Auditdienst Rijk
Ministerie van Financiën

Assurance-rapport
Privacy audit Wet politiegegevens (Wpg) betreffende de directies P, MKB en GO van de Belastingdienst

Verslagperiode 1 januari 2019 – 31 december 2021

Colofon

Titel	Privacy audit Wet politiegegevens (Wpg) betreffende de directies P, MKB en GO van de Belastingdienst
Uitgebracht aan	Persoonsgegevens
Datum	27 juni 2023
Kenmerk	2023-0000150445
Referentienummer	

Inlichtingen
Auditdienst Rijk
Persoonsgegevens

Inhoud

Algemeen

Voor u ligt het assurance-rapport inzake het onderzoek naar de politiegegevens. Dit onderzoek ziet toe op de politiegegevens die door de buitengewoon opsporingsambtenaren (boa's) van de directie Grote Ondernemingen (GO), directie Particulieren (P) en directie Midden- en Kleinbedrijf (MKB) van de Belastingdienst[1] worden verwerkt. Het betreft verwerkingen die in een bestand zijn opgenomen, en/of daarin opgenomen hadden moeten worden. Deze verwerkingen vallen onder de reikwijdte van de Wet politiegegevens (Wpg) en het Besluit politiegegevens voor buitengewoon opsporingsambtenaren (Bpg boa). Dit rapport is gebaseerd op Richtlijn 3000D van de NOREA (Assurance-opdrachten door IT-auditors) en is opgesteld door de Auditdienst Rijk. In dit rapport zijn de door ons vastgestelde bevindingen en aanbevelingen beschreven.

[1] Voor de directie Grote Ondernemingen (GO) is dit onderzoek exclusief Bureau Economische Handhaving (BEH) opgesteld, omdat BEH in 2022 een aparte privacy audit door de ADR heeft laten uitvoeren.

De directies P, MKB, GO van de Belastingdienst voldoen in belangrijke mate niet aan de Wpg

Het doel van dit assurance-onderzoek is met een redelijke mate van zekerheid een oordeel te geven of door de directies Grote Ondernemingen (GO)[2], Particulieren (P) en Midden- en Kleinbedrijf (MKB) van de Belastingdienst (hierna: de betreffende directies) op adequate wijze uitvoering is gegeven aan de bepalingen van de Wpg. Dit hebben wij vastgesteld voor de periode 1 januari 2019 t/m 31 december 2021.

Afkeurend oordeel

Op basis van de significantie van de aangelegenheid die staat beschreven in de sectie 'De basis voor ons afkeurend oordeel', zijn wij tot de conclusie gekomen dat de betreffende directies van de Belastingdienst in de periode 1 januari 2019 t/m 31 december 2021 in belangrijke mate niet voldeden aan de Wpg.

De basis voor ons afkeurend oordeel

Uit ons onderzoek komt naar voren dat de betreffende directies in de periode 1 januari 2019 t/m 31 december 2021 in belangrijke mate niet voldeden aan de Wpg onderwerpen in opzet, bestaan en/of effectieve werking. In tabel 1 is een toelichting van de gebruikte kleuren opgenomen, in tabel 2 een overzicht van conclusies per Wpg-onderwerp.
Het oordeel betreft een afkeurend onderdeel om de reden dat de betreffende directies van de Belastingdienst onvoldoende konden aantonen dat zij voldoen aan de Wpg-onderwerpen. De bestanden met politiegegevens zijn niet volledig geïdentificeerd en gedocumenteerd. Tevens ontbreken er uitgangspunten aangaande noodzakelijkheid, rechtmatigheid, juistheid en volledigheid van politiegegevens. Ook zijn bewaar-, verwijder- en vernietigstermijnen niet aantoonbaar inzichtelijk gemaakt.

Tabel 1: Toelichting gebruikte kleuren

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 wanneer de opzet niet voldoende duidelijk is, kan het bestaan en de werking niet gecontroleerd worden.	
De norm is niet van toepassing of de maatregel is niet gecontroleerd tijdens het onderzoek.	

Tabel 2: Overzicht conclusie per Wpg-onderwerp

Nr.	Norm	Key control	Conclusie		
			Opzet	Bestaan	Werking
1.	Reikwijdte	X			
2.	Doelbinding	X			

[2] Directie Grote Ondernemingen is exclusief Bureau Economische Handhaving (BEH) omdat daar reeds een separate privacy audit voor is opgesteld.

Nr.	Norm	Key control	Conclusie		
			Opzet	Bestaan	Werking
3.	Noodzakelijkheid & rechtmatigheid politiegegevens				
4.	Juistheid en volledigheid politiegegevens				
5.	Onderscheid feiten en persoonlijk oordeel				
6.	Gegevensbescherming door beveiliging en ontwerp	X			
7.	Gegevensbescherming door standaardinstellingen				
8.	Gegevensbeschermingseffectbeoordeling/ DPIA	X			
9.	Bijzondere categorieën van politiegegevens	X			
10.	Autorisaties en toegang tot politiegegevens	X			
11.	Autorisaties: aanwijzen functionarissen				
12.	Onderscheid tussen verschillende categorieën van betrokkenen				
13.	Verwerker en verwerkersovereenkomst	X			
14.	Geheimhoudingsplicht				
15.	Geautomatiseerde individuele besluitvorming				
16.	Uitvoering van de dagelijkse politietaak				
17.	Ter beschikking stellen van politiegegevens binnen het Wpg-domein				
18.	Geautomatiseerd vergelijken en in combinatie zoeken	X			
19.	Ondersteunende taken				
20.	Bewaartermijnen, verwijderen en vernietigen	X			
21.	Verstrekking van politiegegevens aan anderen dan politie en Koninklijke marechaussee	X			
22.	Doorgiften aan derde landen	X			
23.	Verstrekking aan derden structureel voor samenwerkingsverbanden	X			
24.	Rechtstreekse verstrekking				
25.	Informatie aan de betrokkene, recht op inzage, rectificatie en verwijdering	X			
26.	Register	X			
27.	Documentatie	X			
28.	Logging	X			
29.	Audits	X			
30.	Melding datalekken	X			
31.	Functionaris voor gegevensbescherming				
32.	Privacyfunctionaris				

1 Inleiding onderzoek

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 aanpassing van de Europese richtlijn gegevensbescherming politie en justitie[3], 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 ook van toepassing op de taken van de Belastingdienst, onderdeel van het ministerie van Financiën.

