NOREA Handreiking Privacy audit Wpg voor boa's Versie 2024

NOREA
DE BEROEPSORGANISATIE VAN IT-AUDITORS

1.0 – Definitief

3 september 2024

Verantwoording

Deze handreiking is uitgegeven door NOREA, de beroepsorganisatie van IT-auditors in Nederland, en is ontwikkeld om Nederlandse gekwalificeerde IT-auditors (Register IT-auditors, RE's) handvatten te bieden om een assurance-rapport op te stellen in lijn met de Wet politiegegevens (Wpg) en het Besluit politiegegevens buitengewoon opsporingsambtenaren (Bpg boa), en relevante standaarden voor assurance-opdrachten.

De handreiking mag worden gebruikt en/of gedistribueerd, mits met bronvermelding.

Consultatie

De concept handreiking is ter consultatie voorgelegd aan verschillende partijen, w.o. de Vaktechnische Commissie van NOREA en de Autoriteit Persoonsgegevens (AP). De opmerkingen en aanbevelingen zijn in de voorliggende, definitieve versie verwerkt. Daarbij wordt opgemerkt dat de reactie van de AP moet worden gezien als een ambtelijk advies. De verantwoordelijkheid voor de inhoud van de handreiking ligt bij NOREA. De inbreng van de AP kan niet gezien worden als een goed- of afkeuring van de handreiking.

Deelnemers werkgroep

De volgende personen hebben namens de NOREA werkgroep Privacy audit Wpg een bijdrage aan deze handreiking geleverd:

drs. Rene IJpelaar RE CISA CIPP/e, Frank Kossen RE, Niels van der Meij RE Msc, Rogier Haest RE CISA, mr. Winfried Nanninga RE CIA MMC, drs. Henri Raaphorst RE.

Coördinatie en redactie versie 2024:

Frank Kossen RE, drs. Rene IJpelaar RE CISA CIPP/e

Postbus 242 2130 AE Hoofddorp

telefoon: 088-4960380

e-mail: norea@norea.nl www.norea.nl

Versiebeheer		
Versie	**Datum**	**Wijzigingen**
1.0	21 juni 2021	Vorige versie (vervallen)
0.1–0.9.3	mei–juli 2024	Werkversies
0.99	25 juli 2024	Initiële versie voor consultatie
1.0	**3 september 2024**	**Definitieve versie**
Deze versie is geldig vanaf de publicatiedatum (3 september 2024) en komt in de plaats voor alle eerdere versies. In deze versie zijn eveneens alle faq's van een datum vóór 3 september 2024 opgenomen.		
Belangrijkste wijzigingen in deze versie:		
Ten opzichte van versie 1.0 d.d. 21 juni 2021 van de Handreiking Privacy audit Wpg voor boa's zijn in deze versie een viertal wijzigingen doorgevoerd: 1. de toezichtmaatregelen waarover de controle op werking zich uitstrekt zijn van zeven beheersingsmaatregelen teruggebracht tot twee beheersingsmaatregelen (29 Audit en 31 Functionaris Gegevensbescherming(FG)). Het interne toezicht van de FG was een toets element bij een groot aantal beheersingsmaatregelen in de vorige Handreiking waardoor, indien dit toezicht ontbrak of slechts deels door de FG werd uitgevoerd, dit bij al deze beheersingsmaatregelen tot een oordeel met een beperking resulteerde. Dit is aangepast en de beoordeling van het interne toezicht door de FG is nu beperkt tot beheersingsmaatregel 31; 2. Op suggestie van de AP is de hercontrole aangepast. De hercontrole moet op basis van de Regeling Periodieke Audits plaatsvinden binnen één jaar na rapportdatum van de externe audit. Over de 1e helft van dat jaar blijft de hercontrole beperkt tot het beoordelen van de opzet en het bestaan. Echter, gedurende de 2e helft van dat jaar wordt niet alleen de opzet en het bestaan maar ook de effectieve werking van de beheersingsmaatregelen voortaan beoordeeld bij die beheersingsmaatregelen die bij de externe audit 2024 als 'voldoet niet' of 'voldoet deels' zijn beoordeeld; 3. bijlage 4 is transparanter gemaakt om meer inzicht te verschaffen voor verwerkingsverantwoordelijke en toezichthouder: de beheersingsmaatregelen in de guidance zijn eenduidiger geformuleerd zodat uitsluitend op het hoofdonderwerp van de beheersingsmaatregel wordt beoordeeld en niet langer op nevenonderwerpen, die bij andere beheersingsmaatregelen ook een rol spelen; 4. artikel 32a van de Wpg (logging) is door de wetgever inmiddels onverkort van toepassing verklaard waaruit volgt dat alle informatiesystemen aan de loggingsverplichtingen dienen te voldoen.		

Inhoud

1 INLEIDING 5

1.1 DOEL HANDREIKING 5
1.2 ACHTERGROND PRIVACY AUDIT WPG VOOR BOA'S 5
1.3 (WETTELIJKE) KADERS 6
1.3.1 Wettelijke grondslag en periodiciteit privacy audits Wpg 7
1.3.2 Object en scope van onderzoek 8
1.3.3 Aspecten van onderzoek 8

2 AUDIT AANPAK 10

2.1 BEGRIPPENKADER EN RELEVANTE FUNCTIES 10
2.2 INTERNE AUDIT 10
2.3 EXTERNE PRIVACY AUDIT 12
2.4 HERCONTROLE 13
2.5 COMPETENTIE-EISEN INTERNE- EN EXTERNE AUDITOR 15
2.5.1 Competenties externe auditor 15
2.5.2 Competenties interne auditor 16
2.6 TOETSING OP WERKING 16
2.7 AUDITCYCLUS 16
2.8 WPG AUDIT BIJ SERVICEORGANISATIES 17
2.9 CONSULTATIE 18

BIJLAGE 1 - BEGRIPPENKADER EN RELEVANTE FUNCTIES 19

Begrippenkader in het Wpg-domein 19
Relevante functies in het Wpg-domein 26

BIJLAGE 2 - MODEL ASSURANCE-RAPPORTEN VOOR PRIVACY AUDIT WPG (BOA) 30

BIJLAGE 3 - GUIDANCE BIJ DE TE ONDERZOEKEN WPG BEHEERSINGSMAATREGELEN 31

BIJLAGE 4 - GUIDANCE BIJ DE TE ONDERZOEKEN ORGANISATORISCHE EN TECHNISCHE BEHEERSINGSMAATREGELEN 60

1 Inleiding

1.1 Doel handreiking

Doelstelling 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). De handreiking geeft de bandbreedte aan waarbinnen de IT-auditor de werkzaamheden verricht. Hiermee wordt voorkomen dat er grote verschillen ontstaan in de mate van diepgang bij uitvoering van de audits en het beoordelen van afwijkingen. In deze Handreiking is duidelijk gemaakt welke werkzaamheden door de IT-auditor moeten worden uitgevoerd om tot oordelen met redelijke mate van zekerheid te komen. Het blijft echter de professionele verantwoordelijkheid van de IT-auditor om op basis van een deugdelijke grondslag tot een oordeel te komen per beheersingsmaatregel. Richtlijn 3000 van NOREA is daarbij leidend.

1.2 Achtergrond privacy audit Wpg voor boa's

Tot de inwerkingtreding van de Algemene verordening gegevensbescherming (AVG) verwerkten boa's politiegegevens onder het regime van de Wet bescherming persoonsgegevens (Wbp). In de AVG (artikel 10) is opgenomen dat: *Persoonsgegevens betreffende strafrechtelijke veroordelingen en strafbare feiten of daarmee verband houdende veiligheidsmaatregelen mogen op grond van artikel 6, lid 1, alleen worden verwerkt onder toezicht van de overheid of indien de verwerking is toegestaan bij Unierechtelijke of lidstaatrechtelijke bepalingen die passende waarborgen voor de rechten en vrijheden van de betrokkenen bieden. Omvattende registers van strafrechtelijke veroordelingen mogen alleen worden bijgehouden onder toezicht van de overheid.*

Om aan deze bepaling invulling te geven is de Wet politiegegevens, die oorspronkelijk dateert uit juli 2007, in 2019 aangepast (laatste versie 1 november 2023[1]), en is het Besluit politiegegevens buitengewoon opsporingsambtenaar (Bpg boa) per 6 februari 2019 in werking getreden. Vanaf dat moment verwerken boa's politiegegevens onder het regime van de Wpg. Voor wat betreft het toepassingsbereik sluiten de Verordening (AVG) en de Richtlijn gegevensbescherming bij rechtshandhaving (RGR) (Wpg) elkaar

[1] De versie van 1 november 2023 is hier te vinden: https://wetten.overheid.nl/BWBR0022463/

wederzijds uit, hoewel er materieel sprake is van een zekere overlap. Andere verplichtingen zijn vergelijkbaar maar kennen verschillen in de concrete uitwerking, zoals de verplichting voor de verwerkingsverantwoordelijke passende technische en organisatorische maatregelen te treffen ter bescherming en beveiliging van de gegevens. Voor meer onderwerpen geldt dat die zowel in de richtlijn als de verordening worden geregeld, maar niet op identieke wijze. Dit leidt tot verschillen van uiteenlopende aard en omvang. Het NOREA Privacy Control Framework (PCF) is geënt op de Verordening (AVG) en sluit daarbij niet volledig aan op de Wpg. Daarnaast schrijft de wet een compliance audit voor en geen risico gebaseerde aanpak. Dat maakt dat voor de beoordeling van de verwerking van politiegegevens een eigen, op de Wpg toegesneden, aanpak noodzakelijk is.

Volgens de laatste informatie op politie.nl werken in Nederland ongeveer 23.000 boa's. Het gaat hier om gemeentelijke handhavers, Milieu-boa's (groen en grijs), leerplichtambtenaren, boa's openbaar vervoer, Sociaal Rechercheurs en boa's generieke opsporing. Er zijn zes boa-werkterreinen, ook wel domeinen genoemd. Per domein gelden specifieke opleidingseisen. Een individuele boa kan maximaal voor twee van de volgende domeinen werken:

I. Openbare ruimte, met functies zoals parkeercontroleur/ integraal handhaver
II. Milieu, welzijn en infrastructuur, met functies zoals jachtopziener, boswachter (o.a. Staatsbosbeheer, Natuurmonumenten, Landschappen), medewerker bouw- en woningtoezicht, inspecteur dierenbescherming
III. Onderwijs, met de functie leerplichtambtenaar.
IV. Openbaar vervoer, met functies zoals conducteur, controleur openbaar vervoer (BOA-OV).
V. Werk, inkomen en zorg, met functies zoals sociaal rechercheur, medewerkers arbeidsinspectie.
VI. Generieke opsporing, met functies zoals medewerker Dienst Vervoer & Ondersteuning (DJI), medewerker Belastingdienst/ douanebeambte, weginspecteurs van Rijkswaterstaat (Dienst Verkeers- en Watermanagement), NVWA-ambtenaar, boa in dienst bij politie, boa in dienst bij de Koninklijke Marechaussee.

1.3 (Wettelijke) kaders

Bij het uitvoeren van een privacy audit dient de IT-auditor de volgende documenten -in volgorde van belang- als uitgangspunt te hanteren:

1. **Wet politiegegevens**, Wet van 21 juli 2007 (laatste update 1 november 2023), houdende regels inzake de verwerking van politiegegevens.
2. **Besluit politiegegevens**, Besluit van 14 december 2007, houdende bepalingen ter uitvoering van de Wet politiegegevens.
3. **Besluit politiegegevens buitengewoon opsporingsambtenaren**, Besluit van 6 februari 2019, houdende bepalingen inzake de overeenkomstige toepassing van de Wet politiegegevens op de verwerking van persoonsgegevens door personen die als buitengewoon opsporingsambtenaar zijn belast met de opsporing van strafbare feiten.
4. **Regeling periodieke audit politiegegevens**, Regeling van de Minister van Justitie, de Minister van Binnenlandse Zaken en de Minister van Defensie van 9 december 2008, nr. 5578598/08, houdende nadere regels ten aanzien van het toezicht op de naleving van de bij of krachtens de Wet politiegegevens gegeven voorschriften.
5. **Eventueel formeel van toepassing zijnde sectorale wet- en regelgeving**, zoals de Participatiewet of de Leerplichtwet, gedragscodes, jurisprudentie en publieke afspraken.
6. **Andere, van (informatief) belang zijnde wet- en regelgeving,** zoals de Politiewet 2012 (hierin is o.m. de uitvoering van de politietaak beschreven), het Wetboek van Strafvordering (in artikel 142 is bepaald wie als buitengewoon opsporingsambtenaar met de opsporing van strafbare feiten is belast), de Beleidsregels Buitengewoon Opsporingsambtenaar (het doel van het boa-beleid is om de kwaliteit van de strafrechtelijke handhaving door de boa's te borgen en te verbeteren zodat boa's deze belangrijke rol op een kwalitatief goede wijze kunnen invullen).
7. **De voorliggende NOREA handreiking**, deze handreiking is geldig vanaf het moment van publicatie door NOREA en is bedoeld voor de (interne/externe) privacy audit (zie volgende paragraaf).

1.3.1 Wettelijke grondslag en periodiciteit privacy audits Wpg

De Wpg schrijft voor dat *'Twee jaren na inwerkingtreding van de wet, en vervolgens eenmaal in de vier jaren, laat de verwerkingsverantwoordelijke de uitvoering van de bij of krachtens de wet gegeven regels door een privacy audit controleren, op bij*

ministeriële regeling te bepalen wijze.[2]' (Besluit politiegegevens (Bpg), artikel 6:5 lid 1)

Hieruit volgt dat de verwerkingsverantwoordelijke (doorgaans is dit de werkgever van de boa) in het kalenderjaar 2025 voor de tweede keer een externe privacy audit Wpg laat uitvoeren. In artikel 3 van de Regeling periodieke audits politiegegevens staat dat de verwerkingsverantwoordelijke ervoor zorg moet dragen dat, mede ter voorbereiding op de privacy audit, tenminste jaarlijks een interne audit plaatsvindt.

1.3.2 Object en scope van onderzoek

Het object van onderzoek van een privacy audit Wpg bestaat uit de verwerking(en) van politiegegevens die onder verantwoordelijkheid van de verwerkingsverantwoordelijke plaatsvinden.

Voor de afbakening van de scope van het onderzoek is van belang in aanmerking te nemen dat boa's vaak meerdere taken hebben en verschillende soorten gegevens verwerken. Zo zijn er toezichttaken en opsporingstaken. Dit markeert het onderscheid tussen verwerking onder de AVG en de Wpg (toezicht = AVG, opsporing van strafbare feiten = Wpg). Idealiter zijn voor beide taken aparte gegevenshuishoudingen, systemen en werkprocessen ingericht, maar in de praktijk is dit niet altijd het geval. Hier dient dus rekening mee te worden gehouden voor een juiste afbakening van de scope van onderzoek. Verwerking in het kader van toezichttaken valt niet onder de scope van onderzoek, verwerking in het kader van opsporingstaken wel. Tot slot dient bij het bepalen van de scope van onderzoek rekening te worden gehouden met het feit dat een 'toezicht gegeven' door een besluit van een verwerker in een 'politiegegeven' kan veranderen. Dit is bijvoorbeeld aan de orde als een boa aantekeningen uit zijn toezichttaak door middel van het opstellen van een proces verbaal in een 'artikel 8 Wpg' verwerking omzet. Ook het omgekeerde kan het geval zijn als een politiegegeven wordt verstrekt en daarmee verder onder het regime van de AVG wordt verwerkt.

1.3.3 Aspecten van onderzoek

De Autoriteit Persoonsgegevens (AP) heeft voor de verwerking van persoonsgegevens/ politiegegevens de kwaliteitsaspecten *rechtmatigheid*,

[2] De ministeriële regeling waar hier naar wordt verwezen betreft de Regeling periodieke audit politiegegevens.

transparantie, *doelbinding* en *juistheid* geformuleerd, en voor de beveiliging de kwaliteitsaspecten *beschikbaarheid*, *integriteit* en *vertrouwelijkheid.*

2 Audit aanpak

Uitgangspunt is dat op basis van uitgevoerde interne audits de verwerkersverantwoordelijke afdoende inzicht heeft. Is dat ontoereikend dan kan een directe opdracht (3000D) worden uitgevoerd.

Indien bij aanvang van de opdracht kan worden vastgesteld dat de verwerkingsverantwoordelijke zelf wel afdoende inzicht heeft in interne beheersingsmaatregelen om verantwoording te kunnen afleggen in hoeverre wordt voldaan aan de Wpg, zal de IT-auditor ervoor kiezen een 'Attest opdracht' (3000A) uit te voeren. Hetzelfde geldt voor de assurance-rapporten van de leveranciers van informatiesystemen die politiegegevens verwerken. Opgemerkt wordt dat, indien een opdracht gestart is als 3000D en na verkregen inzicht na aanvang wordt overgeschakeld naar 3000A, Richtlijn 3000A een andere verdeling van rollen en verantwoordelijkheden geeft. Dit vergt dan een nieuwe opdrachtbevestiging.

Met betrekking tot de rapportages is de verwerkingsverantwoordelijke verplicht om de assurance-rapporten van de externe privacy audit en de (eventuele) hercontrole aan de AP te sturen. Voor wat betreft format en vermelding van gevoelige (persoons)gegevens zijn hier met de AP nadere afspraken over gemaakt. De AP heeft aangegeven voorkeur te hebben voor het in deze Handreiking geformuleerde rapportageformat.

2.1 Begrippenkader en relevante functies

Voor een goed begrip en leesbaarheid van deze handreiking is het van belang dat de IT-auditor de gehanteerde begrippen, definities en functies kan plaatsen in het kader van de wet- en regelgeving en de privacy audit Wpg voor boa's. Het begrippenkader en de relevante functies in het Wpg-domein zijn opgenomen in Bijlage 1.

