Auditdienst Rijk
Ministerie van Financiën

departementaal VERTROUWELIJK

Assurancerapport

Privacy-audit Wet politiegegevens Bureau Economische Handhaving

Verslagperiode 9 maart 2019 – 31 december 2021

Colofon

Titel	Privacy-audit Wet politiegegevens Bureau Economische Handhaving
Uitgebracht aan	Persoonsgegevens
Datum	15 december 2022
Kenmerk	2022-0000323799

Inlichtingen
Auditdienst Rijk
Persoonsgegevens

Inhoud

Bureau Economische Handhaving voldoet 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 het Bureau Economische Handhaving aan de bepalingen van de Wpg op adequate wijze uitvoering is gegeven in de periode 9 maart 2019 t/m 31 december 2021.

Afkeurend oordeel

Op basis van de significantie van de aangelegenheid die staat beschreven in de sectie 'basis voor ons een afkeurend oordeel', zijn wij tot de conclusie gekomen dat het Bureau Economische Handhaving in de periode 9 maart 2019 t/m 31 december 2021 de Wpg niet getrouw naleefde.

De basis voor ons afkeurend oordeel

Uit ons onderzoek is naar voren gekomen dat het Bureau Economische Handhaving (BEH) in de periode 9 maart 2019 t/m 31 december 2021 in belangrijke mate niet voldeed aan de Wpg. Het BEH heeft nog niet alle bestanden met politiegegevens geïdentificeerd en gedocumenteerd. Daarnaast is het doel van de verwerkingen niet vastgelegd. 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

	Groen	Voldoet aan de norm
	Oranje	Voldoet deels aan de norm
	Rood	Voldoet niet aan de norm
	Grijs	Norm is niet onderzocht
	Wit	Norm is niet van toepassing

Tabel 2: Overzicht conclusie per Wpg-onderwerp

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

Nr.	Norm	Key control	Conclusie		
			Opzet	Bestaan	Werking
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				

Tabel 3: Organisatorische en technische beheersingsmaatregelen (t.b.v. normen 6, 7, 10, 13 en 24)

Nr.	Norm	Conclusie		
		Opzet	Bestaan	Werking
1.	Wijzigingenbeheer			
2.	Logische toegangs-beveiliging			

3.	Beheer van kwetsbaarheden (patch-management)			
4.	Cryptografie			
5.	Vulnerability scans en Penetratietesten			

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 inwerkingtreding 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 uit te voeren 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 2 jaar na inwerkingtreding moet worden uitgevoerd. De auditverplichting is met ingang van 09-03-2019 van kracht geworden voor (de werkgevers van) boa's. 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 het BEH is aan de Auditdienst Rijk (ADR) gevraagd om deze eerste Privacy audit in 2022 uit te voeren.

1.2 Doelstelling

Het doel van dit Assurance-onderzoek is om met een redelijke mate van zekerheid een oordeel te geven of door het Bureau Economische Handhaving aan de bepalingen van de Wpg op adequate wijze uitvoering is gegeven in de periode 9 maart 2019 t/m 31 december 2021. Om dit oordeel te geven is er door de ADR gekeken naar:

- De opzet en het bestaan van maatregelen en procedures die in de borging van de wettelijke eisen moeten voorzien;
- 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).

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.

2 Bevindingen onderzoek

2.1 Bevindingen per Wpg-onderwerp

2.1.1 *Reikwijdte: nog niet alle bestanden met politiegegevens binnen het BEH zijn geïdentificeerd en vastgelegd*

Wij hebben vastgesteld dat het BEH nog niet alle bestanden met politiegegevens binnen de organisatie heeft geïdentificeerd en vastgelegd. Het onderscheid tussen toezicht (AVG) en opsporing (Wpg) is niet aantoonbaar en in het register van verwerkingsactiviteiten zijn niet alle taken van het BEH vastgelegd. Dit geldt tevens voor de onderliggende systemen gespecificeerd naar taak en soort politiegegevens. Wij hebben geen procedure aangetroffen om het overzicht van de inventarisatie van verwerkingen van politiegegevens periodiek te actualiseren.

