FAQ – PRIVACY AUDIT WPG VERSIE 1 – 17 NOVEMBER 2021

Update van de testaanpak Privacy audit Wpg voor boa's d.d. 24 juni 2021

Naar aanleiding van de gestelde vragen aan de Wpg-Werkgroep over de testaanpak Privacy audit Wpg (1.0) d.d. 24 juni 2021 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 (1.1) van het voorbeeld assurance-rapport op de website van NOREA is gepubliceerd, waarin enkele onvolkomenheden/onjuistheden zijn gecorrigeerd.

#	Vraag	Antwoord
1	Wij doen de Wpg audit bij een organisatie waar binnen verschillende organisatieonderdelen in meerdere domeinen verschillende verwerkingen plaatsvinden. Moet over al deze verwerkingen worden gerapporteerd, of mag bijvoorbeeld een steekproef worden getrokken.	De wet stelt dat de verwerkingsverantwoordelijke zich verantwoord over alle verwerkingen. Mede doordat de verwerkingen per domein zeer verschillend kunnen zijn is het niet mogelijk dit middels een steekproef te doen: alle verwerkingen zullen dus in scope moeten worden genomen. De template van het assurance-rapport sorteert hierop voor.
2	Het door VNG uitgebrachte *'Werkdocument Audit Wet politiegegevens voor gemeenten'* wijkt op onderdelen af van de NOREA Handreiking. Hoe dient hiermee te worden omgegaan?	Indien documenten onderling tegenstrijdig zijn, geldt, tenzij een andere bedoeling uit de Wet voortvloeit, de volgende rangorde: 1. de toepasselijke wet- en regelgeving; 2. de NOREA Handreiking Privacy audit Wpg voor boa's; 3. door andere partijen uitgebrachte instructies, werkdocumenten e.d. (w.o. het werkdocument van VNG).
3	In de handreiking wordt gesproken over een externe privacy audit. Wat wordt hier met 'extern' bedoeld? In de regelgeving, zoals de regeling periodieke audit politiegegevens, lees ik niet terug dat de privacy audit door een extern bureau o.i.d. moet worden uitgevoerd. Is het ook toegestaan dat een 'interne' RE, de privacy audit voor de eigen werkgever (een overheidsinstelling) uitvoert (zoals bijvoorbeeld ook de jaarlijkse DigiD-audit intern wordt uitgevoerd)?	Met het woord 'extern' hebben we expliciet het verschil tussen de 'interne audit' en de 'privacy-audit' willen benadrukken. Het lijkt ons, met inachtneming van de vakregels t.a.v. o.m. onafhankelijkheid en deskundigheid, zeker wel mogelijk dat een auditor van een interne auditdienst ('interne RE') de (externe) privacy audit uitvoert.
4	1. In aansluiting bij de regelgeving is in de praktijkhandreiking onderscheid gemaakt tussen de interne audit (jaarlijks) en de externe audit (1x per 4 jaar). In de praktijk zal het voorkomen dat er onvoldoende kennis/capaciteit bij organisaties aanwezig is om zelf de interne audit uit te voeren. De organisatie zou er dan voor kunnen kiezen om de interne audit uit te besteden aan een externe partij. Is het mogelijk/wenselijk dat de organisatie aan de externe auditor (de partij die 1x per 4 jaar de externe audit doet) opdracht geeft ook de jaarlijkse interne audit te verrichten? Indien ja, worden ten aanzien van norm #29 (Audits) extra waarborgen verlangd van de externe auditor bij de uitvoering van de externe audit? 2. Het is mij niet duidelijk of de interne audit door dezelfde partij mag worden uitgevoerd als de externe audit. Zou een auditorganisatie de externe, maar ook de interne audit kunnen uitvoeren?	Er is overwogen om dit in de Handreiking op te nemen, maar we hebben besloten om dit vooraleerst in/door de praktijk te laten vormgeven. We zien nu al dat er verschillende 'varianten' ontstaan, w.o. de onder vraag 1 aangegeven mogelijkheid, bijvoorbeeld d.m.v. jaarlijkse interim-controles. Een optie kan ook zijn om de interne audit t.z.t. in ENSIA op te nemen (v.w.b. boa's bij de gemeenten en andere organisaties die ENSIA toepassen, zoals Waterschappen e.d.). Vanzelfsprekend dient dan wel te worden bepaald of, en zo ja hoe, de externe auditor norm #29 beoordeeld (m.b.t. de door hemzelf uitgevoerde interne audit werkzaamheden). Zoals in de Handreiking al aangegeven mag de externe auditor de interne audit desgewenst uitvoeren mits hij/zij aan de competentie-eisen voor de interne auditor voldoet.
