AUTORITEIT
PERSOONSGEGEVENS

# Wpg-audit
# Onderzoek auditrapporten hercontroles

Publicatiedatum: 22 juli 2024

AUTORITEIT
PERSOONSGEGEVENS

# Inhoudsopgave

# 1. Inleiding

Het verwerken van politiegegevens vraagt om zorgvuldigheid. Burgers moeten kunnen vertrouwen op een goede en zorgvuldige verwerking van persoonsgegevens. Zeker als het gaat om gevoelige gegevens zoals gegevens die door buitengewone opsporingsambtenaren (boa's) worden verwerkt bij de uitvoering van hun strafvorderlijke of opsporingstaak. Een boa kan door persoonsgegevens te registreren een grote invloed hebben op iemands levenssfeer. Een proces-verbaal van een boa heeft in het strafrecht speciale bewijskracht. Registraties kunnen voor politietaken gebruikt worden. Geregistreerde gegevens kunnen bijvoorbeeld in een persoonsdossier van een leerplichtambtenaar of sociaal rechercheur komen te staan, of gebruikt worden voor een beoordeling van een aanvraag voor een Verklaring Omtrent het Gedrag (VOG). Registraties kunnen een jarenlange impact hebben op mensen. Als boa's onzorgvuldig omgaan met deze informatie, of onjuiste informatie vastleggen, kunnen iemands rechten en vrijheden in het gedrang komen. Om dat te voorkomen, moeten boa's zich aan regels houden.

Sinds 1 januari 2008 bevat de Wet politiegegevens (Wpg) de verplichting voor verwerkingsverantwoordelijken om periodiek een privacy-audit te laten uitvoeren door een externe auditor. Door de komst van de Richtlijn gegevensbescherming bij rechtshandhaving [1] wijzigde de Wpg per 1 januari 2019. Sindsdien vallen boa's die voor hun opsporingstaak persoonsgegevens verwerken onder de Wpg. Daarmee is de auditplicht ook gaan gelden voor de werkgevers van boa's. Dit zijn meer dan 600 organisaties.[2]

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 stelt de AP in staat om effectief toezicht te houden op de verwerking van politiegegevens. Wanneer uit de audit blijkt dat beheersingsmaatregelen onvoldoende worden ingevuld, moet de verwerkingsverantwoordelijke voor deze punten een verbeterplan opstellen en binnen een jaar opnieuw laten beoordelen. De verwerkingsverantwoordelijke moet het verslag van deze hercontrole ook aan de AP sturen.

Deze rapportage over de Wpg-audit van de AP is een vervolg op de rapportage van de AP van juni 2023.[3] In die rapportage lag de nadruk op de aanlevering van de auditrapporten. Ook gaf een 'quickscan' op basis van een steekproef inzicht in de resultaten van de audits van een selectie van boa-werkgevers, met een visuele weergave. Ook voor deze nieuwe rapportage over de resultaten van de hercontroles heeft de AP een quickscan uitgevoerd onder organisaties. De resultaten daarvan geven inzicht in de vorderingen die de organisaties hebben gemaakt en de verbeteringen die zij nog moeten doorvoeren. Ook staan in deze rapportage inzichten uit gesprekken met boa-werkgevers.

[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.
[2] Opgave 7 juli 2022, Ministerie van J&V.
[3] Autoriteit Persoonsgegevens, 12 juni 2023, "Wpg-audit, Onderzoek aanlevering auditrapporten", Nieuwsbericht Veel boa-werkgevers voldoen niet aan verplichte Wpg-audit

# 2. Conclusie

De AP heeft een quickscan uitgevoerd naar de resultaten van de hercontroles. De AP constateert dat boa-werkgevers vorderingen maken in het op de juiste manier verwerken van persoonsgegevens op grond van de Wpg. Tegelijkertijd constateert de AP dat geen van de boa-werkgevers uit de quickscan volledig voldoet aan de beoordeelde beheersingsmaatregelen. Daarmee kunnen zij niet aantonen dat zij de persoonsgegevens verwerken in overeenstemming met de Wpg. Ondanks de vorderingen zullen veel boa-werkgevers nog flinke stappen moeten zetten om de opzet en het bestaan van de beheersingsmaatregelen op orde te krijgen én aan te tonen dat deze in de praktijk werken.