2.1.2 *Doel van verwerkingen(doelbinding) niet vastgelegd*

Wij hebben vastgesteld dat het BEH in het register van verwerkingsactiviteiten de in de wet genoemde doeleinden niet vastgelegd en gekoppeld heeft aan de taken van het BEH. Er wordt enkel verwezen naar een taak van het BEH en niet naar het Wpg-artikel. Daarnaast hebben wij niet in opzet en bestaan uitgangspunten aangetroffen aangaande het vastleggen van het doel in onderliggende systemen alsmede de controle hierop.

2.1.3 *Noodzakelijkheid en rechtmatigheid van politiegegevens niet geborgd*

Wij hebben geen uitgangspunten dan wel procedures aangetroffen die borgen dat de politiegegevens daartoe toereikend, ter zake dienend en beperkt zijn tot wat noodzakelijk is en dat de herkomst van gegevens voor art 9 verwerkingen wordt vermeld. 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 vastgelegd.

2.1.4 *Juistheid en volledigheid van politiegegevens niet geborgd*

Wij hebben vastgelegd dat het BEH geen controles dan wel procedures op de kwaliteit heeft ingericht ten behoeve van de borging van de juistheid en nauwkeurigheid van politiegegevens. 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 vastgelegd.

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 vastgelegd.

2.1.6 *Gegevensbescherming door beveiliging en ontwerp niet aanwezig of aantoonbaar geïmplementeerd*

Wij hebben geen vastgesteld beleid en procedures voor de bescherming van de politiegegevens alsmede uitgangspunten aangaande privacy by design aangetroffen. Er is geen aantoonbare risicoanalyse uitgevoerd waaruit het risiconiveau blijkt met betrekking tot ongeoorloofde of onrechtmatige verwerking en tegen opzettelijk verlies, vernietiging of beschadiging (zie verder 2.1.8). Passende technische en organisatorische maatregelen zijn niet in opzet beschreven en in bestaan aantoonbaar geïmplementeerd.

2.1.7 *Gegevensbescherming door standaardinstellingen niet aanwezig of aantoonbaar geïmplementeerd*

Wij hebben geen vastgesteld beleid en procedures voor de bescherming van de politiegegevens aangetroffen alsmede uitgangspunten aangaande privacy by default. Passende technische en organisatorische maatregelen zijn niet in opzet beschreven en niet in bestaan aantoonbaar geïmplementeerd.

2.1.8 *Gegevensbeschermingseffectbeoordeling / DPIA niet beschreven en uitgevoerd*

Wij hebben vastgesteld dat het BEH geen proces heeft beschreven aangaande het uitvoeren van een DPIA. In de praktijk voert het BEH geen DPIA uit wanneer een verwerking waarschijnlijk een hoog risico voor de rechten en vrijheden van betrokkenen kan opleveren. Hierdoor worden binnen het BEH geen risico's systematisch geïdentificeerd en beoordeeld waardoor een geen passend pakket van organisatorische en technische maatregelen geïmplementeerd kan worden. Wel hebben wij een pre-pia / WMK-toets (willen, mogen, kunnen) uit het verleden aangetroffen voor de taak deponeren jaarrekening. De verdere handelingen naar aanleiding van de WMK-toets zijn niet inzichtelijk.

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

Wij hebben geen uitgangspunten in opzet aangetroffen betreffende de verwerking van bijzondere categorieën van politiegegevens. In het register van verwerkingsactiviteiten staat aangegeven dat geen bijzondere categorieën van politiegegevens worden verwerkt. In de praktijk blijkt dit echter wel het geval te zijn. Wij hebben geen passende technische en organisatorische maatregelen aangetroffen om de verwerking van deze bijzondere categorieën van politiegegevens te beschermen.

2.1.10 *Autorisaties en toegang tot politiegegevens niet inzichtelijk*

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

2.1.11 *Autorisaties: aangewezen functionarissen niet vastgelegd*

Wij hebben vastgesteld dat een lijst van bevoegde functionarissen ontbreekt. In de praktijk is de Teamleider als bevoegd functionaris aangewezen. Formalisatie hiervan ontbreekt.