2.2 Interne audit

In het Besluit politiegegevens staat dat ter voorbereiding op de externe privacy audit interne audits plaatsvinden. In de Regeling periodieke audit politiegegevens (art. 3 Interne audit) zijn nadere regels gesteld over de wijze waarop deze audits moeten worden verricht. Samengevat zijn deze:

- de interne audit vindt, ter voorbereiding op de externe privacy audit, tenminste jaarlijks plaats. De interne audit wordt uitgevoerd door middel van een IT-audit;
- de interne audit heeft betrekking op één dan wel een aantal onderdelen van de

wet en heeft tot doel voor het onderdeel of de onderdelen van de wet waar de interne audit zich op richt, op systematische wijze te toetsen of aan de bepalingen van de wet op adequate wijze uitvoering is gegeven. 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.
- de interne audit vindt plaats aan de hand van een overeenkomstig een auditplan. In het auditplan komen minimaal de volgende elementen aan de orde:
    - het doel van de interne audit;
    - de inhoud/object van de interne audit;
    - de doorlooptijd van de interne audit;
    - de onderzoeksinstrumenten die bij de interne audit worden ingezet en de bijdrage daarvan;
    - de wijze waarop en de termijn waarbinnen wordt gerapporteerd;
    - de beveiliging van de ten behoeve van de interne audit verzamelde informatie;
    - de geheimhoudingsplicht waartoe eenieder die betrokken is bij een interne audit verplicht is;
    - de aanbieding en verspreidingskring van de interne auditrapportage.
- indien de verwerkingsverantwoordelijke de toegang tot bepaalde gegevens noodzakelijk noch wenselijk acht voor een goede uitvoering van de interne audit, kan hij de toegang daartoe weigeren, dan wel aan beperkende voorwaarden verbinden. De verwerkingsverantwoordelijke deelt de interne auditor schriftelijk en gemotiveerd zijn beslissing mede;
- de resultaten van de interne audit worden in een auditrapportage vermeld. De auditrapportage bevat minimaal:
    - een beschrijving van de bij het uitvoeren van de audit gevolgde werkwijze;
    - een beschrijving van de resultaten van de interne audit;
    - het oordeel en de aanbevelingen van de auditor.
- na afronding van de interne audit wordt de rapportage onverwijld aangeboden aan de verwerkingsverantwoordelijke. De interne auditrapportage wordt niet aangeboden aan de AP.

Op basis van vorenstaande zouden boa-organisaties, ter voorbereiding op de (externe) privacy audit, in de periode 2021-2024 interne audits uitgevoerd moeten hebben. De interne audit is opgenomen in de Regeling periodieke audit politiegegevens in artikel 3 en daarmee een jaarlijkse verplichting. Mede ter

voorkoming van een dubbele audit last is het wenselijk dat de interne en externe audit op elkaar worden afgestemd zodat ze elkaar versterken. Het is aan de auditor van de externe privacy audit om te bepalen of en hoe deze bij zijn onderzoek gebruik maakt van de uitkomsten van de interne audit. Voor richtlijnen m.b.t. het steunen op de werkzaamheden van de interne auditor wordt verwezen naar NOREA Richtlijn 3000 paragraaf 55 en paragrafen A120 t/m A135. Voor aanvullende guidance kan gebruik gemaakt worden van ISA-610 van de IFAC[3].

Als rapportageformat kan voor de interne audit in beginsel het rapportageformat van de externe privacy audit met een aantal aanpassingen, worden gebruikt.

2.3 Externe privacy audit

In het Besluit politiegegevens staat dat de privacy audit betrekking heeft op de wijze waarop het verwerken van politiegegevens is georganiseerd, de maatregelen en procedures die daarop van toepassing zijn en de werking van deze maatregelen en procedures. In de Regeling periodieke audit politiegegevens (art. 2 Privacy audit) zijn nadere regels gesteld over de wijze waarop deze audits moeten worden verricht. Samengevat zijn dat deze:

- de externe privacy audit wordt uitgevoerd door middel van IT-audit;
- het gaat om een vierjaarlijkse externe privacy audit.
- de externe privacy audit heeft tot doel op systematische wijze te toetsen of aan de bepalingen van de wet op adequate wijze uitvoering is gegeven. 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;
- de resultaten van de interne audits worden betrokken bij de externe privacy audit;
- indien de verwerkingsverantwoordelijke de toegang tot bepaalde gegevens niet wenselijk en/of niet noodzakelijk acht voor een goede uitvoering van de privacy audit, kan hij de toegang daartoe weigeren, dan wel aan beperkende voorwaarden verbinden. De verwerkingsverantwoordelijke deelt de auditor schriftelijk en gemotiveerd zijn beslissing mede. *Opmerking: indien een dergelijke weigering tot gevolg heeft dat onvoldoende geschikte controle-informatie beschikbaar is (zgn. 'objectieve verhindering'), dient een 'oordeel met beperking' te worden afgegeven;*

[3] NOREA is (affiliated) lid van IFAC (International Federation of Accountants).

- de resultaten van de privacy audit worden in een auditrapportage vermeld. De auditrapportage bevat ten minste:
    - een beschrijving van de bij het uitvoeren van de audit gevolgde aanpak;
    - een beschrijving van de resultaten van de privacy audit;
    - het oordeel en de aanbevelingen van de auditor;
    - indien uit de resultaten van de privacy audit blijkt dat niet of niet geheel wordt voldaan aan het bij of krachtens de wet bepaalde, de aanbeveling van de auditor inzake de uitvoering van een hercontrole door een externe dan wel interne auditor;
- De IT-auditor gebruikt het rapportageformat waarnaar in bijlage 2 van deze handreiking wordt verwezen.
- na afronding van de privacy audit wordt de rapportage onverwijld aangeboden aan de verwerkingsverantwoordelijke.

De verwerkingsverantwoordelijke zendt een afschrift van assurance-rapportage van de privacy audit (short-form) aan de Autoriteit persoonsgegevens (art. 33 lid 2 Wpg). De verwerkingsverantwoordelijke levert het rapport van de externe Wpg-audit digitaal aan via: wpg-audit@autoriteitpersoonsgegevens.nl. Let hierbij op de volgende punten:

- verwijder namen van personen uit het document (met uitzondering van de namen van het auditteam). Het is daarna niet nodig het document versleuteld of via een systeem voor beveiligd e-mailen te versturen;
- kies voor een leesbaar bestandsformaat, bij voorkeur PDF/A;
- zorg dat de grootte van het bestand niet meer is dan enkele MB's;
- laat de IT-auditor het assurance-rapport ondertekenen met een EUTL gekwalificeerde handtekening zodat het rapport onweerlegbaar is.

2.4 Hercontrole

De Regeling periodieke audit politiegegevens schrijft voor dat, indien bij het uitvoeren van de externe privacy audit tekortkomingen zijn geconstateerd, de verwerkingsverantwoordelijke binnen drie maanden na oplevering van het externe auditrapport een verbeterrapport (verbeterplan[4]) opstelt waarin de maatregelen

[4] De Regeling periodieke audit politiegegevens spreekt over 'verbeterrapport'. Uit het feit dat de hercontrole binnen een jaar moet worden uitgevoerd, kan worden op gemaakt dat hier 'verbeterplan' bedoelt wordt.

worden beschreven die getroffen zijn (of zullen worden) ter verbetering van de geconstateerde tekortkomingen.

De IT-auditor geeft geen oordeel over de toereikendheid (en uitvoering) van het verbeterrapport van de verwerkingsverantwoordelijke.

Op basis van het verbeterrapport vindt binnen een jaar na oplevering van het externe auditrapport, de hercontrole plaats. De hercontrole heeft betrekking op het onderdeel of de onderdelen van de wet ten aanzien waarvan tekortkomingen zijn geconstateerd (Wpg art. 33 lid 3). Ergo: dus alleen op die beheersingsmaatregelen waar het oordeel “niet voldaan” of “deels voldaan” is bij de externe privacy audit. Op suggestie van de AP en ter bevordering van een efficiënt systeemtoezicht dient in het rapport van de hercontrole een volledige tabel van resultaten te worden opgeleverd en niet alleen een tabel met de in de hercontrole betrokken beheersingsmaatregelen.

De hercontrole wordt uitgevoerd door een externe auditor indien deze daartoe heeft geadviseerd. In alle andere gevallen wordt de hercontrole door een interne auditor uitgevoerd. De Wet beschrijft niet waarop dit advies dient te worden gebaseerd. Als basis voor het advies zouden de volgende aspecten in overweging kunnen worden genomen:

- mate van deskundigheid bij (of de aanwezigheid van) een interne auditfunctie binnen de organisatie;
- significantie van de bevindingen.

Anders dan de eerste auditcyclus, wordt in de tweede auditcyclus op suggestie van de AP de diepgang van de hercontrole gewijzigd: Als de hercontrole plaatsvindt binnen een half jaar na uitvoering van de externe audit, volstaat een beoordeling van de opzet en het bestaan van de beheersmaatregelen. Wordt de hercontrole uitgevoerd tussen een half jaar en een jaar, dan vindt deze plaats op opzet, bestaan en werking van de beheersmaatregelen.

De resultaten van de hercontrole worden in een rapportage vastgelegd. Het format dat IT-auditors hiervoor gebruiken is grotendeels overeenkomstig het format van de externe privacy audit. Na afronding van de hercontrole wordt de rapportage onverwijld aangeboden aan de verwerkingsverantwoordelijke. De verwerkingsverantwoordelijke zendt een afschrift van de rapportage van de hercontrole aan de Autoriteit persoonsgegevens (Wpg art. 33 lid 2) op dezelfde wijze als bij de externe privacy audit. De AP gebruikt de resultaten van de privacy audits en de hercontroles voor haar systeemtoezicht op de naleving van de Wpg.

2.5 Competentie-eisen interne- en externe auditor

De Wpg en meer in het bijzonder de Regeling periodieke audit politiegegevens stelt eisen aan de competentie van zowel de interne als de externe auditor.

Belangrijk: Het algemene uitgangspunt is dat voor wat betreft benodigde vaardigheden, kennis en ervaring met betrekking tot het onderzoeksobject en de meting of evaluatie hiervan het gestelde in paragraaf 31c van NOREA Richtlijn 3000 onverkort van toepassing is. Echter wordt benadrukt dat met name de hierna opgesomde wettelijke eisen t.a.v. specifieke kennis en vaardigheden op het gebied van de politieorganisatie en de verwerking van politiegegevens bijzondere aandacht verdienen bij de opdrachtaanvaarding door de IT-auditor (zie ook A-16 van het Reglement Kwaliteitsbeheersing NOREA (RKBN) en de fundamentele beginselen t.a.v. vakbekwaamheid en zorgvuldigheid zoals beschreven in de NOREA Code of Ethics).

2.5.1 Competenties externe auditor

- De auditor is ingeschreven als Register EDP-auditor bij de Nederlandse Orde van Register EDP-Auditors, dan wel bij een internationaal of Europees equivalent daarvan.
- De auditor beschikt over gedegen en aantoonbare kennis en vaardigheden op het gebied van:
    - de politieorganisatie (in deze: de boa-organisatie);
    - de informatievoorziening en processen van verwerking van politiegegevens;
    - de vigerende wet- en regelgeving, in het bijzonder de Wet politiegegevens (in deze ook: het Besluit politiegegevens buitengewoon opsporingsambtenaar), het Besluit politiegegevens en de Algemene verordening gegevensbescherming en Uitvoeringswet Algemene verordening gegevensbescherming.
- De auditor is onafhankelijk ten opzichte van de auditee.
- De auditor is verplicht tot volledige geheimhouding van de informatie die hij in de loop van zijn auditactiviteiten verkrijgt, behoudens voor zover enig wettelijk voorschrift hem tot mededeling verplicht. Hij legt daartoe een geheimhoudingsverklaring af.
- De functie van auditor kan worden voorgedragen voor aanwijzing als vertrouwensfunctie ingevolge artikel 3 van de Wet veiligheidsonderzoeken.

2.5.2 Competenties interne auditor

- De interne auditor heeft een auditorenopleiding van de politie gevolgd[5].
- De interne auditor beschikt over voldoende kennis en vaardigheden op het gebied van:
    - geautomatiseerde informatiesystemen en methoden en technieken rond IT-auditing;
    - de boa-organisatie;
    - de informatievoorziening en processen van verwerking van politiegegevens;
    - de vigerende wet- en regelgeving, in het bijzonder de Wet politiegegevens, het Besluit politiegegevens en de Algemene verordening gegevensbescherming en Uitvoeringswet Algemene verordening gegevensbescherming.
- De interne auditor stelt zich onafhankelijk op ten opzichte van de auditee.

2.6 Toetsing op werking

De Wpg en meer in het bijzonder de Regeling periodieke audit politiegegevens stellen dat de privacy audit Wpg gericht is op *'de opzet en het bestaan van maatregelen en procedures die in de borging van de wettelijke eisen moeten voorzien, alsmede de werking van de getroffen maatregelen en procedures'*.

Gelet op de periodiciteit van de externe privacy audit Wpg (één keer in de vier jaar), acht NOREA het niet wenselijk, zo niet onmogelijk, om de werking voor alle beheersingsmaatregelen over zo een lange periode te beoordelen. Daarom zal de werking in beginsel alleen worden getoetst over een periode van 12 maanden, voorafgaande aan de privacy audit. Uitzondering hierop vormen de zogenaamde **'Toezichtmaatregelen'**: deze worden wel over de gehele controleperiode op de werking getoetst. De toezichtmaatregelen zijn in het normenkader aangeduid met '**TZM**'.

2.7 Auditcyclus

Doordat de eerste auditcyclus eindigde op 1 januari 2021, zal voor de tweede auditcyclus het volgende auditstramien worden gehanteerd:

5 De politie(academie) heeft geen invulling gegeven aan een dergelijke opleiding. Voor deze wettelijke eis kan daarom worden gelezen dat de interne auditor een training moet hebben gevolgd waarbij invulling is gegeven aan kennis m.b.t. auditing, de boa-organisatie en het verwerken van politiegegevens.

- **controleperiode:** 1 januari 2021 – einddatum onderzoek externe privacy audit Wpg 2024 (31 december 2024);
- **toetsing opzet en bestaan:** gelegen binnen de controleperiode van 12 maanden (1 januari 2024 – 31 december 2024);
- **toetsing werking, maatregelen niet zijnde toezichtmaatregelen (TZM):** een aaneengesloten periode van 12 maanden (1 januari 2024 – 31 december 2024);
- **toetsing werking toezichtmaatregelen (TZM):** de controleperiode 1 januari 2021 – 31 december 2024);
- **inleveren assurance-rapport bij AP:** het assurance-rapport van de privacy audit dient in de periode 1 maart 2025 – 1 maart 2026 aan de AP te worden gezonden;
- **hercontrole**: De hercontrole vindt binnen een jaar na oplevering van het externe auditrapport plaats. Als de startdatum voor de berekening van de termijn van 1 jaar geldt de datum van het assurance-rapport. Gedurende het eerste half jaar na de datum van het assurance-rapport vindt alleen een beoordeling van de opzet en het bestaan van de beheersingsmaatregelen plaats en gedurende het tweede half jaar op opzet, bestaan en werking van de beheersingsmaatregelen.

2.8 Wpg audit bij serviceorganisaties

Voor de verwerking van politiegegevens door boa's wordt in veel gevallen gebruik gemaakt van een informatiesysteem dat wordt beheerd en onderhouden door een derde partij (zgn. serviceorganisatie). Een deel van de beheersingsmaatregelen, zoals de General IT- en Application Controls, valt in die gevallen onder de (uitvoerings)verantwoordelijkheid van de betreffende serviceorganisatie. Het onderzoek bij de serviceorganisatie wordt in beginsel volgens de opname methode (*inclusive methode)* uitgevoerd, tenzij de auditor van de boa-organisatie tijdig kan beschikken over een recente assurance-rapportage van de serviceorganisatie, waarin (tenminste) de volgende zaken zijn opgenomen:

1. een overzicht van de beoordeling en conclusies inzake de opzet, het bestaan en de werking van de passende technische en organisatorische maatregelen, zoals beschreven in bijlage 4 van deze handreiking;
2. een overzicht van de relevante beheersingsmaatregelen Wpg, zoals beschreven in bijlage 3 van deze handreiking met de conclusies inzake de opzet, het bestaan en de werking;
3. een overzicht van de 'verantwoordelijkheden voor de gebruikersorganisatie'.

In dat geval kan voor het onderzoek bij de serviceorganisatie de uitsluitingsmethode (carve-out methode) methodiek worden toegepast. We constateren dat steeds meer serviceorganisatie beschikken over een Wpg assurance-rapport.

Overigens wordt nog opgemerkt dat de verwachting is dat in de praktijk niet altijd afspraken zullen zijn gemaakt met serviceorganisaties om ter plekke een audit te mogen doen ('right to audit'). Het ontbreken van deze (contractuele) mogelijkheid kan ertoe leiden dat onvoldoende assurance-informatie beschikbaar is en daarmee tot een oordeel met beperking.

2.9 Consultatie

Indien een auditor in het kader van de uitvoering van een Wpg-audit wil afwijken van Handreikingen / formats voorgeschreven door stelselhouder(s) / stelselbeheerder(s) / toezichthouder(s) of van de onderhavige Handreiking Privacy audit Wpg voor boa's en/of de formats assurance-rapporten, dient de auditor dit tijdig af te stemmen met NOREA. Afwijken van een door de AP gegeven handreiking of aanwijzing kan niet worden goedgekeurd door andere partijen dan de AP.

Op basis van een door de auditor concreet uitgewerkt voorstel zal onder verantwoordelijkheid van het bestuur van NOREA door ter zake deskundige leden een beoordeling plaatsvinden. Hierbij zullen, waar nodig, overige gremia binnen NOREA waaronder de Vaktechnische Commissie en het bestuur betrokken worden. Tevens zal, voor aangelegenheden die onder de verantwoordelijkheid van de stelsel- of toezichthouder vallen, afstemming plaatsvinden met stelselhouder(s) / stelselbeheerder(s) / toezichthouder(s).

De uitkomsten van de beoordeling worden meegedeeld aan de auditor en zijn bindend voor alle betrokken partijen bij de verdere uitvoering van zijn werkzaamheden.