5	**Hoe** moet het Wpg-audit rapport worden aangeleverd bij de AP?	Het Wpg-auditrapport wordt digitaal aangeleverd bij de AP via: wpg-audit@autoriteitpersoonsgegevens.nl Let hierbij op de volgende punten:

#	Vraag	Antwoord
		- beperk het rapport tot de 'short form' versie dus zonder bijlagen; - verwijder namen van personen uit het document; - kies voor een leesbaar bestandsformaat, bij voorkeur pdf/a; - zorg dat de grootte van het bestand niet meer is dan enkele MB's.
6	**Wanneer** moet het Wpg-audit rapport worden aangeleverd bij de AP?	In eerste instantie had de AP aangegeven dat het onderzoek in 2021 zou moeten zijn afgerond en dat de rapportage uiterlijk in februari/maart door de AP moest zijn ontvangen. Gelet op de vele verzoeken om uitstel, heeft de AP recent het volgende op haar website gepubliceerd: *Uitstel tot en met 2022* *U zou de externe Wpg-audit dus voor het eerst in 2021 moeten laten uitvoeren. Maar let op: de AP geeft u 1 jaar uitstel. Dat betekent dat u uw Wpg-auditrapport **tot en met 31 december 2022** aan de AP mag sturen.* *De AP geeft deze extra tijd omdat Wpg-audits een belangrijk instrument zijn voor uw interne toezicht.* *De AP vindt het daarom belangrijk dat u de audit goed doorloopt en u de kans krijgt om verbeterplannen op te stellen en hercontroles uit te voeren, als dat nodig is. Zorgvuldigheid vindt de AP hierbij van groter belang dan snelheid.* (Zie verder deze link).
7	De beheersingsmaatregelen worden 'illustratief' genoemd. Wat houdt dat in? Verder mis ik in de handreiking voor de beheersingsmaatregelen in bijlage 3 de doelstelling. Juist de doelstelling geeft een ijkpunt om vast te kunnen stellen of afdoende maatregelen geïmplementeerd zijn.	'illustratief' is toegevoegd, om reden dat er (wellicht) ook andere manieren zijn om aan de wettelijke bepaling te voldoen. Over beheersingsdoelstellingen is ook nagedacht, maar onze conclusie was dat dit in de basis de betreffende wettelijke bepalingen zijn. Zo staat dat ook vermeld in de kop van bijlage 3. Het is niet aan NOREA dan wel de auditor om iets toe of af te doen aan de wettelijke bepalingen.
8	Wie is verantwoordingsplichtig bij uitbesteding van taken? Milieu inspectie wordt bijvoorbeeld door gemeentes vaak belegd bij een omgevingsdienst. Dient dergelijke uitbesteding meegenomen te worden in de verantwoording door de gemeente? Dient de omgevingsdienst dan een TPM aan de gemeente te leveren? Of moet een omgevingsdienst zich rechtstreeks verantwoorden naar de AP?	Wij gaan er vooralsnog vanuit dat de omgevingsdienst in dit voorbeeld zich direct verantwoordt aan de AP. In de Handreiking staat 'Hieruit volgt dat de verwerkingsverantwoordelijke (doorgaans is dit de werkgever van de boa) in het kalenderjaar 2021 een externe privacy audit Wpg laat uitvoeren.' Wellicht komen we in de praktijk nog andere situaties tegen die nopen tot bijstelling van dit uitgangspunt, maar vooralsnog zien wij die niet. Dit is in lijn met de tekst in artikel 1 lid c is in het Besluit politiegegevens buitengewoon opsporingsambtenaren "verwerkingsverantwoordelijke: de werkgever, bedoeld in artikel 1, onderdeel h, van het Besluit buitengewoon opsporingsambtenaar".
