Auditdienst Rijk
Ministerie van Financiën

Assurancerapport Wpg hercontrole Bureau Economische Handhaving

Definitief

Colofon

Titel	Wpg hercontrole Bureau Economische Handhaving
Uitgebracht aan	Persoonsgegevens
Datum	22 februari 2024
Kenmerk	2024-0000184220

Inlichtingen
Auditdienst Rijk
Persoonsgegevens

Inhoud

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 inwerkingtrede van de Algemene verordening gegevensbescherming (AVG) in 2018, is de Wpg in 2019 aangepast en is het Besluit politiegegevens buitengewoon opsporingsambtenaar (Bpg boa) in werking getreden. Vanaf dat moment vallen buitengewone opsporingsambtenaren (boa's) die voor hun opsporingstaak persoonsgegevens verwerken onder de Wpg. De Wpg is daarmee van toepassing op de taken van het Bureau Economische Handhaving (BEH) 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. Werkgevers van boa's zijn verplicht om elk jaar een interne Wpg-audit te doen en elke 4 jaar een externe Wpg-audit (hierna Privacy audit). 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 inwerkintreding moet worden uitgevoerd. De auditverplichting is met ingang van 01-01-2019 van kracht geworden voor (de werkgevers van) boa's. In november 2022 is door de Auditdienst Rijk (ADR) de eerste Privacy audit uitgevoerd (kenmerk 2022-0000323799). De resultaten van deze audit zijn door de BEH gedeeld met de AP. De rapportage leidde tot een groot aantal bevindingen die middels een verbetertraject door BEH is opgepakt.

Door het BEH 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)controleresultaten aan de AP dient te zenden.

Het BEH is verantwoordelijk voor de opzet en het bestaan van de aanvullende beheersingsmaatregelen om alsnog te kunnen voldoen aan het bij of krachtens de Wpg bepaalde binnen een jaar na de initiële externe privacy audit[1].

1.2 Context

Het BEH valt organisatorisch onder Belastingdienst/Grote ondernemingen. Zij is belast met niet-fiscale toezichts- en opsporingstaken. Het BEH voert een achttal toezichts- en opsporingstaken uit, waarvan de volgende vier in het kader van de verplichtende Wpg audit voor Boa's onderzocht zullen worden:

1. Opsporing van overtredingen van artikel 2:394, derde lid Burgerlijk Wetboek (het niet of niet tijdig openbaar maken van de jaarrekening door een rechtspersoon).
2. Toezicht op de naleving van de artikelen 47 en 48 van de Wet op het consumentenkrediet. Alsmede opsporing van overtredingen van voorschriften in het kader van het verbod op het verrichten van schuldbemiddeling tegen betaling.

[1] Artikel 33 Wet politiegegevens en Artikel 4 Regeling periodieke audit politiegegevens.

3. Opsporing van overtredingen van de artikelen 340 en verder (Tweede Boek, Titel XXVI. Benadeling van schuldeisers of rechthebbenden) van het wetboek van Strafrecht (eenvoudige of bedrieglijke bankbreuk door failliet of bestuurder(s)/commissaris(sen) van failliete rechtspersonen).
4. Opsporing van overtredingen van voorschriften, gesteld bij of krachtens artikel 27 en 47 van de Handelsregisterwet 2007 (het in strijd handelen met dan wel niet voldoen aan de inschrijfplicht door de onderneming of rechtspersoon).

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.

2 Oordelen en bevindingen hercontrole

2.1 BEH heeft op een aantal onderdelen verbeteringen gerealiseerd echter nog niet op alle onderwerpen zijn verbeteringen in gang gezet

Wij hebben de beheersingsmaatregelen, welke bij de initiële privacy audit zijn beoordeeld als 'voldoet deels' of 'voldoet niet' én waarvan de organisatie heeft aangegeven verbeteringen te hebben gerealiseerd van materieel belang, opnieuw beoordeeld. Naar ons oordeel zijn de algehele beheersingsmaatregelen om te voorzien in de borging van de wettelijke eisen met betrekking tot de verwerking van politiegegevens door boa's door het BEH niet op afdoende wijze in opzet en bestaan ingevuld. Het BEH voldoet hiermee, ondanks gerealiseerde verbetermaatregelen op een aantal onderwerpen, niet aan de Wpg.

Wanneer in het licht van de gehele eerdere uitgevoerde audit wordt gekeken, is te zien dat het opgestelde verbeterplan tot het wegwerken van tekortkomingen heeft geleid maar dat deze niet allemaal zijn opgelost. Bij de onderwerpen waar het BEH wel mee aan slag is gegaan, zijn in opzet grote stappen gezet maar mist nog in een aantal gevallen een verdere uitwerking in het bestaan alsmede de controle hierop. De resultaten per onderwerp uit hercontrole worden verder toegelicht in paragraaf 2.2.