Veel organisaties hebben moeite om te voldoen aan de wettelijke eisen om een audit uit te voeren en de resultaten daarvan tijdig aan te leveren bij de AP. De AP heeft bij de hercontrole ruim 300 auditrapporten tijdig ontvangen. Daarmee is meer dan de helft van de ruim 600 boa-werkgevers in gebreke gebleven. In meerdere gevallen gaat het om partijen die ook geen initieel auditrapport hebben aangeleverd.[4] Dit zijn vrijwel allemaal boa-werkgevers met minder dan 5 boa's in dienst.

De AP gaat ervan uit dat organisaties bij de volgende audit en eventuele hercontrole op alle beheersingsmaatregelen voldoende naleving kunnen aantonen van de opzet, het bestaan én de werking van de beheersingsmaatregelen. Bij de volgende initiële audit in 2025 hebben organisaties meerdere jaren de tijd gehad om beheersingsmaatregelen in te richten conform de Wpg. Als een boa-werkgever niet voldoet aan de eisen uit de Wpg, dan kan de AP beslissen om te handhaven.

[4] Zie het eerdere bericht 'Veel boa-werkgevers voldoen niet aan verplichte Wpg-audit', 12 juni 2023: https://www.autoriteitpersoonsgegevens.nl/actueel/veel-boa-werkgevers-voldoen-niet-aan-verplichte-wpg-audit

# 3. Over het onderzoek

## 3.1 Procesverloop

Op 12 juni 2023 publiceerde de AP de rapportage 'Wpg-audit: Onderzoek aanlevering auditrapporten' en verwees naar de aanleverdatum van 31 december 2023 voor de resultaten van de hercontrole.[5] Op 1 december 2023 publiceerde de AP het nieuwsbericht 'Hercontrole Wpg-audit door boa-werkgevers'[6] waarin de AP boa-werkgevers herinnert aan de hercontrole. In dat artikel stelt de AP de uiterlijke datum voor het aanleveren van de resultaten uit tot 1 maart 2024 om ruimte te geven aan bestuurlijke processen. De AP verwachtte van ruim 600 organisaties een rapport. Op 22 maart 2024 had de AP ongeveer 300 rapporten ontvangen.

### Gesprekken met werkgevers

De AP heeft de resultaten van de hercontroles van organisaties die in de eerdere steekproef waren opgenomen, opnieuw beoordeeld. Daarna heeft de AP geanalyseerd welke organisaties de meeste verbetering en welke organisaties de minste verbetering hebben laten zien ten opzichte van de resultaten van de initiële audit. Ook heeft de AP een selectie gemaakt van organisaties die op (vrijwel) alle beoordelingscriteria een voldoende scoren en organisaties die nog een flinke stap moeten zetten. Op basis van deze grove selectie zijn 9 organisaties uitgenodigd voor een gesprek.

In de periode april 2023 – juni 2024 heeft de AP met deze 9 werkgevers gesprekken gevoerd over de resultaten van de hercontrole. Hierbij lag de nadruk op de vergelijking tussen de resultaten van de initiële audit met die van de hercontrole, en factoren die de verbetering of het ontbreken daarvan kunnen verklaren. De AP heeft tegen geen van de werkgevers aanvullende handhavende acties uitgevoerd.

## 3.2 Bevindingen

De hierna beschreven bevindingen komen uit:

- het proces van aanleveren van de auditrapporten;
- de gesprekken die de AP heeft gevoerd met een aantal boa-werkgevers;
- overige signalen.

### Systemen kunnen compliance bevorderen

Meerdere organisaties geven aan dat zij voor de verwerking van gegevens zijn afgestapt of zullen afstappen van het gebruik van algemene e-mailprogramma's, gedeelde netwerkschijven of generieke dossier-en brievensystemen. Zij maken nu gebruik (of gaan gebruikmaken) van specifieke, vaak beter beveiligde registratiesystemen en verwachten hiermee structureel aan meerdere Wpg-eisen te voldoen. Het gebruik van dergelijke systemen blijkt als voordeel te hebben dat resultaten van een audit van het systeem door middel van een goedkeurende TPM-verklaring[7] worden meegenomen in de Wpg-audit, wat de auditlast verlaagt. Vrijwel alle organisaties die gemiddeld betere resultaten laten zien, maken gebruik van systemen met een TPM-verklaring.

