



Ministerie van Veiligheid en Justitie

Audit Wpg politie Amsterdam- Amstelland

Rapport

Datum
Status

13 januari 2012
Definitief

Colofon

Afzendgegevens

Departementale Auditdienst

Kalvermarkt 53
2511 CB Den Haag
Postbus 20301
2500 EH Den Haag
www.rijksoverheid.nl/venj

Contactpersonen

[REDACTED]

T 070 370 [REDACTED]
M wpg@minvenj.nl

Projectnaam

Audit Wet Politiegegevens

Ons kenmerk

DDS/5719586/11

Auteurs

[REDACTED]

Inhoud

Colofon 3

1 Assurance Verklaring 7

2 Samenvatting 9

3 Inleiding 18

- 3.1 Algemeen 18
- 3.2 Aanleiding 18
- 3.3 Doelstelling, aard en scope van de opdracht 18
- 3.4 Afbakening 19
- 3.5 Normenkader 19
- 3.6 Beperkingen voor de privacy audit 20
- 3.7 Onderzoeksmethoden en werkwijze 20
- 3.8 Doelgroep van het rapport 20

4 Bevindingen 21

- 4.1 Inleiding 21
- 4.2 Verantwoordelijke (artikel 1.f) 22
- 4.3 Kwaliteitsaspecten van politiegegevens (artikel 3 en 4) 22
- 4.4 Gevoelige gegevens (artikel 5) 24
- 4.5 Autorisatie (artikel 6) 25
- 4.6 Geautomatiseerd Vergelijken/In Combinatie Met Elkaar Verwerken (artikel 11) 26
- 4.7 Bewaartermijnen (artikel 14) 27
- 4.8 Ter beschikking stellen (artikel 15) 28
- 4.9 Verstrekken (artikel 16/24) 29
- 4.10 Rechten van betrokkenen (artikel 25/28) 30
- 4.11 Protocolplicht (artikel 32) 30
- 4.12 Audits (artikel 33) 32
- 4.13 Privacy functionaris (artikel 34) 32
- 4.14 Functionaris Gegevensbescherming (artikel 36) 33

1 Assurance Verklaring

In het jaar 2011 heeft de Departementale Auditdienst (DAD) van het ministerie van Veiligheid en Justitie (VenJ) in opdracht van de landelijke stuurgroep implementatie Wpg, waarin de Directeur-Generaal Politie en het Korpsbeheerders Beraad (KBB) zijn vertegenwoordigd, privacy audits op grond van de Wet politiegegevens (Wpg) uitgevoerd naar de verwerkingen die in de Wpg zijn beschreven bij de politiekorpsen. In 2011 is een privacy audit uitgevoerd bij het korps Amsterdam-Amstelland.

Deze privacy audit had tot doel op systematische wijze te toetsen of aan de bepalingen van de Wpg op adequate wijze uitvoering is gegeven ten aanzien van de in de wet genoemde verwerkingen bij het korps Amsterdam-Amstelland.

Dit onderzoek is uitgevoerd conform de richtlijn 3600N, 'Assurance-opdrachten met betrekking tot de bescherming van persoonsgegevens (privacy audits)' van juni 2006, van de NIVRA en de NOREA.

Op grond van onze werkzaamheden concluderen wij dat het stelsel van maatregelen en procedures gericht op de bescherming van de politiegegevens, betrekking hebbende op de in de Wpg genoemde artikelen bij het korps Amsterdam-Amstelland, naar de stand van ultimo december 2011, in opzet, bestaan en werking niet volledig heeft voldaan aan de vereisten zoals genoemd in de Wpg.

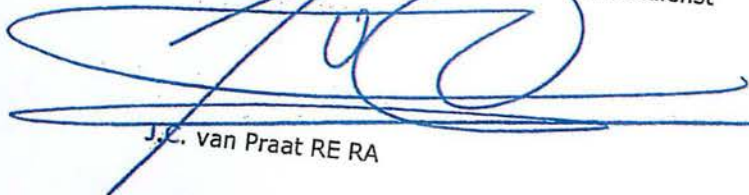
Deze conclusie is onderworpen aan de inherente beperkingen die elders in dit assurance-rapport zijn genoemd.