Voor zover relevant en waar nodig geacht, vindt communicatie in breder verband plaats. Denk daarbij aan alle bij de uitvoering van Wpg-audits betrokken auditors / alle leden NOREA (verantwoordelijkheid NOREA) en/of stelselhouder(s) / stelselbeheerder(s) / toezichthouder(s).

Bijlage 1 – Begrippenkader en relevante functies

Begrippenkader in het Wpg-domein

Artikel 8 gegevens

Dit zijn gegevens die worden verwerkt in het kader van de dagelijkse politietaak. Dit gaat over zaken als wildplassen, foutief aanbieden van afval, alcohol gebruiken op de openbare weg en loslopende honden. Ook proces-verbaal opmaken bij reizen zonder geldig vervoersbewijs, onrechtmatig afgeschoten wild of tuinafvaldump valt hieronder.

Artikel 9 gegevens

Dit zijn gegevens die worden verwerkt in het kader van zogenaamde gerichte verwerkingen. Hierbij kan gedacht worden aan onderzoeken waarbij bijzondere opsporingsbevoegdheden worden ingezet, zoals het plaatsen van een baken onder een auto bij verdenking van stroperij of stelselmatige observatie bij verdenking van bepaalde strafbare feiten.

Betrokkene

De persoon op wie een persoonsgegeven of politiegegeven betrekking heeft. Elke betrokkene heeft een aantal rechten, bijvoorbeeld om de gegevens in te zien die over hem zijn vastgelegd. Deze rechten zijn in de Wpg ingeperkt om het belang van het onderzoek niet te schaden.

Bewaartermijn

De Wpg kent een bewaartermijn; deze volgt op de verwerkingstermijn. Tijdens de bewaartermijn zijn gegevens buiten de operationele omgeving geplaatst, maar nog niet fysiek vernietigd.
Gedurende de bewaartermijn kunnen de gegevens gebruikt worden voor het afhandelen van klachten en voor audits of een controle door de Autoriteit Persoonsgegevens. Verder geldt dat deze gegevens onder bepaalde omstandigheden ter beschikking kunnen worden gesteld voor hernieuwde verwerking. Ze komen dan als het ware opnieuw tot leven in een actueel opsporingsonderzoek. Gegevens mogen gedurende de bewaartermijn ook verwerkt worden voor wetenschappelijk onderzoek en statistiek.

Bijzonder persoonsgegeven

Persoonsgegeven waaruit ras of etnische afkomst, politieke opvattingen, religieuze of levensbeschouwelijke overtuigingen, of het lidmaatschap van een vakbond blijkt. Ook

genetische en biometrische gegevens en gegevens over gezondheid, seksueel gedrag of seksuele gerichtheid zijn bijzondere persoonsgegevens. Het is verboden bijzondere persoonsgegevens te verwerken, tenzij sprake is van een uitzondering die is genoemd in de wet. Een foto (waaronder ook camerabeelden) van een persoon bevat mogelijk informatie over zijn of haar ras en wellicht zijn er meer bijzondere gegevens uit af te leiden, zoals de religie op basis van de gedragen kleding.

Datalek

Een inbreuk in verband met persoonsgegevens kan, wanneer deze niet tijdig en adequaat wordt aangepakt, resulteren in lichamelijke, materiële of immateriële schade voor natuurlijk personen, zoals verlies van controle over hun persoonsgegevens, of beperking van hun rechten, discriminatie, identiteitsdiefstal of -fraude, financiële verliezen, ongeoorloofde ongedaan making van pseudonimisering, reputatieschade, verlies van vertrouwelijkheid van door beroepsgeheim beschermde gegevens of enig ander aanzienlijk economische of maatschappelijk nadeel voor de natuurlijke persoon in kwestie.

Domein

Het in de akte vermelde maatschappelijke deelterrein waarop de buitengewoon opsporingsambtenaar werkzaam is, als aangewezen in de domeinlijsten I tot en met VI van de Beleidsregels Buitengewoon Opsporingsambtenaar.

EDP

De afkorting ‘EDP’ staat voor ‘Electronic Data Processing’ (elektronische gegevensverwerking). Tegenwoordig wordt i.p.v. EDP de afkorting IT gebruikt.

Externe privacy audit

In artikel 6:5, lid 1 Bpg is beschreven dat twee jaren na inwerkingtreding van de wet de verwerkingsverantwoordelijke een privacy audit moet laten uitvoeren. Dit dient te gebeuren conform de regels uit de Regeling periodieke audit politiegegevens. Daarna moet dat elke vier jaar gebeuren. De audit heeft betrekking op de wijze waarop de verwerkingen georganiseerd zijn, de maatregelen en procedures die daarop van toepassing zijn en de werking van deze maatregelen en procedures.

Free flow of information

In principe dienen politiegegevens gedeeld te worden met eenieder die de gegevens nodig heeft voor zijn de uitoefening van zijn taak. Het ter beschikking stellen van politiegegevens is beschreven in artikel 15 van de Wpg. Uitgangspunt is dat

politiegegevens onder voorwaarden kunnen worden gedeeld met eenieder die de gegevens nodig heeft voor zijn de uitoefening van zijn (opsporings-)taak.

Geautomatiseerd vergelijken
Het met een binaire zoeksleutel van (een) trefwoord(en) zoeken van bepaalde politiegegevens. Het resultaat van deze gerichte zoekslag is een uitkomst in de zin van “hit/no hit”.

Gecombineerd verwerken
Zonder binaire zoeksleutel binnen (een selectie van) beschikbare politiegegevens zoeken naar verbanden. Het resultaat van deze vrije zoekslag is een verzameling van gegevens die voldoen aan bepaalde gemeenschappelijke kenmerken. Deze gemeenschappelijke kenmerken kunnen een profiel van indicatoren of bepaalde kenmerken (trefwoorden) inhouden.

Need-to-know- principe
De ontvanger van de politiegegevens moet de gegevens nodig hebben voor de uitvoering van zijn taak.

Normenkader
Het normenkader voor de Wpg privacy audit is volgens de Regeling periodieke audit politiegegevens de Wet politiegegevens zelf. In de privacy audit wordt derhalve de compliancy met de Wpg beoordeeld. Het in deze handreiking opgenomen normenkader is een weerslag van de geldende wet- en regelgeving.

Opsporingsbevoegdheid
De Minister van Justitie en Veiligheid verleent een titel van opsporingsbevoegdheid indien de noodzaak voor (extra) opsporingsbevoegdheid is aangetoond en de betreffende persoon heeft voldaan aan de betrouwbaarheidseis en bekwaamheidseis. Deze toekenning geschiedt formeel tijdens de beëdiging van een persoon als boa door of namens de Minister van Justitie en Veiligheid.

Opsporingsinstantie
Hiermee wordt gedoeld op de politie, de Rijksrecherche, de Koninklijke marechaussee, de Fiscale Inlichtingen- en Opsporingsdienst/Economische Controledienst (FIOD-ECD), de Inspectie Sociale Zaken en Werkgelegenheid (ISZW), directie opsporing, de Inlichtingen- en Opsporingsdienst van de Inspectie

Leefomgeving en Transport (ILT-IOD) en de Inlichtingen- en Opsporingsdienst van de nieuwe Voedsel en Waren Autoriteit (VWA-IOD).

Opsporingstaak

De opsporing van de strafbare feiten, bedoeld in de akte of aanwijzing van opsporingsbevoegdheid, bedoeld in artikel 142, tweede lid, van het Wetboek van Strafvordering. Een boa heeft deze bevoegdheid, een medewerker die alleen toezichthouder is, heeft deze bevoegdheid niet.

Persoonsgegeven

Elk gegeven betreffende een identificeerbaar of geïdentificeerde natuurlijke persoon. Het gaat dus om alles dat in verband kan worden gebracht met een natuurlijke persoon: naam, foto, telefoonnummer, personeelsnummer, maar ook een bankrekeningnummer, gps-positie of kenteken. Audio- en video-opnames zijn ook persoonsgegevens. Belangrijk is dat de persoon nog niet geïdentificeerd hoeft te zijn: het is al een persoonsgegeven als het tot identificatie kán leiden. Denk hierbij aan het BSN.

Politiegegevens

Politiegegevens zijn persoonsgegevens die worden verwerkt in het kader van de uitvoering van de politietaak (artikel 1 sub a Wet Politiegegevens). Te denken valt hierbij aan de persoonsgegevens van verdachten, getuigen en slachtoffers, maar ook camerabeelden en biometrische gegevens. Hiervoor geldt de Wet politiegegevens. Een politiegegeven is dus een specifieke versie van een persoonsgegeven.

Privacy by design

Zowel in de AVG als in de Wpg staat een bepaling over ‘Privacy by design’. De verwerkingsverantwoordelijke moet passende technische en organisatorische maatregelen treffen om rechtmatigheid, proportionaliteit en beveiliging van de gegevensverwerking te garanderen. En dit moet niet achteraf gebeuren, maar al aan de tekentafel waar de verwerking wordt ontworpen (‘by design’). Daarnaast kennen beide wetten ‘Privacy by default’: de standaardinstellingen moeten zo zijn dat de privacy maximaal wordt gewaarborgd.

Rechten van betrokkene

De rechten van betrokkenen zijn in de AVG en Wpg op verschillende manieren gecodificeerd. Het recht op inzage kan onder de Wpg bijvoorbeeld worden beperkt. De Memorie van Toelichting (MvT) geeft aan dat onder meer van toepassing is ter

voorkoming van nadelige gevolgen voor de opsporing en vervolging van strafbare feiten en de bescherming van de rechten en vrijheden van derden (artikel 15 Rl). Dit zien we terug in artikel 27 van de Wpg. Het recht op inzage en het recht op rectificatie zijn geen absolute rechten. Deze rechten kunnen worden beperkt vanwege zwaarder wegende belangen, zoals het belang van het opsporingsonderzoek of van de strafvervolging.

Ter beschikking stellen

Het delen van politiegegevens binnen het Wpg-domein. Dit is beschreven in artikel 15 van de Wpg. Een synoniem hiervoor is 'free flow of information': in principe dienen politiegegevens gedeeld te worden met eenieder die de gegevens nodig heeft voor zijn de uitoefening van zijn taak.
Daarbij geldt altijd het 'need-to-know- principe': de ontvanger moet de gegevens nodig hebben voor zijn taak. De strekking van de wet is dat het breed delen van gegevens de kwaliteit van het werk verbetert.

Verstrekken

Het delen van politiegegevens buiten het Wpg-domein. Denk hierbij aan Bureau Halt, de burgemeester, Belastingdienst of het Centraal Justitieel Incassobureau. Ook in een samenwerkingsverband kunnen, onder voorwaarden, politiegegevens verstrekt worden aan partners, zoals een woningbouwvereniging of winkeliers. In het Bpg boa zijn twee mogelijkheden beschreven om te verstrekken die voor de politie niet gelden. Artikel 6 en 7 van het Bpg boa spreken over het verstrekken van opsporingsgegevens die een boa zelf heeft verzameld en mogelijk heeft verrijkt. Artikel 6 biedt de mogelijkheid om – als boa-werkgever – vaak voor een specifieke groep boa's structureel verstrekken mogelijk te maken aan een instantie. De officier van justitie moet met de verstrekking akkoord gaan, er moet een zwaarwegend algemeen belang zijn en er moet een publicatie over in de Staatscourant komen. Artikel 7 biedt de optie om opsporingsgegevens te verstrekken ten behoeve van de toezichtstaak, voor zover het toezicht binnen hetzelfde boa-domein plaatsvindt. Dit artikel is zowel van toepassing als een boa gegevens wil delen met een partner, als wanneer zijn rol verandert van opsporing naar toezicht.

Verwerken

Elke handeling met een persoons- of politiegegeven. Dus onder andere opschrijven, registreren, vastleggen, filmen, opnemen, raadplegen, vergelijken, wijzigen, tonen, verstrekken en zelfs wissen van persoonsgegevens zijn allemaal vormen van verwerken.

Verwerker

De (rechts)persoon die politiegegevens verwerkt voor een verwerkingsverantwoordelijke. Dit zijn o.a. (interne of externe) hostingorganisaties, particuliere alarmcentrales die beelden van bewakingscamera's ontvangen en bekijken of een leverancier van een boa registratiesysteem als het gaat om gegevens die in het betreffende registratiesysteem worden verwerkt. Elke verwerker werkt onder de verantwoordelijkheid van een verwerkingsverantwoordelijke en volgt zijn aanwijzingen op. Ook moet er een verwerkersovereenkomst worden gesloten tussen de verwerker en de verwerkingsverantwoordelijke om de afspraken helder vast te leggen en verantwoordelijkheden en aansprakelijkheid te regelen.

Verwerkingsgrondslag

De basis waarop persoons- of politiegegevens worden verwerkt. Er zijn verschillende grondslagen voor de verwerking met ieder eigen voorwaarden. Zo kennen artikel 8 gegevens een andere verwekingstermijn dan artikel 9 gegevens. De verwerkingsgrondslagen zijn opgenomen in paragraaf 2 van de Wpg. De AVG kent zes verschillende verwerkingsgrondslagen.

Verwerkingsregister

In het verwerkingsregister moet door de verwerkingsverantwoordelijke het volgende worden vastgelegd: de verwerkingsgrondslag, welke categorieën van betrokkenen en categorieën van gegevens het betreft, de verwijdertermijnen, wie er toegang heeft en welke technische en organisatorische maatregelen, zoals logging, zijn genomen voor de beveiliging van de gegevens.

Verwerkingstermijn

De termijn waarbinnen politiegegevens verwerkt mogen worden. Artikel 8 gegevens hebben een andere verwerkingstermijn dan artikel 9 gegevens. De Wpg kent ook een bewaartermijn; deze volgt op de verwerkingstermijn. Tijdens de bewaartermijn zijn gegevens buiten de operationele omgeving geplaatst, maar nog niet fysiek vernietigd.

Verwerkingsverantwoordelijke

Dit is de (rechts)persoon die het doel en de middelen bepaalt voor de verwerking van persoonsgegevens (AVG) of politiegegevens (Wpg). Bij de politie is dit de korpschef. Bij de Koninklijke marechaussee is het de Minister van Defensie. Voor de boa is het de werkgever van de boa (zie Bpg boa artikel 1 onder c). De verwerkingsverantwoordelijke draagt de algehele verantwoordelijkheid dat

politiegegevens worden verwerkt conform de regels uit de Wpg, waaronder mede begrepen het uitvoering geven aan de Regeling Periodieke audit politiegegevens.

Werkgever boa

Gelet op de grote impact die het gebruik van opsporingsbevoegdheid en geweldsmiddelen op burgers en ondernemingen kan hebben blijven deze bevoegdheden een privilege dat voorbehouden is aan de overheid. Dit betekent dat boa's in beginsel in bezoldigde dienst moeten zijn van een publiekrechtelijk rechtspersoon of een privaatrechtelijk rechtspersoon die voldoet aan de navolgende voorwaarden:

1) de rechtspersoon is een overheidslichaam of is volledig in handen van een overheidslichaam. In het geval van een BV of NV is hiervan sprake indien de aandelen volledig in handen zijn van de overheid (van bijvoorbeeld één of meer gemeenten). In het geval van een stichting of vereniging dienen in de statuten te zijn opgenomen dat het stichtings- of verenigingsbestuur wordt gevormd door afgevaardigden van een overheidslichaam dat de stichting of vereniging heeft opgericht);
2) indien er voor een stichting of vereniging als rechtsvorm wordt gekozen, mogen er geen private partijen in het (dagelijks dan wel stichtings- of verenigings)bestuur van de stichting of vereniging participeren. Tevens dienen de bestuursposities functie gebonden te zijn. Dat wil zeggen dat, indien er bijvoorbeeld een burgemeester in het bestuur zitting heeft, hij die functie ambtshalve bekleedt en niet als privépersoon;
3) de democratische controle op de rechtspersoon dient gewaarborgd te zijn opdat de democratische controle op de handhavings- en opsporingsactiviteiten van de rechtspersoon in volle omvang uitgeoefend kan worden (hiertoe dienen tevens de voorwaarden 1 en 2);
4) de lokale driehoek is het overleg dat plaatsvindt over de taakuitvoering van de politietaken, namelijk door de burgemeester, de (hoofd)officier van justitie, de lokale politiechef en zo nodig de korpschef. De lokale driehoek dient in te stemmen met het onderbrengen van de betreffende boa-taken in de betreffende rechtspersoon. Het is raadzaam om voor de organisatorische inbedding instemming van de lokale driehoek te vragen. Dit sluit aan op het vereiste van inbedding in het lokale veiligheidsbeleid;
5) de boa's dienen operationeel samen te werken met de politie.

Uitzonderingen:

Op het hiervoor beschreven algemene uitgangspunt dat boa's in (a) bezoldigde dienst moeten zijn van (b) een overheidsorgaan zijn drie uitzonderingen mogelijk:

1) functies betreffende de uitoefening van specifieke en beperkte taken waarmee een zwaarwegend maatschappelijk belang is gemoeid. Hierbij kan gedacht worden aan boa's die reeds van oudsher taken uitvoeren voor een particuliere werkgever met een publieke taak belast of gevallen waarbij als uitvloeisel van privatiseringsoperaties specifieke opsporingsbevoegdheden zijn overgeheveld van de publieke naar de private sector. In dit geval is het dus mogelijk dat de boa niet in overheidsdienst is, en ook dat de boa geen loon ontvangt van de betrokken particuliere werkgever. Er moet wel sprake zijn van een gezagsverhouding tussen de particuliere werkgever en de boa;
2) inhuur van een particuliere functionaris voor boa-functies. Een overheidsorgaan of particuliere werkgever kan onder de voor het betreffende domein geldende voorwaarden een particuliere functionaris inzetten voor de uitoefening van de opsporingsbevoegdheden 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. Hierbij heeft deze boa een arbeidsovereenkomst met een particuliere werkgever en ontvangt van deze werkgever loon. 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;
3) het lopen van een stage met de status van buitengewoon opsporingsambtenaar. Indien hier geen sprake is van bezoldiging, moet er een gezagsverhouding zijn tussen de partij waarbij stage wordt gelopen en de stagiair.