De Wpg schrijft voor dat de verwerkingsverantwoordelijke de naleving van de regels controleert door middel van periodieke audits. Werkgevers van boa's zijn verplicht elk jaar een interne Wpg-audit uit te voeren en elke vier 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 inwerkingtreding moet worden uitgevoerd. Dit betekent dat de eerste privacy audit in 2021 uitgevoerd moet worden. De AP heeft echter de werkgevers van boa's 1 jaar uitstel gegeven waardoor zij tot en met 31-12-2022 de tijd hebben om het resultaat van de eerste privacy audit naar de AP te sturen.

Door Persoonsgegevens is aan de Auditdienst Rijk (ADR) gevraagd om deze eerste privacy audit uit te voeren voor de directies Particulieren, Midden-en Kleinbedrijf, Grote Ondernemingen (exclusief Bureau Economische Handhaving, omdat daar reeds een separate privacy audit voor is opgesteld).

1.2 Doelstelling

De privacy audit heeft tot doel om met een redelijke mate van zekerheid een oordeel te geven of aan de bepalingen van de wet (Wpg specifieke bepalingen voor boa's) wordt voldaan. De onderzoeksperiode is van 01-01-2019 tot en met 31-12-2021. Hiertoe vindt een beoordeling plaats van de volgende aspecten binnen de organisatie van de betreffende directies van de Belastingdienst:

a. de opzet en het bestaan van maatregelen en procedures in de periode van 01-01-2019 tot en met 31-12-2021 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 de wetsartikelen van de Wpg en Bpg voor boa's die betrekking hebben op de hoofdgebieden:
- Algemene bepalingen (art 3-7);
- Verwerking van politiegegevens (art 8-15);
  - *bij dit onderdeel worden alleen artikel 8, 9 en 13 beoordeeld.*
- Verstrekking van politiegegevens (art 16-24);

[3] 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.

- Rechten van betrokkenen (art 25-31);
- Controle en toezicht (art 32-34, art 36).

Het onderzoek is uitgevoerd met het toetsingskader dat gebaseerd is op de in de Wpg en Besluit politiegegevens (Bpg) gestelde eisen evenals de NOREA Handreiking Privacy audit Wet politiegegevens (Wpg) voor Boa's Versie 1.0 d.d. 24 juni 2021.

2 Bevindingen onderzoek

2.1 Bevindingen per Wpg-onderwerp

Voorafgaand aan het onderzoek hebben wij informatie opgevraagd over de inrichting om de waarborgen van de naleving die de Wpg stelt over de verschillende onderwerpen te kunnen beoordelen. De betreffende directies van de Belastingdienst hebben de beschikbare informatie verstrekt. De ontvangen informatie dekt niet volledig de Wpg-onderwerpen af. Dit duidt erop dat er binnen de betreffende directies onvoldoende kennis aanwezig is om de vereisten uit de Wpg aantoonbaar vorm te geven, evenals het delen en uitdragen van informatie over de Wpg te realiseren. Hieronder zijn onze bevindingen per onderwerp uit de Wpg (zoals weergegeven in tabel 2) uiteengezet.

2.1.1 *Reikwijdte: binnen de betreffende directies van de Belastingdienst is geen eenduidig inzicht in de verwerkingen die onder Wpg vallen*

Wij hebben geconstateerd dat de betreffende directies van de Belastingdienst geen eenduidig inzicht hebben in de verwerkingen die onder de Wpg vallen. Daarnaast hebben wij geen processen en/of procedures aangetroffen die toezien op de periodieke inventarisatie van de verwerkingen en de actualisatie van een overzicht van de verwerkingen.

2.1.2 *Doel van verwerkingen niet vastgelegd*

Wij hebben geen eenduidige uitgangspunten en/of procedures aangetroffen die borgen dat politiegegevens enkel verwerkt worden voor de in de wet genoemde doeleinden. In het Protocol aanmelding en afhandeling fiscale delicten, douane- en toeslagendelicten (AAFD) is opgenomen dat de gegevens enkel binnen het strafrechtelijke domein worden verwerkt als de zaak voldoet aan de wegingscriteria. Dit is een besluit dat in het wegingsteam wordt genomen. Hier dient een besluitdocument aan ten grondslag te liggen. Echter, is vernomen dat voorafgaand aan het weegmoment, verwerking van persoonsgegevens plaatsvindt om de besluitvorming te ondersteunen.
Daarnaast vindt geen periodieke controle plaats op de rechtmatigheid van de verwerking. Hierdoor bestaat de kans dat politiegegevens voor meerdere, wellicht niet verenigbare doelen, verwerkt worden.

2.1.3 *Noodzakelijkheid en rechtmatigheid verwerkingen politiegegevens niet geborgd*

Wij hebben geen uitgangspunten en/of processen aangetroffen die borgen dat enkel persoonsgegevens verwerkt worden die noodzakelijk en rechtmatig zijn. Tevens hebben wij geen instructies aangetroffen waarin aanwijzingen worden gegeven hoe gegevens verwerkt mogen worden. Wij hebben geen processen en/of procedures aangetroffen die toezien op de periodieke controle op de noodzakelijkheid en rechtmatigheid van de verwerkingen.

