



AUTORITEIT
PERSOONSGEGEVENS

Wpg-audit

Onderzoek aanlevering auditrapporten

Over de Autoriteit Persoonsgegevens

Iedereen heeft recht op een zorgvuldige omgang met zijn persoonsgegevens. De Autoriteit Persoonsgegevens houdt toezicht op de naleving van de wettelijke regels voor bescherming van persoonsgegevens en adviseert over nieuwe regelgeving.



Inhoudsopgave

1.	Inleiding	3
2.	Conclusie	3
3.	Over het onderzoek	4
3.1	Procesverloop	4
	Aanlevering blijft achter, AP verleent uitstel	4
	Deel werkgevers blijft in gebreke, AP gaat in gesprek met werkgevers	5
	Gesprekken met werkgevers	5
3.2	Bevindingen	5
	Opzet van de audits vergelijkbaar	5
	Deel werkgevers levert geen rapport aan of niet tijdig	6
	Redenen voor geen of verlate aanlevering	6
	Betrokkenheid functionaris voor gegevensbescherming	6
	Geen externe audit uitgevoerd, maar wel een interne audit	6
4.	Quickscan van inhoudelijke bevindingen	7
5.	Afsluitend en hoe nu verder	9
6.	Bijlage: Visuele weergave resultaten	10
	Tabel 1: Aantal boa's per werkgever	10
	Tabel 2: Aantal domeinen per werkgever	10
	Tabel 3: Aantallen domeinen en boa's per domein	11
	Tabel 4: Aanlevering rapporten naar aantal boa's in dienst	11
	Tabel 5: Visuele weergave resultaten van de quickscan	12



1. Inleiding

Sinds 1 januari 2008 bevat de Wet Politiegegevens (Wpg) in artikel 33 de verplichting voor de verwerkingsverantwoordelijke om periodiek een privacy audit te laten uitvoeren door een externe auditor. Door de komst van de Richtlijn voor gegevensbescherming door politie en justitie¹ wijzigde met per 1 januari 2019 de Wpg. Sindsdien vallen buitengewone opsporingsambtenaren (boa's) die voor hun opsporingstaak persoonsgegevens verwerken onder de Wpg. Daarmee is de auditplicht ook van toepassing geworden op de werkgevers van de boa's.

Een groot deel van deze werkgevers betreft gemeentes. Daarnaast gaat het om andere overheidsorganisaties, zoals de Douane, of private organisaties als de NS, Staatsbosbeheer of Natuurmonumenten.

De boa-werkgevers waren verplicht om in 2021 voor de eerste keer de externe audit te laten uitvoeren en de resultaten daarvan aan de Autoriteit Persoonsgegevens (AP) te sturen. Het toesturen van het rapport is als verplichting opgenomen in de wet om de AP in staat te stellen effectief toezicht te houden. Dit rapport richt zich op de aanlevering van de rapporten. Op basis van een steekproef is een quickscan uitgevoerd naar de resultaten op hoofdlijnen. Een meer inhoudelijke beoordeling van de aangeleverde resultaten van de audit volgt op een later moment.

2. Conclusie

Werkgevers van boa's die voor de uitvoer van hun opsporingstaak persoonsgegevens verwerken zijn verplicht om eens per vier jaar een externe privacy audit uit te voeren. Deze verplichting heeft sinds de wijziging van de Wpg per 1 januari 2019 betrekking op meer dan 600 organisaties.

De AP heeft van minder dan de helft van de boa-werkgevers een auditrapport ontvangen. Daarmee is meer dan de helft van de boa-werkgevers in gebreke gebleven.

Daarnaast heeft de AP een quick scan uitgevoerd naar de resultaten uit de auditrapporten. Uit deze quick scan naar de resultaten van een selectie van 56 aangeleverde rapporten blijkt dat de meeste boa-werkgevers ruim onvoldoende aan de getoetste criteria voldoen. Wanneer criteria als onvoldoende zijn beoordeeld zal een organisatie een verbeterplan moeten opstellen en binnen een jaar een herbeoordeling laten uitvoeren. De resultaten van de herbeoordeling zullen eind 2023 aan de AP toegestuurd moeten worden.

De AP zal na ontvangst van de resultaten van de herbeoordelingen een vervolg geven aan dit rapport. Waar nodig zal de AP daarbij ook andere toezichtsinstrumenten inzetten.

¹ Richtlijn 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 (...), (EU) 2016/680.