Relevante functies in het Wpg-domein

Het is van belang dat de IT-auditor bekend is met de verschillende rollen en functies in het Wpg- en Bpg boa-domein.

<u>Bevoegd gezag</u>

Het verwerken van politiegegevens is een aangelegenheid van beheer, en niet van gezag. De Wpg richt zich dan ook voornamelijk tot 'de verwerkingsverantwoordelijke'. Dit laat onverlet dat de officier van justitie vanuit zijn wettelijk gezag over de opsporing van strafbare feiten (art. 148 van het Wetboek van Strafvordering (Sv) en art. 12 Politiewet 2012) zeggenschap heeft over het daadwerkelijke gebruik van de

politiegegevens die zijn verwerkt ten behoeve van de strafrechtelijke handhaving van de rechtsorde. Ook kunnen belangen van opsporing en vervolging richtinggevend zijn voor het beheer van politiegegevens.

Buitengewoon opsporingsambtenaar (boa)

De uitvoering en de handhaving van met name bijzondere wetgeving en verordeningen van provincies, gemeenten en waterschappen, is opgedragen aan een scala aan publiekrechtelijke en aan een beperkt aantal privaatrechtelijke organisaties. Indien nodig kan aan werknemers van zo'n organisatie opsporingsbevoegdheid worden toegekend. Zij zijn dan boa. Daarvoor is nodig dat betrokkene beschikt over een titel van opsporingsbevoegdheid, over de vereiste bekwaamheid en betrouwbaarheid, en over een akte van beëdiging (zie artikel 2 van het Besluit buitengewoon opsporingsambtenaar (hierna ook: BBO)). De titel van opsporingsbevoegdheid wordt verleend door de Minister van Justitie en Veiligheid op grond van artikel 142 eerste lid, onder a en b, en derde lid van het Wetboek van Strafvordering of bij of krachtens een bijzondere wet of (decentrale) verordening. Voor economische delicten wordt de titel verleend door de Minister van Justitie en Veiligheid, in overeenstemming met de minister wie het aangaat, op grond van artikel 17, eerste lid, onder 2°, van de Wet op de Economische Delicten.

De Minister van Justitie en Veiligheid verleent een titel van opsporingsbevoegdheid indien de noodzaak voor (extra) opsporingsbevoegdheid is aangetoond en de betreffende persoon heeft voldaan aan de betrouwbaarheidseis en bekwaamheidseis. Deze toekenning geschiedt formeel tijdens de beëdiging van een persoon als boa door of namens de Minister van Justitie en Veiligheid.

De Minister van Justitie en Veiligheid kan bepalen dat een boa geweld of vrijheidsbeperkende middelen kan gebruiken en bevoegd is tot verschillende vormen van fouillering (zie artikel 7 lid 9 Politiewet 2012), in deze beleidsregels aangeduid als politiebevoegdheden. Ook kunnen aan een boa geweldsmiddelen worden toegekend. Onder geweldsmiddelen worden in deze beleidsregels verstaan: handboeien, wapenstok, pepperspray, vuurwapen en surveillancehond (gecertificeerde diensthond).

Met het scala aan organisaties belast met de uitvoering en handhaving van een grote variëteit aan wettelijke regelingen is de diversiteit van boa's een gegeven. Niet alleen het werkveld van boa's is divers. Aangezien bevoegdheden op maat worden toegekend, variëren deze evenzeer. De boa heeft in de regel beperkte opsporingsbevoegdheid die is gerelateerd aan zijn functie en taakomschrijving. De boa wordt ingezet daar waar opsporing door de politie niet gewenst, vanwege

prioritering, of niet mogelijk is vanwege onvoldoende deskundigheid of capaciteit bij de politie.
Een boa is dus in beginsel geen integrale handhaver met algemene opsporingsbevoegdheid die concurreert met de politie. Immers, de boa zou dan een vierjarige politieopleiding moeten hebben gevolgd om te beschikken over dezelfde bekwaamheid. De boa heeft een specifieke, afgebakende taak waarvoor hij gericht opgeleid kan worden.
Het bovenstaande in aanmerking genomen is een boa een functionaris die uit hoofde van zijn taak, in ondergeschiktheid aan het bevoegde gezag, in overeenstemming met de geldende rechtsregels en met behulp van de hem daartoe beschikbaar gestelde bevoegdheden en middelen, zorgdraagt voor de opsporing van strafbare feiten alsmede met de voorbereiding van de eventuele vervolging van deze feiten.

Bevoegde functionaris (BF)
Dit is de 'hoeder' van de gegevens die onder artikel 9 Wpg worden verwerkt. Deze functionaris is beschreven in artikel 2:10, eerste lid, van het Besluit politiegegevens (Bpg). Het moet een persoon zijn met voldoende kennis en vaardigheden over dit type gegevens. Deze functionaris beslist bijvoorbeeld wie er toegang mag hebben tot deze gegevens en of ze verstrekt kunnen worden aan een samenwerkingspartner. Iedere artikel 9-verwerking dient een bevoegde functionaris (BF) te hebben. Binnen de politie wordt vaak een teamchef of coördinator aangewezen om binnen een rechercheonderzoek deze rol op zich te nemen. Ook als een boa een dergelijke verwerking doet, dient er een BF te worden aangewezen. De BF wordt aangewezen door de werkgever van de boa.
De BF heeft onder andere de volgende taken:

- het doel van de artikel 9-verwerking omschrijven en vastleggen (zie Wpg art. 32);
- het autoriseren van personen voor de betreffende verwerking;
- bepalen of gegevens voor andere doeleinden mogen worden gebruikt – zie Wpg art. 9, lid 3;
- zorgen dat voor alle gegevens de herkomst en wijze van verkrijgen wordt vastgelegd – zie Wpg art. 3, lid 5;
- bewaken dat gegevens rechtmatig worden verkregen en verwerkt. Hierbij moet vooral worden gelet op de termijnen.

Functionaris voor de Gegevensbescherming (FG)
De FG is een onafhankelijke functionaris die binnen de organisatie van de verwerkingsverantwoordelijke toezicht houdt op naleving van de AVG en/of de Wpg. De FG wordt door de verwerkingsverantwoordelijke aangewezen en wordt betrokken

bij alle aangelegenheden die gaan over de bescherming van persoonsgegevens. De FG wordt op grond van haar of zijn professionele kwaliteiten en deskundigheid op het gebied van de wetgeving gekozen en is het eerste aanspreekpunt voor de AP. Van belang is dat apart voor de Wpg een FG dient te worden aangewezen door de verwerkingsverantwoordelijke aangezien de Wpg een aantal specifieke taken toebedeelt aan de FG-Wpg.
In artikel 36 Wpg is een aantal (specifieke) taken voor de FG-Wpg beschreven:

- het toezien op de naleving van het bepaalde bij of krachtens deze wet en op het beleid van de verwerkingsverantwoordelijke met betrekking tot de bescherming van persoonsgegevens, met inbegrip van de toewijzing van de autorisaties, bedoeld in artikel 6, de bewustmaking en opleiding van de boa's die zijn betrokken bij de verwerking van politiegegevens en de audits, bedoeld in artikel 33;
- het informeren en adviseren van de verwerkingsverantwoordelijke en de boa's die politiegegevens verwerken over hun verplichtingen op grond van het bepaalde bij of krachtens deze wet en andere gegevensbeschermingsbepalingen op grond van het Unierecht of het Nederlandse recht;
- het desgevraagd verstrekken van advies over de gegevensbeschermingseffect-beoordeling, bedoeld in artikel 4c, en het toezien op de uitvoering ervan;
- het samenwerken met de Autoriteit persoonsgegevens;
- het optreden als contactpunt voor de Autoriteit Persoonsgegevens inzake aangelegenheden in verband met de verwerking van persoonsgegevens en, voor zover dienstig, het plegen van overleg over enige andere aangelegenheid.

<u>Privacyfunctionaris</u>
De privacyfunctionaris (ook wel: privacy-officer) geeft advies en houdt toezicht. Deze formele rol komt alleen voor in de Wpg en niet in de AVG. Bij de politie – waar ruim 65.000 mensen werken – zijn verschillende van deze functionarissen actief. Het Bpg boa schrijft geen privacyfunctionaris binnen de boa- organisaties voor. In artikel 2, lid 1 van het Bpg boa staat namelijk dat artikel 34 Wpg is uitgezonderd. Een privacyfunctionaris naast een FG is volgens de wetgever een (te) zware belasting, zeker voor kleine organisaties. Dit neemt niet weg dat het verstandig kan zijn toch een privacyfunctionaris aan te stellen. Deze persoon kan een adviserende rol innemen bij bijvoorbeeld het inrichten van het verwerkingsregister, het aanwijzen van bevoegde functionarissen en andere Wpg-vraagstukken.

Bijlage 2 - Model assurance-rapporten voor privacy audit Wpg (boa)

Model assurance-rapporten voor de (externe) privacy audit Wpg (boa) en de hercontrole worden als download beschikbaar op de NOREA website.

Bijlage 3 - Guidance bij de te onderzoeken Wpg beheersingsmaatregelen

Criteria

De (generieke) algehele beheersingsdoelstelling voor de privacy audit Wpg voor boa's is het voorzien in de borging van de wettelijke eisen met betrekking tot de verwerking van politiegegevens door boa's. **Hiertoe heeft de organisatie beheersingsmaatregelen getroffen die in opzet, bestaan en werking door de auditor worden getoetst. De IT-auditor maakt bij deze toetsing gebruik van de volgende criteria:**	
Criteria met betrekking tot de opzet, het bestaan en de werking:	
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 controleperiode volgens de opzet toegepast. In het geval van handmatige beheersingsmaatregelen zijn deze toegepast door competente én bevoegde personen.

Tabel met illustratieve beheersingsmaatregelen, nadere toelichtingen en voorgestelde testaanpak o.b.v. de Wet Politiegegevens (Wpg), het Besluit politiegegevens (Bpg), het Besluit politiegegevens buitengewoon opsporingsambtenaar (Bpg boa) en aanvullende wet- en regelgeving.

Bijlage 3 - Guidance bij de te onderzoeken Wpg beheersingsmaatregelen					
#	**Onderwerp**	**Verwijzing**	**Beheersingsmaatregelen**	**Nadere toelichting**	**Voorgestelde testaanpak**
1	Reikwijdte	Art 2 lid 1 en 2	De verwerkingsverantwoordelijke heeft bestanden met politiegegevens binnen de organisatie geïdentificeerd en gedocumenteerd.	Voor de boa gelden twee privacy regimes: de AVG en de Wpg. Dat levert meestal twee aparte gegevensverzamelingen op die aan twee aparte werkprocessen gekoppeld zijn: toezicht en opsporing. Het is raadzaam om de opslag van de gegevens in verschillende informatiesystemen te laten plaatsvinden. Als gegevens toch in hetzelfde informatiesysteem staan, moeten ze in elk geval goed 'gelabeld' worden zodat duidelijk is wat het doel van de verwerking is: opsporing of toezicht. Tevens moet – als het om opsporing gaat – zichtbaar zijn welke Wpg-verwerkingsgrondslag van toepassing is: 8, 9, 11 (m.u.v. lid 2) of 13. Er gelden tenslotte andere regels en termijnen. Voor iedere artikel 9-verwerking geldt bovendien dat er een bevoegd functionaris aan gekoppeld moet kunnen worden, dat er selectief geautoriseerd moet kunnen worden, et cetera. Alle bestanden met politiegegevens zijn bekend en zowel het doel als de inhoud zijn bekend.	• Controleer of de verantwoordelijkheden voor het identificeren en documenteren van verwerkingen zijn belegd. • Inspecteer het register van verwerkingen. • Controleer of de verwerkingen van politiegegevens binnen de organisatie zijn geïdentificeerd en gedocumenteerd. Dit omvat ook de bijbehorende processen en systemen, informatiestromen, classificatie van gegevens, alsmede derde partijen die politiegegevens verwerkt. • Controleer of het overzicht van de inventarisatie periodiek wordt geactualiseerd. • Interview de verantwoordelijke functionarissen.

Bijlage 3 - Guidance bij de te onderzoeken Wpg beheersingsmaatregelen					
#	Onderwerp	Verwijzing	Beheersingsmaatregelen	Nadere toelichting	Voorgestelde testaanpak
				Aanvullend wordt opgemerkt dat de Wpg van toepassing is op de verwerking van politiegegevens die in een bestand zijn opgenomen of bestemd zijn daarin te worden opgenomen. Onder 'bestanden met politiegegevens' worden zowel de geautomatiseerde als handmatige verwerking van politiegegevens verstaan. Feitelijk valt het 'opschrijfboekje' van de boa ook onder de reikwijdte van de Wpg.	
2	Doelbinding	Art 3 lid 1, 3 en 4 Art 8 lid 1 Art 9 lid 1 en 2 Art 11 (m.u.v. lid 2) Art 13	Politiegegevens worden alleen verwerkt als dat nodig is voor de in de wet genoemde doeleinden. Geborgd is dat bij het verwerken van politiegegevens altijd sprake is van doelbinding en dat de gegevens niet op een onrechtmatige wijze, worden verwerkt.	Geborgd is dat bij het verwerken van politiegegevens alleen plaatsvindt voor de in de wet genoemde doeleinden. De verwerkingsverantwoordelijke legt van alle verwerkingen de doelbinding vast (bijvoorbeeld in het verwerkingsregister).	• Inspecteer de procedure/werkinstructie(s) (minimaal: noodzaak doelbinding verschillende artikelen, controle op doelbinding, voor art. 9: het vastleggen van doel onderzoek binnen een week en melden hiervan aan de Bevoegde Functionaris (BF). • Controleer of de Bevoegde Functionaris (BF) instemming heeft gegeven voor de (verdere) verwerking conform art. 9.3, 11.1, 11.4 en/of 13.3 en dat dit is vastgelegd. • Stel vast of conform de opzet wordt gewerkt. • Interview de verantwoordelijke functionarissen.
3	Nood-zakelijkheid & rechtmatig-heid, vermelding herkomst	Art 3 lid 2 en 5	Er wordt geborgd dat de politiegegevens daartoe toereikend, ter zake dienend en beperkt zijn tot wat noodzakelijk is (niet bovenmatig) en dat de herkomst van gegevens voor art 9 verwerkingen wordt vermeld.	Er wordt (in o.a. werkinstructies, procedures en helpteksten in informatiesystemen) geborgd dat de politiegegevens daartoe toereikend, ter zake dienend en beperkt zijn tot wat noodzakelijk is (niet bovenmatig) en dat de herkomst van gegevens voor artikel 9 verwerkingen wordt vermeld. Geborgd is dat bij het verwerken van art 9 politiegegevens er tijdig vastlegging van het doel plaatsvindt.	• Controleer procedure/werkinstructie(s) (minimaal moet deze de maatregelen bevatten die zouden moeten borgen dat de verwerking noodzakelijk en rechtmatig is, vastlegging herkomst en wijze van verkrijging, controle op deze maatregelen). • Stel vast of conform de opzet wordt gewerkt. • Steekproef met deelwaarnemingen waaruit de noodzakelijkheid en rechtmatigheid van

Bijlage 3 - Guidance bij de te onderzoeken Wpg beheersingsmaatregelen					
#	Onderwerp	Verwijzing	Beheersingsmaatregelen	Nadere toelichting	Voorgestelde testaanpak
				De verwerking vindt slechts plaats wanneer dit strikt noodzakelijk is, met inachtneming van passende waarborgen voor de rechten en vrijheden van de betrokkene. De passende waarborgen voor de betrokkene kunnen bijvoorbeeld inhouden dat de gegevens enkel mogen worden verzameld in samenhang met andere gegevens over de natuurlijke persoon in kwestie, dat de verzamelde gegevens afdoende kunnen worden beveiligd, dat strengere regels gelden voor de toegang van het personeel van de bevoegde autoriteit tot de gegevens, en dat de doorzending van die gegevens wordt verboden. Met de vereisten dat de gegevens worden verwerkt in aanvulling op de verwerking van andere politiegegevens en dat wordt voorzien in een afdoende niveau van beveiliging wordt hieraan invulling gegeven.	de gegevensverwerking herleid kan worden. • Interview de verantwoordelijke functionarissen.
4	Juistheid en volledigheid politie-gegevens	Art 4 lid 1	De verwerkingsverantwoordelijke heeft controles op de kwaliteit ingericht ten behoeve van de borging van de juistheid en nauwkeurigheid van politiegegevens.	In artikel 4 eerste lid is de algemene verplichting voor de verwerkingsverantwoordelijke opgenomen om de nodige maatregelen te treffen opdat politiegegevens die, gelet op de doeleinden waarvoor zij worden verwerkt, onjuist, onvolledig of niet meer actueel zijn, niet worden verstrekt of beschikbaar gesteld. Het is van belang dat bijv. de juistheid van namen en BSN's worden gecontroleerd, bijvoorbeeld door controle met gemeentelijke basisadministratie. Ook interne procedures voor tegenlezen, application controls (bijv. veld controles voor juiste manier invoeren	• Inspecteer de procedures die een juiste en volledige verwerking van politiegegevens waarborgen. • Inspecteer de procedurele- en/of application controls in systemen (gericht op juistheid en nauwkeurigheid van politiegegevens). • Stel vast of conform de opzet wordt gewerkt. • Interview de verantwoordelijke functionarissen.

