FAQ – PRIVACY AUDIT WET POLITIEGEGEVENS

VERSIE: 5 FEBRUARI 2025

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 testaanpak Privacy audit Wpg (1.0) d.d. 3 september 2024 van NOREA brengen we onderstaande FAQ uit om de vragen van een eenduidig antwoord te voorzien.

Tevens maken wij u erop attent dat een nieuwe versie van het voorbeeld assurance-rapport op de website van NOREA is gepubliceerd: **https://www.norea.nl/uploads/bfile/50cff39b-9926-4d95-825d-42ecb83c36a3.** U wordt gevraagd deze template te gaan gebruiken.

#	Vraag	Antwoord
1	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	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.

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