffen die in opzet en bestaan door de IT-auditor worden getoetst. De IT-auditor maakt bij deze hercontrole gebruik van de volgende criteria:

Opzet	De organisatie heeft de beheersingsmaatregelen beschreven die, indien deze werken zoals beschreven, een redelijke mate van zekerheid bieden dat voorzien is aan de borging van de wettelijke eisen met betrekking tot de verwerking van politiegegevens door boa's.
Bestaan	De organisatie heeft de beheersingsmaatregelen overeenkomstig de opzet daadwerkelijk geïmplementeerd en toegepast.

3.2 Gehanteerde Standaard

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

3.3 Verspreiding rapport

De opdrachtgever Persoonsgegevens is eigenaar van dit rapport en dient ingevolge artikel 33 2e lid van de Wpg een afschrift van de controleresultaten van deze hercontrole aan de Autoriteit persoonsgegevens te zenden.

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.

4 Ondertekening

Den Haag, 22 februari 2024

Persoonsgegevens

Auditdienst Rijk

Bijlage | Managementreactie

Persoonsgegevens

Persoonsgegevens



> Retouradres Postbus 20201 2500 EE Den Haag

Auditdienst Rijk

Persoonsgegevens

Postbus 20201
2500 EE Den Haag

Persoonsgegevens

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

Inlichtingen

Persoonsgegevens

www.mfin.nl

Ons kenmerk

2024-0000173770

Uw brief (kenmerk)

Assurancerapport Wpg
hercontrole Belastingdienst
(directies MKB, P & GO (excl.
BEH), d.d. 20 februari 2024

Datum 22-02-2024

Betreft Managementreactie bij Assurancerapport
Wpg hercontrole Belastingdienst (directies MKB, P & GO
(excl. BEH))

Geachte Persoonsgegevens

De Belastingdienst dankt de Auditdienst Rijk (ADR) voor het uitvoeren van de wettelijk verplichte Wpg hercontrole en dit hercontrole rapport.

De ADR heeft samen met de betrokken directies 10 van de 32 oorspronkelijke auditpunten aangemerkt als te onderzoeken normen voor de Wpg hercontrole. Daarbij heeft de ADR aangegeven dat wordt beoordeeld of door de opvolging van de bevindingen voor de geselecteerde normen per 1 december 2023 in voldoende mate is geborgd dat in opzet en bestaan wordt voldaan aan de desbetreffende wetsartikelen van de Wpg.

De ADR stelt vast op basis van door de directie Grote Ondernemingen (GO) verstrekte informatie, die voortvloeit uit een door GO gedane analyse, dat de werkzaamheden van de buitengewoon opsporingsambtenaren (boa's) van GO (exclusief Bureau Economische Handhaving) niet onder het Wpg regime vallen. Het gevolg hiervan is dat de ADR in hoofdstuk 2 van haar rapport (Oordeel en bevindingen hercontrole), geen toets met betrekking tot GO heeft uitgevoerd.

Voor wat betreft de directies Midden- en Kleinbedrijf (MKB) en Particulieren (P), geeft de ADR aan: "Naar ons oordeel zijn de beheersingsmaatregelen om te voorzien in de borging van de wettelijke eisen met betrekking tot de verwerking van politiegegevens door boa's van de betreffende directies (nog) niet op al deze 10 auditpunten afdoende wijze opgezet en ingericht (bestaan)."

Daarbij merkt de ADR op dat bij de onderwerpen waarop verbeteringen zijn doorgevoerd in opzet (grote) stappen zijn gezet maar mist het nog, in een aantal gevallen, een verdere uitwerking en inrichting in het bestaan alsmede de controle hierop.

De directies MKB en P herkennen zich in de bevindingen van de ADR, waaronder de constatering dat er (grote) stappen voorwaarts zijn gezet tussen de initiële privacy-audit Wpg op 27 juni 2023, het verbeterrapport op 27 september 2023 en het moment waarop de hercontrole is uitgevoerd, de status van 1 december 2023.

We zien voortgang waarbij de periode voor het kunnen doorvoeren van verbeteringen te kort is geweest om alle verbeterpunten volledig te implementeren. We realiseren ons dat we de komende periode flinke inspanningen moeten verrichten om op alle punten te voldoen aan de Wpg en zullen de door de ADR gedane adviezen en aanbevelingen waar nodig toevoegen aan het verbeter**rapport**.

Hoochachtend

Persoonsgegevens

Persoonsgegevens

Ons kenmerk
2024-0000173770

Auditdienst Rijk
Postbus 20201
2500 EE Den Haag
Persoonsgegevens