Bijlage 3 - Guidance bij de te onderzoeken Wpg beheersingsmaatregelen					
#	Onderwerp	Verwijzing	Beheersingsmaatregelen	Nadere toelichting	Voorgestelde testaanpak
				kentekens), kunnen invulling geven aan de controles op juistheid en volledigheid. In artikel 4 vierde lid is opgenomen dat, als blijkt dat onjuiste gegevens zijn verstrekt, de ontvanger daarvan onverwijld in kennis gesteld.	
5	Onderscheid feiten en persoonlijk oordeel	Art 4 lid 3	Er zijn maatregelen genomen om politiegegevens die op feiten zijn gebaseerd, voor zover mogelijk, te onderscheiden van politiegegevens die op een persoonlijk oordeel zijn gebaseerd.	Voor het strafvorderingsproces is het van belang dat onderscheid wordt gemaakt tussen vaststaande feiten en persoonlijke oordelen. Opgemerkt wordt dat dit onderscheid een relatief karakter heeft aangezien gedurende het onderzoek gegevens waarvan is aangenomen dat die op vaststaande feiten zijn gebaseerd, op persoonlijke opvattingen blijken te berusten en vice versa. Voor de vastlegging worden doorgaans redenen van wetenschap gebruikt, bijv. ik zag / voelde / rook daar enzv.…). Een beheersingsmaatregel om dit te borgen kan bijvoorbeeld zijn dat alle processen verbaal worden 'tegengelezen' met aandacht voor (o.m.) het onderscheid tussen feiten en persoonlijk oordeel.	• Inspecteer de opzet van de technische en organisatorische maatregelen om onderscheid tussen feitelijke en subjectieve gegevens te waarborgen. • Inspectie van de werkprocedures, instructies en de labeling van de gegevens. • Stel vast of conform de opzet wordt gewerkt. • Interview de verantwoordelijke functionarissen.
6	Gegevens-bescherming door beveiliging en ontwerp	Art 4a lid 1 t/m 5	Er is (aantoonbaar) een risicoanalyse uitgevoerd waaruit het risiconiveau blijkt m.b.t. ongeoorloofde of onrechtmatige verwerking en tegen opzettelijk verlies, vernietiging of beschadiging. De verwerkingsverantwoordelijke identificeert, evalueert en	Dit betreft 'Privacy by design'. De verwerkingsverantwoordelijke moet passende technische en organisatorische maatregelen treffen om rechtmatigheid, proportionaliteit en beveiliging van de gegevensverwerking te garanderen. En dit moet niet achteraf gebeuren, maar al aan de tekentafel waar de verwerking wordt ontworpen ('by design').	• Controleer of het gegevensbeschermingsbeleid van de organisatie is vastgelegd en vastgesteld. • Controleer of er een duidelijke relatie ligt tussen de maatregelen en de uitgevoerde DPIA. • Controleer of er een procedure is voor het periodiek testen en evalueren van de doeltreffendheid van de technische en organisatorische maatregelen.

Bijlage 3 - Guidance bij de te onderzoeken Wpg beheersingsmaatregelen					
#	Onderwerp	Verwijzing	Beheersingsmaatregelen	Nadere toelichting	Voorgestelde testaanpak
			mitigeert systematisch en periodiek factoren die het beschermen van politiegegevens tegen ongeoorloofde of onrechtmatige verwerking en tegen opzettelijk verlies, vernietiging of beschadiging in gevaar brengen en past de maatregelen hierop aan. De organisatie heeft gegevensbeschermingsbeleid en procedures ontwikkeld en vastgesteld. De verwerkingsverantwoordelijke heeft de maatregelen die nodig zijn om het risico te beperken (passende technische en organisatorische maatregelen) aantoonbaar geïmplementeerd. Privacy by design wordt toegepast/geborgd (bijv. bij ontwikkelingen/ wijzigingen).		• Inspectie van de uitgevoerde DPIA's. • Inspectie van contracten met leveranciers, SLA's en andere gerelateerde documenten met focus. • Stel vast of conform de opzet wordt gewerkt. • Interview de verantwoordelijke functionarissen.
7	Gegevens-bescherming door standaard-instellingen	Art 4b lid 1a en lid 1b	De verwerkingsverantwoordelijke treft passende technische en organisatorische maatregelen om te waarborgen dat standaard: a) alleen die politiegegevens worden verwerkt die noodzakelijk zijn voor elk specifiek doel van de verwerking;	De Wpg kent (evenals de AVG) 'Privacy by default': de standaardinstellingen moeten zo zijn dat de privacy maximaal wordt gewaarborgd. Om dit te kunnen aantonen moet de verwerkingsverantwoordelijke intern beleid vaststellen en maatregelen implementeren die in het bijzonder voldoen aan de beginselen van gegevensbescherming door ontwerp en gegevensbescherming door standaard-instellingen ('privacy by design and by default').	• Inspecteer het interne beleid ten aanzien van de beginselen van gegevensbescherming door ontwerp en gegevensbescherming door standaardinstellingen ('privacy by design and by default'). • Inspecteer de implementatie van het beleid. • Stel vast of conform de opzet wordt gewerkt. • Interview de verantwoordelijke functionarissen.

Bijlage 3 - Guidance bij de te onderzoeken Wpg beheersingsmaatregelen					
#	**Onderwerp**	**Verwijzing**	**Beheersingsmaatregelen**	**Nadere toelichting**	**Voorgestelde testaanpak**
			b) politiegegevens niet zonder tussenkomst van een natuurlijke persoon voor een onbeperkt aantal natuurlijke personen toegankelijk worden gemaakt.	Bij de ontwikkeling van die maatregelen en procedures moeten de resultaten van DPIA's in acht worden genomen.	
8	Gegevensbe-schermings-effectbeoor-deling/ Data protection impact assessment (DPIA)	Art 4c	Indien een verwerking waarschijnlijk een hoog risico voor de rechten en vrijheden van personen oplevert worden binnen de organisatie de risico's systematisch geïdentificeerd, beoordeeld en aangepakt door middel van een DPIA die ten minste aan de eisen gesteld in de wet voldoet. De verwerkingsverantwoordelijke beoordeelt, indien nodig of wanneer sprake is van een verandering van het risico, of de verwerking in overeenstemming met de DPIA wordt uitgevoerd en past de DPIA zo nodig aan.	In dit lid is de verplichting opgenomen voor de verwerkingsverantwoordelijke om een beoordeling te verrichten van het effect van beoogde verwerkingsactiviteiten op de bescherming van persoonsgegevens. Dit is ook bekend als een DPIA. Deze verplichting geldt wanneer een soort verwerking, in het bijzonder een verwerking waarbij nieuwe technologieën worden gebruikt, gelet op de aard, het toepassingsgebied, de context of de doeleinden daarvan, waarschijnlijk een hoog risico voor de rechten en vrijheden van natuurlijke personen oplevert. Hiervoor kan worden gedacht aan het onderzoek van DNA-profielen van grote aantallen personen of bevolkingsgroepen. Hierbij wordt met name gekeken naar de voorgenomen maatregelen, waarborgen en mechanismen voor het beschermen van persoonsgegevens en het aantonen dat aan de richtlijn is voldaan. Effectbeoordelingen dienen relevante systemen en procedures van verwerkingsactiviteiten te bestrijken maar geen individuele gevallen.	• Stel vast dat voor alle verwerkingen is bepaald of sprake is van een hoog privacy risico (bijv. door middel van een 'pre-PIA'). • Stel vast of een procesbeschrijving bestaat t.a.v. het uitvoeren van DPIA's, waarin ook het proces is opgenomen dat DPIA's periodiek opnieuw dienen te worden beoordeeld en zo nodig aangepast. • Stel (o.a. op basis van het verwerkingsregister) vast of in de controleperiode verwerkingen zijn gestart die (waarschijnlijk) een hoog risico voor de rechten en vrijheden van personen opleveren. • Stel vast of t.a.v. deze verwerking(en) DPIA('s)zijn opgesteld dan wel via een verkorte DPIA is vastgesteld dat een volledige DPIA niet nodig is.[6] • Inspecteer de rapportage van de uitgevoerde DPIA('s) en stel vast of deze aan de wettelijke eisen voldoet; • Stel vast of conform de opzet wordt gewerkt. • Interview de verantwoordelijke functionarissen.

[6] In de Staatscourant is een lijst van verwerkingen van persoonsgegevens gepubliceerd waarvoor een gegevensbeschermingseffectbeoordeling (DPIA) volgens de AP verplicht is.

Bijlage 3 - Guidance bij de te onderzoeken Wpg beheersingsmaatregelen					
#	**Onderwerp**	**Verwijzing**	**Beheersingsmaatregelen**	**Nadere toelichting**	**Voorgestelde testaanpak**
9	Bijzondere categorieën van politie-gegevens	Art 5	Er vindt geen verwerking van bijzondere categorieën van politiegegevens plaats, tenzij: • dat onvermijdelijk is voor het doel van de verwerking; • dit in aanvulling is op de verwerking van andere politiegegevens betreffende de persoon; • de gegevens afdoende zijn beveiligd.	Dit artikel betreft bijzondere categorieën van politiegegevens. Dit betreft niet alleen persoonsgegevens betreffende iemands godsdienst of levensovertuiging, ras, politieke gezindheid, gezondheid, seksuele leven, of het lidmaatschap van een vakvereniging maar ook gegevens betreffende etnische afkomst, genetische gegevens en biometrische gegevens met het oog op de unieke identificatie van een natuurlijke persoon.	• Inspecteer het verwerkingsregister. • Stel vast of er bijzondere persoonsgegevens worden verwerkt. Indien dit tijdens de controleperiode niet het geval is geweest, kan hier 'non-occurrence' t.a.v. bestaan en werking worden vermeld. Indien dit wel het geval is geweest, Stel vast dat: ○ deze verwerking(en) van bijzondere categorieën van politiegegevens onvermijdelijk was/waren voor het doel van de verwerking; ○ Dit in aanvulling was op de verwerking van andere politiegegevens betreffende de persoon; ○ De gegevens afdoende zijn beveiligd. • Interview de verantwoordelijke functionarissen.
10	Autorisaties en toegang tot politie-gegevens	Art 6 lid 1 t/m 6 Art 6a	Er is een systeem van autorisaties dat voldoet aan de vereisten van zorgvuldigheid en evenredigheid. Dit houdt in dat: De verwerkingsverantwoordelijke heeft die personen die vanuit hun functie en de wet toegang mogen hebben tot bepaalde politiegegevens geautoriseerd voor alleen die gegevens (need-to-know). Er is een proces voor het toewijzen, wijzigen en intrekken van autorisaties t.b.v. de toegang tot politiegegevens.	Het autorisatiebeheerproces dient te voldoen aan de vereisten van zorgvuldigheid en evenredigheid. In de basis betekent dit dat voor elke toegang een aantoonbare functionele behoefte (need-to-know) dient te zijn. In bijzondere gevallen kunnen personen die geen ambtenaar van politie (boa) zijn worden geautoriseerd voor de verwerking van politiegegevens ter uitvoering van specifieke onderdelen van de politietaak. Ook kunnen in bijzondere gevallen boa's die onder de verantwoordelijkheid van een andere verwerkingsverantwoordelijke vallen, worden geautoriseerd voor de verwerking van politiegegevens ter uitvoering van in de	• Inspecteer de autorisatieprocedure, afspraken met leveranciers met betrekking tot toegang tot de systemen en data en andere gerelateerde documenten. • Inspecteer de autorisatiematrix en stel vast dat: ○ autorisaties worden verleend op basis van functionele behoefte ('need to know'); ○ in de autorisatiematrix alle personen (boa's en niet-boa's) zijn vermeld die politiegegevens in bestanden verwerken; ○ de autorisatiematrix up to date is; ○ periodiek controles plaatsvinden op

Bijlage 3 - Guidance bij de te onderzoeken Wpg beheersingsmaatregelen					
#	Onderwerp	Verwijzing	Beheersingsmaatregelen	Nadere toelichting	Voorgestelde testaanpak
			Er zijn maatregelen vastgesteld en geïmplementeerd die de identiteit en de toegangsrechten van een gebruiker controleert en rechtmatige toegang tot de gegevens borgt.	autorisatie omschreven onderdelen van de politietaak.	de toegekende autorisaties (minimaal 2x per jaar). • Beoordeel de technische en organisatorische maatregelen zoals aangegeven in Bijlage 4. • Stel vast of conform de opzet wordt gewerkt. • Interview de verantwoordelijke functionarissen.
11	Autorisaties: aanwijzen functionaris-sen	Art 6 lid 7	Er is een actuele lijst van, door de verwerkings-verantwoordelijke aangewezen, bevoegde functionarissen.	De verwerkingsverantwoordelijke wijst een Bevoegde Functionaris (BF) aan, zoals bedoeld in artikel 9, derde lid, 11, eerste en vierde lid, en 13, derde lid. Het verdere gebruik van de in deze artikelen genoemde verwerkingen is gekoppeld aan instemming van de BF. Deze instemming dient te worden vastgelegd.	• Stel vast of op basis van artikel 9 politiegegevens worden verwerkt. Indien dat niet het geval is, is deze beheersingsmaatregel niet van toepassing. Indien dit wel het geval is: ○ Inspecteer de lijst van bevoegde functionarissen, hun functie- of rolbeschrijving. ○ Stel vast dat voor verwerkingen zoals bedoeld in artikel 9, derde lid, 11, eerste en vierde lid, en 13, derde lid instemming is gegeven door de BF en dat deze instemming is vastgelegd. ○ Stel vast of conform de opzet wordt gewerkt. ○ Interview de verantwoordelijke functionarissen.
12	Onderscheid tussen verschillende categorieën van betrokkenen	Art 6b	De verwerkingsverantwoordelijke heeft geborgd dat, voor zover mogelijk, duidelijk onderscheid wordt gemaakt in de verschillende categorieën van betrokkenen.	De meest voorkomende categorieën van betrokkenen zijn: • verdachten • slachtoffers (benadeelden) • derden (zoals getuigen of deskundigen)	• Inspecteer het verwerkingsregister en eventueel aanvullende documentatie zoals het privacybeleid. • Stel vast dat in de gebruikte informatiesystemen onderscheid wordt gemaakt in de verschillende categorieën van betrokkenen.

Bijlage 3 - Guidance bij de te onderzoeken Wpg beheersingsmaatregelen					
#	Onderwerp	Verwijzing	Beheersingsmaatregelen	Nadere toelichting	Voorgestelde testaanpak
				Dit betreft echter geen absoluut onderscheid omdat een verdachte gedurende het opsporingsonderzoek tot getuige kan transformeren en andersom. Doorgaans zal een dergelijke verandering onverwijld in de systemen worden verwerkt.	• Stel vast dat, in voorkomend geval, de verandering van categorie in de systemen is verwerkt. • Interview de verantwoordelijke functionarissen.

13	Verwerker en Verwerkers-overeen-komst	Art 6c	De verwerker stelt de verwerkingsverantwoordelijke alle informatie ter beschikking heeft die nodig is om aantoonbaar te maken dat de verplichtingen in de verwerkersovereenkomst en de Wpg worden nageleefd en die nodig is om audits mogelijk te maken.
			
			De verwerking door een verwerker vindt alleen plaats als een verwerkingsverantwoordelijke afdoende garanties heeft over de toereikendheid van de geïmplementeerde technische en organisatorische maatregelen.
			
			Bij elke uitvoering van een gegevensverwerking door een verwerker zijn de taken en afspraken schriftelijk vastgesteld en vastgelegd in een (toereikende) overeenkomst of andere rechtshandeling.
			
			Er zijn afspraken vastgesteld en vastgelegd m.b.t. de
				Kenmerkend verschil met de AVG is de verplichte vastlegging in de verwerkersovereenkomst van afspraken m.b.t. de handelswijze bij een inbreuk op de beveiliging zie ook art. 33a (control # 30).	• Inspecteer de contracten en verwerkersovereenkomsten met de relevante verwerkers.
					• Inspecteer de contracten en verwerkersovereenkomsten met de relevante verwerkers. Stel vast dat hierin is opgenomen dat:
					  ○ de verwerker inbreuken op de beveiliging moet melden aan de verwerkingsverantwoordelijke;
					  ○ door de verwerker afdoende garanties worden verstrekt over de toereikendheid van de geïmplementeerde technische en organisatorische maatregelen;
					  ○ een andere partij alleen wordt ingeschakeld bij de uitvoering van de verwerking met toestemming van de verwerkingsverantwoordelijke;
					  ○ indien dit het geval is de afspraken back-to-back worden doorgeleid;
					  ○ de verwerker de verwerkingsverantwoordelijke alle informatie ter beschikking stelt die nodig is om aantoonbaar te maken dat aan de verplichtingen in de verwerkersovereenkomst worden nageleefd.