Het oordeel heeft betrekking op de zogenaamde verwerkingen genoemd in de Wpg. Het hierbij gehanteerde normenkader omvat de door het korps Amsterdam-Amstelland te nemen maatregelen. Ook is gebleken dat het korps Amsterdam-Amstelland voor het volledig kunnen voldoen aan de Wpg eisen mede afhankelijk is van besluiten die buiten het korps Amsterdam-Amstelland dienen te worden genomen, bijvoorbeeld op landelijk niveau door de minister van VenJ, het KBB of de Raad van Korpschefs. Tekortkomingen op al deze vlakken hebben uiteindelijk geleid tot het geformuleerde oordeel.

De verantwoordelijke, zijnde de korpsbeheerder van het korps Amsterdam-Amstelland, is, op grond van artikel 4 lid 1 van de Regeling Periodieke Audit Politiegegevens, verplicht binnen drie maanden een verbeterrapport op te stellen waarin de maatregelen worden beschreven die getroffen zijn ter verbetering van de in de privacy audit geconstateerde tekortkomingen. Op grond van artikel 4 lid 3 dient hercontrole plaats te vinden. Wij adviseren deze hercontrole te laten uitvoeren door de interne auditfunctie van het korps Amsterdam-Amstelland. Het verbeterrapport en de uitgevoerde hercontrole zullen in de navolgende jaren door de privacyauditor worden beoordeeld.

Den Haag, 13 januari 2012

De Directeur van de Departementale Auditdienst



J.C. van Praat RE RA

2 Samenvatting

Het korps Amsterdam-Amstelland heeft een aantal zaken in opzet goed opgepakt, zoals het beschrijven van procedures, het centraal beheren van de convenanten door het NAC, het schonen van BVH en het aanstellen van een interne auditfunctie. Het korps heeft ook een interne audit naar de Wpg uitgevoerd. De korpsleiding toont hiermee en met andere initiërende activiteiten haar aandacht voor de Wpg. Niettemin voldoet het door ons beschouwde stelsel van maatregelen nog niet in opzet, bestaan en werking aan de vereisten van de Wpg.

De bevindingen vanuit de privacy audit zijn hieronder samengevat per artikellid in volgorde van de oordeelsvorming binnen de onderscheiden thema's.

Criteria:

- Groen = Er wordt in hoofdlijnen voldaan aan de norm.
- Oranje = Er wordt niet of niet geheel voldaan aan de norm of er is een acceptabel actieplan.
- Rood = Er wordt niet voldaan aan de norm en er is geen acceptabel actieplan.
- Grijs = Niet van toepassing.

Norm	Aspect		Bevinding en oordeel
Art. 1.f, Verantwoordelijke			
1.f	Mandaatbesluit		Er is een Mandaatbesluit van 17 december 2004, getiteld "Mandaatbesluit Regionale Politiekorps Amsterdam-Amstelland 2005". Hierin wordt aangetoond dat het bevoegd gezag (korpsbeheerder) zijn mandaat verleent aan de korpschef van het regionaal politiekorps Amsterdam-Amstelland. Er is geen specifiek mandaatbesluit voor de Wet Politiegegevens. Volgens de afdeling Juridische Zaken van Politie Amsterdam-Amstelland valt de verantwoordelijkheid voor de Wet Politiegegevens onder het algemene mandaatbesluit. Hiermee wordt deels voldaan aan de Wpg.
Art. 3 en 4, Kwaliteitsaspecten van politiegegevens			
8.1 en 9.1	Onderscheid onderzoek Dagelijkse Politietask (8) versus Bepaald geval (9)		Op het intranet van het korps is een instructie "onderscheid art 8/9" d.d. 10-10-2010 opgenomen. Deze instructie is een hulpmiddel om te kunnen bepalen onder welk regime artikel 8 of 9 wpg-gegevens verwerkt moeten worden. Hiermee wordt voldaan aan de Wpg.
3.1 t/m 3.3 (8) 4.1 (8)	Noodzakelijkheid (8) Doelbinding Rechtmatigheid Juistheid Volledigheid		Op het intranet van het korps staat de instructie "Algemene voorschriften gegevensverwerking WPG". Deze behandelt de kwaliteitscriteria zoals in de wet beschreven staat. Daarnaast is er in opleidingen en via een elektronische briefing aandacht besteed aan hoe Blauw invulling aan deze kwaliteitscriteria moet geven. Hiermee wordt voldaan aan de Wpg.
3.1 t/m 3.4 (9)	Noodzakelijkheid (9) Doelbinding		Er zijn voor opsporing twee procedures met betrekking tot een aantal kwaliteitscriteria aanwezig.