Bij sommige onderwerpen waar tekortkomingen zijn geconstateerd tijdens de initiële audit, is door BEH 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 audit staan.

	Onderwerpen	Initiële audit			Her-controle	
		O	B	W	O	B
1.	Reikwijdte					
2.	Doelbinding					
3.	Noodzakelijkheid en rechtmatigheid, vermelding herkomst					
4.	Juistheid en volledigheid politiegegevens					
5.	Onderscheid feiten en oordeel					
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					
12.	Onderscheid tussen verschillende categorieën van betrokkenen					
13.	Verwerker en Verwerkersovereenkomst					
14.	Geheimhoudingsplicht				NO	NO
15.	Geautomatiseerde individuele besluitvorming	Nvt				
16.	Uitvoering van de dagelijkse politietaak	Nvt				
17.	Ter beschikking stellen van politiegegevens binnen het WPG-domein	Nvt				
18.	Geautomatiseerd vergelijken en in combinatie zoeken	Nvt				
19.	Ondersteunende taken	Nvt				

20.	Bewaartermijnen, verwijderen en vernietigen						
21.	Verstrekking van politiegegevens aan anderen dan politie en KMar	Nvt					
22.	Doorgiften aan derde landen	Nvt					
23.	Verstrekking aan derden structureel voor samenwerkingsverbanden	Nvt					
24.	Rechtstreekse verstrekking	Nvt					
25.	Informatie aan de betrokkene, recht op inzage, rectificatie en verwijdering					NO	NO
26.	Register						
27.	Documentatie						
28.	Logging					NO	NO
29.	Audits						
30.	Melding datalekken					NO	NO
31.	Persoonsgegevens						

Toelichting gebruikte kleuren:

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

2.2 Bevindingen per onderwerp

2.2.1 *Reikwijdte (1)*

De verwerkingsverantwoordelijke heeft bestanden met politiegegevens binnen de organisatie geïdentificeerd en vastgelegd in een Exel overzicht dat periodiek wordt geactualiseerd. Hier mee wordt in opzet en bestaan aan de gestelde eis in de norm voldaan.

2.2.2 *Doelbinding (2)*

In het Kwaliteitshandboek Wet politiegegevens voor BEH staat beschreven dat bij het verwerken van politiegegevens altijd sprake is van doelbinding en dat de gegevens niet op een onrechtmatige wijze worden verwerkt. Hiermee wordt aan de opzet voldaan. Controles, zoals ook in de opzet omschreven, worden niet uitgevoerd waardoor niet aan de gestelde eis in de norm wordt voldaan voor het bestaan.

2.2.3 *Noodzakelijkheid & rechtmatigheid, vermelding herkomst (3)*

In het Kwaliteitshandboek is per werkproces de noodzakelijkheid en rechtmatigheid opgenomen. Artikel 9 onderzoeken worden niet meer door het BEH uitgevoerd. Deze onderzoeken zijn ook niet meer in het handhavingsarrangement opgenomen. Controles worden op dit moment nog niet uitgevoerd. Controle op de herkomst van gegevens die via de Signalen Postbus binnenkomen is niet ingericht. Hiermee wordt in opzet aan de gestelde eis in de norm voldaan maar niet in het bestaan.

2.2.4 *Juistheid en volledigheid politiegegevens (4)*

In de werkbeschrijvingen zoals opgenomen in het Kwaliteitshandboek zijn de te implementeren werkwijzen aangaande de juistheid en volledigheid beschreven waarmee in opzet wordt voldaan. Uitkomsten van controles en rapportages zijn niet voorhanden. Met ingang van 2024 zal een Interne Controle-plan worden opgesteld. Er wordt nu niet aan het bestaan in de norm voldaan.

2.2.5 *Onderscheid feiten en persoonlijk oordeel (5)*

In het Handboek beschreven voorgenomen werkwijze wordt middels invulvelden in processenverbaal onderscheid tussen feiten en persoonlijk oordeel afgedwongen. Ook geeft het praktijkhandboek WPG dat door de BOA's wordt gebruikt aandacht aan het onderscheid waarmee in opzet aan de norm wordt voldaan. Doordat de

werkwijze nog niet effectief is en controles ontbreken wordt niet aan het bestaan voldaan.

2.2.6 *Autorisaties en toegang tot politiegegevens (10)*

Voor de uitgifte van autorisaties op de dossiers van de BOA's wordt een Identity Management System van de belastingdienst gebruikt. De specifieke autorisatiematrix en waarborgen ten aanzien van de autorisaties dienen voor BEH beter beschreven te worden. Periodieke controles en rapportages over het autorisatiebeheer zijn niet aangetroffen. Hiermee wordt in opzet ten dele en in het bestaan niet aan de norm voldaan.