2.1.12 *Onderscheid tussen verschillende categorieën van betrokkenen is onduidelijk*

Wij hebben vastgesteld dat in het register van verwerkingsactiviteiten summier de verschillende categorieën van betrokkenen zijn weergegeven. Waar en op welke manier deze categorieën van betrokkenen in de onderliggende systemen worden verwerkt, is niet inzichtelijk.

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 geborgd*

Wij hebben vastgesteld dat geheimhoudingsplicht voor Boa's op diverse manieren is geborgd: de eed en gelofte bij indiensttreding, een specifieke aanvullende VOG en de aandacht tijdens diverse bewustwordingsinitiatieven.

2.1.15 *Geautomatiseerde individuele besluitvorming*

Door BEH worden geen besluiten genomen die alleen zijn gebaseerd op geautomatiseerde verwerking. Derhalve is deze norm niet verder onderzocht.

2.1.16 *Uitvoering van de dagelijkse politietaak*
Door het BEH worden geen art. 8 gegevens worden verwerkt. Derhalve is deze norm niet verder onderzocht.

2.1.17 *Ter beschikking stellen van politiegegevens binnen het Wpg-domein*
Door BEH worden geen politiegegevens ter beschikking gesteld binnen het Wpg-domein. Derhalve is deze norm niet onderzocht.

2.1.18 *Geautomatiseerd vergelijken en in combinatie zoeken*
BEH maakt geen gebruik van gegevens die geautomatiseerd vergleken worden of combinatie met elkaar worden verwerkt. Derhalve is deze norm niet onderzocht.

2.1.19 *Ondersteunende taken*
Door het BEH worden geen gegevens verwerkt waarbij sprake is van art. 13 verwerkingen. Derhalve is deze norm niet verder onderzocht.

2.1.20 *Bewaartermijnen, verwijderen en vernietigen zijn 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 conform de wet worden gecontroleerd, verwijderd en vernietigd.

2.1.21 *Verstrekking van politiegegevens aan anderen dan politie en Koninklijke marechaussee*
Door het BEH vinden geen verstrekkingen plaats aan anderen dan politie en Koninklijke marechaussee. Deze norm is niet verder onderzocht.

2.1.22 *Doorgiften aan derde landen*
Door het BEH vindt geen doorgifte plaats van gegevens aan derde landen. Derhalve is deze norm niet onderzocht.

2.1.23 *Verstrekking aan derden structureel voor samenwerkingsverbanden*
Vestrekking van politiegegevens aan derden structureel voor samenwerkingsverbanden, vindt niet plaats. Derhalve is deze norm niet onderzocht.

2.1.24 *Rechtstreekse verstrekking*
Door het BEH vinden geen rechtstreekse verstrekkingen plaats. Derhalve is deze norm niet onderzocht.

2.1.25 *Informatie aan de betrokkene, recht op inzage, rectificatie en verwijdering is geborgd*
Het BEH maakt gebruik van de standaard processen van de Belastingdienst ten aanzien van het verstrekken van informatie, recht op inzage, rectificatie en verwijdering aan de betrokkene. Omdat de afgelopen periode geen verzoeken hebben plaatsgevonden zijn het bestaan en werking niet door ons vast te stellen.

2.1.26 *Register van verwerkingsactiviteiten is niet actueel*
Wij hebben vastgesteld dat het register van verwerkingsactiviteiten niet volledig en actueel is.

2.1.27 *Documentatie*
Wij hebben vastgesteld dat geen volledige schriftelijke vastlegging aanwezig is van de onderdelen genoemd in art 32 lid 1 dan wel een proces om invulling te geven aan de documentatieplicht.

2.1.28 *Logging*

De norm aangaande logging kent nog geen wettelijke basis, aangezien art 32a Wpg (nog) niet in werking is getreden. Derhalve is deze niet verder getoetst en geëvalueerd.