Bijlage 3 - Guidance bij de te onderzoeken Wpg beheersingsmaatregelen					
#	Onderwerp	Verwijzing	Beheersingsmaatregelen	Nadere toelichting	Voorgestelde testaanpak
			handelswijze bij een inbreuk op de beveiliging. Een andere partij is alleen ingeschakeld bij de uitvoering van de verwerking met toestemming van de verwerkingsverantwoordelijke. Aan deze andere verwerker (subverwerker) is bij een overeenkomst dezelfde verplichtingen inzake gegevensbescherming opgelegd.		• Stel vast of de contractuele eisen worden nageleefd door de verwerker (bijvoorbeeld door het overleggen van een Wpg assurance-rapport t.a.v. de gebruikte informatiesystemen). • Interview de verantwoordelijke functionarissen.
14	Geheim-houdings-plicht	Art 7	Er is geborgd dat de boa of een andere persoon aan wie politiegegevens ter beschikking zijn gesteld formeel bekend is met de plicht tot geheimhouding en de consequenties bij schending van deze plicht.	M.u.v. een bij of krachtens de wet gegeven voorschrift tot verstrekking, is de BOA of de persoon aan wie politiegegevens ter beschikking zijn gesteld verplicht tot geheimhouding daarvan. De formele bekendmaking van deze verplichting vindt op verschillende momenten plaats: het screeningsproces, de aanstellingsprocedure en het afleggen van de eed, belofte of verklaring. Als gegevens verstrekt worden, reist de geheimhoudingsplicht mee. Ze vallen na verstrekking onder de AVG, de ontvanger mag de gegevens alleen verwerken voor het doel waarvoor hij ze verkregen heeft en verder is nog steeds de geheimhoudingsplicht van kracht.	• Controleer of in de aanstellingsprocedure is vastgelegd: ○ afleggen eed, screeningsproces en eisen voor niet-politieambtenaren & tijdelijke functionarissen. • Inspecteer de checklist voor nieuwe medewerkers. • Controleer of nieuwe medewerkers verplicht een bewustwordingscursus moeten volgen. • Controleer of er binnen de organisatie aandacht is voor bewustwording m.b.t. privacy en meer specifiek op geheimhouding t.a.v. politiegegevens. • Inspecteer de disciplinaire procedures en/of arbeidsovereenkomst(en). • Stel vast of conform de opzet wordt gewerkt. • Interview de verantwoordelijke functionarissen.
15	Geauto-matiseerde individuele	Art 7a	Besluiten die uitsluitend zijn gebaseerd op geautomatiseerde verwerking die voor de	De Wpg voorziet in een verbod op uitsluitend op geautomatiseerde verwerking gebaseerde besluiten, met inbegrip van profilering, die voor	• Stel vast of er sprake is van besluiten die uitsluitend zijn gebaseerd op geautomatiseerde verwerking. Indien dit

Bijlage 3 - Guidance bij de te onderzoeken Wpg beheersingsmaatregelen					
#	Onderwerp	Verwijzing	Beheersingsmaatregelen	Nadere toelichting	Voorgestelde testaanpak
	besluit-vorming		betrokkene nadelige rechtsgevolgen (kunnen) hebben of hem in aanmerkelijke mate treft, worden niet genomen tenzij voorzien is in de voorwaarden genoemd in de wet. Het verbod op het gebruik van profilering dat leidt tot discriminatie van personen op grond van de bijzondere categorieën van politiegegevens (art 5) is bekend binnen de organisatie. Dit beperkte verbod op profilering is onderwerp van de bewustwordingssessies binnen de organisatie.	de betrokkene nadelige rechtsgevolgen hebben of hem in aanmerkelijke mate treffen. Dit verbod geldt echter niet als het betrokken besluit is toegestaan op grond van het recht van de lidstaten en het besluit voorziet in passende waarborgen voor de rechten en vrijheden van de betrokkene, waaronder ten minste het recht op menselijke tussenkomst van de verwerkingsverantwoordelijke.	tijdens de controleperiode niet het geval is geweest, kan hier 'non-occurrence' t.a.v. bestaan en werking worden vermeld. • Stel vast dat het verbod op het gebruik van profilering die leidt tot discriminatie van personen op grond van de bijzondere categorieën van politiegegevens (art 5) onderdeel uitmaakt van de bewustwordingssessies binnen de organisatie. • Interview de verantwoordelijke functionarissen.
16	Uitvoering van de dagelijkse opsporings-taak	Art 8 lid 1 en 2	Geborgd is dat art 8 politiegegevens één jaar na de datum van de eerste verwerking zodanig worden opgeslagen (achter een schot worden geplaatst) dat ze alleen nog beschikbaar komen voor verdere verwerking op basis van de vergelijking van gegevens (hit-no-hit basis). Geborgd is voor zover dat noodzakelijk is met het oog op de uitvoering van de dagelijkse politietaak politiegegevens ten aanzien waarvan in art 8 lid 1 genoemde termijn is verstreken geautomatiseerd worden	Persoonsgegevens die verwerkt worden in het kader van de dagelijkse opsporingstaak, vallen onder artikel 8 van de Wpg. Dit gaat over zaken als wildplassen, foutief aanbieden van afval, alcohol gebruiken op de openbare weg en loslopende honden. Ook proces-verbaal opmaken bij onrechtmatig afgeschoten wild of tuinafvaldump valt hieronder. Artikel 8-gegevens mogen tot vijf jaar na de eerste verwerkingsdatum met een gerichte zoekvraag worden geraadpleegd en verwerkt. Bijvoorbeeld door te zoeken op een naam, adres of kenteken. Daarna worden ze vijf jaar bewaard (bewaartermijn) en daarna dienen ze te worden vernietigd.	• Inspecteer de systeembeschrijving en/of handleidingen. • Inspecteer de application controls die zorgdragen voor het 'achter schot plaatsen'. • Stel vast dat gegevens maximaal 5 jaar na eerste datum van verwerking met een gerichte zoekvraag kunnen worden geraadpleegd en verwerkt. • Stel vast of conform de opzet wordt gewerkt. • Interview de verantwoordelijke functionarissen.

Bijlage 3 - Guidance bij de te onderzoeken Wpg beheersingsmaatregelen					
#	Onderwerp	Verwijzing	Beheersingsmaatregelen	Nadere toelichting	Voorgestelde testaanpak
			vergeleken met politiegegevens die worden verwerkt op grond van art 8 lid 1 teneinde vast te stellen of verbanden bestaan tussen de betreffende gegevens. De gerelateerde gegevens kunnen verder worden verwerkt met het oog op de uitvoering van de dagelijkse politietaak.		
17	Ter beschikking stellen van politie-gegevens binnen het Wpg-domein	Art 4 lid 1 Art 8 lid 4 Art 9 lid 3 Art 15 lid 1 en 2 Art 15a lid 1 en 2	Geborgd is dat de verdere verwerking van art 9 gegevens alleen plaats vindt na toestemming (aantoonbaar) van de daartoe bevoegde functionaris. Geborgd is dat de ter beschikking stellen van politiegegevens aan bevoegde autoriteiten in andere lidstaten van de Europese Unie of aan organen en instanties belast met de taken, bedoeld in art 1, onderdeel a conform de richtlijnen gesteld in de wet plaatsvindt.	Ter beschikking stellen betreft het delen van politiegegevens binnen het Wpg-domein. Dit is beschreven in artikel 15 van de Wpg. Uitgangspunt is dat politiegegevens onder voorwaarden kunnen worden gedeeld met eenieder die de gegevens nodig heeft voor zijn de uitoefening van zijn (opsporings)taak. De strekking van de wet is dat het breed delen van gegevens de kwaliteit van het werk verbetert. Je weet dan bijvoorbeeld wie bezig is op hetzelfde terrein en welke antecedenten iemand heeft. Het Bpg (art. 2:13) beschrijft in welke gevallen het ter beschikking stellen geweigerd kan worden. Bijvoorbeeld als er gevaar voor leven of gezondheid van betrokkene is te duchten. De meeste weigeringsgronden zullen voor de boa niet spelen, bijvoorbeeld als het gaat om gegevens over politie-informanten of gegevens verwerkt onder artikel 10 Wpg (dit artikel is in het Bpg boa niet van toepassing verklaard).	• Stel vast of er een procedure of beleidsstuk is op grond waarvan politiegegevens ter beschikking worden gesteld binnen het Wpg-domein. • Inspecteer de vastlegging van de instemming door de daartoe bevoegde functionaris. • Stel vast of conform de opzet wordt gewerkt. • Interview de verantwoordelijke functionarissen.

Bijlage 3 - Guidance bij de te onderzoeken Wpg beheersingsmaatregelen					
#	Onderwerp	Verwijzing	Beheersingsmaatregelen	Nadere toelichting	Voorgestelde testaanpak
				Relevant is dat een andere boa of politie contact opneemt over een mutatie en dat de boa bijvoorbeeld eerst nog een getuigenverhoor of zoeking moet verrichten voordat gegevens door een ander gebruikt kunnen worden. Dit is geen weigering van ter beschikking stellen maar eerder het onderling afstemmen welke gegevens wanneer door wie gebruikt kunnen worden.	
18	Geautomati-seerd vergelijken en in combinatie zoeken	Art 11 lid 1, 3, 4 en 5 Art 8 lid 3 Art 2:1 en 2:2 lid 1 Bpg	Geborgd is dat gegevens alleen geautomatiseerd worden vergeleken met andere politiegegevens of met andere dan politiegegevens binnen de richtlijnen gesteld in art 11. Geborgd is dat gegevens alleen in combinatie met elkaar worden verwerkt binnen de richtlijnen gesteld in art 11 lid 4. Geborgd is dat het in combinatie verwerken van art 8 politiegegevens beperkt is tot de boa's die daarvoor geautoriseerd zijn. Geborgd is dat de ambtenaren die geautomatiseerd vergelijken en ambtenaren die in combinatie zoeken over voldoende kennis en vaardigheden beschikken.	Politiegegevens kunnen worden vergeleken met andere politiegegevens teneinde vast te stellen of verbanden bestaan tussen de betreffende gegevens. De verwerkingsmogelijkheden geautomatiseerd vergelijken en in combinatie zoeken zijn gebonden aan strikte criteria. Dit blijkt uit de vereisten 'in bijzondere gevallen' en 'in opdracht van'. De Wpg kent (limitatief) twee verschillende vormen van doorzoeken van politiegegevens: geautomatiseerd vergelijken (art 8 lid 2, 11 lid 1, 11 lid 2 en 12 lid 4 Wpg) en in combinatie verwerken (art 8 lid 3 en 11 lid 4). De wet geeft geen technische omschrijving van het verschil tussen geautomatiseerd vergelijken en gecombineerd verwerken. Op basis van de abstractere omschrijvingen gaan wij uit van de volgende definities: Geautomatiseerd vergelijken: het met een binaire zoeksleutel van (een) trefwoord(en) zoeken van bepaalde politiegegevens. Het resultaat van deze gerichte zoekslag is een uitkomst van hit/no hit. Gecombineerd verwerken: zonder binaire zoeksleutel binnen (een selectie van)	• Stel vast of tijdens de controleperiode sprake is geweest van geautomatiseerd vergelijken en in combinatie zoeken. Indien dit niet het geval is kan hier 'non-occurrence' t.a.v. bestaan en werking worden vermeld.. Indien dit wel het geval is: ○ Inspecteer de relevante gegevensverwerkingen en beoordeel testgevallen met betrekking tot vergelijkingen. ○ Interview de verantwoordelijke functionarissen.

Bijlage 3 - Guidance bij de te onderzoeken Wpg beheersingsmaatregelen					
#	Onderwerp	Verwijzing	Beheersingsmaatregelen	Nadere toelichting	Voorgestelde testaanpak
				beschikbare politiegegevens zoeken naar verbanden. Het resultaat van deze vrije zoekslag is een verzameling van gegevens die voldoen aan bepaalde gemeenschappelijke kenmerken. Deze gemeenschappelijke kenmerken kunnen een profiel van indicatoren of bepaalde kenmerken (trefwoorden) inhouden.	
19	Onder-steunende taken	Art 13	Geborgd is dat voor de verwerkingen bedoeld in art 13 lid 1 t/m 3, van tevoren is voldaan aan de schriftelijke vereisten (art 13 lid 4).	Dit artikel biedt de mogelijkheid om gegevens die oorspronkelijk zijn verwerkt op basis van artikel 8 of 9, vaak landelijk, verder te verwerken. De verwerkingsverantwoordelijke kan zelf een artikel 13- verwerking starten, nadat een bijbehorend artikel 13-protocol is opgesteld. De gegevens die onder artikel 13 verwerkt worden, komen voort uit artikel 8- of 9-verwerkingen. Bepaalde gegevens kunnen tegelijkertijd onder artikel 13 als onder 8 of 9 verwerkt worden. Vooralsnog zijn er geen artikel 13-verwerkingen voor boa's bekend. Aangezien de behoefte wel bestaat, is de verwachting dat dit slechts een kwestie van tijd is. Het zou bijvoorbeeld kunnen gaan om het bieden van raadpleegmogelijkheden voor alle opsporingsambtenaren in Nederland van processen-verbaal, boetes, overtredingen van gebiedsverboden of gevarenclassificaties (welke burger is wapen dragend of heeft een gevaarlijke hond?).	• Stel vast of tijdens de controleperiode artikel 13-verwerkingen zijn geweest. Indien dit niet het geval is, kan hier 'non-occurrence' t.a.v. bestaan en werking worden vermeld. Indien dit wel het geval is: ○ Controleer of een overzicht beschikbaar is van art 13-verwerkingen (en wie de verwerkingsverantwoordelijke is). ○ Controleer of vastgesteld is hoe art 8 en 9 politiegegevens ter beschikking worden gesteld aan de verschillende art 13-verwerkingen (selectie, eisen aan invoer, invoeren in art 13 verwerking of beschikbaar stellen aan betreffende verwerkingsverantwoordelijke t.b.v. invoer). ○ Controleer of is vastgelegd wie geautoriseerd is voor het verwerken van art 13.1 onderdeel e, 13.2 en 13.3. ○ Controleer of voor verwerkingen bedoeld in artikel 13, eerste, tweede en derde lid, van de wet, tevoren de gegevens zoals gespecificeerd in de wet (doel, categorieën van personen,

Bijlage 3 - Guidance bij de te onderzoeken Wpg beheersingsmaatregelen					
#	Onderwerp	Verwijzing	Beheersingsmaatregelen	Nadere toelichting	Voorgestelde testaanpak
					categorieën van persoonsgegevens, controle frequentie beëindiging van de verwerking, de verwerkingsverantwoordelijke, de verwerker) zijn vastgelegd. ○ Controleer de art 13 verwerking: (geldige rechtsgrond, categorieën personen / persoonsgegevens conform protocol, zijn de geautomatiseerde of handmatige controles geïmplementeerd om termijnen te borgen, verantwoordelijkheden belegd, toegang conform het Bpg en protocol). ○ Controleer of de gegevens ter voldoening van de verplichting tot beëindiging van de verwerking conform de vastgelegde frequentie (aantoonbaar) worden gecontroleerd. ○ Interview de verantwoordelijke functionarissen.
20	Bewaar-termijnen, verwijderen en vernietigen	Art 4 lid 2 Art 8 lid 6 Art 9 lid 4 Art 14	Politiegegevens worden niet langer bewaard dan de minimale tijd die nodig is, zoals vereist door de toepasselijke wet- en regelgeving, of voor de doeleinden waarvoor deze zijn verwerkt. De verwerkingsverantwoordelijke voorziet in voldoende waarborgen om te	De Wpg bevat diverse bepalingen die beschrijven welke typen gegevens hoe lang verwerkt en vervolgens bewaard mogen worden. Voor de verschillende artikel 8-, 9- en 13-verwerkingen gelden verschillende termijnen.	• Controleer of inzichtelijk is waar en hoe gegevens zijn opgeslagen (systemen, archieven, back-ups, overige media). • Stel vast dat de geautomatiseerde controlemaatregelen in het systeem of de handmatige maatregelen om het systeem heen bestaan en werken: ○ Vastlegging datum eerste verwerking art 8 gegevens; ○ Maatregel verwijdering art 8

Bijlage 3 - Guidance bij de te onderzoeken Wpg beheersingsmaatregelen					
#	Onderwerp	Verwijzing	Beheersingsmaatregelen	Nadere toelichting	Voorgestelde testaanpak
			bewerkstelligen dat de gegevens conform de wet worden gecontroleerd, verwijderd en vernietigd. Geborgd is dat Politiegegevens na verwijdering maximaal vijf jaar worden bewaard. Indien van cultureel of historisch belang kan worden afgezien van vernietiging van de gegevens. Er wordt dan aan de bewaareisen als genoemd in de Archiefwet voldaan.		gegevens vijf jaar na datum eerste verwerking ○ Vastlegging begin half jaar termijn voor analyse art 9 gegevens gebruik voor nieuw onderzoek; ○ Maatregel(en) voor verwijdering art 9 gegevens na verstrekking half jaar termijn; • Interview de verantwoordelijke functionarissen.
21	Verstrekking van politie-gegevens aan anderen dan politie en Koninklijke mare-chaussee	Art 16 Art 18 Art 19 Art 21 Art 22 Art 7 lid 1 Art 4	Geborgd is dat politiegegevens alleen worden verstrekt aan personen of instanties buiten het politiedomein, voor zover dit noodzakelijk is voor de doeleinden zoals deze in de Wet politiegegevens en het Besluit politiegegevens zijn genoemd. Geborgd is dat wanneer gegevens verstrekt worden er wordt voldaan aan de documentatieplicht (conform 6 lid 4 Bpg). Geborgd is dat verstrekking alleen plaatsvindt in overeenstemming met het bevoegd gezag indien dit vereist is in de wet.	Het gaat hier om het delen van politiegegevens buiten het Wpg-domein, bijvoorbeeld Bureau Halt, de burgemeester, Belastingdienst of het Centraal Justitieel Incassobureau. Ook in een samenwerkingsverband kan, onder voorwaarden, verstrekt worden aan partners, zoals een woningbouwvereniging of winkeliers. Voor verstrekkingen wordt gebruik gemaakt van de zogenaamde 'verstrekkingenwijzer'.	• Controleer of er een werkinstructie / verstrekkingenwijzer is voor verstrekkingen met aandacht voor o.a.: borging rechtmatige verstrekking, taken & verantwoordelijkheden, advies functie PF of BF, beperkingen bij het verstrekken (art 4:5 Bpg), weigeringsgronden & vastlegging, verificatie verzoeker, beveiliging, toezicht op verstrekkingen. • Controleer of maatregelen zijn geïmplementeerd om de beveiliging van de politiegegevens tijdens verstrekking te borgen. • Controleer of er een werkinstructie is voor de documentatieplicht bij verstrekkingen. • Trek o.b.v. een overzicht van verstrekkingen een steekproef en controleer de verstrekkingen (ook voor 22.2 en 22.3) (rechtmatigheid, documentatieplicht, verificatie ontvanger, wijzen op

Bijlage 3 - Guidance bij de te onderzoeken Wpg beheersingsmaatregelen					
#	Onderwerp	Verwijzing	Beheersingsmaatregelen	Nadere toelichting	Voorgestelde testaanpak
			Bij verstrekkingen is geborgd dat de ontvangende partij wordt gewezen op zijn geheimhoudingsplicht. De juistheid, volledigheid, actualiteit en betrouwbaarheid van politiegegevens bij verstrekking wordt, voor zover mogelijk, gecontroleerd en inzichtelijk gemaakt voor de ontvangende partij. Er is een procedure voor het onverwijld in kennis stellen van de ontvanger van politiegegevens indien geconstateerd wordt dat onjuiste politiegegevens zijn verstrekt of dat politiegegevens op onrechtmatig wijze zijn verstrekt.		geheimhoudingsplicht, vereiste toestemming) • Controleer of controle/ toezicht plaats vindt op de verstrekkingen. • Controleer of/ hoe de ontvangende partij op de geheimhoudingsplicht gewezen wordt (bij verstrekking op grond van art 19 en 20). • Stel vast of er conform opzet wordt gewerkt. • Interview de verantwoordelijke functionarissen.
22	Doorgiften aan derde landen	Art 17a	De doorgifte van gegevens aan verwerkingsverantwoordelijke in derde landen vindt alleen plaats indien er een adequaatsheidsbesluit is van de Commissie van de Europese Unie of indien één van de uitzonderingsgronden zoals genoemd in de wet van toepassing is.	Derde landen zijn alle landen buiten de EU, met uitzondering van de landen in de Europese Economische Ruimte (EER). Dit zijn Noorwegen, Liechtenstein en IJsland. Als sprake is van doorgifte aan de Verenigde Staten, dient in het bijzonder aandacht te worden besteed aan de 'Schrems-II' uitspraak van het Hof van Justitie van de Europese Unie[7].	• Stel vast of tijdens de controleperiode politiegegevens zijn verstrekt aan derde landen. Indien dit niet het geval is kan hier 'non-occurrence' t.a.v..opzet, bestaan en werking worden vermeld. Indien dit wel het geval is: ○ stel op basis van een steekproef vast of aan de gestelde eisen is voldaan. ○ Interview de verantwoordelijke functionarissen.