Norm	Aspect	Bevinding en oordeel
4.1 (9)	Rechtmatigheid Herkomst en wijze van verkrijging Juistheid Nauwkeurig Volledigheid	In de procedure "vastleggen doel art 9" d.d. 30-7-2011 is beschreven waarom en op welke wijze het doel van het onderzoek vastgelegd moet worden. In het Handboek Bevoegd Functionaris d.d. 13-12-2010 staat dat de bevoegd functionaris controleert of gegevens rechtmatig worden verwerkt (rechtmatig verkregen + verwerkingstermijn). Beide procedures zijn terug te vinden op intranet. Hiermee wordt voldaan aan de Wpg.
3.4 (10 en 12) 4.1 (10 en 12)	Noodzakelijkheid (10 en 12) Doelbinding Rechtmatigheid Herkomst en wijze van verkrijging Juistheid Nauwkeurig Volledigheid	Bij de CIE en de RID zijn de kwaliteitscriteria in verband met de aard van het werk goed ingeregeld. Bij de CIE gebeurt dit volgens het landelijk proceshandboek CIE en de toezichthoudende rol van de CIE-OvJ. Bij de RID liggen de kwaliteitscriteria al in het doel van de taak vast. De RID werkt volgens de handleiding openbare orde, waarin de wettelijke bevoegdheden uiteen worden gezet. Ook is bij de RID Amsterdam-Amstelland aandacht gegeven aan de invoering van de Wpg en laten zij zich rechtstreeks leiden door de artikelen in de Wpg die voorschrijven hoe verzamelde informatie dient te worden verwerkt, te worden opgeslagen en te worden verwijderd/vernietigd. Hiermee wordt voldaan aan de Wpg.
4.3	Beveiliging	Het autorisatiesbeheer is bij Amsterdam-Amstelland nog niet goed op orde. De landelijke systemen BVO en BVH zijn nog niet Wpg-proof. De gebruikte SLA's en de aanvullende contracten voldoen nog niet aan de aspecten van de Wpg. Hiermee wordt niet voldaan aan de Wpg.
Art. 5, Gevoelige Gegevens		
• Gevoelige gegevens		In de "Algemene voorschriften gegevensverwerking Wpg" die te vinden is op het intranet van het korps Amsterdam-Amstelland is een voorschrift opgenomen voor de verwerking van gevoelige gegevens. Hierin wordt beschreven wat gevoelige gegevens zijn en wanneer je ze mag verwerken. Er is ook een richtlijn aanwezig voor de beveiliging van het verwerken van gevoelige gegevens. Deze is terug te vinden in het Handboek Bevoegd functionaris. Binnen het korps Amsterdam-Amstelland geldt dat documenten met gevoelige informatie (welk niet aangeleverd mogen worden aan Blue View) handmatig op autorisatieniveau 6 in BVO worden geplaatst. Hiermee wordt voldaan aan de Wpg.
Art. 6, Autorisatie		
• Korpsautorisatiematrix		De autorisatiematrix is nog in ontwikkeling. Hiermee wordt niet voldaan aan de Wpg.
• Aanvraagproces		Een procedurebeschrijving voor autorisatiebeheer gericht op het toekennen van autorisaties staat op