2.1.29 *Audits*

Wij hebben vastgesteld dat aan de eisen zoals gesteld in de Regeling Periodieke Audit politiegegevens geen uitvoering is gegeven.

2.1.30 *Melding datalekken*

Wij hebben vastgesteld dat BEH voor het melden van datalekken BEH gebruik maakt van de standaard procedure van de belastingdienst. Omdat zich de afgelopen periode geen datalekken hebben voorgedaan is het bestaan en de werking niet door ons vast te stellen.

2.1.31 *Functionaris voor gegevensbescherming*

Wij hebben vastgesteld dan de FG voor het ministerie van Financiën is aangesteld en aangemeld bij de AP. Ook hebben wij vastgesteld dat een jaarlijks verslag van de bevindingen van de FG vanwege het Wpg-volwassenheidsniveau van de gegevensverwerkende organisatie niet voorhanden is.

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 organisatie 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 kwaliteitshandboek 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 het BEH. Beschrijf daarnaast in opzet een Wpg kwaliteitshandboek waarin het vastleggen van het doel evenals de controle is opgenomen.

3. **Noodzakelijkheid & rechtmatigheid politiegegevens**: beschrijf in opzet een Wpg kwaliteitshandboek waarin de noodzakelijkheid en rechtmatigheid van de verwerking van politiegegevens is opgenomen. Besteed daarbij tevens aandacht dat de herkomst van gegevens voor art. 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 kwaliteitshandboek 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 kwaliteitshandboek 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 kwaliteitshandboek waarin het verwerken van bijzondere persoonsgegevens is opgenomen en de manier waarop het BEH 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 kwaliteitshandboek waarin de functie-en rolbeschrijving van de bevoegde functionarissen is opgenomen.

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

13. Verwerker en verwerkersovereenkomst, geen aanbevelingen.

14. Geheimhoudingsplicht, geen aanbevelingen.

15. Geautomatiseerde individuele besluitvorming, geen aanbevelingen.

16. Uitvoering van de dagelijkse politietaak, geen aanbevelingen.

17. Ter beschikking stellen van politiegegevens binnen het Wpg-domein, geen aanbevelingen.

18. Geautomatiseerd vergelijken en in combinatie zoeken, geen aanbevelingen.

19. Ondersteunende taken, geen aanbevelingen.

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 gecontroleerd, verwijderd en vernietigd

21. Verstrekking van politiegegevens aan anderen dan politie en Koninklijke marechaussee, geen aanbevelingen.

22. Doorgiften aan derde landen, geen aanbevelingen.

23. Verstrekking aan derden structureel voor samenwerkingsverbanden, geen aanbevelingen.

24. Rechtstreekse verstrekking, geen aanbevelingen.

25. Informatie aan de betrokkene, recht op inzage, rectificatie en verwijdering, geen aanbevelingen.

26. **Register:** zorg dat het register van verwerkingen actueel is en borg dat bij de geplande verbeteringsslag de verplichte onderdelen in het register worden opgenomen.

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

28. Logging, geen aanbevelingen

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

30. Melding datalekken, geen aanbevelingen.

31. Functionaris voor gegevensbescherming, geen aanbevelingen.

4 Verantwoording onderzoek

4.1 Werkzaamheden en afbakening

4.1.1 *Object van onderzoek*

Het object van onderzoek van deze Privacy audit zijn de verwerkingen van politiegegevens die onder de verantwoordelijkheid van de verwerkingsverantwoordelijke binnen het BEH plaatsvinden. Het onderzoek richt zich hierbij op de beheersingsmaatregelen in de processen en de systemen die gebruikt worden bij de uitvoering van de opsporingstaak en de vastlegging van de politiegegevensgegevens 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 09-03-2019 tot en met 31-12-2021.

4.1.2 *Afbakening*

Het onderzoek richt zich alleen op de procedures en maatregelen die het BEH moet treffen. De ADR verricht geen onderzoek naar door derden aan het BEH geleverde faciliteiten, voor zover de verantwoordelijkheid is belegd bij andere dan het BEH. In dergelijke gevallen wordt wel gekeken naar de gemaakte afspraken tussen de partijen en de regie vanuit het BEH gericht op de realisatie van de afspraken.