9	Maakt het voor de Wpg verantwoording bij uitbesteding van taken nog uit of deze zijn gemandateerd of gedelegeerd aan een andere overheidsorganisatie?	Nee, bij uitbesteding van taken is de werkgever van de boa verantwoordingsplichtig.
10	In het kader van 'ondermijning' vinden verwerkingen plaats die mogelijk ook opsporingsgegevens zijn. Deze verwerkingen vinden niet noodzakelijk plaats	De Wet gegevensverwerking door samenwerkingsverbanden ligt nu bij de Eerste

#	Vraag	Antwoord
	door Boa's. Vallen deze verwerkingen wel of niet binnen de scope van de audit? Zijn er meer van dergelijke niet-boa gerelateerde verwerkingen van opsporingsgegevens? Zijn het überhaupt opsporingsgegevens?	Kamer. Hierin wordt dit punt geadresseerd. Vooralsnog denken we dat beide smaken voor komen (het zijn wel/ geen politiegegevens), afhankelijk van waar zich dat in dit verwerkingsproces voordoet. In de praktijk zien we dat medewerkers van gemeenten (geen Boa's) gegevens verzamelen voor verdere verwerking door het Regionale Informatie- en Expertise Centra (RIEC). We zien dit als een artikel 13 lid 2 verwerking (ten behoeve van de ondersteuning van de taak, bedoeld in artikel 1, onderdeel a, kunnen de politiegegevens die worden verwerkt overeenkomstig artikel 8, 9 of 10 door een verwerkingsverantwoordelijke centraal verder worden verwerkt voor zover zij relevant zijn voor het verkrijgen van landelijk inzicht in specialistische onderwerpen. De verder verwerkte gegevens worden ter beschikking gesteld aan door een verwerkingsverantwoordelijke geautoriseerde personen voor zover zij deze behoeven voor de uitvoering van de taak, bedoeld in artikel 1, onderdeel a.).
11	Op welke wijze kan de volledigheid van de verwerkingen vastgesteld worden? Het beeld wat wij tot nog toe ophalen is dat gemeentes niet altijd goed zicht hebben op welke Boa's ingezet worden, zeker niet wanneer er sprake is van inhuur of uitbesteding. Laat staan dat er zicht is op de volledigheid van de afzonderlijke verwerkingen en bijbehorende systemen (tot MS Word, Excel en opschrijfboekjes aan toe).	Het blijkt inderdaad lastig om dat limitatief vast te stellen. De verwerkingen die we bij gemeenten tegenkomen zijn: - Handhaving (sommige gemeenten maken onderscheid in 'openbare buitenruimte' en 'openbare binnenruimte'(denk aan Alcoholwet en de Huisvestingswet); - Werk & Inkomen (denk aan de sociaal rechercheur); - Maatschappelijke Ontwikkeling/ Onderwijs (denk aan de leerplichtambtenaar); - Cameratoezicht openbare orde. Bij sommige gemeenten zijn markt- en/of havenmeesters in dienst die Boa zijn. Voor Handhaving komen we veel het Boa Registratiesyteem (BRS) van NatuurNetwerk en CityControl van Sigmax tegen, bij Leerplicht CAReL van Eljakim en LBA van Pronexus. Ook zien we dat verwerkingen plaatsvinden op netwerkschijven en (uiteindelijk) vaak in 'zaaksystemen' terecht komen. Voor de goede orde: deze systemen zijn in scope van de audit.
12	Hoe stel je vast of de interne auditor voldoende competenties heeft? Dient het een RE te zijn? Of is elke willekeurig training (zie voetnoot 3 in de handreiking) afdoende?	De interne auditor hoeft geen RE te zijn (mag wel). M.b.t. de competenties hebben we daar vooralsnog geen concrete criteria voor opgesteld. Materie-/ objectdeskundigheid, aangevuld met kennis van audittechnieken liggen voor de hand. De competenties afmeten aan de kwaliteit waarmee de interne audit is uitgevoerd en gerapporteerd is een manier om dit te toetsen.