Norm	Aspect	Bevinding en oordeel
		Intranet. Na ondertekening van de tekenbevoegde controleert de afdeling Autorisaties de aangevraagde autorisaties. Hiermee wordt voldaan aan de Wpg.
	• Wijziging en verwijdering	Het wijzigingen en verwijderen van autorisaties verloopt via Beaufort en het verwijderen verloopt via de autorisatieprocedure. Na ondertekening van de tekenbevoegde controleert de afdeling Autorisaties de gewijzigde en verwijderde autorisaties. Hiermee wordt voldaan aan de Wpg.
	• Autorisatiebeheer CIE en RID	Autorisaties voor medewerkers van de CIE en de RID worden toegekend door het hoofd van de CIE respectievelijk de RID. De CIE OvJ keurt het autorisatiebeleid goed. Hiermee wordt voldaan aan de Wpg.
32.1.c	Protocollering autorisaties	De autorisatieformulieren van voor november 2011 worden in mappen bewaard. Na november 2011 worden de autorisatieformulieren ingescanned. Hiermee wordt voldaan aan de Wpg.
32.3 voor 32.1.c	Bewaren protocolgegevens autorisaties	De autorisatieformulieren van voor november 2011 worden op papier bewaard. De formulieren van na november 2011 zijn gescanned. Hiermee wordt voldaan aan de Wpg.
Art. 11, Geautomatiseerd vergelijken en in combinatie zoeken		
	• Hanteerbare interpretatie	De definitie van de twee termen wordt toegelicht in de procedure "Aanvragen opdracht bevoegd gezag t.b.v. in combinatie verwerken", d.d. 04-10-2010. Er is op intranet ook casuïstiek aanwezig over het verschil tussen de twee termen. Hiermee wordt voldaan aan de Wpg.
	• Aangewezen functionarissen	Geautomatiseerd vergelijken (hit/no hit) mag bij een artikel 8 doel zonder toestemming van het bevoegd gezag gedaan worden. Bij in combinatie verwerken moet toestemming verkregen worden van het OM of burgemeester. In de procedure "Aanvragen opdracht bevoegd gezag t.b.v. in combinatie verwerken", d.d. 04-10-2010 wordt aangegeven welke functionarissen er in combinatie mogen verwerken. Hiermee wordt voldaan aan de Wpg.
11.4	Bevoegd gezag	In de procedure "Aanvragen opdracht bevoegd gezag t.b.v. in combinatie verwerken", d.d. 04-10-2010 wordt aangegeven dat bij in combinatie verwerken toestemming verkregen moet worden van het OM of de burgemeester (bevoegd gezag). Hiermee wordt voldaan aan de Wpg.
32.1.d en 32.1.h	Protocollering 11.1, 11.2, 11.4 en 11.5	De aanvragen worden via vaststaand formulier vastgelegd in het onderzoeksdossier. Er is een aparte procedure beschrijving voor artikel 11.5 verwerkingen (andere gegevens), "Onderkennen en aanmelden art. 11.5 verwerking". Artikel 11.5 verwerkingen moeten bij de privacy functionaris worden aangemeld.

Norm	Aspect	Bevinding en oordeel
		Hiermee wordt voldaan aan de Wpg.
32.3 voor 32.1.d en 32.1.h	Bewaren protocolgegevens 11.1, 11.2, 11.4 en 11.5	De protocolgegevens worden bewaard in het onderzoeksdossier. Hiermee wordt voldaan aan de Wpg.
Art. 14, Bewaartermijnen		
8.2 en 8.3	(8) van 1 tot 5 jaar	Bij korps Amsterdam-Amstelland is begin december 2011 voor BVH de nieuwe release 1.2.2. geïmplementeerd. In deze release is de Wpg- beslotenheid doorgevoerd. De wijzigingen zijn in het handboek WPG in BVH (versie 1.0, 9-8-2011) beschreven. Door de nieuwe release zijn registraties alleen het eerste jaar voor iedereen toegankelijk. Bij gegevens van 1 tot 5 jaar oud kunnen alleen beperkte groepen gebruikers bij de registratie. Voor het bewaren in de Kantoorautomatiseringsomgeving is een instructie "inrichting groepsmappen" d.d. 21-9-2010 (versie 1.0) opgesteld. Deze instructie is een hulpmiddel om de groepsmappen waarin politiegegevens worden opgeslagen volgens de richtlijnen van de Wpg in te richten. Hiermee wordt voldaan aan de Wpg.
8.6	(8) verwijderen na 5 jaar	BVH is in november 2010 geschoond, er staan geen gegevens ouder dan 5 jaar in. Het verwijderen van de informatie uit de operationele BVH en het overzetten ervan naar de historische BVH gebeurt iedere nacht door middel van een script. De informatie in de historische BVH kan dan gebruikt worden voor analyse werkzaamheden conform Wpg. Het verzoek daartoe verloopt via de Poortwachter. Indien het verzoek wordt gehonoreerd, wordt de gewenste data door Functioneel Beheer BVH teruggezet. Indien er binnen 3 maanden geen wijzigingen worden aangebracht op de teruggezette data, dan wordt automatisch de teruggezette data weer verwijderd. Hiermee wordt voldaan aan de Wpg.
14.1 (8)	(8) vernietigen na 5 jaar verwijderd	Uit het handboek Wpg in BVH (versie 1.0, 9-8-2011) blijkt dat om onrechtmatige verwerking te voorkomen, registraties ouder dan 10 jaar uit BVH worden verwijderd, mits deze niet langer noodzakelijk zijn met het oog op het maatschappelijk belang. Hiermee wordt voldaan aan de Wpg.
9.4	(9) verwijderen na OH plus ½ jaar	Een zaak wordt in VSO (Voortschrijdend overzicht) gesloten/dichtgezet als het proces-verbaal naar Justitie is gestuurd. In principe mogen onderzoeken geraadpleegd blijven worden tot een halfjaar na OH. Dit kan alleen worden opgevolgd als via het OM afloopberichten binnen komen. Dit komt soms voor. Dan wordt het autorisatieniveau van de