3. Over het onderzoek

3.1 Procesverloop

Verplichting tot aanlevering en informatie over de auditplicht

De AP heeft begin juni 2021 informatie geplaatst op de AP-website over de auditplicht van boa-werkgevers.²

In de markt zijn meerdere initiatieven genomen om de audit te ondersteunen. Zo heeft de NOREA, de beroepsvereniging van IT-auditors, de handreiking 'Privacy audit Wet politiegegevens (Wpg) voor boa's' gepubliceerd.³ Het doel van deze handreiking is "om de IT-auditor relevante informatie te verstrekken en een uniform toetsbaar normenkader te bieden voor het zorgvuldig uitvoeren van een Assurance-opdracht (Privacy audit) op basis van de Wet politiegegevens (Wpg) en het Besluit politiegegevens buitengewoon opsporingsambtenaren (Bpg boa)." Door de handreiking te volgen zijn de uitvoering van de (externe) audits en de rapportages van vergelijkbare kwaliteit en daardoor onderling vergelijkbaar.⁴ De AP heeft op de AP-website naar het door NOREA ontwikkelde model/template voor een Wpg privacy audit verwezen.

De VNG heeft in september 2021 het werkdocument 'Audit wet politiegegevens voor gemeenten' gepubliceerd.⁵ Dit werkdocument steunt op de NOREA-handreiking. Daarnaast zijn meerdere kennisdocumenten gepubliceerd die gemeenten helpen bij de uitvoering van de Wpg.⁶

Aanlevering blijft achter, AP verleent uitstel

Op 15 november 2021 heeft de AP boa-werkgevers 1 jaar uitstel gegeven voor het toesturen van het Wpg-auditrapport. Dat betekende dat zij tot en met 31 december 2022 de tijd hadden om hun auditrapport aan de AP te sturen. Verzoeken tot nader uitstel zijn afgewezen. Omdat halverwege 2022 nog weinig auditrapporten waren ontvangen door de AP, is op 21 juni 2022 aandacht besteed aan het belang van een tijdige aanlevering in het nieuwsbericht "Nog weinig boa-werkgevers hebben verplichte Wpg-audit aangeleverd".⁷ Daarbij is ook het belang benadrukt van het tijdig uitvoeren van de audit. Interne of bestuurlijke processen kunnen immers een vertragende werking hebben. Het is daarom aan te raden om daarmee in de planning rekening te houden.

Op 31 december 2022 verwachtte de AP van ruim 600 boa-werkgevers een auditrapport te hebben ontvangen. Op 11 oktober 2022 waren dit er echter nog maar 34. Op 21 november was dit aantal gestegen tot 45 en op 14 december waren 90 rapporten ontvangen. In de periode tussen kerst en oud en nieuw is door veel boa-werkgevers (en door hen ingehuurde auditoren) een inhaalslag gemaakt. Op het meetmoment dat is gebruikt voor dit rapport, 16 januari 2023, hadden uiteindelijk 299 organisaties een auditrapport aangeleverd of laten weten dat het rapport onderweg was. Daarmee heeft de AP van ongeveer de helft van de boa-werkgevers een rapport ontvangen. Dat waren vooral de grotere boa-werkgevers. Veel kleinere boa-werkgevers hebben geen auditrapport aangeleverd.

² Website AP, [Voor professionals | Autoriteit Persoonsgegevens](#)

³ Zie het nieuwsbericht van 24 juni 2021 <https://www.norea.nl/nieuws/handreiking-privacy-audit-wet-politiegegevens-wpg-voor-boas>.

⁴ Daarnaast wordt opgemerkt dat de regeling periodieke audit politiegegevens voorschrijft dat de privacy audit wordt uitgevoerd door middel van een Electronic Data Processing (EDP) audit, ook wel IT-audit genoemd. Aan een IT-auditor worden beroepseisen gesteld. Hierdoor wordt de kwaliteit van de audit ook geborgd in de kwaliteit van de auditoren.

⁵ [Producten - Informatiebeveiligingsdienst](#)

⁶ [Kennisproducten met betrekking tot de Wet politiegegevens - Informatiebeveiligingsdienst](#)

⁷ <https://autoriteitpersoonsgegevens.nl/nl/nieuws/nog-weinig-boa-werkgevers-hebben-verplichte-wpg-audit-aangeleverd>



Deel werkgevers blijft in gebreke, AP gaat in gesprek met werkgevers

Een aantal van de boa-werkgevers die nog geen auditrapport had aangeleverd, heeft dit aan de AP gemeld en een toelichting gegeven. Een groot deel van de boa-werkgevers heeft dat echter niet gedaan. De AP kondigde daarom in januari 2023 aan boa-werkgevers aan te spreken op het niet of niet tijdig aanleveren. Daarbij gaf de AP aan niet uit te sluiten dat daaruit handhavende activiteiten zullen voortvloeien. Hierover publiceerde de AP het persbericht "*AP treedt op tegen boa-werkgevers die verplichte Wpg-audit niet toesturen*" op de website.⁸ De AP selecteerde vervolgens 15 boa-werkgevers voor een gesprek, met als belangrijkste doel te achterhalen wat de reden was van het niet of niet tijdig aanleveren van het auditrapport. De selectie van die werkgevers was gebaseerd op een aantal criteria:

1. op de werkgever rust sinds 2019 de auditplicht;
2. de werkgever heeft meer dan 26 boa's in dienst;^{9 10}
3. de werkgever heeft geen auditverslag ingediend en ook niet laten weten wanneer de aanlevering te verwachten is.