[5] Wpg-audit Onderzoek aanlevering auditrapporten, hoofdstuk 5
[6] Hercontrole Wpg-audit door boa-werkgevers | Autoriteit Persoonsgegevens
[7] Een TPM (Third Party Memorandum) is een verklaring van een onafhankelijke derde partij

### Inrichting interne audit

Bij meerdere boa-werkgevers bestaan onduidelijkheden over de verhouding tussen interne en externe audits. Meerdere organisaties maken voor de interne audit gebruik van een extern auditbureau. De eisen aan interne auditors zijn echter anders (minder zwaar) dan die aan externe auditors worden gesteld. De AP verwijst naar de Regeling periodieke audit politiegegevens[8] en de handreiking van NOREA voor meer informatie.

### Wpg-audit nuttig, kennisborging blijft belangrijk

In het algemeen ervaren organisaties dat de audit helpt om verbeterpunten en knelpunten in de uitvoering zichtbaar te maken. Anderzijds zien meerdere organisaties de vertaling van de wet en het auditkader naar de praktijk als lastig en een behoorlijke inspanning van de organisatie.

Herhaaldelijk bleek verloop of (tijdelijke) uitval van personeel direct gevolgen te hebben voor de opvolging van het verbeterplan. Organisaties die betere resultaten lieten zien, konden juist bouwen op een goede kennisborging. Daarnaast helpt kennisdelen en samenwerken met andere organisaties zoals buurgemeenten of in samenwerkingsverbanden ook om te voldoen aan de inhoudelijke Wpg-verplichtingen en de eisen aan (de uitvoering van) de audits en hercontroles. Meerdere organisaties geven echter aan dat samenwerking beperkt van de grond kwam, omdat zij eerst vooral bezig waren om hun eigen organisatie in te richten. De AP merkt op dat de auditplicht zoals die is opgenomen in de Wpg blijft bestaan en raadt aan om te investeren in de ontwikkeling van kennis binnen de organisatie en samenwerking.

### Betrokkenheid functionaris gegevensbescherming (FG)

De AP kreeg in enkele gevallen vragen over de rol en positie van de FG in relatie tot de Wpg-audit. De AP vindt het belangrijk dat de organisatie de FG tijdig om advies vraagt, dat de FG de middelen krijgt om de audit te onderzoeken en vervolgens een advies te geven aan het bestuur. Om onbevooroordeeld te kunnen adviseren, behoort de FG een professionele afstand te bewaren tot de uitvoering. De FG is niet verantwoordelijk voor de naleving van de Wpg, maar is belast met het (interne) toezicht daarop, en heeft de taak daarover te informeren en te adviseren. Daarnaast treedt de FG op als contactpunt voor de AP. Dit laatste laat echter onverlet dat de verplichting van de audit en het toesturen van het rapport bij de verwerkingsverantwoordelijke ligt, niet bij de FG.[9]

[8] Vergelijk bijvoorbeeld artikel 5 lid 1 met artikel 6 lid 1 Regeling periodieke audit politiegegevens

[9] Wanneer een FG wordt aangesteld voor de Wpg, dan moet de verwerkingsverantwoordelijke deze apart aanmelden bij de AP. Anders gaat de AP ervan uit dat de FG toeziet op zowel de AVG als de Wpg. Zie ook de website FG aanmelden bij de AP | Autoriteit Persoonsgegevens.

# 4. Quickscan van inhoudelijke bevindingen

De AP heeft op basis van een steekproef naar de inhoudelijke resultaten van de initiële audits gekeken. Uit deze quickscan bleek dat de meeste boa-werkgevers ruim onvoldoende scoorden op de getoetste beheersingsmaatregelen. Die boa-werkgevers moesten voor deze punten een verbeterplan opstellen, binnen een jaar een hercontrole laten uitvoeren en de resultaten aan de AP sturen.

De AP heeft die resultaten vervolgens vergeleken met het initiële rapport.[10] [11] De auditors hebben, net als bij de initiële audit, bij 31 beheersingsmaatregelen getoetst of deze in voldoende mate (groen), niet volledig (oranje) of niet (rood) zijn opgezet en bestaan (daadwerkelijk zijn geïmplementeerd en toegepast). In de tabel staan alleen resultaten van de toetsing op de 'opzet'.