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 heeft het BEH 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.
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 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 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 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 onze conclusie met beperking te bieden.

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 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, 20 december 2022

Persoonsgegevens

Auditdienst Rijk

Managementreactie BEH

Belastingdienst

Belastingdienst, Postbus 19500, 3501 CM Utrecht

Auditdienst Rijk
Account FIN/EZK/LNV
t.a.v. Persoonsgegevens
Postbus 20701
2500 CW Den Haag

Grote Ondernemingen
Landelijke directie

Croeselaan 14
3521 CA Utrecht
Postbus 19500
3501 CM Utrecht
belastingdienst.nl

Contactpersoon

Persoonsgegevens

belastingdienst.nl

Datum
20 december 2022

Uw kenmerk
Audit Wet Politiegegevens Bureau Economische Handhaving, 2022-0000277629

Betreft: Managementreactie bij Assurancerapport Privacy-audit Wet politiegegevens Bureau Economische Handhaving

Geachte Persoonsgegevens

De Belastingdienst/Directie Grote ondernemingen herkent zich in de conclusies van het onderzoek van de Audit Dienst Rijk (ADR) naar het voldoen aan de verplichtingen uit de Wet politiegegevens (Wpg) in de periode 2019 tot en met 2021 door het Bureau Economische Handhaving (BEH). Ik dank de ADR voor het uitvoeren van de audit en de aanbevelingen in het rapport. Ik neem de aanbevelingen integraal over.

BEH kwam in 2021 tot het inzicht dat bepaalde verplichtingen uit de Wpg van toepassing zijn, waarna voorbereidingen zijn getroffen voor de verplichte in- en externe audits. In het najaar 2022 zijn daarbij de eerste bevindingen opgekomen, die op dat moment aanleiding zijn geweest om de verbeterpunten projectmatig inzichtelijk te maken en op te pakken. De aanbevelingen van de ADR worden in dit project betrokken. In januari 2023 zal dit leiden tot een integraal verbeterplan en in maart 2023 tot een verbeterrapport.

Vooruitlopend hierop maakt BEH op dit moment werk van de in het ADR-rapport opgenomen aanbevelingen. Zo is een aanvang gemaakt met het opstellen van DPIA's en worden procesbeschrijvingen versneld opgepakt. Ook wordt onderzoek gedaan naar de aanschaf of ontwikkeling van een ondersteunend ICT-systeem dat voorziet in de Wpg-specifieke verplichtingen. Daarnaast is per werkproces een risicoregister opgesteld met de daarbij te nemen beheersmaatregelen en zijn stappen gezet in het aanwijzen van bevoegd functionarissen en het opzetten van een register. BEH zal alle inspanningen betrachten om eind januari 2023 al een groot deel van de aanbevelingen opgevolgd te hebben.

Realistisch gezien zal een deel van de verbetermaatregelen niet op korte termijn zijn geïmplementeerd. De aanschaf van een passend ICT-systeem is bijvoorbeeld een traject dat langer dan een jaar zal duren. We onderzoeken of tijdelijke alternatieve beheersmaatregelen mogelijk zijn om de risico's zo goed mogelijk te beperken. Aanbevelingen die niet op korte termijn kunnen worden geïmplementeerd, zullen in de jaarlijkse interne audit worden meegenomen.

Eind 2023 zal BEH een hercontrole laten uitvoeren door de ADR. Het is onze verwachting dat door de maatregelen die genomen worden een belangrijke verbetering te zien zal zijn ten opzichte van het voorliggende rapport.

Hoogachtend,

Persoonsgegevens

Grote Ondernemingen
Landelijke directie

Datum
20 december 2022

Ons kenmerk
Audit Wet Politiegegevens Bureau Economische Handhaving, 2022-0000027629

departementaal VERTROUWELIJK

Auditdienst Rijk
Postbus 20201
2500 EE Den Haag
Persoonsgegevens