Norm	Aspect	Bevinding en oordeel
		medewerkers op 0 gezet en de superregistratie eraf gehaald door Functioneel Beheer. Hiermee wordt deels voldaan aan de Wpg.
14.1 (9)	(9) vernietigen na 5 jaar verwijderd	Er wordt nog geen informatie in BVO vernietigd. Hiermee wordt niet voldaan aan de Wpg.
10.6	(10) verwijderen na 5 jaar geen subjectwaardige registratie	Dit wordt door de CIE en de RID nageleefd en bij de CIE gecheckt door de CIE-officier. Hiermee wordt voldaan aan de Wpg.
14.1 (10)	(10) vernietigen na 5 jaar verwijderd	Dit wordt door de CIE en de RID nageleefd en bij de CIE gecheckt door de CIE-officier. Hiermee wordt voldaan aan de Wpg.
14.3	Hernieuwde verwerking	Er is een procedure Hernieuwd Verwerken (01-10-2010, versie 1.4) aanwezig. Deze is bestemd voor alle medewerkers werkzaam binnen Handhaving en Opsporing en staat op intranet. Hiermee wordt voldaan aan de Wpg.
32.1.e	Protocollering 14.3	Volgens de procedure geeft de bevoegd functionaris toestemming om een aanvraag tot hernieuwing in te dienen. Daarna wordt er contact opgenomen met het bevoegd gezag (OM). De hernieuwde gegevens worden vastgelegd in BVH en de Poortwachters registreren de hernieuwde verwerking. Hiermee wordt voldaan aan de Wpg.
32.3 voor 32.1.e	Bewaren protocolgegevens 14.3	De hernieuwde gegevens worden bewaard in BVH met de daarbij behorende bewaartermijnen. De Poortwachters registreren de hernieuwde verwerking. Hiermee wordt voldaan aan de Wpg.
12.2	(12) verwijderen na 4 maanden	Informatie wordt binnen een termijn van een week (wettelijk: maximaal 4 maanden) verwerkt en van BVO-bruto in BVO-netto gezet. Dit zit vast in de werkwijze van de CIE. Hiermee wordt voldaan aan de Wpg.
12.6	(12) controleren en vernietigen	Informatie wordt binnen de CIE en de RID regelmatig gecontroleerd en handmatig geschoond, automatisch is niet mogelijk in BVO. Bij de CIE toetst de CIE-OvJ jaarlijks het informantenregister en bij de RID gebeurt dit door een operationeel analist. Hiermee wordt voldaan aan de Wpg.
Art. 15, Ter beschikking stellen		
• Infodesk voor bevraging		De Infodesk heeft een procedure voor ter beschikking stellen en verstrekken. De infodesk behandelt alleen verzoeken die via de mail binnenkomen en benadert de bevoegd functionaris bij ontvangen aanvragen. De Infodesk geeft geen ongevraagde informatie af en beoordeelt ook de noodzaak van de verzoeken. Hiermee wordt voldaan aan de Wpg.
• Codering		De infodesk stelt alleen informatie uit artikel 8 en artikel 13 ter beschikking. Bij opsporingsinformatie