2.1.4 *Juistheid en volledigheid van politiegegevens niet geborgd*

Uit de aangereikte documentatie en beoordeling wordt opgemaakt dat de betreffende directies van de Belastingdienst criteria geformuleerd hebben voor toetsing van de juistheid van de verwerkte gegevens. Tevens zijn in het "Handboek Controle" maatregelen beschreven omtrent de kwaliteitsborging. Uit de interviews blijkt echter dat deze criteria en maatregelen niet verder verwerkt zijn in onderliggende instructies. Als gevolg hiervan vindt in het operationeel proces geen kwaliteitstoetsing plaats.

Verder hebben wij geen procedures voor het vernietigen en rectificeren van politiegegevens aangetroffen. In de interviews is aangegeven dat deze procedures niet bekend zijn.

2.1.5 *Onderscheid feiten en persoonlijk oordeel niet geborgd*

Wij hebben geen uitgangspunten dan wel procedures aangetroffen om politiegegevens die op feiten zijn gebaseerd, voor zover mogelijk, te onderscheiden van politiegegevens die op een persoonlijk oordeel zijn gebaseerd. Het collegiaal tegenlezen/vier-ogen-principe dat is aangedragen heeft enkel betrekking op grammatica en strafrechtelijke onderbouwing. Het omvat geen Wpg-aspecten en het tegenlezen is niet in opzet geformaliseerd.

2.1.6 *Gegevensbescherming door beveiliging en ontwerp niet geborgd*

Wij hebben geen informatie aangetroffen waaruit blijkt op welke manier de betreffende directies van de Belastingdienst een gegevensbeschermingsbeleid dan wel procedures ontwikkeld en vastgesteld heeft. Dit geldt tevens voor een overzicht van passende technische en organisatorische maatregelen voortkomend uit een Data Protection Impact Assessment (DPIA) die nodig zijn om privacyrisico's bij verwerking van politiegegevens te mitigeren. Privacy by design is daarmee niet geborgd binnen de Belastingdienst.

2.1.7 *Gegevensbescherming door standaardinstellingen niet geborgd*

Wij hebben geen informatie aangetroffen waaruit blijkt op welke manier de betreffende directies van de Belastingdienst een gegevensbeschermingsbeleid dan wel procedures ontwikkeld en vastgesteld heeft. Dit geldt tevens voor een overzicht van passende technische en organisatorische maatregelen voortkomend uit een DPIA die nodig zijn om privacyrisico's bij verwerking van politiegegevens te mitigeren. Privacy by default is daarmee niet geborgd binnen de Belastingdienst.

2.1.8 *Gegevensbeschermingseffectbeoordeling/DPIA niet beschreven en uitgevoerd*

Wij hebben geen informatie aangetroffen waaruit blijkt dat de betreffende directies van de Belastingdienst procedures ontwikkeld en vastgesteld hebben voor het uitvoeren van DPIA's aangaande Wpg verwerkingen.

2.1.9 *Uitgangspunten verwerking bijzondere categorieën van politiegegevens niet beschreven en technische en organisatorische maatregelen niet aangetroffen*

Wij hebben geen uitgangspunten en/of procedures aangetroffen met betrekking tot de verwerking van bijzondere persoonsgegevens. Binnen de betreffende directies van de Belastingdienst is de boa verantwoordelijk voor de verwerking van bijzondere categorieën van politiegegevens. Deze bepaalt wat nodig is om een zaak aanhangig te kunnen maken. Er wordt veelvuldig gebruik gemaakt van BSN en van strafrechtelijke gegevens. Wij hebben geen instructies aangetroffen hoe een medewerker dient om te gaan met deze (politie)gegevens.

2.1.10 *Autorisaties en toegang tot politiegegevens niet inzichtelijk*

Wij hebben geen geformaliseerde procesbeschrijvingen en procedures voor het autorisatiebeheer aangetroffen voor de toegang tot politiegegevens. Een autorisatie- en functiescheidingsmatrix en controles met rapportages zijn niet aanwezig. Het is niet aantoonbaar inzichtelijk gemaakt welke personen vanuit hun functie toegang hebben tot bepaalde (politie)gegevens.

2.1.11 *Autorisaties: geen aangewezen functionarissen benoemd*

In de periode waarop de audit betrekking heeft zijn er geen bevoegde functionarissen, in de zin van de Wpg, benoemd bij de directies. Hierdoor is vastlegging van een lijst met namen niet aanwezig.

2.1.12 *Onderscheid tussen verschillende categorieën van betrokkenen niet vastgelegd*

Er zijn geen procesbeschrijvingen of instructies aanwezig betreffende het maken van onderscheid tussen verschillende categorieën van betrokkenen in het kader van de Wpg. Aangegeven is dat in het proces-verbaal de rol van de betrokkenen wel beschreven wordt. Echter, betreft dit een ongestructureerde registratie van persoonsgegevens die lastig te reproduceren/achterhalen is.

2.1.13 *Verwerker en verwerkersovereenkomst niet in opzet beschreven*
Wij hebben geen uitgangspunten in opzet aangetroffen betreffende verwerkers dan wel het opstellen van verwerkersovereenkomsten. In het register van verwerkingsactiviteiten is aangegeven dat er geen sprake is van verwerkers.