Werkgevers die op eigen initiatief hebben laten weten dat de aanlevering van hun auditrapport vertraagd was, zijn uitgezonderd van de selectie voor gesprekken. Deze partijen hebben weliswaar niet voldaan aan de auditverplichting, maar in vrijwel alle gevallen is de reden daarvan gemeld. Aangezien het belangrijkste doel van de gesprekken het achterhalen van de reden van de niet-aanlevering was, is ervoor gekozen deze partijen niet uit te nodigen voor een gesprek.

Gesprekken met werkgevers

In februari 2023 heeft de AP met 9 werkgevers gesprekken gevoerd. Hierbij heeft de AP gesproken over de aanleverplicht, het belang van het uitvoeren van audits en de rol van de AP hierin. Ook is gesproken over de inrichting van audits en specifiek de Wpg-audit. De AP heeft tegen geen van de werkgevers aanvullende handhavende acties uitgevoerd.

3.2 Bevindingen

De hierna beschreven bevindingen zijn ontleend aan:

- het proces van aanlevering van de auditrapporten;
- de gesprekken die de AP heeft gevoerd met een aantal boa-werkgevers;
- mailberichten en brieven die de AP heeft ontvangen;
- overige signalen die bijvoorbeeld via de VNG zijn gemeld.

Opzet van de audits vergelijkbaar

Bijna alle ontvangen auditrapporten zijn opgemaakt met de door NOREA opgestelde template. Een aantal werkgevers geeft in het auditrapport aan dat één of meer onderwerpen uit de NOREA-template niet op de organisatie van toepassing zijn.

⁸ Persbericht 12 januari 2023, [AP treedt op tegen boa-werkgevers die verplichte Wpg-audit niet toesturen | Autoriteit Persoonsgegevens](#)

⁹ Vaststelling op basis van een overzicht van vergunningen, bron: ministerie van justitie en veiligheid, dd 07-07-2022

¹⁰ 51% van het aantal werkgevers heeft vijf of minder boa's in dienst. Door de grens te leggen bij 26 of meer boa's wordt een bepaalde omvang van de organisatie verondersteld. Daarnaast is de AP er van uit gegaan dat naarmate een organisatie meer boa's in dienst heeft de risico's ten aanzien van persoonsgegevens groter zijn.



Deel werkgevers levert geen rapport aan of niet tijdig

Een behoorlijk deel van de boa-werkgevers heeft de audit wel uitgevoerd en toegestuurd. Toch heeft meer dan de helft van de boa-werkgevers uiteindelijk geen auditrapport bij de AP aangeleverd. Een deel van de rapporten is te laat aangeleverd. Een deel van de boa-werkgevers heeft geen externe audit laten uitvoeren. De AP is door enkele partijen benaderd die aangaven dat de audit een te grote belasting vormt voor de organisatie.

Een aantal werkgevers heeft de AP geïnformeerd over een verlate aanlevering en/of gevraagd om uitstel. Bij dergelijke mededelingen of verzoeken heeft de AP benadrukt dat het aanleveren van het rapport voortvloeit uit de wet en dat een verwerkingsverantwoordelijke hiervan niet op eigen initiatief kan afwijken. Omdat het de eerste keer was dat de externe audit moest worden uitgevoerd, heeft de AP desalniettemin een verlate aanlevering in alle gevallen geaccepteerd.

Redenen voor geen of verlate aanlevering

Meerdere werkgevers hebben de rapportage niet tijdig aangeleverd. Daarvoor zijn verschillende redenen aangedragen:

- Een aantal werkgevers geeft aan niet op tijd te zijn begonnen. Of de interne werk- en afstemmingsprocessen nog niet (voldoende) te hebben ingericht op de uitvoering van de audits. Er werd bijvoorbeeld aangegeven nog in afwachting te zijn van oplevering door het auditbureau of dat het college van een gemeente geen zitting meer had, zodat geen intern akkoord gegeven kon worden. Of een vergelijkbare reden in de proces- of planningssfeer.
- Een aantal werkgevers geeft aan niet bekend te zijn met de auditplicht. Dit betreft vooral kleine boa-werkgevers.
- De wetgever duidt de werkgever van de boa aan als de verwerkingsverantwoordelijke. Deze is verantwoordelijk voor het uitvoeren van de Wpg-audits. Enkele als boa-werkgever aangemerkte organisaties geven echter aan dat de auditplicht niet op hen van toepassing is. Bijvoorbeeld omdat zij de boa's die bij hen in dienst zijn op basis van detachering of opleidingsplaatsen bij andere organisaties plaatsen. Zij sturen de boa's niet zelf aan en hebben geen toegang tot de door boa's gebruikte systemen en de daarin opgenomen verwerkingen van persoonsgegevens.
- Een werkgever gaf aan dat de auditplicht 'van de radar was geraakt' door personele wisselingen.

Betrokkenheid functionaris voor gegevensbescherming

De AP constateert dat regelmatig de functionaris voor gegevensbescherming (FG) het Wpg-auditrapport aanleverde, maar dat de FG bij de gesprekken met de AP niet altijd aanwezig was.¹¹

De AP acht het van belang dat de FG betrokken wordt bij de uitvoering en opvolging van de Wpg-audit. De FG is belast met het toezicht op de naleving van de Wpg en met het daarover informeren en adviseren op grond van artikel 36, 3^e lid onder a, Wpg. Daarnaast treedt de FG op grond van artikel 36, 1^e lid onder e, Wpg op als contactpunt voor de AP. Dat laat onverlet dat de auditplicht op de verwerkingsverantwoordelijke rust en deze daarover dient te rapporteren, niet de FG.

Geen externe audit uitgevoerd, maar wel een interne audit

Een aantal werkgevers heeft geen externe audit uit laten voeren, maar wel een interne audit uitgevoerd. Daarbij is, voor zover de AP steekproefsgewijs heeft geconstateerd, gebruik gemaakt van de NOREA- of

¹¹ Uit de ontvangen rapportages is geen beeld gevormd van de frequentie, aard en intensiteit van de betrokkenheid van de FG bij de Wpg-audits. Dat zal in een later stadium aan de orde komen.



VNG-template voor de audit. Als de audit echter niet door een externe, onafhankelijke auditor is uitgevoerd, dan voldoet die audit niet aan de eisen die aan de vierjaarlijkse externe audit zijn gesteld.¹²

Deze groep werkgevers was van mening dat uit de interne audit voldoende duidelijk werd op welke punten de naleving van de Wpg tekortschoot. En dat een externe audit daaraan niets zou kunnen toevoegen en daarom een verspilling van tijd en geld zou zijn. In plaats daarvan hebben deze werkgevers ervoor gekozen om direct aan de slag te gaan met het verbeterplan en vervolgens als hercontrole alsnog die externe audit te laten uitvoeren. De AP heeft die werkwijze ditmaal geaccepteerd, maar benadrukte dat die werkgevers de auditplanning moeten aanpassen aan de oorspronkelijke planning of cyclus die volgt uit de Wpg, en die geldt voor alle boa-werkgevers.

4. Quickscan van inhoudelijke bevindingen

De AP heeft op basis van een steekproef naar de inhoud van de rapporten gekeken, om zo een quickscan van de naleving krijgen. Hiervoor heeft de AP iets meer dan een derde van de aangeleverde rapportages nader onder de loep genomen. In bijlage 4 zijn de resultaten in meer detail te vinden.

Uit de quickscan volgt in zijn algemeenheid dat de naleving van de Wpg bij veel boa-werkgevers op meerdere terreinen nog niet op orde is. De externe auditors hebben bij 31 Wpg-onderwerpen getoetst of deze in voldoende mate (groen), niet volledig (oranje) of niet (rood) zijn opgezet, bestaan en/of effectief werken. Wanneer enkel naar de opzet van de onderzochte Wpg-onderwerpen wordt gekeken, blijkt dat in ongeveer de helft van de bekeken rapporten in voldoende mate wordt voldaan aan de beoordeelde normvereisten zoals die zijn benoemd in de opzet van de Norea.

In onderstaande overzicht zijn de resultaten van de steekproef gevisualiseerd.¹³ Daarbij is de gemiddelde score weergegeven van 112 beoordeelde domeinen van 56 boa-werkgevers. Zie voor een nadere toelichting en een detailoverzicht in hoofdstuk 6, bijlage 5.