Uit de quickscan blijkt dat de opzet van beheersingsmaatregelen over het algemeen flink is toegenomen. De grootste stijging is te zien bij de meer technische beheersingsmaatregelen, zoals autorisaties (beheersingsmaatregel 10) en bewaartermijnen (beheersingsmaatregel 20). De minste vooruitgang is geboekt op onderwerpen die meer organisatorische inspanning vergen, zoals de criteria rondom samenwerking, de structurele verstrekking van gegevens aan derden (beheersingsmaatregel 23) en de rechtstreekse verstrekking (beheersingsmaatregel 24).

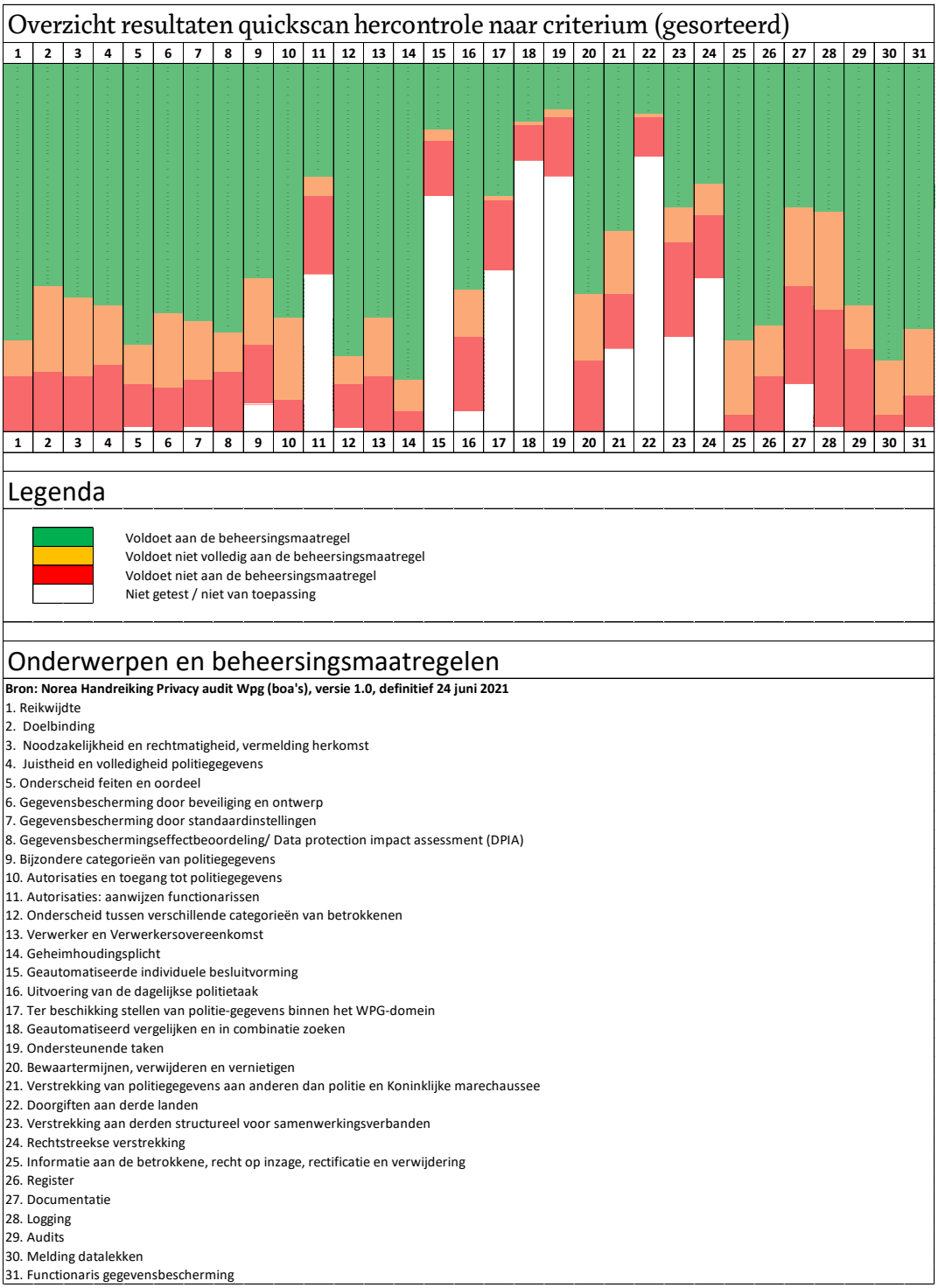
De resultaten van de quickscan laten zien dat organisaties op vrijwel alle criteria oranje of lichtgroen scoren en dus gemiddeld redelijk voldoen. Maar: zij voldoen niet aan het gewenste niveau (score 3). In de tabel is te zien dat de organisaties uit de quickscan gemiddeld gezien op géén van de criteria dat niveau haalt voor de opzet van beheersingsmaatregelen.