[7] Op 16 juli 2020 heeft het Hof van Justitie EU in reactie op de vragen van de Ierse rechter het Privacy Shield ongeldig verklaard. Dit is met onmiddellijke ingang van kracht. Organisaties in de EU kunnen geen persoonsgegevens aan de Verenigde Staten meer doorgeven op grond van het Privacy Shield.

Bijlage 3 - Guidance bij de te onderzoeken Wpg beheersingsmaatregelen					
#	Onderwerp	Verwijzing	Beheersingsmaatregelen	Nadere toelichting	Voorgestelde testaanpak
			De doorgifte van gegevens aan derde landen wordt vastgelegd (documentatieplicht). Indien doorgifte plaatsvindt op basis van art 17a lid 2 onderdeel a of b, lid 3 of lid 5 is (aantoonbaar) voldaan aan de gestelde eisen in de wet. Indien politiegegevens van een andere lidstaat afkomstig worden doorgegeven aan derde landen is de toestemming van de verantwoordelijke autoriteit van deze lidstaat beschikbaar.		
23	Verstrekking aan derden structureel voor samen-werkings-verbanden	Art 20	De verwerkingsverantwoordelijke heeft inzicht in de samenwerkingsverbanden waarbij politiegegevens worden verstrekt. In de beslissing voor het verstrekken van politiegegevens t.b.v. een samenwerkingsverband wordt vastgelegd: • Ten behoeve van welk zwaarwegend algemeen belang de verstrekking noodzakelijk is, • Ten behoeve van welk samenwerkingsverband de politiegegevens worden verstrekt,	Jaarlijks wordt door de verwerkingsverantwoordelijke een verslag opgesteld voor het periodieke overleg tussen de verwerkingsverantwoordelijke en het bevoegde gezag met een overzicht van de art. 20 besluiten en samenwerkingsverbanden, en het binnen dat kader gedane verstrekkingen.	• Inspecteer het overzicht van de samenwerkingsverbanden waarbij politiegegevens worden verstrekt; • Stel vast dat vast dat voor elk samenwerkingsverband een convenant aanwezig is; • Stel vast of tijdens de controleperiode structureel politiegegevens zijn verstrekt aan (één of meer) samenwerkingsverbanden. Indien hiervan tijdens de controleperiode geen sprake is kan hier 'non-occurrence' t.a.v. bestaan en werking worden vermeld. Indien dit wel het geval is: • Stel op basis van een steekproef vast dat de volgende zaken zijn vastgelegd: o ten behoeve van welk zwaarwegend algemeen belang de verstrekking noodzakelijk is;

Bijlage 3 - Guidance bij de te onderzoeken Wpg beheersingsmaatregelen					
#	Onderwerp	Verwijzing	Beheersingsmaatregelen	Nadere toelichting	Voorgestelde testaanpak
			• Het doel waartoe dit is opgericht, • Welke gegevens worden verstrekt, • De voorwaarden onder welke de gegevens worden verstrekt en • Aan welke personen of instanties de gegevens worden verstrekt. • De daadwerkelijke verstrekking van gegevens wordt vastgelegd.		○ ten behoeve van welk samenwerkingsverband de politiegegevens worden verstrekt; ○ het doel waartoe het samenwerkingsverband is opgericht: voor de boa zal dit altijd het voorkomen en opsporen van strafbare feiten moeten zijn; ○ welke typen gegevens worden verstrekt; ○ de voorwaarden waaronder de gegevens worden verstrekt; ○ aan welke personen en instanties de gegevens worden verstrekt; ○ met welke Officier van Justitie (bevoegd gezag) overeenstemming is bereikt over deze samenwerking en verstrekking. • Interview de verantwoordelijke functionarissen.
24	Recht-streekse verstrekking	Art 23	De organisatie heeft geborgd dat rechtstreekse verstrekking uitsluitend plaatsvindt voor zover noodzakelijk op grond van art 23 en alleen voor zover voldaan kan worden aan de beveiligingseisen. De rechtstreekse verstrekking op basis van art 23 lid 2 vindt alleen plaats aan de aangewezen personen.	Ingevolge art 23 kunnen politiegegevens rechtstreeks worden verstrekt aan de leden van het Openbaar Ministerie met het oog op strafvorderlijke beslissingen omtrent opsporing en vervolging en de hulp aan slachtoffers van strafbare feiten of bij algemene maatregel van bestuur aan te wijzen beslissingen. Rechtstreekse verstrekkingen zoals hier bedoeld is het aan een derde langs geautomatiseerde weg, niet zijnde niet telefoon, fax of mail inzage geven in politiegegevens. Hierbij kan men	• Stel vast of rechtstreekse verstrekkingen plaatsvinden op grond van art 23. • Indien dit het geval is, stel vast dat de verwerkingsverantwoordelijke passende technische en organisatorische maatregelen heeft getroffen. • Interview de verantwoordelijke functionarissen.

Bijlage 3 - Guidance bij de te onderzoeken Wpg beheersingsmaatregelen					
#	Onderwerp	Verwijzing	Beheersingsmaatregelen	Nadere toelichting	Voorgestelde testaanpak
				denken aan het koppelen van informatiesystemen met het OM en Slachtofferhulp.	
25	Informatie aan de betrokkene, recht op inzage, rectificatie en verwijdering.	Art 24a lid 1 t/m 4 Art 24b Art 25 Art 26 Art 27 Art 28	De verwerkingsverantwoordelijke biedt de betrokkene informatie over de verwerking van persoonsgegevens en doet dit beknopt, toegankelijk en duidelijk, zodat de betrokkene zijn rechten kan uitoefenen. De informatievoorziening voldoet aan de eisen gesteld in art 24b lid 1 en 2. Bij uitstel, beperking of achterwege laten van de verstrekking van informatie bedoeld in 24b lid 2 is de uitstel, beperking of achterwege laten alsmede de duur van deze maatregel onderbouwd. Verzoeken tot inzage, rectificatie, vernietiging van betrokkenen worden - met inachtneming van het gestelde in artikel 27 - tijdig en adequaat afgehandeld. De organisatie borgt dat bij een verzoek tot inzage (art 25 lid 1) of rectificatie (art 28 lid 1) dat de betrokkene zonder onnodige vertraging in kennis wordt gesteld van de ontvangst van het	De Wpg bevat verschillende richtlijnen m.b.t. de plichten van de verwerkingsverantwoordelijke en de rechten van betrokkene. In artikel 27 zijn verschillende uitzonderingen genoemd t.a.v. de rechten van betrokkene. In zijn algemeenheid geldt dat de verwerkingsverantwoordelijke gehouden is aan de betrokkene informatie over de verwerking van politiegegevens te verstrekken in een beknopte, heldere en gemakkelijk toegankelijke vorm en in duidelijke en heldere taal. Deze verplichting is in het bijzonder van toepassing bij de verwerking van politiegegevens in het kader van geautomatiseerde besluitvorming, bij het inzagerecht en beperkingen daarop, bij het recht op rectificatie en vernietiging van gegevens en beperkingen daarop, bij de uitoefening van rechten door de betrokkene en controle door de toezichthouder, bij de rechten van de betrokkene bij de strafrechtelijke onderzoeken en procedures, en bij een mededeling van een inbreuk in verband met persoonsgegevens aan een betrokkene.	• Controleer de procesbeschrijving/ werkinstructie waarmee invulling wordt gegeven aan de informatieplicht aan de betrokkene en de uitzonderingen hierop. • Controleer of uitvoering wordt gegeven aan de informatieplicht aan de betrokkene en uitzonderingen hierop. • Controleer of er een procedure/ werkinstructie is over de rechten van de betrokkenen (behandelen van verzoeken, taken/verantwoordelijkheden, borgen tijdigheid). • Controleer of de verwerkingsverantwoordelijke een dossier bijhoudt van de verzoeken, ontvangstbevestigingen, verificatie identiteit, besluit over verzoek, schriftelijke mededeling of afwijking aan betrokkene, controle op uitvoering rectificatie/ verwijdering (indien van toepassing). • Verkrijg inzage in het dossier met verzoeken. • Stel, op basis van een steekproef, vast of het proces conform de procesbeschrijving wordt uitgevoerd (met inachtneming van het bepaalde in art 25-28 (inclusief verificatie van de identiteit). • Stel vast dat afwijzingen van een inzage, rectificatie of verwijderverzoek altijd schriftelijk plaatsvinden en alleen voor zover dit een noodzakelijke en evenredige

Bijlage 3 - Guidance bij de te onderzoeken Wpg beheersingsmaatregelen					
#	**Onderwerp**	**Verwijzing**	**Beheersingsmaatregelen**	**Nadere toelichting**	**Voorgestelde testaanpak**
			verzoek, de termijn voor uitsluitsel en de mogelijkheid een klacht in te dienen bij de AP. Een weigering gevolg te geven aan het verzoek conform art 24a lid 4 is onderbouwd. Elke weigering of beperking van de inzage wordt aan de betrokkene toegelicht, met vermelding van de feitelijke of juridische gronden die aan het besluit ten grondslag liggen.		maatregel is zoals gesteld in art 27.1 onderdelen a t/m f. • Interview de verantwoordelijke functionarissen.
26	Register	Art 31d lid 1 en 2	De verwerkingsverantwoordelijke houdt een register bij dat de volgende gegevens bevat: a) de naam en de contactgegevens van de verwerkings-verantwoordelijke, de gezamenlijk verwerkings-verantwoordelijken en de functionaris voor gegevensbescherming; b) de doelen van de verwerking; c) de categorieën van ontvangers aan wie politiegegevens zijn of zullen worden verstrekt, met inbegrip van ontvangers in derde landen of internationale organisaties; d) een beschrijving van de categorieën van betrokkenen	De Wpg beschrijft, naast de gegevens die in art 30 AVG zijn opgesomd, een aantal aanvullende gegevens. Deze zijn in de kolom 'beheersingsmaatregelen' **vet** gedrukt.	• Controleer of een verwerkingsregister aanwezig is en de beschrijving bevat van de verwerkingsactiviteiten aangegeven in lid 1a-j van artikel 31d. • Stel vast dat een proces bestaat dat zorgt voor het actueel houden van het register. • Stel vast dat het proces van aanmelden van nieuwe verwerkingen bekend is gesteld binnen de organisatie. • Neem een steekproef van verwerkingen en controleer of de vastlegging voldoet aan de eisen gesteld in de wet. • Interview de verantwoordelijke functionarissen.

Bijlage 3 - Guidance bij de te onderzoeken Wpg beheersingsmaatregelen					
#	Onderwerp	Verwijzing	Beheersingsmaatregelen	Nadere toelichting	Voorgestelde testaanpak
			en van de categorieën van persoonsgegevens; **e) in voorkomend geval, het gebruik van profilering;** f) in voorkomend geval, de categorieën van doorgiften van politiegegevens aan een derde land of een internationale organisatie; **g) een aanwijzing van de rechtsgrondslag van de verwerking, met inbegrip van doorgiften, waarvoor de politiegegevens bedoeld zijn;** h) zo mogelijk, de beoogde termijnen waarbinnen de verschillende categorieën van gegevens worden verwijderd of vernietigd; i) zo mogelijk, een algemene beschrijving van de technische en organisatorische maatregelen ter beveiliging, bedoeld in artikel 4a; j) **de toekenning van de autorisaties, bedoeld in artikel 6.** De verwerker houdt een register bij dat de volgende gegevens bevat: a) de naam en de contactgegevens van de		

Bijlage 3 - Guidance bij de te onderzoeken Wpg beheersingsmaatregelen					
#	Onderwerp	Verwijzing	Beheersingsmaatregelen	Nadere toelichting	Voorgestelde testaanpak
			verwerker of verwerkers en van iedere verwerkings-verantwoordelijke ten behoeve van wie de verwerker handelt en, in voorkomend geval, van de functionaris voor gegevensbescherming; b) de categorieën van verwerkingen die namens iedere verwerkings-verantwoordelijke zijn uitgevoerd; c) indien van toepassing, doorgiften van politiegegevens aan een derde land of een internationale organisatie, onder vermelding van dat derde land of die internationale organisatie, indien door de verwerkings-verantwoordelijke uitdrukkelijk daartoe geïnstrueerd d) indien mogelijk, een algemene beschrijving van de technische en organisatorische maatregelen, bedoeld in artikel 4a.		
27	Documen-tatie	Art 32 lid 1 t/m 4	De verwerkingsverantwoordelijke borgt een volledige en toegankelijke schriftelijke vastlegging (documentatieplicht)	Een ander element als het gaat om het afleggen van verantwoording en het creëren van transparantie is de documentatieplicht.	• Controleer of er een procedure/werkinstructie(s) is voor de documentatieplicht. In de werkinstructie is o.a. vastgelegd: wijze van vastlegging,

Bijlage 3 - Guidance bij de te onderzoeken Wpg beheersingsmaatregelen					
#	Onderwerp	Verwijzing	Beheersingsmaatregelen	Nadere toelichting	Voorgestelde testaanpak

			van de onderdelen genoemd in art 32 lid 1. De bedoelde politiegegevens worden conform art 32 lid 4 bewaard.
			
			De verwerkingsverantwoordelijke borgt een volledige en toegankelijke schriftelijke vastlegging (documentatieplicht) van de doorgifte van politiegegevens aan een verwerkingsverantwoordelijke in een derde land of aan een internationale organisatie.
			
			De schriftelijke melding van een gemeenschappelijke verwerking van politiegegevens aan de AP is geborgd.
				Artikel 32 Wpg beschrijft vier gegevensverzamelingen waar de verwerkingsverantwoordelijke zorg voor moet dragen. Hij moet zorgen dat alle verstrekkingen worden vastgelegd, dat alle artikel 9- doeleinden worden vastgelegd, alle datalekken en alle weigeringen van inzageverzoeken.
				
				Hoe meer en hoe beter deze werkprocessen geautomatiseerd ondersteund worden (een 'vinkje' om aan te geven dat gegevens verstrekt zijn en aan wie), hoe eenvoudiger het is om aan de documentatieplicht te voldoen.
					volledigheid vastlegging, toegang tot documentatieplicht, gebruik/controle, melding aan AP van gemeenschappelijke verwerkingen, bewaartermijnen.
					• Controleer of de organisatie de juistheid en volledigheid van de documentatieplicht controleert.
					• Controleer of voldaan wordt aan de documentatieplicht voor de doelen van art 9 onderzoeken:
					  ○ doel onderzoek,
					  ○ omschrijving van het onderwerp waar het onderzoek op is gericht en
					  ○ deel politietaak waarop het onderzoek betrekking heeft.
					• Controleer of voldaan wordt aan de documentatieplicht voor de verstrekkingen.
					• Controleer of voldaan wordt aan de documentatieplicht van de feitelijke of juridische redenen die ten grondslag liggen aan een afwijzing, bedoeld in artikel 27, eerste lid (inzage, rectificatie, verwijder verzoek);
					• Controleer of voldaan is aan de documentatieplicht voor een inbreuk op de beveiliging van persoonsgegevens, bedoeld in artikel 33a, inclusief de feiten omtrent de inbreuk, de gevolgen ervan en de maatregelen die zijn getroffen ter correctie (zie ook melding datalekken);
					• Controleer of voldaan wordt aan de documentatieplicht doorgifte van politiegegevens aan een verwerkingsverantwoordelijke in een derde land of aan een internationale organisatie

Bijlage 3 - Guidance bij de te onderzoeken Wpg beheersingsmaatregelen					
#	Onderwerp	Verwijzing	Beheersingsmaatregelen	Nadere toelichting	Voorgestelde testaanpak
					(art 17a, tweede lid, onderdeel b, en derde lid): • Interview de verantwoordelijke functionarissen.
28	Logging	Art 32a	De verwerkingsverantwoordelijke en de verwerker dragen zorg voor de vastlegging langs elektronische weg (logging) van ten minste de volgende verwerkingen van politiegegevens in geautomatiseerde systemen: het verzamelen, wijzigen, raadplegen, verstrekken onder meer in de vorm van doorgiften, combineren of vernietigen van politiegegevens (32a lid1). De organisatie gebruikt de logging uitsluitend ter controle van de rechtmatigheid van de gegevensverwerkingen, voor interne controles, ter waarborging van de integriteit en de beveiliging van politiegegevens en voor strafrechtelijke procedures (32a lid 2).	In artikel 32a (logging) wordt logging van het verzamelen, wijzigen, raadplegen, verstrekken onder meer in de vorm van doorgiften, combineren of vernietigen van politiegegevens verplicht gesteld.	• Stel voor elk informatiesysteem waarin politiegegevens worden verwerkt, vast dat een logregel minimaal het verzamelen, wijzigen, raadplegen, verstrekken (onder meer in de vorm van doorgiften), combineren of vernietigen van politiegegevens bevat. • Stel vast dat logbestanden afdoende zijn beschermd tegen (ongeautoriseerde) wijzingen. • Stel vast dat logbestanden beschikbaar zijn over de afgelopen controleperiode. • Stel vast dat een intern controleproces is ingericht en geïmplementeerd om de logbestanden periodiek te beoordelen. • Stel vast dat periodiek (minimaal jaarlijks) een interne controle is uitgevoerd om vast te stellen dat logging plaatsvindt conform art. 32a lid 1 en dat de logging uitsluitend gebruikt wordt voor de doelen zoals beschreven in art. 32a lid 2. • Interview de verantwoordelijke functionarissen.
29	Audits	Art 33	Er wordt uitvoering gegeven aan de eisen zoals gesteld in de Regeling Periodieke Audit politiegegevens.	Elke vier jaar moet er een externe privacy audit voor alle Wpg verwerkingen te worden uitgevoerd. Deze audit dient te gebeuren conform de regels uit de Regeling periodieke audit politiegegevens.	• **Inspecteer de auditplanning (zowel intern als extern) voor de controleperiode 2021-2024 (TZM).** • **Inspecteer de relevante interne auditrapportage(s) (TZM).**

