FAQ – PRIVACY AUDIT WET POLITIEGEGEVENS

VERSIE 1.3 – 17 MAART 2026

Update van de testaanpak Privacy audit Wpg voor boa's 2024 d.d. 3 september 2024

Naar aanleiding van de gestelde vragen aan de Wpg-Werkgroep over de NOREA Handreiking Privacy audit Wpg 2024 d.d. 3 september 2024 brengen we onderstaande FAQ uit om de vragen van een eenduidig antwoord te voorzien.

#	Vraag	Antwoord
1	**5-2-2025:** De externe initiële audit was in de praktijk destijds over de over de periode 2019-2021. Nu de controleperiode voor de tweede externe audit is bepaald op de periode 2021-2024 is er dan geen sprake van een zekere dubbeling?	Dat klopt. De oorspronkelijke initiële audit ging formeel over de twee jaar tussen 9 maart 2019 (datum inwerkingtreding Bpg boa) tot 9 maart 2021. In de auditpraktijk hebben we in de vorige Handreiking inderdaad aangegeven dat IT-auditors als controleperiode 9 maart 2019 tot en met 31 december 2021 konden hanteren. Voor zover we hebben kunnen waarnemen is dat in verreweg de meeste gevallen ook gebeurd. Om "dubbeling" te voorkomen hebben we daarom in de onlangs gepubliceerde template van het Wpg assurancerapport opgenomen, dat de IT-auditor dient vast te stellen of er over de vereisten van de Wpg in het kalenderjaar 2021 al eerder assurance is gegeven. Indien dat het geval is dan wordt de controleperiode voor de 2e externe audit beperkt tot de periode vanaf de laatste auditdatum tot en met 31 december 2024.
2	**5-2-2025:** Verschillende auditpartijen hebben tijdens de eerste auditcyclus vragen gesteld over het geven van een 'afkeurend oordeel'.	In overleg met verschillende partijen (o.a. AP en ADR) is besloten in het template assurance-rapport drie keuzes m.b.t. oordelen op te nemen: 'oordeel (zonder beperking)', 'oordeel met beperking' en 'afkeurend oordeel'. Voor een 'afkeurend oordeel' geldt dat dit oordeel gegeven wordt als er bij 10[1] of meer beheersingsmaatregelen in opzet, bestaan en/of werking niet wordt voldaan aan de door de wetgever gestelde eisen. In dat geval zijn deze aangelegenheden materieel en van diepgaande negatieve invloed op het beschermen van de privacy van betrokkenen. Ten behoeve van het systeemtoezicht door de AP dienen IT-Auditors het genoemde aantal normen dat niet in opzet, bestaan en/of werking voldoet (10) strikt te hanteren bij de keuze voor het geven van het soort oordeel.
2a	**3-10-2025:** Er zijn vragen gesteld over het hanteren van het aantal normen waarbij een 'afkeurend oordeel' wordt gegeven. Is dit bijvoorbeeld per domein en tellen ook de ITGC maatregelen hierbij mee?	Het aantal normen dat niet voldoet wordt bepaald per domein en bestaat uit de optelsom van de normen 1 t/m 31 en de 5 ITGC maatregelen (in totaal dus 36 normen). Indien in één (1) of meerdere domeinen voor 10 of meer van de 36 normen niet wordt voldaan in opzet, bestaan en/of werking, wordt een afkeurend oordeel gegeven.
3	**3-10-2025:** Het Nederlands Genootschap van Functionarissen Gegevensbescherming (NGFG.nl) heeft gemeld dat niet alle in art. 36 Wpg genoemde onderwerpen zijn uitgewerkt in de testaanpak van norm 31.	In overleg met de NGFG is besloten dat de hierna genoemde onderwerpen worden toegevoegd aan de testaanpak van norm 31: ○ Toetsen of de FG is aangemeld bij de AP. ○ Toetsen of er een aanstellingsbesluit voor de FG is en of hij daarin adequaat is belast met de taken zoals opgenomen in de wet. ○ Toetsen of de FG jaarlijks verslag uitbrengt (naast het expliciet vaststellen dat een FG-jaarverslag is opgesteld en uitgebracht aan de verwerkingsverantwoordelijke, is het

[1] Hieronder worden zowel de algemene als de technische en organisatorische (IT) beheersingsmaatregelen verstaan.