Overzicht resultaten quickscan naar criterium (gemiddelde score)

Criterium (o.b.v. Norea) ¹⁴	Gemiddelde Score ¹⁵
1.Reikwijdte	1,99
2.Doelbinding	1,75
3.Noodzakelijkheid en rechtmatigheid, vermelding herkomst	1,77
4.Juistheid en volledigheid politiegegevens	1,78
5.Onderscheid feiten en oordeel	1,94
6.Gegevensbescherming door beveiliging en ontwerp	2,04
7.Gegevensbescherming door standaardinstellingen	2,00
8.Gegevensbeschermingseffectbeoordeling/ DPIA	1,95

¹² Aan wie ingevolge artikel 2 van het Besluit politiegegevens buitengewoon opsporingsambtenaren in samenhang met artikel 6:5?? van het Besluit politiegegevens eisen worden gesteld met betrekking tot werkwijze, deskundigheid en betrouwbaarheid.

¹³ De kleurschaal van rood (laagste score) naar groen (hoogste score) is bedoeld als visuele ondersteuning.

¹⁴ Voor een toelichting op de criteria, zie Norea <https://www.norea.nl/nieuws/handreiking-privacy-audit-wet-politiegegevens-wpg-voor-boas>.

¹⁵ Score 1=laagst, 3 = hoogst



9. Bijzondere categorieën van politiegegevens	1,89
10. Autorisaties en toegang tot politiegegevens	1,81
11. Autorisaties: aanwijzen functionarissen	1,63
12. Onderscheid tussen categorieën van betrokkenen	2,09
13. Verwerker en Verwerkersovereenkomst	2,16
14. Geheimhoudingsplicht	2,32
15. Geautomatiseerde individuele besluitvorming	1,79
16. Uitvoering van de dagelijkse politietaak	1,54
17. Ter beschikking stellen van politiegegevens	1,63
18. Geautomatiseerd vergelijken en in combinatie zoeken	1,83
19. Ondersteunende taken	1,61
20. Bewaartermijnen, verwijderen en vernietigen	1,50
21. Verstrekking van politiegegevens aan anderen	1,84
22. Doorgiften aan derde landen	1,71
23. Verstrekking aan derden structureel voor samenwerkingsverbanden	1,89
24. Rechtstreekse verstrekking	2,03
25. Rechten van de betrokkene	2,03
26. Register	1,79
27. Documentatie	1,62
28. Logging	1,43
29. Audits	1,65
30. Melding datalekken	2,34
31. Functionaris voor gegevensbescherming	2,04

Op verschillende punten laten de auditresultaten gemiddeld een positieve score zien (score 2,1 of hoger in een reeks lopend van 1 (minimum) naar 3 (maximum)). Uit de quickscan van de boa-werkgevers blijkt dat 61% van de boa-werkgevers geheel of gedeeltelijk voldoet aan het criterium om onderscheid te maken tussen verschillende categorieën van betrokkenen (criterium 12). Aan de verplichting tot geheimhouding (criterium 14) voldoet 75% in gehele of gedeeltelijke mate. Een vergelijkbaar hoog percentage van 79% geldt voor de meldplicht datalekken (criterium 30).

Op verschillende punten laten de auditresultaten gemiddeld een (zeer) negatieve score zien (score 1,6 of lager in een reeks lopend van 1 (minimum) naar 3 (maximum)). Uit de quickscan van de boa-werkgevers blijkt bijvoorbeeld dat 61% van de boa-werkgevers onvoldoende beleid heeft opgezet voor autorisaties, het aanwijzen van functionarissen (criterium 11). Voor de opzet voor het uitvoeren van de dagelijkse politietaak (criterium 16) scoort 67% onvoldoende. Het beleid voor bewaartermijnen, verwijderen en vernietigen (criterium 20) en logging (criterium 28) wordt in respectievelijk 68% en 70% van de rapporten als onvoldoende beoordeeld.

Een aantal punten is regelmatig niet beoordeeld in rapporten. Zo is het beleid rondom het geautomatiseerd vergelijken en in combinatie zoeken (criterium 18) in 24 van de 112 in de steekproef opgenomen rapporten beoordeeld, en dus 88 keer niet. Voor de geautomatiseerde individuele besluitvorming (criterium 15) is dat 34 keer, en daarmee 78 keer niet. De opzet rondom doorgifte naar derde landen (criterium 22) is 31 keer wel en daarmee 81 keer niet beoordeeld. De AP heeft de redenen voor het weglaten van deze criteria nog niet beoordeeld.



Bij deze cijfers en percentages merkt de AP op dat bij meerdere boa-werkgevers op enkele criteria in de 'werking' een hogere score voorkwam dan voor de 'opzet' of 'bestaan'. Dat zou inhouden dat de Wpg in de praktijk wordt nageleefd, maar dat dit niet gestaafd kan worden aan de hand van beleid of procedures. Bij navraag, onder andere in de interviews, werd als verklaring gegeven dat de Wpg in de praktijk werd gevolgd maar dat beleid of procedures ontbraken.