2.1.14 *Geheimhoudingsplicht is niet aantoonbaar geborgd*
Wij hebben geen informatie aangetroffen ten behoeve van de opzetbeoordeling waaruit blijkt dat de betreffende directies van de Belastingdienst procedures of werkinstructies hebben ingeregeld met betrekking tot de geheimhoudingsplicht in verband. met politiegegevens. Voor de fiscale geheimhoudingsplicht is er een onboardingsprocedure. Uit interviews is gebleken dat geheimhoudingsplicht een belangrijke waarde is. Op welke manier dit structureel tot uiting komt is echter onbekend.

2.1.15 *Geautomatiseerde individuele besluitvorming niet geborgd*
Wij hebben geen uitgangspunten en/of procedures aangetroffen met betrekking tot geautomatiseerde individuele besluitvorming.

2.1.16 *Uitvoering van de dagelijkse politietaak niet geborgd*
Wij hebben geen informatie aangetroffen waaruit blijkt op welke manier de betreffende directies van de Belastingdienst zowel in opzet als in bestaan borgen dat artikel 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). Aangegeven is dat er geen beschreven proces of werkinstructie aanwezig is voor de bewaartermijnen zoals in de Wpg vermeld staan.

2.1.17 *Ter beschikking stellen van politiegegevens binnen het Wpg-domein niet aantoonbaar geborgd*
Wij hebben geen informatie aangetroffen waaruit blijkt op welke manier de betreffende directies van de Belastingdienst borgen zowel in opzet als in bestaan dat de verdere verwerking van artikel 9 gegevens alleen plaats vindt na toestemming (aantoonbaar) van de daartoe bevoegde functionaris. Dit geldt ook voor maatregelen ter waarborging van het conform richtlijnen 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. Aangegeven is dat er geen beschreven proces of werkinstructie aanwezig is.

2.1.18 *Geautomatiseerd vergelijken en in combinatie zoeken vindt niet plaats*
Wij hebben geen informatie aangetroffen waaruit blijkt op welke manier de betreffende directies van de Belastingdienst zowel in opzet als in bestaan borgen dat gegevens alleen geautomatiseerd worden vergeleken met andere politiegegevens of met andere dan politiegegevens binnen de richtlijnen gesteld in artikel 11. Aangegeven is dat geautomatiseerd vergelijken en in combinatie zoeken nu niet plaatsvindt. Momenteel hebben de directies nog geen besluit genomen of dit in de toekomst wel gaat plaatsvinden.

2.1.19 *Ondersteunende taken niet geborgd*
Wij hebben geen informatie aangetroffen waaruit blijkt op welke manier de Belastingdienst zowel in opzet als in bestaan borgt dat voor de verwerkingen bedoeld in artikel 13.1, 13.2 en 13.2 Wpg, van tevoren is voldaan aan de schriftelijke vereisten (13.4 Wpg en 6:2 Bpg). Aangegeven is dat er geen beschreven proces of werkinstructie aanwezig is.

2.1.20 *Bewaartermijnen, verwijderen en vernietigen niet inzichtelijk*
Wij hebben geen uitgangspunten, procesbeschrijving of werkinstructies aangetroffen waarin bewaartermijnen en het verwijderen en vernietigen van politiegegevens zijn beschreven. Ook zijn geen aantoonbare waarborgen aangetroffen die

bewerkstelligen dat gegevens in overeenstemming met de Wpg bewaard, verwijderd en vernietigd worden.

2.1.21 *Verstrekking van politiegegevens aan anderen dan politie en Koninklijke marechaussee niet aantoonbaar geborgd*

Wij hebben vastgesteld dat er geen eenduidige procedures en/of instructies zijn voor het verstrekken van politiegegevens buiten het opsporingsdomein. Verstrekkingen binnen ketens en binnen samenwerkingsverbanden lijken verschillende procedures te doorlopen, echter deze zijn niet helder beschreven. Ook hebben wij geen overzicht van verstrekkingen aangetroffen. Aangegeven is dat deze niet op een centraal punt worden geregistreerd.

Aangegeven is dat bepaalde verzoeken voor verstrekking van politiegegevens doorverwezen worden naar het Openbare Ministerie wanneer de zaak bij de rechter aanhangig is gemaakt.

Wij hebben geen informatie aangetroffen waaruit blijkt dat de ontvangende partij gewezen wordt op de geheimhoudingsplicht. In de interviews is aangegeven dat de informatiedeling uitsluitend binnen de overheid gebeurt en dit door de eed afgedekt wordt.

2.1.22 *Doorgiften aan derde landen geen uitgangspunten*

Er zijn geen uitgangspunten beschreven omtrent het rechtstreeks verstrekken van politiegegevens aan derde landen.

2.1.23 *Verstrekking aan derden structureel voor samenwerkingsverbanden niet geregeld*

Wij hebben geconstateerd dat gegevens uit de controledossiers met meerdere partijen gedeeld kunnen worden. Hier zijn geen procedures voor opgesteld. In de interviews is aangegeven dat de gegevensdeling plaatsvindt op basis van de afspraken overeengekomen in de convenanten. Daarnaast wordt er gebruikgemaakt van een informatieloket dat toeziet op de naleving van deze gemaakte afspraken. Er is geen overzicht van de verschillende samenwerkingsverbanden en de overeengekomen datasets. Ook hebben wij niet vast kunnen stellen of de verstrekkingen conform de afspraken uit de convenanten hebben plaatsgevonden.

2.1.24 *Rechtstreekse verstrekkingen vinden niet plaats*

In de interviews is aangegeven dat er geen rechtstreekse verstrekkingen plaatsvinden. Derhalve is deze norm niet onderzocht.