13	In de NOREA Handreiking Privacy audit Wpg voor boa's Versie 1.0 d.d. 24 juni 2021 staat in § 2.7 (Leveranciersaudit 'inclusive, tenzij') dat gebruik kan worden gemaakt van de 'carve out' methodiek als een recente assurance-rapportage van de serviceorganisatie beschikbaar is, waarbij onder 'recent' wordt verstaan dat het assurance-rapport op de datum van afgifte van het assurance-rapport Privacy audit voor de boa-organisatie maximaal 12 maanden oud is. Heeft deze eis ("maximaal 12 maanden oud") betrekking op de datum die is vermeld op de assurance-rapportage van de serviceorganisatie of heeft deze	Wij gaan uit van het tweede (de einddatum van de verslagperiode van de assurance-rapportage van de serviceorganisatie).

#	Vraag	Antwoord
	eis betrekking op de einddatum van de verslagperiode van de assurance-rapportage van de serviceorganisatie?	
14	In de template Assurance-rapport NOREA Richtlijn 3000D – Privacy-audit Wet politiegegevens zijn in § 1.11 (De basis voor ons oordeel met beperking) voor ieder 'Proces/verwerking' (#1 t/m #4 in de template) aparte tabellen 'Onderwerpen' en 'Technische en organisatorische maatregelen' opgenomen. In Bijlage 1 (Beschrijving van de beheersingsmaatregelen en testresultaten – Wpg beheersingsmaatregelen) en in Bijlage 2 (Beschrijving van de beheersingsmaatregelen en testresultaten – technische en organisatorische beheersingsmaatregelen) wordt echter geen onderscheid gemaakt tussen de verschillende processen/verwerkingen. Hoe moet de externe IT-auditor hier mee omgaan als de conclusies verschillend zijn per proces/verwerking (dat zal dikwijls het geval zijn).	De werkgroep heeft er bewust voor gekozen om dit 'free format' te laten om reden dat de normen binnen boa-organisaties deels organisatie-generiek (o.a. #1) zijn ingericht, en deels domein-specifiek. Omdat deze verdeling ook weer niet voor alle organisaties gelijk zal zijn, hebben we dit vrij gelaten.
15	In de template Assurance-rapport NOREA Richtlijn 3000D – Privacy-audit Wet politiegegevens § 1.11 (De basis voor ons oordeel met beperking) kan in de 'Conclusie' kolommen van de tabellen 'Onderwerpen' en 'Technische en organisatorische maatregelen' met de kleur grijs worden aangegeven dat de desbetreffende onderwerpen niet zijn onderzocht. Hierbij zou naar onze mening onderscheid moeten worden gemaakt tussen onderwerpen die niet zijn onderzocht (bijvoorbeeld omdat geen geschikte assurance-rapportage van een serviceorganisatie beschikbaar is en geen audit kon worden uitgevoerd bij deze serviceorganisatie) en onderwerpen die niet van toepassing zijn (bijvoorbeeld omdat er geen sprake is van doorgifte van de desbetreffende politiegegevens aan derde landen). Kan de NOREA Werkgroep WPG aangeven op welke wijze dit onderscheid moet worden aangegeven in de Privacy Wpg boa assurance-rapportage?	In de (detail-)rapportage kan dat met een uitgeschreven tekst (met een inleiding). In de samenvattende tabel (eventueel) doormiddel van een afkoring. Dan krijg je: • Niet onderzocht, want…. (n.o.) • Niet van toepassing, omdat… (n.v.t.)
16	In de template Assurance-rapport NOREA Richtlijn 3000D – Privacy-audit Wet politiegegevens wordt in § 2.4 (Hercontrole) aangegeven dat hercontrole moet plaatsvinden binnen één jaar na uitbrengen van het verbeterrapport en dat de resultaten van de hercontrole in een rapportage moeten worden vastgelegd, liefst volgen het NOREA template assurance-rapport. Welke periode dient hierbij te worden gehanteerd voor de beoordeling van de werking van de maatregelen?	Dat 'hercontrole moet plaatsvinden binnen één jaar na uitbrengen van het verbeterrapport' staat er niet met zoveel woorden en is ook niet zo bedoeld. Als je deze uitleg letterlijk zou nemen kan de organisatie vijf jaar doen over het opstellen van een verbeterrapport (hier zou overigens moeten staan 'verbeter**plan**'), en dan na in totaal zes jaar de hercontrole kan (laten) uitvoeren. Wij (en de AP heeft dit bevestigd) gaan ervan uit dat de hercontrole plaatsvindt binnen een jaar na rapportagedatum van de initiële audit en dat de hercontrole een audit op opzet en bestaan betreft en dat gerapporteerd wordt dat 'per datum xx-xx-xxxx, in opzet en bestaan, aan alle van materieel van belang zijnde aspecten aan de normen wordt voldaan'.