De AP heeft slechts een globale blik op de rapporten geworpen, gelet op de systematiek van de Wpg-audit. Daarbij krijgt de verwerkingsverantwoordelijke nadrukkelijk de gelegenheid om verbetermaatregelen uit te voeren en binnen een jaar na de audit een hercontrole uit te (laten) voeren. Na ontvangst van de resultaten van deze hercontroles, die de AP eind 2023 verwacht, zal de AP scherper naar de inhoudelijke bevindingen kijken en bepalen of de AP het toezicht nader moet invullen. En zo ja, op welke wijze.

5. Afsluitend en hoe nu verder

Dit rapport gaat vooral in op de aanlevering van auditrapporten. De AP vindt het positief dat vrijwel alle grotere boa-werkgevers een externe audit hebben laten uitvoeren en daarover aan de AP hebben gerapporteerd. De aanlevering is echter niet in alle gevallen tijdig gedaan, terwijl ook een substantieel deel van de boa-werkgevers géén auditrapportage heeft aangeleverd. De AP gaat in gesprek met het ministerie van Justitie en Veiligheid, als primair beleidsverantwoordelijke, om vervolgstappen te bepalen.

Een aantal kleinere boa-werkgevers geeft aan de huidige opzet van de audit niet proportioneel te vinden. Dit signaal zal de AP delen met het ministerie van Justitie en Veiligheid.

De AP heeft de aangeleverde rapporten nu niet inhoudelijk beoordeeld. Werkgevers waarbij uit de controleresultaten blijkt dat zij niet aan de Wpg voldoen, moeten een verbeterplan op stellen en uit voeren. Vervolgens moeten ze binnen een jaar een herbeoordeling laten uitvoeren op die onderdelen die niet voldeden aan de gestelde voorwaarden. De herbeoordeling kan plaatsvinden met actuele informatie. De resultaten van de herbeoordeling worden aan de AP toegezonden. De AP houdt hierbij vast aan de termijnen en intervallen die afgeleid worden uit de wet. De AP verwacht rapporten van herbeoordelingen dan ook vóór 31 december 2023. Gezien de ervaringen raadt de AP partijen aan rekening te houden met de duur van audittrajecten en interne besluitvorming om een tijdige aanlevering mogelijk te maken.

De AP zal na ontvangst van de resultaten van de herbeoordelingen een vervolg geven aan dit rapport. Waar nodig zal de AP daarbij ook andere toezichtsinstrumenten inzetten.



6. Bijlage: Visuele weergave resultaten

Tabel 1: Aantal boa's per werkgever

Onderstaande tabel geeft het totale aantal boa-werkgevers aan. De populatie is daarbij verdeeld naar aantallen boa's, verdeeld in intervallen. Zo is te zien dat 122 werkgevers 1 boa in dienst hebben en 41 werkgevers tussen de 26 en de 50 boa's. Uit de tabel blijkt dat 51% van de werkgevers 5 of minder boa's in dienst heeft. 13% van de werkgevers heeft 26 of meer boa's in dienst, waarbij slechts 3% (20 werkgevers) meer dan 100 boa's in dienst heeft.

boa's in dienst per werkgever			
boa's in dienst	Aantal werkgevers	Aantal werkgevers (cumulatief)	Percentage
1		122	20%
2 – 5		193	31%
6 – 10		114	18%
11 – 25		108	18%
26 – 50		41	7%
51 – 99		19	3%
100 - 5000		20	3%

Tabel 2: Aantal domeinen per werkgever

Onderstaande tabel geeft aan op hoeveel domeinen (zie voor de domeinen tabel 3) een werkgever boa's inzet. Uit de tabel is af te lezen dat 391 werkgevers boa's werkzaam hebben in 1 domein en 71 werkgevers boa's werkzaam hebben in 3 domeinen. Een beperkt aantal werkgevers (24) heeft boa's werkzaam in 4 of 5 domeinen.

BOA-WERKGEVERS MET AANTAL DOMEINEN	AANTAL WERKGEVERS	AANTAL BOA'S
1 DOMEIN	391	4.411
2 DOMEINEN	130	2.358
3 DOMEINEN	71	11.256
4 DOMEINEN	21	4.560
5 DOMEINEN	3	689
6 DOMEINEN	0	0



Tabel 3: Aantallen domeinen en boa's per domein

Onderstaande tabel toont het aantal domeinen, het aantal boa's per domein en het aantal werkgevers. Deze cijfers geven het aantal domeinen per werkgever aan, waarbij deze cijfers niet zijn gecorrigeerd voor werkgevers met boa's in meerdere domeinen. Bijvoorbeeld: een werkgever die boa's in de domeinen I en II in dienst heeft, wordt tweemaal geteld in het aantal domeinen.