[10] De quickscan van de initiële audit bevatte rapporten van 56 organisaties. Het vervolg, de quickscan op basis van resultaten van de hercontrole, omvatte rapporten van 41 organisaties. Voor de tabel zijn alleen de resultaten van de 41 organisaties overgenomen zodat de resultaten vergelijkbaar zijn.

[11] De kleurschaal van rood (laagste score) naar groen (hoogste score) is automatisch gegenereerd en is slechts bedoeld als visuele ondersteuning. De cijfers zijn gebaseerd op een omzetting van de auditresultaten, zo is een onvoldoende score een 1 en een voldoende score een 3.

## 4.1 Visuele weergave resultaten van de quickscan

De onderstaande tabel is een visuele weergave van een steekproef van resultaten van 41 boa-werkgevers. In de tabel staan alleen de resultaten uit de kolom 'opzet' uit de NOREA-template. De resultaten uit de toegestuurde rapporten zijn omgezet naar kleurcoderingen en zijn gesorteerd weergegeven. Hierdoor is geen herleiding naar individuele resultaten mogelijk. Deze sortering heeft alleen een visueel doel.




Figuur 1: Overzicht resultaten bij hercontrole van 41 boa-werkgevers

### 4.2 Visuele weergave vergelijking gemiddelde resultaten quickscan (initieel en hercontrole)

De onderstaande tabel een vergelijking van gemiddelde scores per beheersingsmaatregel van de initiële audit en de hercontrole. De gemiddelde waarde is een indicatie van de mate van naleving. Bijvoorbeeld, de gemiddelde score van de beheersingsmaatregel '14. Geheimhoudingsplicht' was 2,3. Bij de hercontrole is de gemiddelde score 2,8. Als alle organisaties een voldoende resultaat halen is de gemiddelde score op een beheersingsmaatregel 3,0.

| Overzicht resultaten quickscan per beheersingsmaatregel (gemiddelde score) | | |
|---|---|---|
| *Criterium (o.b.v. NOREA-handreiking Privacy-audit Wpg voor boa's, Versie 1.0, Definitief, 24 juni 2021)* | Initiële audit | Her-controle |
| 1.Reikwijdte | 2,0 | 2,6 |
| 2.Doelbinding | 1,9 | 2,4 |
| 3.Noodzakelijkheid en rechtmatigheid, vermelding herkomst | 1,8 | 2,5 |
| 4.Juistheid en volledigheid politiegegevens | 1,9 | 2,5 |
| 5.Onderscheid feiten en oordeel | 2,0 | 2,7 |
| 6.Gegevensbescherming door beveiliging en ontwerp | 2,1 | 2,6 |
| 7.Gegevensbescherming door standaardinstellingen | 2,0 | 2,6 |
| 8.Gegevensbeschermingseffectbeoordeling/ DPIA | 2,0 | 2,6 |
| 9.Bijzondere categorieën van politiegegevens | 2,0 | 2,5 |
| 10.Autorisaties en toegang tot politiegegevens | 1,8 | 2,6 |
| 11.Autorisaties: aanwijzen functionarissen | 1,7 | 2,2 |
| 12.Onderscheid tussen categorieën van betrokkenen | 2,1 | 2,7 |
| 13.Verwerker en Verwerkersovereenkomst | 2,2 | 2,7 |
| 14.Geheimhoudingsplicht | 2,3 | 2,8 |
| 15.Geautomatiseerde individuele besluitvorming | 1,7 | 2,1 |
| 16.Uitvoering van de dagelijkse politietaak | 1,6 | 2,4 |
| 17.Ter beschikking stellen van politiegegevens | 1,7 | 2,3 |
| 18.Geautomatiseerd vergelijken en in combinatie zoeken | 1,7 | 2,2 |
| 19.Ondersteunende taken | 1,7 | 1,9 |
| 20.Bewaartermijnen, verwijderen en vernietigen | 1,6 | 2,4 |
| 21.Verstrekking van politiegegevens aan anderen | 1,9 | 2,4 |
| 22.Doorgiften aan derde landen | 1,8 | 2,1 |
| 23.Verstrekking aan derden structureel voor samenwerkingsverbanden | 1,9 | 2,2 |
| 24.Rechtstreekse verstrekking | 2,0 | 2,3 |
| 25.Reachten van de betrokkene | 2,0 | 2,7 |
| 26.Register | 1,8 | 2,6 |
| 27.Documentatie | 1,7 | 2,1 |
| 28.Logging | 1,5 | 2,1 |
| 29.Audits | 1,7 | 2,4 |
| 30.Melding datalekken | 2,4 | 2,8 |
| 31.Functionaris voor gegevensbescherming | 2,1 | 2,6 |