17	Op bladzijde 25 staat dat **apart voor de Wpg** een FG dient te worden aangewezen (FG-Wpg). Op bladzijde 56/57 staat iets heel anders bij Onderwerp #31.	Beiden kloppen: bij #31 staat (is bedoeld) dat dit wel dezelfde persoon kan zijn (dus wel apart aanwijzen, want het zijn twee verschillende functies) maar dat dit niet per se twee functionarissen hoeven te zijn. Nog aanvullend: de AP heeft aangegeven dat, als er geen FG voor de Wpg is aangemeld, zij ervan uitgaat dat de FG die is aangemeld voor de AVG, ook de FG is voor de Wpg. Dit is ook zo op de website van de AP gepubliceerd.
18	Op bladzijde 27 staat: "…die in opzet, bestaan en werking door de auditor worden getoetst". Zou 'bestaan' niet moeten worden verwijderd? Dit staat immers bij 'werking'.	In de Regeling periodieke audit politiegegevens staat: Hiertoe vindt een beoordeling plaats van de volgende aspecten binnen de organisatie van de auditee: - 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.

#	Vraag	Antwoord
		Wij kiezen ervoor om bij deze compliance audit zoveel mogelijk de wet(teksten) te volgen.
19	Op bladzijde 59 van de Handreiking staat dat bij het uitbrengen van een nieuwe release van de applicatie of een grote upgrade van het onderliggende platform dienen, bij voorkeur door middel van een penetratietest moet worden onderzocht of er geen nieuwe kwetsbaarheden zijn geïntroduceerd. Op bladzijde 63 staat echter dat penetratietests dienen te worden uitgevoerd na significante wijzigingen, zoals vervanging applicatie, nieuwe versie, migratie webservers, database migratie, etc.	Wij hebben, als onderdeel van #1 wijzigingenbeheer, vrijgelaten of dit middels een penetratietest dan wel een andere methodiek wordt onderzocht (denk aan broncode onderzoek). #5 gaat specifiek over het uitvoeren van kwetsbaarhedenscans en penetratietesten.
19	Inhoudelijke vragen/ opmerkingen m.b.t. de Handreiking: Norm 6: Er staat: Inspectie van contracten met leveranciers, SLA's en andere documenten met focus (vraag: er lijkt iets te missen?) Norm 8: Er staat: 'wettelijke eisen voor DPIA's' (vraag: aan welke wettelijke eisen wordt hier gerefereerd?)	Norm 6: Hier dient gelezen te worden: Inspectie van contracten met leveranciers, SLA's en andere documenten met focus **op Privacy by design.** Norm 8: in art 4c lid 2 Wpg staat: De beoordeling bevat tenminste: a. een algemene beschrijving van de beoogde verwerkingen; b. een beoordeling van de risico's voor de rechten en vrijheden van betrokkenen; c. de beoogde maatregelen ter beperking van de risico's; d. de voorzorgs- en beveiligingsmaatregelen en mechanismen om de politiegegevens te beschermen en aan te tonen dat aan het bij of krachtens deze wet bepaalde is voldaan, met inachtneming van de rechten en gerechtvaardigde belangen van de betrokkenen en andere betrokken personen. In het **'Besluit inzake lijst van verwerkingen van persoonsgegevens waarvoor een gegevensbeschermingseffectbeoordeling (DPIA) verplicht is'** van de Autoriteit Persoonsgegevens is limitatief opgesomd voor welke verwerkingen (in ieder geval) een DPIA moet worden uitgevoerd.