2.1.25 *Informatie aan de betrokkene, recht op inzage, rectificatie en verwijdering geënt op AVG*

De Belastingdienst beschikt over een procedure voor het afhandelen van een verzoek voor de rechten van betrokkenen. Dit proces is echter geënt op de Algemene verordening gegevensbescherming (AVG) en niet op de Wpg. Er is geen inzicht in de ontvangen Wpg-verzoeken en derhalve ook geen inzicht of deze verzoeken conform vereisten zijn afgehandeld.

2.1.26 *Register van verwerkingsactiviteiten dient verbeterd te worden*

De Belastingdienst beschikt over een verwerkingsregister. Dit verwerkingsregister is gebaseerd op de AVG, maar bevat ook een module voor Wpg verwerkingen. In het register staan een aantal Wpg verwerkingen, van de Belastingdienst, maar niet van de onderzochte directies.

2.1.27 *Documentatie niet geborgd*

Wij hebben vastgesteld dat er geen stukken beschikbaar zijn waaruit blijkt dat er een opzet is ingericht voor het geven van invulling aan de documentatieplicht door de betrokken directies. Dit blijkt ook uit andere normen zoals vastlegging doel, verstrekking of doorgifte van politiegegevens, afwijzing verzoek betrokkene, melding datalekken.

2.1.28 *Logging*

In de periode waarop deze privacy audit betrekking heeft, was het artikel 32a in de Wpg over logging nog niet in werking getreden. Vandaar dat wij hierop thans geen toets hebben uitgevoerd.

2.1.29 *Auditvereisten geen uitvoering gegeven*

Wij hebben vastgesteld dat aan de eisen zoals gesteld in de Regeling Periodieke Audit politiegegevens geen uitvoering is gegeven. Er zijn helemaal geen (interne) audits uitgevoerd.

2.1.30 *Melding datalekken instructie aanwezig, controle afhandeling niet mogelijk*

Wij hebben een werkinstructie voor de Melddesk Datalekken Belastingdienst ontvangen, waarin is beschreven hoe datalekken moeten worden beoordeeld en afgehandeld. Wij hebben echter geen overzicht met de geregistreerde datalekken ontvangen. Derhalve kunnen wij niet vaststellen of datalekken worden geregistreerd en of hier opvolging aan wordt gegeven.

2.1.31 *Functionaris voor gegevensbescherming aangesteld, toezichtactiviteiten Wpg nog niet uitgevoerd*

Wij hebben vastgesteld dat er een functionaris voor gegevensbescherming is aangesteld die toezicht houdt op onder andere de naleving van de Wpg. Gezien de Wpg volwassenheid van de betreffende directies van de Belastingdienst worden er momenteel nog geen controleactiviteiten uitgevoerd. Er is geen jaarlijks verslag van bevindingen van de functionaris voor gegevensbescherming aanwezig.

2.1.32 *Privacyfunctionaris aangesteld, toezichtactiviteiten Wpg nog niet uitgevoerd*

Voor het interne toezicht op de naleving van de Wpg volgens artikel 34 Wpg is een formele privacyfunctionaris bij de Belastingdienst aangesteld. Aan de eis van periodiek intern toezicht op de Wpg inclusief rapportage wordt nog geen invulling gegeven.

3 Aanbevelingen en/of vervolgstappen

Op basis van de geconstateerde bevindingen uit hoofdstuk 2, doen wij de volgende aanbevelingen:

1. **Reikwijdte**: identificeer de bestanden dan wel informatiestromen van verwerkingen van politiegegevens binnen de betreffende directies van de Belastingdienst en actualiseer naar aanleiding hiervan de registratie in het register van verwerkingsactiviteiten. Besteed hierbij tevens aandacht aan de Wpg-verwerkingsgrondslag. Beschrijf daarnaast in opzet een Wpg procedurebeschrijving waarin het onderscheid tussen toezicht (AVG) en opsporing (Wpg) is opgenomen.

2. **Doelbinding**: update de registratie in het register van verwerkingsactiviteiten door de in de wet genoemde doeleinden te koppelen aan de taken van de Belastingdienst. Beschrijf daarnaast in opzet een Wpg procedure beschrijving waarin het vastleggen van het doel evenals de controle is opgenomen.

3. **Noodzakelijkheid & rechtmatigheid politiegegevens**: beschrijf in opzet een Wpg procedurebeschrijving waarin de noodzakelijkheid en rechtmatigheid van de verwerking van politiegegevens is opgenomen. Besteed daarbij tevens aandacht dat de herkomst van gegevens voor artikel 9 verwerkingen wordt vermeld. Beschrijf daarnaast een werkinstructie betreft een controle hierop alsmede de technische en organisatorische maatregelen die hierbij horen.

4. **Juistheid en volledigheid politiegegevens**: beschrijf in opzet een Wpg procedurebeschrijving waarin de juistheid en volledigheid van de verwerking van politiegegevens is opgenomen. Beschrijf tevens een werkinstructie betreft een controle hierop alsmede de technische en organisatorische maatregelen die hierbij horen.

5. **Onderscheid feiten en persoonlijk oordeel**: beschrijf in opzet een Wpg procedurebeschrijving waarin het onderscheid tussen feiten en persoonlijk oordeel is opgenomen. Beschrijf tevens een werkinstructie betreft een controle hierop alsmede de technische en organisatorische maatregelen die hierbij horen.

6. **Gegevensbescherming door beveiliging en ontwerp**: voer een risicoanalyse uit om het risiconiveau voor de verwerkingen van politiegegevens vast te stellen. Beschrijf en implementeer op basis hiervan passende technische en organisatorische maatregelen die nodig zijn om de risico's te beperken. Leg de uitgangspunten aangaande beveiliging van gegevens en privacy by design vast in een gegevensbeschermingsbeleid. Zie verder relatie met aanbevelingen onder nummer 8.