Bijlage 3 - Guidance bij de te onderzoeken Wpg beheersingsmaatregelen					
#	Onderwerp	Verwijzing	Beheersingsmaatregelen	Nadere toelichting	Voorgestelde testaanpak
				De audit heeft betrekking op de wijze waarop de verwerkingen georganiseerd zijn, de maatregelen en procedures die daarop van toepassing zijn en de werking van deze maatregelen en procedures. Mede ter voorbereiding op de privacy audit dient tenminste jaarlijks een interne audit plaats te vinden (art. 3 Regeling periodieke audit politiegegevens). Zowel aan de interne auditor als aan de audit worden (bekwaamheids)eisen gesteld.	• **Inspecteer de scope en resultaten van de jaarlijkse interne audits en stel vast of de interne audits voldoen aan de vereisten (TZM).** • **Stel vast of de interne auditor(en) voldoet/voldoen aan de bekwaamheidseisen(zie par. 2.5.2 van deze handreiking) (TZM).** • Interview de verantwoordelijke functionarissen.
30	Melding datalekken	Art 33a	De organisatie detecteert en behandelt privacy gerelateerde incidenten op gepaste wijze om de gevolgen te beperken en maatregelen te nemen om toekomstige inbreuken te voorkomen. De verantwoordelijkheden van de behandeling van datalekken zijn belegd in de organisatie, de daadwerkelijke uitvoering wordt beheerst, gedocumenteerd en geëvalueerd. De melding van een datalek aan de AP vindt tijdig en volledig plaats. Betrokkenen worden, indien vereist, tijdig en volledig in kennis gesteld van een inbreuk op de beveiliging als deze	De verwerkingsverantwoordelijke moet de AP zonder onnodige vertraging en waar mogelijk binnen 72 uur nadat hij er kennis van heeft genomen in kennis stellen van een inbreuk op de beveiliging. De melding is mondeling of schriftelijk. Deze verplichting is niet van toepassing als het niet waarschijnlijk is dat de inbreuk een risico voor de rechten en vrijheden van personen met zich meebrengt. Als de melding na 72 uur wordt gedaan wordt daarbij een motivering gegeven voor de vertraging.	• Beoordeel de procedure voor het melden van datalekken. • Stel vast dat er een registratie is van datalekken • Stel vast op basis van een steekproef dat datalekmeldingen tijdig worden gedaan. • Stel vast dat betrokkenen bij een datalek op de hoogte zijn gebracht. • Controleer of er, indien van toepassing, afspraken zijn gemaakt met verwerkers afspraken over het melden van inbreuken. • Controleer of n.a.v. datalekken corrigerende maatregelen zijn genomen en/of implementatie van te nemen maatregelen wordt bewaakt. • Interview de verantwoordelijke functionarissen.

Bijlage 3 - Guidance bij de te onderzoeken Wpg beheersingsmaatregelen					
#	Onderwerp	Verwijzing	Beheersingsmaatregelen	Nadere toelichting	Voorgestelde testaanpak
			inbreuk waarschijnlijk een hoog risico voor hun rechten en vrijheden betekent.		
31	Functionaris voor gegevens-bescherming	Art 36	Er is een functionaris voor gegevensbescherming aangesteld die toezicht houdt op: ○ het naleven van de Wpg; ○ het beleid van de verwerkings-verantwoordelijke met betrekking tot de bescherming van persoonsgegevens; ○ de toewijzing van de autorisaties, bedoeld in art 6; ○ de bewustmaking en opleiding van de boa's betrokken bij de verwerking van politiegegevens; ○ de audits; ○ de uitvoering van de DPIA's. De FG stelt jaarlijks een verslag op van zijn bevindingen en stelt het ter beschikking aan de verwerkingsverantwoordelijke. De functionaris voor gegevensbescherming is aangemeld bij de Autoriteit Persoonsgegevens en de contactgegevens van de FG zijn openbaar gemaakt.	Overheden zijn verplicht een FG aan te stellen en een grote organisatie als de politie heeft er meerdere. Ook de werkgever van de boa is verplicht een FG aan te stellen. Gezien de grote variatie aan boa-organisaties is het echter ook mogelijk om één overkoepelende FG aan te wijzen voor meerdere organisaties voor de verwerking van politiegegevens door boa's.	• **Stel vast dat de FG toezicht houdt op het naleven van de Wpg en dan specifiek:** ○ **de noodzakelijkheid, rechtmatigheid en doelbinding van de verwerkingen beschreven in artikel 3);** ○ **de juistheid en volledigheid van de politiegegevens bedoeld in artikel 4;** ○ **de verwerking van bijzondere persoonsgegevens (artikel 5)** ○ **het beleid van de verwerkingsverantwoordelijke met betrekking tot de bescherming van persoonsgegevens;** ○ **de toewijzing van de autorisaties, bedoeld in art 6;** ○ **de bewustmaking en opleiding van de boa's en andere functionarissen die betrokken zijn bij de verwerking van politiegegevens;** ○ **de audits (artikel 33);** ○ **de uitvoering van de DPIA's. (TZM)** • **Stel vast dat de FG tijdens de controleperiode 2021-2024 jaarlijks een verslag opstelt over de bevindingen m.b.t. de Wpg. (TZM)** • Stel vast of de FG is aangemeld bij de AP als FG voor de Wpg. • Interview de verantwoordelijke functionarissen.

Bijlage 4 - Guidance bij de te onderzoeken organisatorische en technische beheersingsmaatregelen

De Wpg stelt, evenals de AVG, dat de verwerkingsverantwoordelijke 'passende' technische en organisatorische maatregelen moeten treffen voor o.a. de beveiliging en het ontwerp van informatiesystemen.
Het is afhankelijk van de specifieke situatie wat passend zal zijn. Doorgaans zal dit worden bepaald aan de hand van een DPIA.
Ook de BIO zal, in het geval van overheidsinstellingen, in acht moeten worden genomen door de verwerkingsverantwoordelijke.
In deze bijlage geven wij de minimale set aan passende maatregelen die voor de beheersingsmaatregelen 6, 7, 10, 13 en 24 moeten worden getest.
Dit normenkader is eveneens van toepassing voor de leveranciers (serviceorganisaties).

Bijlage 4 – Guidance bij de te onderzoeken organisatorische en technische beheersingsmaatregelen				
#	Onderwerp	Beheersingsmaatregelen	Nadere toelichting	Testaanpak
1	Wijzigingenbeheer	Wijzigingenbeheer is procesmatig en procedureel zodanig uitgevoerd dat wijzigingen in de ICT-voorzieningen van webapplicaties tijdig, geautoriseerd en getest worden doorgevoerd. Doelstelling: Zeker stellen dat wijzigingen op een correcte en gecontroleerde wijze worden doorgevoerd waardoor de veilige werking van ICT-voorziening wordt gegarandeerd.	De focus ligt op het vaststellen dat het proces wijzigingsbeheer zodanig is opgezet en werkt dat alle wijzigingen altijd eerst worden getest voordat deze in productie worden genomen en via wijzigingsbeheer worden doorgevoerd. In sommige gevallen kunnen wijzigingen worden geïmplementeerd die beveiligingsrisico's introduceren. Ingeval van SAAS-toepassingen ligt de verantwoordelijkheid voor het testen van	• Inspecteer de wijzigingsprocedure en de inrichting van de Ontwikkel-, Test-, Acceptatie- en Productieomgeving (OTAP) omgeving. • Inspecteer, op basis van deelwaarneming voor elk type wijziging (applicatie, servers, netwerk), de gerelateerde documentatie. • Interview de verantwoordelijke functionarissen.

Bijlage 4 - Guidance bij de te onderzoeken organisatorische en technische beheersingsmaatregelen				
#	Onderwerp	Beheersingsmaatregelen	Nadere toelichting	Testaanpak
		Scope: Applicatie-, hosting (verwerker)- of Software as a Service (SaaS) leverancier van de Wpg-geclassificeerde verwerkende systemen.	wijzigingen aan de applicatie doorgaans bij de leverancier en/of gebruikersgroep. Aandachtspunten hierbij zijn: • Wijzigingsbeheer procedure, waarbij zo nodig onderscheid wordt gemaakt tussen wijzigingen op de applicatie, de servers en de netwerkcomponenten. • Functiescheiding tussen aanvragen, goedkeuren en doorvoeren van wijzigingen. • Het inrichten van een OTAP omgeving zodat wijzigingen eerst in een testomgeving worden getest voordat zij in productie kunnen worden genomen (n.b. voor netwerk wijzigingen is een testomgeving vaak niet mogelijk). • Het hanteren van een testscript en de vastlegging van de testresultaten. • Een formele acceptatie voor het in productie nemen van de wijziging. • Het beperken van het aantal personen die wijzigingen in productie kunnen nemen. • Bij het uitbrengen van een nieuwe release van de applicatie of een grote upgrade van	

Bijlage 4 – Guidance bij de te onderzoeken organisatorische en technische beheersingsmaatregelen				
#	**Onderwerp**	**Beheersingsmaatregelen**	**Nadere toelichting**	**Testaanpak**
			het onderliggende platform moet, bij voorkeur door middel van een penetratietest, worden onderzocht of er geen nieuwe kwetsbaarheden zijn geïntroduceerd.	
2	Logische toegangs-beveiliging	De inzet van identiteit- en toegangsmiddelen levert betrouwbare en effectieve mechanismen voor het vastleggen en vaststellen van de identiteit van gebruikers, het toekennen van de rechten aan gebruikers, het controleerbaar maken van het gebruik van deze middelen en het automatiseren van arbeidsintensieve taken. <u>Doelstelling:</u> Het efficiënter maken van het identiteit- en toegangsbeheer en zorgen dat functies en gegevens uitsluitend beschikbaar worden gesteld aan diegenen waarvoor deze bedoeld zijn als waarborg voor vertrouwelijkheid en integriteit. <u>Scope:</u> Hosting, leverancier van de Wpg-geclassificeerde verwerkende systemen.	De focus ligt op het vaststellen van maatregelen die de authenticiteit van de gebruiker borgt. *Note: Het verschil met beheersingsmaatregel 10 in bijlage 3 (Autorisaties en toegang tot politie-gegevens) is dat het hier gaat om de technische mogelijkheden voor logische toegangsbeveiliging en bij beheersingsmaatregel 10 in bijlage 3 om het daadwerkelijk correct autoriseren van medewerkers die toegang mogen hebben tot politiegegevens.* Aandachtspunten hierbij zijn: • Toekennen, controleren en intrekken van autorisaties. • Eisen aan wachtwoordinstellingen.	• Inspecteer de autorisatieprocedure, afspraken met leveranciers met betrekking tot toegang tot systemen en data en andere gerelateerde documenten. • Stel voor elk van deze processen en systemen op basis van een steekproef de werking vast. • Inspecteer de periodieke review en de opvolging van de resultaten. • Inspecteer de wachtwoordinstellingen. • Interview de verantwoordelijke functionarissen.

Bijlage 4 – Guidance bij de te onderzoeken organisatorische en technische beheersingsmaatregelen				
#	Onderwerp	Beheersingsmaatregelen	Nadere toelichting	Testaanpak
			○ Periodiek wijzigen van wachtwoorden. ○ Voldoende complex wachtwoord. ○ Twee-factor authenticatie. ○ Versleuteld opslaan van wachtwoorden. ○ Automatisch blokkeren na x-aantal foutieve inlogpogingen. • Aantoonbare controle op joiners/movers/leavers. • Wijzigen van de standaard wachtwoorden van administrator accounts. • Beperken eventuele admin- en shared accounts • Uitvoeren periodieke reviews, minimaal jaarlijks. Specifieke aandacht gaat uit naar wachtwoorden die leveranciers hebben om toegang tot de systemen of data te krijgen (wie hebben die wachtwoorden, hoe worden die opgeslagen en wie hebben toegang. Hoe vaak worden ze gewijzigd, et cetera).	

Bijlage 4 - Guidance bij de te onderzoeken organisatorische en technische beheersingsmaatregelen				
#	**Onderwerp**	**Beheersingsmaatregelen**	**Nadere toelichting**	**Testaanpak**
3	Beheer van kwetsbaarheden (patch-management)	Informatie over technische kwetsbaarheden van informatiesystemen die worden gebruikt behoort tijdig te worden verkregen, de blootstelling van de organisatie aan dergelijke kwetsbaarheden te worden geëvalueerd en passende maatregelen te worden genomen om het risico dat ermee samenhangt aan te pakken. <u>Doelstelling:</u> Zeker stellen dat technische en software kwetsbaarheden tijdig en effectief worden aangepakt en zo een stabiele omgeving wordt gecreëerd. <u>Scope:</u> Hosting, leverancier van de Wpg-geclassificeerde verwerkende systemen.	De focus is op het patching proces. Dit proces kan gedifferentieerd zijn naar bijvoorbeeld het Operating System (OS), Database Management System (DBMS) en netwerk. Applicaties en systemen dienen gepatcht te worden bij kwetsbaarheden. Een maandelijks patching cyclus is aanvaardbaar tenzij er security alerts zijn. Voor internet facing systemen dienen de laatste stabiele beveiligingspatches te zijn geïnstalleerd. Indien patching niet mogelijk is in verband met een legacy applicatie die niet meer zou functioneren na patching, zal dit risico aantoonbaar moeten zijn afgewogen. Aandachtpunten hierbij zijn: • Het beschrijven van beheer van kwetsbaarheden en/of patchmanagement-beleid waarin is aangegeven hoe de organisatie omgaat met updates: hoe snel implementeert de organisatie een kritieke patch en welke stadia moet de patch doorlopen.	• Inspectie van het patchmanagementbeleid. • Inspecteer of de versie van gehanteerde systemen bekende kwetsbaarheden bevatten en of hiervoor een patch beschikbaar is. • Interview de verantwoordelijke functionarissen.

Bijlage 4 - Guidance bij de te onderzoeken organisatorische en technische beheersingsmaatregelen				
#	Onderwerp	Beheersingsmaatregelen	Nadere toelichting	Testaanpak
			• Registratie van kwetsbaarheden en patches met vastlegging of de patches niet, wel of versneld worden doorgevoerd. • Het tijdig doorvoeren van patches.	
4	Cryptografie	Ter bescherming van politiegegevens behoort een beleid voor het gebruik van cryptografische beheersingsmaatregelen te worden ontwikkeld en geïmplementeerd. Doelstelling: Zorgen voor correct en doeltreffend gebruik van cryptografie om de vertrouwelijkheid, authenticiteit en/of integriteit van politiegegevens te beschermen. Scope: Hosting, leverancier van de Wpg-geclassificeerde verwerkende systemen.	De focus van het toepassen van cryptografie ligt op zowel opslag als transport van politiegegevens. Aandachtspunten hierbij zijn: • Het beschrijven van het cryptografiebeleid waarin is aangegeven wat versleuteld wordt en op welke wijze. • Encryptie tijdens transport voldoende sterk • Encryptie van opgeslagen politiegegevens, bij afwijking dient een risico analyse te worden gemaakt.	• Inspecteer de classificatie van gegevens en daaraan gerelateerde risicoanalyse, de netwerkarchitectuur en het inrichtingsdocument waar de encryptie van gegevens in staat beschreven. • Inspecteer of de toegepaste cryptografische configuratie voldoet aan de laatste stand der techniek. • Interview de verantwoordelijke functionarissen.
5	Vulnerability scans en Penetratietesten	Penetratietesten en vulnerability scans worden procesmatig en procedureel, ondersteund door richtlijnen, uitgevoerd op de infrastructuur van de systemen waarin politiegegevens verwerkt worden.	De voorkeur heeft het op basis van een risicoafweging enkele keren per jaar penetratietesten en vulenerability scans te laten uitvoeren, zodat ingespeeld kan worden op nieuwe bedreigingen.	• Inspecteer het netwerkarchitectuur schema en de opdracht tot het uitvoeren van de penetratie test. • Inspecteer het penetratietest en vulnerability scan rapporten, het actieplan naar aanleiding van de bevindingen en de status (opvolging) van de bevindingen.

Bijlage 4 - Guidance bij de te onderzoeken organisatorische en technische beheersingsmaatregelen				
#	**Onderwerp**	**Beheersingsmaatregelen**	**Nadere toelichting**	**Testaanpak**
		Doelstelling: Het verkrijgen van inzicht in de weerstand die de systemen kunnen bieden aan pogingen om het te compromitteren. Scope: Hosting, leverancier van de Wpg-geclassificeerde verwerkende systemen.	Aandachtspunten hierbij zijn: • De penetratietest dient minimaal eenmaal per jaar te worden uitgevoerd en na significante wijzigingen, zoals vervanging applicatie, nieuwe versie, migratie webservers, database migratie, et cetera. • De vulnerability scans dienen minimaal vier keer per jaar te worden uitgevoerd en na significante wijzigingen, zoals vervanging applicatie, nieuwe versie, migratie webservers, database migratie, et cetera. • De scope van de penetratietest en vulnerabilty scans omvat tenminste de systemen en de infrastructuur voor het netwerksegment die politiegegevens verwerken. • Naar aanleiding van de resultaten van de penetratietesten en vulnerability scans is een actieplan opgesteld om de tekortkomingen op te heffen. • Er is voldoende voortgang geboekt in het opvolgen van bevindingen gezien de aard en complexiteit van de bevindingen.	• Interview de verantwoordelijke functionarissen.