DOMEINEN ¹⁶		AANTAL BOA'S IN DOMEIN	AANTAL WERKGEVERS MET BOA'S IN HET BETREFFENDE DOMEIN ¹⁷
DOMEIN I	Openbare ruimte	4.411	341
DOMEIN II	Milieu, welzijn, infra	2.358	270
DOMEIN III	Onderwijs	740	216
DOMEIN IV	Openbaar vervoer	4.560	13
DOMEIN V	Werk, inkomen, zorg	689	101
DOMEIN VI	Generieke opsporing	10.516	58
TOTAAL		23.274	

Tabel 4: Aanlevering rapporten naar aantal boa's in dienst

In totaal heeft iets minder dan de helft van de boa-werkgevers een audit aangeleverd. Gerekend naar de hoeveelheid boa's in dienst, dan zijn er grote verschillen te zien tuss.

De werkgevers van boa's in domein IV, openbaar vervoer, hebben vrijwel allemaal tijdig de audit uitgevoerd en het rapport toegezonden. De werkgevers van het domein generieke opsporing vallen grotendeels al langere tijd onder de Wpg en de auditplicht. Hierdoor loopt de betreffende auditcyclus anders dan bij de groep waarop de auditverplichting vanaf 1 januari 2021 is gaan lopen. Meerdere grote boa-werkgevers zijn in dit domein te vinden, zoals de Belastingdienst (douane), de Koninklijke Marechaussee en de politie. Dit verklaart het relatief lage aantal aanleveringen bij de grootste boa-werkgevers.

Aantal boa's in dienst en percentage aanlevering rapporten

BOA'S IN DIENST	Aantal werkgevers	Aangeleverd	Percentage (%)
1		122	16
2 – 5		193	83
6 – 10		114	67
11 – 25		108	47
26 – 50		41	29
51 – 99		19	12
100 – 5000		20	7
	Totaal 617	Totaal 261	Gemiddeld 42%

¹⁶ In de [Beleidsregels Buitengewoon Opsporingsambtenaar](#) zijn de domeinen en bevoegdheden van boa's per domein opgenomen.

¹⁷ Een boa-werkgever kan boa's in meerdere domeinen werkzaam hebben. Zie ook tabel 2.



Tabel 5: Visuele weergave resultaten van de quickscan

De AP heeft in een quickscan de resultaten van een aantal Wpg audits bekeken. Hiermee heeft de AP een indruk gekregen van de mate van naleving van de Wpg over het gemeten tijdvak. De resultaten van 'de opzet' van een aantal rapporten zijn hieronder visueel in een tabel weergegeven.

Opmerkingen over de tabel

De tabel is een visuele weergave van een steekproef van 112 beoordeelde domeinen van 56 boa-werkgevers. Hoewel het geen volledig willekeurige steekproef is, is de spreiding van de resultaten dusdanig dat het beeld naar verwachting representatief is. De selectie is samengesteld met:

- rapporten die op volgorde van aanlevering zijn verwerkt;
- alle aangeleverde rapporten van gemeenten met 100.000 of meer inwoners;
- een selectie van rapporten uit alle domeinen.

In de tabel zijn alleen de resultaten opgenomen uit de kolom 'opzet' uit de NOREA-template.¹⁸ Meerdere partijen geven aan dat zij op het punt 'opzet' tekort schieten, maar dat naleving van de vereisten ('werking') in de praktijk wel voldoende is. Dit heeft de AP niet nader uitgewerkt of onderzocht. De toelichting geeft bij de begrippen aan:

- **Opzet:** De organisatie heeft de interne beheersingsmaatregelen beschreven die, indien deze werken zoals beschreven, een redelijke mate van zekerheid bieden dat voorzien is in de borging van de wettelijke eisen met betrekking tot de verwerking van politiegegevens door boa's.
- **Bestaan:** De organisatie heeft de interne beheersingsmaatregelen overeenkomstig de opzet daadwerkelijk geïmplementeerd en toegepast.
- **Werking:** De organisatie heeft de interne beheersingsmaatregelen gedurende de verslagperiode volgens de opzet toegepast. In het geval van handmatige beheersingsmaatregelen zijn deze toegepast door competente én bevoegde personen.¹⁹