#	Vraag	Antwoord
		inhoudelijk beoordelen van het FG-jaarverslag daarbij niet de bedoeling). ○ Toetsen of de contactgegevens van de FG door de verwerkingsverantwoordelijke openbaar zijn gemaakt.
4	**17-11-2025:** Er zijn verschillende vragen gesteld over de 'Werkgever' versus de 'Verwerkingsverantwoordelijke'	In de NOREA Handreiking Privacy audit Wpg voor boa's staat dat de werkgever (doorgaans) de verwerkingsverantwoordelijke is. Hierop zijn verschillende uitzonderingen denkbaar. In de basis is degene 'onder wiens gezag' de boa de politiegegevens verwerkt, de verwerkingsverantwoordelijke. Hieruit volgt dat dit niet altijd de werkgever van de boa die de politiegegevens verwerkt. Uitzonderingsgevallen zijn o.a. wanneer een boa in een samenwerkingsverband de werkzaamheden verricht of wanneer een boa is 'uitgeleend' aan een andere organisatie (bijvoorbeeld een buurgemeente). Ook kan sprake zijn van inhuur van een boa (zie ook #5). In deze gevallen is niet de werkgever van de boa de verwerkingsverantwoordelijke, maar de organisatie waar de boa de werkzaamheden uitvoert. Op deze 'inlenende' organisatie rust dan ook de verplichting om over de verwerkingen van deze boa een audit te laten uitvoeren.
5	**17-11-2025** Er zijn vragen gesteld over de inhuur van boa's. Kan dit wel en wie is hier dan de verwerkingsverantwoordelijke?	Uitgangspunt is dat boa's in beginsel in bezoldigde dienst moeten zijn van een publiekrechtelijk rechtspersoon of een privaatrechtelijk rechtspersoon die voldoet aan de voorwaarden, genoemd in de *Regeling Beleidsregels Buitengewoon Opsporingsambtenaar*. In de regeling worden verschillende uitzonderingen genoemd, o.a. inhuur van een particuliere functionaris voor boa-functies*, het lopen van een stage met de status van buitengewoon opsporingsambtenaar en de onbezoldigde vrijwillige ambtenaar van politie. * Ingevolge de voornoemde Regeling is inhuur van een particuliere functionaris alleen mogelijk in de domeinen I Openbare Ruimte, II Milieu, Welzijn en Infrastructuur (uitsluitend voor de handhaving en het toezicht in buitengebieden), III Onderwijs en IV Openbaar Vervoer. Voor ingehuurde boa's geldt dat zij moeten voldoen aan dezelfde eisen en gehouden zijn aan dezelfde voorwaarden zoals deze gelden voor niet-ingehuurde boa's. Daarnaast worden aan de mogelijkheid van inhuur bijzondere voorwaarden gesteld, deze zijn vermeld bij het betreffende domein (9.2 e.v.).
6	**17-03-2026** Er zijn vragen gesteld over de Wet administratiefrechtelijke handhaving verkeersvoorschriften (Wahv, ook bekend onder de naam 'Wet Mulder'), en meer specifiek of dit de verwerking van politiegegevens betreft.	De 'Wet Mulder bon' betreft een **administratieve afdoening** (geen bestuursrechtelijke) van een feitegedraging die wordt geconstateerd door een opsporingsambtenaar conform zijn bevoegdheden genoemd in zijn akte (domein). Belangrijk is hierbij om te weten dat de opsporingsambtenaar die gebruik maakt van zijn bevoegdheden en hierbij politiegegevens verwerkt, dat dit niets te maken heeft met bestuursrecht. Het feit dat een 'Wet Mulder bon' ingevolge de Wet Mulder administratief wordt afgehandeld, doet hier niets aan af. Er zijn meer mix vormen zoals de Bestuursrechtelijk Straf Beschikking (BSB). Ook die wordt vastgesteld door een opsporingsambtenaar, echter wordt hier de **afdoening bestuursrechtelijk** gedaan en opgelegd door het bevoegd gezag, bijvoorbeeld de Directeur Omgevingsdienst. (en dus niet de OVJ). Ook hier worden politiegegevens verwerkt zoals in de vorige alinea is beschreven. **Resume: De bovenstaande beschrijvingen betreffen de verwerking van politiegegevens en vallen dan ook onder de**

#	Vraag	Antwoord
		betreffende wet- en regelgeving (Wpg, Bpg boa e.d.) en niet onder de AVG.
7	**17-03-2026** Er zijn vragen gesteld over het toepassingsbereik van de NOREA Handreiking Wpg voor Boa's en meer specifiek of deze ook geldt voor de Bijzondere Opsporingsdiensten (BOD's).	Bij het opstellen van de NOREA Handreiking Wpg voor boa's zijn de wettelijke bepalingen uit de Wpg vertaald in concrete, toetsbare normen. Deze wettelijke bepalingen uit de Wpg gelden niet alleen voor boa-organisaties maar ook voor iedere andere organisatie die politiegegevens verwerkt – waaronder de BOD's.- en daarmee onder de auditplicht van de Wpg valt. Hierbij dient wel rekening te worden gehouden met de aard dan wel gevoeligheid van de verwerkten politiegegevens. Waar bij boa-organisaties het merendeel van politiegegevens art. 8 en soms art. 9 zal betreffen, komt het bij de BOD's in voorkomende gevallen voor dat er ook art. 10, art. 11 en/of art. 12 politiegegevens worden verwerkt. Uitgangspunt was (en is) dat de betreffende wetgeving voor alle boa-organisaties geldt. Dit neemt niet weg dat we er tijdens de uitvoering van de Wpg audits achter zijn gekomen dat de verwerking van politiegegevens bij boa-organisaties onderling nogal kunnen verschillen. BOD'en verwerken in voorkomende gevallen ook art. 10, 11 en/of 12 politiegegevens. Nu ook de wetgever (JenV) voornemens is het Boa-bestel, en meer specifiek de opsplitsing van de domeinen, te vereenvoudigen, heeft NOREA het voornemen om op basis hiervan in de volgende Handreiking meer aandacht te geven aan de onderscheidende kenmerken van de verschillende Boa-organisaties (met inachtneming van de wet- en regelgeving). **We merken hierbij op dat voor de huidige auditcyclus de *NOREA Handreiking Privacy audit Wpg voor boa's Versie 2024* voor alle boa-organisaties geldt.**
8	**17-03-2026** Er zijn (aanvullende) vragen gesteld m.b.t. het inhuren van boa's en meer specifiek wie dan de verwerkingsverantwoordelijke is (zie ook #5)	Indien de organisatie die de boa's inhuurt doel en middelen bepaalt en de ingehuurde boa's voldoen aan de eerder genoemde voorwaarden, dan is de inhurende organisatie n principe verwerkingsverantwoordelijk en derhalve auditplichtig. Let wel, omdat er in de praktijk allerlei varianten van inhuur en detachering bestaan, kan hiervan in concrete situaties met goede redenen worden afgeweken.