2.2.7 *Autorisaties: aanwijzen functionarissen (11)*

In het Kwaliteitshandboek worden rol en taken van Bevoegd functionaris (BF) beschreven. Een aangewezen bevoegde functionaris is niet benoemd waarmee in opzet wel maar in het bestaan niet aan de norm wordt voldaan.

2.2.8 *Onderscheid tussen verschillende categorieën van betrokkenen (12)*

In het handboek zijn de categorieën van betrokken bij de BEH onderzoeken (BOA of bestuurder/rechtspersoon) opgenomen. Wij hebben vastgesteld dat dit onderscheid in het proces-verbaal wordt opgenomen waarmee in opzet en bestaan aan de gestelde eis in de norm wordt voldaan.

2.2.9 *Verwerker en verwerkersovereenkomst (13)*

In het register van verwerkingsactiviteiten zijn vermeldingen voor artikel 8 en artikel 9 verwerkingen aangetroffen. Bij beide vermeldingen is aangegeven dat er geen sprake is van verwerkers en daardoor geen verwerkersovereenkomsten noodzakelijk zijn. In het handboek staan de uitgangspunten aangaande verwerkers en verwerkingsovereenkomsten van het BEH beschreven waarmee de opzet aan de gestelde eis in de norm wordt voldaan.

2.2.10 *Bewaartermijnen, verwijderen en vernietigen (20)*

In het handboek is de werkbeschrijving proces bewaren, verstrekken, verwijderen en vernietigen politiegegevens opgenomen waarin de bewaar- en vernietigingstermijn zijn opgenomen. Aantoonbare controles op de bewaar- en vernietigingstermijnen zijn niet aangetroffen waarmee in opzet maar nog niet in het bestaan aan de norm wordt voldaan.

2.2.11 *Register (26)*

In het register van verwerkingsactiviteiten zijn 2 vermeldingen aangetroffen één voor de opsporing overtredingen (economische delicten) (art 8 Wpg) en één voor de opsporing misdrijven (economische delicten) (art 9 Wpg) waarmee in opzet aan de norm wordt voldaan. Op enkele gegevens na zijn deze vermeldingen volledig zodat in het bestaan ten dele aan de norm wordt voldaan.

2.2.12 *Documentatie (27)*

Wij hebben vastgesteld dat in opzet de schriftelijke vastlegging van de onderdelen genoemd in art 32 lid 1 middels procesbeschrijvingen is vastgelegd. Een overzicht van verstrekkingen, meldingen datalekken en inzage verzoeken hebben wij niet in het dossier aangetroffen waardoor in opzet wel maar in het bestaan nog niet aan de norm wordt voldaan.

2.2.13 *Audits (29)*

Wij hebben vastgesteld dat externe- en interne audits periodiek worden uitgevoerd dan wel dat deze gepland zijn opgenomen in de auditkalender. De eerste jaarlijkse interne audit zal plaatsvinden in het eerste kwartaal 2024. Met ingang van 2024 wordt aanvullend het Interne Controle-plan (kortheidshalve IC-plan) opgesteld. Hiermee wordt in opzet en bestaan aan de norm voldaan.

2.2.14 Persoonsgegevens *(31)*

Wij hebben vastgesteld dat een Persoonsgegevens is aangesteld. Een jaarlijks verslag van de bevindingen van P-gv over de het naleven van de WPG, het beleid van de verwerkingsverantwoordelijke met betrekking tot de bescherming van persoonsgegevens, de toewijzing van de autorisaties, bedoeld in art 6, de bewustmaking en opleiding van de ambtenaren van politie betrokken bij de verwerking van politiegegevens, de audits en de uitvoering van de DPIA's is niet aangetroffen. Wel is een verslag van een afstemmingsoverleg van het BEH met de P-gv over eerdere audits en bevindingen aangetroffen. Hiermee wordt in opzet maar niet in het bestaan aan de norm voldaan.