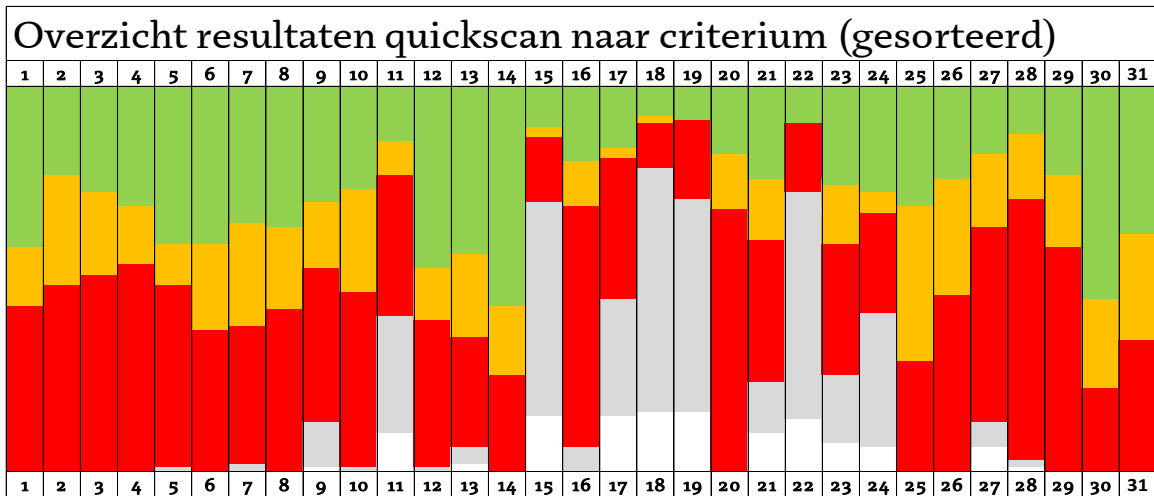
De resultaten uit de toegestuurde rapporten zijn omgezet naar kleurcoderingen die in lijn liggen met de coderingen die gebruikt worden in de rapporten.

Kleur	Toelichting
groen	voldoet aan de beheersingsmaatregel
oranje	voldoet niet volledig aan de beheersingsmaatregel
rood	voldoet niet aan de beheersingsmaatregel
grijs	niet getest
wit	niet van toepassing

De resultaten zijn gesorteerd weergegeven. Hierdoor is geen herleiding naar individuele resultaten mogelijk. Deze sortering heeft alleen een visueel doel.

¹⁸ Met het criterium opzet wordt bedoeld dat de organisatie de beheersingsmaatregelen heeft 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. De andere criteria waarop getoetst is zijn 'bestaan' en 'werking'.

¹⁹ Norea, Handreiking Privacy audit Wpg voor boa's, v1 24 juni 2021, bijlage 3 Guidance bij de te onderzoeken Wpg beheersingsmaatregelen



Legenda

- voldoet aan de beheersingsmaatregel
- voldoet niet volledig aan de beheersingsmaatregel
- voldoet niet aan de beheersingsmaatregel
- niet getest
- niet van toepassing

Onderwerpen en beheersingsmaatregelen

Bron: NOREA Handreiking Privacy audit Wpg (boa), Versie 1.0, Definitief 24 juni 2021

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
7. Gegevensbescherming door standaardinstellingen
8. Gegevensbeschermingseffectbeoordeling/ Data protection impact assessment (DPIA)
9. Bijzondere categorieën van politiegegevens
10. Autorisaties en toegang tot politiegegevens
11. Autorisaties: aanwijzen functionarissen
12. Onderscheid tussen verschillende categorieën van betrokkenen
13. Verwerker en Verwerkersovereenkomst
14. Geheimhoudingsplicht
15. Geautomatiseerde individuele besluitvorming
16. Uitvoering van de dagelijkse politietaak
17. Ter beschikking stellen van politie-gegevens binnen het WPG-domein
18. Geautomatiseerd vergelijken en in combinatie zoeken
19. Ondersteunende taken
20. Bewaartermijnen, verwijderen en vernietigen
21. Verstrekking van politiegegevens aan anderen dan politie en Koninklijke marechaussee
22. Doorgiften aan derde landen
23. Verstrekking aan derden structureel voor samenwerkingsverbanden
24. Rechtstreekse verstrekking
25. Informatie aan de betrokkene, recht op inzage, rectificatie en verwijdering
26. Register
27. Documentatie
28. Logging
29. Audits
30. Melding datalekken
31. Functionaris voor gegevensbescherming

Figuur 1: Overzicht steekproef scores van 56 boa-werkgevers



Vragen over de Algemene verordening gegevensbescherming

Op onze website autoriteitpersoonsgegevens.nl vindt u informatie en antwoorden op vragen over de Algemene verordening gegevensbescherming (AVG). Heeft u op deze website geen antwoord op uw vraag gevonden? Dan kunt u contact opnemen met het Informatie- en Meldpunt Privacy van de Autoriteit Persoonsgegevens op 088-1805 250.