7. **Gegevensbescherming door standaardinstellingen**: beschrijf en implementeer op basis van een risicoanalyse passende technische en organisatorische maatregelen die nodig zijn om de risico's te beperken. Leg de uitgangspunten aangaande beveiliging van gegevens en privacy by default vast in een gegevensbeschermingsbeleid. Zie verder relatie met aanbevelingen onder nummer 8.

8. **Gegevensbeschermingseffectbeoordeling DPIA**: beschrijf in opzet het proces aangaande de uitvoering van een DPIA en voer een DPIA uit voor de verwerkingen die waarschijnlijk een hoog risico voor de rechten en vrijheden van betrokkenen kunnen opleveren. Beschrijf en implementeer op basis hiervan passende technische en organisatorische maatregelen om de geïdentificeerde risico's te kunnen mitigeren (zie tevens onderdeel 6 en 7).

9. **Bijzondere categorieën van politiegegevens**: beschrijf in opzet een Wpg procedurebeschrijving waarin het verwerken van bijzondere persoonsgegevens is opgenomen en de manier waarop de betreffende directies van de Belastingdienst hiermee omgaat. Beschrijf tevens in een werkinstructie de controle hierop alsmede de technische en organisatorische maatregelen die hierbij horen.

10. **Autorisaties en toegang tot politiegegevens:** beschrijf in opzet het autorisatiebeheer en laat de autorisatie- en functiescheidingsmatrices door de verantwoordelijken vastleggen. Zorg periodiek voor een controle van deze en rapporteer waar nodig doorbrekingen. De implementatie van een ondersteunend, faciliterend systeem voor de gegevensverwerkingen kan hierbij helpen.

11. **Autorisaties: aanwijzen functionarissen**: beschrijf in opzet een lijst van bevoegde functionarissen alsmede een proces dat deze lijst actueel dient te houden. Beschrijf in opzet een Wpg procedurebeschrijving waarin de functie-en rolbeschrijving van de bevoegde functionarissen is opgenomen.

12. **Onderscheid tussen verschillende categorieën van betrokkenen**: beschrijf in opzet een Wpg procedurebeschrijving waarin het onderscheid tussen verschillende categorieën van betrokken is opgenomen alsmede het vastleggen van dit onderscheid in de onderliggende informatiesystemen.

13. **Verwerker en verwerkersovereenkomst:** beschrijf in opzet een Wpg procedurebeschrijving waarin verwerkingsovereenkomst in het kader van de politietaak Wpg wordt vastgelegd.

14. **Geheimhoudingsplicht:** De fiscale geheimhoudingsplicht is geregeld, echter niet specifiek voor de Wpg.

15. **Geautomatiseerde individuele besluitvorming**: beschrijf in opzet een Wpg procesbeschrijving waarin geautomatiseerde individuele besluitvorming plaatsvindt.

16. **Uitvoering van de dagelijkse politietaak**: zorg ervoor dat een beschrijving opgesteld wordt van dit onderwerp in een Wpg procedurebeschrijving.

17. **Ter beschikking stellen van politiegegevens binnen het Wpg-domein**, zorg ervoor de er een beschrijving wordt opgesteld van dit onderwerp in een Wpg procedurebeschrijving.

18. **Geautomatiseerd vergelijken en in combinatie zoeken:** zorg ervoor de er een beschrijving wordt opgesteld van dit onderwerp in een Wpg procedurebeschrijving.

19. **Ondersteunende taken**: zorg dat er een procesbeschrijving of werkinstructie wordt opgezet van dit onderwerp.

20. **Bewaartermijnen, verwijderen en vernietigen:** beschrijf in opzet de wijze waarop met bewaartermijnen en het verwijderen en vernietigen van gegevens moet worden omgegaan. Voorziet hierbij in voldoende waarborgen om te bewerkstelligen dat de gegevens conform de wet worden bewaard, verwijderd en vernietigd.

21. **Verstrekking van politiegegevens aan anderen dan politie en Koninklijke marechaussee**: eenduidige procedures en/of instructies opstellen voor het verstrekken van politiegegevens buiten het opsporingsdomein.

22. **Doorgiften aan derde landen:** het register met Wpg verwerkingen aanpassen op het punt van doorgiften aan derde landen zodat duidelijk en eenduidig is in welk geval er sprake of geen sprake is van doorgiften aan derde landen.

23. **Verstrekking aan derden structureel voor samenwerkingsverbanden:** het opstellen van een overzicht van de verschillende samenwerkingsverbanden en de overeengekomen datasets is een vereiste.

24. **Rechtstreekse verstrekking:** het register met Wpg verwerkingen aanpassen op het punt van rechtstreekse verstrekking zodat duidelijk en eenduidig is in welk geval er sprake of geen sprake is van rechtstreekse verstrekking.

25. **Informatie aan de betrokkene, recht op inzage, rectificatie en verwijdering:** eenduidige procedures en/of instructies opstellen voor het verstrekken van Informatie aan de betrokkene, recht op inzage, rectificatie en verwijdering wanneer de betrekking heeft op de Wpg.

26. **Register:** zorg dat het register van verwerkingen goed wordt gebruikt.

27. **Documentatie:** borg een volledige en toegankelijke schriftelijke vastlegging (documentatieplicht) van de onderdelen genoemd in art 32 lid 1.

28. **Logging:** zorg voor de logging van verwerkingen zoals opgenomen in artikel 32a lid 1 en de logging en uitsluitend gebruikt ter controle van de rechtmatigheid van de gegevensverwerkingen, interne controles, ter waarborging van de integriteit en de beveiliging van politiegegevens en voor strafrechtelijke procedures.

29. **Audits:** zorg dat interne audits periodiek worden uitgevoerd en laat deze opnemen in de auditkalender.