# 5. Vooruitblik naar tweede auditcyclus

Bij de volgende verplichte initiële audit in 2025 hebben organisaties meerdere jaren de tijd gehad om beheersingsmaatregelen in te richten conform de Wpg. De AP gaat ervan uit dat organisaties bij die volgende initiële audit en eventuele hercontrole op alle beoordelingscriteria voldoende naleving kunnen aantonen bij de opzet, het bestaan én de werking. Als een boa-werkgever hier niet aan voldoet, dan kan de AP handhaven.

Audits moeten worden uitgevoerd conform de Regeling periodieke audit politiegegevens. Onderdeel daarvan zijn de eisen aan de privacy-audit zelf en aan de auditor.[12] De eisen aan een externe audit verschillen van de eisen aan een interne audit. De externe audit laten uitvoeren door een interne auditor of door middel van collegiale beoordeling is bijvoorbeeld niet toegestaan. Een hercontrole kan wel worden uitgevoerd door een interne auditor als de externe auditor dat heeft geadviseerd.[13]

De AP gaf in de rapportage van juni 2023 over de Wpg-audit aan van een aantal kleinere boa-werkgevers het signaal te krijgen dat de audit voor hen niet proportioneel zou zijn, en dat de AP dat signaal wilde bespreken met het ministerie. Deze gesprekken hebben plaatsgevonden. In die gesprekken heeft de AP benadrukt veel waarde te hechten aan het mechanisme van audits, omdat dit de verwerkingsverantwoordelijke een sturingsinstrument in handen geeft en leidt tot het ontdekken en oplossen van omissies of gebreken. Voor de AP biedt het een waardevol instrument voor effectief toezicht op de naleving van de Wpg. In de gesprekken heeft de AP aangegeven geen bezwaar te hebben tegen wijzigingen in de opzet van de audits, mits de toegevoegde waarde van de audits niet vermindert en de wijzigingen de AP niet hinderen in effectief toezicht. Het ministerie kijkt naar mogelijke aanpassingen en de AP wacht de verdere ontwikkelingen af.

In de praktijk blijkt dat vrijwel alle organisaties de NOREA-handreiking Privacy-audit Wpg voor boa's gebruiken. Hoewel de handreiking en het daarin opgenomen format niet bij wet of door de AP is voorgeschreven, adviseert de AP organisaties om deze handreiking te volgen voor zowel de externe als ook de interne audit. Of om de handreiking in zoverre te volgen dat de resultaten van de audits vergelijkbaar zijn. Voor specifieke aanwijzingen voor de opzet van Wpg-audits, inclusief een overzicht van termijnen, verwijst de AP naar de NOREA-handreiking. NOREA zal de handreiking naar verwachting in het derde kwartaal van 2024 actualiseren.

[12] Art 33 vijfde lid Wpg jo artikel 6:4 besluit politiegegevens jo artikel 2a Regeling periodieke audit politiegegevens
[13] Artikel 4 lid 3 Regeling periodieke audit politiegegevens

AUTORITEIT
PERSOONSGEGEVENS

# 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.