3 Verantwoording onderzoek

3.1 Werkzaamheden en afbakening

3.1.1 Object van onderzoek

Het object van onderzoek van deze audit bestond uit de beoordeling van de procedures en maatregelen die het BEH heeft getroffen naar aanleiding van de geconstateerde tekortkomingen tijdens de initiële Privacy Audit. Het BEH heeft 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
3. Noodzakelijkheid en rechtmatigheid politiegegevens
4. Juistheid en volledigheid politiegegevens
5. Onderscheid feiten en oordeel
10. Autorisaties en toegang tot politiegegevens
11. Autorisaties: aanwijzen functionarissen
12. Onderscheid verschillende categorieën van betrokkenen
13. Verwerker en verwerkersovereenkomst
20. Bewaartermijnen, verwijderen en vernietigen
26. Register
27. Documentatie
29. Audits
32. Persoonsgegevens

De ADR geeft in dit rapport geen overall beeld betreft 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 waar het BEH geen verbetermaatregelen heeft volbracht, zijn niet meegenomen in scope van onderzoek. De bevindingen op die onderwerpen tijdens de initiële audit blijven staan. Tevens doen wij geen uitspraak over de werking van de gerealiseerde verbetermaatregelen[2].

3.1.2 Criteria

Het onderzoek is uitgevoerd met 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.

Wij hebben uitsluitend onderzoek uitgevoerd naar de bij de initiële privacy audit als 'deels' of 'niet voldoende' in opzet en bestaan beoordeelde beheersingsmaatregelen én waarvan de organisatie heeft aangegeven verbeteringen te hebben gerealiseerd van materieel belang. Wij hebben geen onderzoek gedaan naar de bij de initiële audit niet beoordeelde normen en doen daar derhalve ook geen uitspraak over. Tevens doen wij geen uitspraak over de werking van de gerealiseerde verbetermaatregelen[3].

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

[2] De hercontrole heeft in beginsel alleen betrekking op opzet en bestaan, omdat de tijdspanne om een gewogen oordeel te geven over de werking in veel gevallen te kort zal zijn.
[3] De hercontrole heeft in beginsel alleen betrekking op opzet en bestaan, omdat de tijdspanne om een gewogen oordeel te geven over de werking in veel gevallen te kort zal zijn.

worden getoetst. De IT-auditor maakt bij deze hercontrole gebruik van de volgende criteria:

Opzet	De organisatie heeft de beheersingsmaatregen 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 BEH

Ministerie van Financiën

> Retouradres Postbus 19266 3501 DG Utrecht

Auditdienst Rijk
Account FIN/EZK/LNV
Persoonsgegevens
Postbus 20701
2500 CW Den Haag
Nederland

BELASTINGDIENST/ DIRECTIE GROTE ONDERNEMINGEN
Croeselaan 14
3521 CA Utrecht
Postbus 19500
3501 CM Utrecht
Inlichtingen
Persoonsgegevens

Ons kenmerk
2024-0000173470
Uw brief (kenmerk)

Bijlagen
Assurancerapport WPG
Hercontrole Bureau
Economische Handhaving

Datum 20 februari 2024
Betreft Managementreacties bij Assurancerapport WPG hercontrole Bureau Economische Handhaving

Geachte Persoonsgegevens

Ik onderschrijf de bevindingen van het onderzoek van de Audit Dienst Rijk (ADR) naar de opvolging van de bevindingen door het Bureau Economische Handhaving (BEH) uit de initiële privacy audit. Het onderzoek geeft een goed inzicht in hoe door BEH uitvoering is en wordt gegeven aan de opvolging van de bevindingen die tijdens de initiële Privacy Audit zijn geformuleerd.

In aanloop naar en op basis van de initiële auditrapportage van 20 december 2022 heb ik direct maatregelen genomen om de hoogste risico's te mitigeren. Op 20 maart 2023 is een integrale verbeterrapportage vastgesteld.

De ADR heeft op verzoek 14 van de 32 in de initiële audit opgenomen onderdelen beoordeeld. U heeft daarbij beoordeeld of de getroffen procedures en maatregelen per 1 december 2023 in opzet en bestaan in voldoende mate borgen dat wordt voldaan aan de wettelijke vereisten van de Wpg. Uw conclusie is dat de opzet van 13 procedures en maatregelen als voldoende beoordeeld wordt en één deels.

Hoewel er in de afgelopen periode naar mijn mening stevige stappen zijn gezet, ben ik met u van mening dat er nog noodzakelijke stappen moeten volgen om de procedures en maatregelen te implementeren (bestaan). Dat lag ook in de lijn der verwachting. Ik span mij in om voor 1 september 2024 deze concrete verbeteringen te hebben geïmplementeerd met als doel te voldoen aan de wettelijke vereisten van de Wpg. Voor de realisatie van alle verbeteringen is ook een goede ondersteunende ICT voorziening noodzakelijk. De ontwikkeling daarvan is afhankelijk van schaarse en tijdige beschikbaarheid van ICT-capaciteit.

Hoogachtend,

Persoonsgegevens

Pagina 1 van 1

Auditdienst Rijk
Postbus 20201
2500 EE Den Haag
Persoonsgegevens