30. **Melding datalekken:** zorg dat wanneer er sprake is van datalekken met betrekking tot Wpg deze apart worden geregisterd een afgehandeld.

31. **Functionaris voor gegevensbescherming:** zorg voor de volwassenheid van Wpg waardoor de functionaris voor gegevensbescherming haar rol goed kan invullen.

Privacyfunctionaris: de privacyfunctionaris is aangesteld. Zorg aan de eis van periodiek intern toezicht op de Wpg inclusief rapportage waardoor ook rol goed invulling kan worden gegeven.

4 Verantwoording onderzoek

4.1 Werkzaamheden en afbakening

4.1.1 *Object van onderzoek*

Het object van onderzoek van deze privacy audit betreft de hiervoor genoemde artikelen van de Wpg die van toepassing[4] zijn op de directies P, MKB, GO van de Belastingdienst bij de verwerking[5] van politiegegevensgegevens in het kader van de opsporingstaken door buitengewone opsporingsambtenaren. Het onderzoek richt zich op de beheersingsmaatregelen in de processen en de systemen die gebruikt worden bij de uitvoering van deze taken en de vastlegging van politiegegevens hierbij.

De redelijke mate van zekerheid die gegeven is of aan de bepalingen van de Wpg op adequate wijze uitvoering is gegeven, gaat over de vastgestelde wettelijke periode van onderzoek van 01-01-2019 tot en met 31-12-2021.

De werking van een norm is alleen gecontroleerd indien de opzet en het bestaan als voldoende is beoordeeld.

4.1.2 *Afbakening*

Het onderzoek, richt zich alleen op de procedures en maatregelen die de betreffende directies van de Belastingdienst in het kader van de Wpg moeten treffen. De onderzoeksperiode is 01-01-2019 tot en met 31-12-2021. Daarbij wordt gebruik gemaakt van de aangeleverde documentatie en interviews. De ADR verricht geen onderzoek naar door derden aan de Belastingdienst geleverde faciliteiten, voor zover de verantwoordelijkheid is belegd bij anderen dan de Belastingdienst. In dergelijke gevallen wordt wel gekeken naar de gemaakte afspraken met betrekking tot de Wpg tussen de partijen en de regie vanuit de Belastingdienst gericht op de realisatie van de afspraken.
Het onderzoek vindt plaats over meerdere regio's, voor de directies Grote Ondernemingen (GO), directie Particulieren (P) en voor de directie MKB, zijn interviews afgenomen bij boa's binnen de teams Intensief Toezicht en Externe Overheidssamenwerking (ITE) evenals daarbuiten. De selectie is afgestemd met de contactpersonen.

4.1.3 *Criteria*

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 hebben bovengenoemde directies van de Belastingdienst beheersingsmaatregelen getroffen die in opzet, bestaan en werking door de ADR worden getoetst. De ADR maakt bij deze toetsing gebruik van de volgende criteria:

Opzet	De organisatie heeft de beheersingsmaatregen beschreven die, indien deze werken zoals beschreven, een redelijke mate van zekerheid bieden voor de borging van de wettelijke eisen met betrekking tot de verwerking van politiegegevens door boa's.

[4] Zie Besluit politiegegevens buitengewone opsporingsambtenaren.
[5] 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.

Bestaan	De organisatie heeft de beheersingsmaatregelen overeenkomstig de opzet daadwerkelijk geïmplementeerd en toegepast.
Werking	De organisatie heeft de beheersingsmaatregelen gedurende de verslaggevingsperiode volgens de opzet toegepast, ingeval van handmatige beheersingsmaatregelen zijn deze toegepast door competente en bevoegde personen.

Om tot een beoordeling te komen worden de bevindingen en eventuele (rest)risico's gewogen, waarbij gebruik wordt gemaakt van vooraf gedefinieerde key controls. Hierbij wordt rekening gehouden met mitigerende maatregelen en de risico's voor de rechten van betrokkenen. In het toetsingskader zijn de key controls aangegeven in de laatste kolom. 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.

Indien niet of niet helemaal wordt voldaan aan een norm, wordt het restrisico beoordeeld. Bij het beoordelen van het restrisico wordt rekening gehouden met het feit of een norm als key control is gedefinieerd.

4.1.4 *Verantwoordelijkheden Belastingdienst*

De onderzochte de betreffende directies van de Belastingdienst zijn verantwoordelijk voor de opzet, het bestaan en de werking van de relevante beheersingsmaatregelen gedurende de periode 01-01-2019 – 31-12-2021.

4.1.5 *Onze onafhankelijkheid en kwaliteitsbeheersing.*

Wij hebben de vereisten van het Reglement Gedragscode ('Code of Ethics') van NOREA nageleefd, welke is gebaseerd is op de fundamentele beginselen van integriteit, objectiviteit, vakbekwaamheid en zorgvuldigheid, vertrouwelijkheid en professioneel gedrag.
Wij passen het Reglement Kwaliteitsbeheersing NOREA (RKBN) toe en bijgevolg onderhouden wij een uitgebreid systeem van kwaliteitscontrole met inbegrip van gedocumenteerd beleid en de procedures met betrekking tot de naleving van de ethische voorschriften, professionele standaarden en de van toepassing zijnde wet- en regelgeving.
Wij voldoen aan de specifieke vereisten voor de uitvoering van de externe privacy audit, zoals bepaald in artikel 5 van de Regeling periodieke audit politiegegevens[6].

4.1.6 *Verantwoordelijkheden van de IT-Auditor*

Onze verantwoordelijkheid is, op basis van onze werkzaamheden, het geven van een oordeel over de opzet, het bestaan en de werking van beheersingsmaatregelen die verband houden met de beheersingsdoelstellingen. Wij hebben onze opdracht uitgevoerd overeenkomstig 'Richtlijn 3000D Directe opdrachten' vastgesteld door Nederlandse Orde van Register EDP-Auditors (NOREA). Dit vereist dat wij voldoen aan de voor ons geldende ethische voorschriften en onze werkzaamheden zodanig plannen en uitvoeren dat een redelijke mate van zekerheid wordt verkregen over de vraag of de beheersmaatregelen, in alle van materieel belang zijnde aspecten, op afdoende wijze zijn opgezet, bestaan en werkten gedurende de controleperiode.

Een assurance-opdracht om te rapporteren over de opzet, het bestaan en de werking van beheersingsmaatregelen omvat het uitvoeren van werkzaamheden ter verkrijging van assurance-informatie over de opzet, het bestaan en de werking van beheersingsmaatregelen. De geselecteerde werkzaamheden zijn afhankelijk van de

[6] *Zie hiervoor de Regeling van de Minister van Justitie, de Minister van Binnenlandse Zaken en de Minister van Defensie van 9 december 2008, nr. 5578598/08, houdende nadere regels ten aanzien van het toezicht op de naleving van de bij of krachtens de Wet politiegegevens gegevens voorschriften (Regeling periodieke audit politiegegevens).*

door de IT-auditor toegepaste oordeelsvorming, met inbegrip van het inschatten van de risico's dat beheersingsmaatregelen zijn opgezet en werkten.

Wij zijn van mening dat de door ons verkregen assurance-informatie voldoende en geschikt is om een onderbouwing voor ons afkeurend oordeel te bieden.

4.1.7 Beperkingen van het onderzoek

Wij kunnen niet uitsluiten dat, indien wij aanvullende beheersingsmaatregelen zouden hebben onderzocht, wellicht andere onderwerpen zouden zijn geconstateerd die voor rapportering in aanmerking zouden zijn gekomen.
Bovendien is de projectie van oordelen naar de toekomst onderhevig aan het risico dat interne beheersingsmaatregelen ineffectief kunnen worden.

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, Persoonsgegevens , is eigenaar van dit rapport.

De Belastingdienst dient ingevolge artikel 33 2e lid van de Wet politiegegevens een afschrift van de controleresultaten van de privacy audit aan de Autoriteit persoonsgegevens te zenden. Het is, zonder onze uitdrukkelijke voorafgaande schriftelijke toestemming, niet toegestaan de rapportages met anderen dan de Autoriteit persoonsgegevens te delen. Het verstrekken van deze toestemming kan omgeven zijn met nadere voorwaarden. Het is niet toegestaan deze rapportage te gebruiken in juridische conflicten tussen de Belastingdienst en andere (rechts)personen.

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

5 Ondertekening

Den Haag, 27 juni 2023

Persoonsgegevens

Auditdienst Rijk

6 Bijlage: Managementreactie

Belastingdienst

Retourdatum Postbus 20201 2500 EE Den Haag

Auditdienst Rijk
Persoonsgegevens
Postbus 20201
2500 EE Den Haag

Persoonsgegevens
Korte Voorhout 72511
CW Den Haag
Postbus 20201
2500 EE Den Haag

Datum
26 juni 2023

Contactpersoon
Persoonsgegevens

Uw kenmerk
Privacy audit politiegegevens (Wpg) betreffende de directies P, MKB en GO (exclusief BEH) van de Belastingdienst.

Betreft: Managementreactie bij Assurancerapport Privacy audit Wpg Belastingdienst; directies MKB, P, GO (excl. BEH) van de Belastingdienst

Geachte Persoonsgegevens

De Belastingdienst dankt de Auditdienst Rijk (ADR) voor het uitgebreide onderzoek naar de mate van voldoen aan de verplichtingen uit de Wet politiegegevens (Wpg) bij de verwerking van politiegegevens door buitengewoon opsporingsambtenaren (BOA's) in de periode 2019 tot en met 2021 van de directies Midden- en Kleinbedrijf, Particulieren en Grote Ondernemingen.

De ADR komt op basis van de privacy-audit tot het oordeel dat de desbetreffende directies in belangrijke mate niet voldoen aan de Wpg en dat het daadwerkelijk implementeren en borgen van de bevindingen om structurele aandacht en inzet vraagt.

De Belastingdienst onderschrijft de geconstateerde tekortkomingen en neemt alle aanbevelingen over. De benodigde verbeteracties worden met urgentie geïmplementeerd. De eerder uitgebrachte en bij de directies bekende Wpg-auditrapporten voor Douane en Bureau Economische Handhaving (BEH) gaven al een indicatie welke bevindingen van de ADR bij deze privacy-audit te verwachten waren. Vooruitlopend op het rapport zijn we in maart 2023 gestart met het inzetten van diverse verbetertrajecten zoals het beschrijven van werkprocessen en het inventariseren van beveiligde IT-systemen voor Wpg-verwerkingen. Ook is inmiddels het proces ingericht om te borgen dat de auditverplichting tijdig wordt voldaan.

Een gezamenlijk verbeterrapport van de directies, volgt op grond van de wet- en regelgeving binnen drie maanden na het uitbrengen van de definitieve privacy-auditrapportage. In het verbeterrapport zullen, overeenkomstig de aanbevelingen van de ADR, aan de bevindingen van de ADR verbeteracties worden gekoppeld. We zullen alle inspanningen betrachten om nog dit jaar een groot deel van de aanbevelingen opgevolgd te hebben.

Hoogachtend,

Persoonsgegevens

Auditdienst Rijk
Postbus 20201
2500 EE Den Haag

Persoonsgegevens