Norm	Aspect	Bevinding en oordeel
		wordt de aanvrager door verwezen naar de bevoegd functionaris. Codering wordt daarom alleen gebruikt bij embargo-onderzoeken en CIE-informatie. Hier zijn richtlijnen voor opgesteld. Hiermee wordt voldaan aan de Wpg.
	• Aanwijzing Bevoegd Functionaris	Het korps heeft een "aanwijzingsbesluit bevoegde functionarissen op grond van de Wpg", die met terugwerkende kracht vanaf 1 januari 2008 geldig is en getekend is door de plaatsvervangend korpsbeheerder. Hiermee wordt voldaan aan de Wpg.
	• Opleiding Bevoegd Functionaris	De Bevoegd Functionarissen hebben een training doorlopen, waarbij het Handboek Bevoegd functionaris d.d. 13-12-2010 (versie 1.2) als trainingsmateriaal is gebruikt. Hiermee wordt voldaan aan de Wpg.
15.2	Weigeringgronden	In het Handboek Bevoegd functionaris d.d. 13-12-2010 (versie 1.2) staan in paragraaf 4.4 criteria beschreven op basis waarvan een bevoegd functionaris mag weigeren om informatie ter beschikking te stellen. Hiermee wordt voldaan aan de Wpg.
Art. 16 t/m 24, Verstrekking		
	• Verstrekkingenwijzer (landelijk)	Er is een landelijke verstrekkingenwijzer. Deze is uitgedeeld binnen het korps en is digitaal beschikbaar op intranet. Hiermee wordt voldaan aan de Wpg.
	• Proces voor convenanten	Het proces voor convenanten gaat via het convenantenloket (NAC). NAC ontwikkelt beleid en hulpmiddelen voor het opstellen en afsluiten van convenanten. Ze hebben een modelconvenant opgesteld en het beheer ligt centraal bij het NAC. De richtlijn voor het verstrekken en afsluiten van convenanten staat op intranet. Hiermee wordt voldaan aan de Wpg.
	• Proces voor Art. 20 Besluiten	Er is een procedure voor artikel 20 besluiten beschreven op intranet. Dit proces verloopt ook via het convenantenloket (NAC). Hiermee wordt voldaan aan de Wpg.
	• Verstrekkingenschema (regio)	Op intranet staan de algemene procedure verstrekken (versie 0.96, 13-07-2010), de procedure artikel 19-verstrekking (versie 0.9, 13-07-2010) en de Alfabetische verkorte verstrekkingentabel (versie 01-09-2009). De infodesk heeft voor elke ketenpartner een protocol beschreven. Dit protocol bestaat uit een beschrijving van de ketenpartner in relatie tot het opvragen van informatie. Daarin is beschreven welke functionaris van de ketenpartner bevoegd is om informatie te mogen opvragen. In het protocol zijn twee werkinstructies opgenomen: 1) welke informatie mag ter beschikking worden gesteld of

Norm	Aspect	Bevinding en oordeel
		verstrekt en 2) hoe moet deze worden vastgelegd. Volgens het Inrichtingsvoorstel Verstrekkingen ligt vast wie aan wie mag verstrekken. Dit is te vinden via intranet. Hiermee wordt voldaan aan de Wpg.
	• Proces voor geautomatiseerde verstrekking	Binnen het korps bestaat inzicht in het proces voor "Geautomatiseerd verstrekken". Dit is opgenomen in een memo. Hiermee wordt voldaan aan de Wpg.
7.2	Geheimhouding	In het handboek verstrekken en handboek bevoegd functionaris komt de geheimhoudingsplicht aan de orde. Hierin wordt beschreven dat de geheimhoudingsplicht moet worden opgenomen in de convenanten. Hiermee wordt voldaan aan de Wpg.
32.1.f	Protocollering verstrekking	Vastlegging verstrekkingen gebeurt bij de Infodesk conform werkwijze ter beschikking stellen. Daarnaast moeten conform de protocolplicht de losse verstrekkingen eveneens worden geadministreerd. Dit laatste dient plaats te vinden volgens de procedure "administreren verstrekkingen". Deze procedure is in het handboek verstrekkingen opgenomen als bijlage 6 paragraaf 8.6. Hiermee wordt voldaan aan de Wpg.
32.3 voor 32.1.f	Bewaren protocolgegevens verstrekking	De protocolgegevens worden via de I90-formulieren in BVH bewaard, conform de bewaartermijnen van BVH. De losse verstrekkingen worden door de privacy functionaris bewaard. Hiermee wordt voldaan aan de Wpg.
	• Toezicht door leidinggevenden op verstrekkingen en protocollering	De privacy functionaris kan een totaaloverzicht van de verstrekkingen krijgen. De privacy functionaris voert geen toetsing op de vastlegging van verstrekkingen uit. Hiermee wordt deels voldaan aan de Wpg.
Art. 25 t/m 31, Rechten van de betrokkene		
25.1	Verzoek om kennisneming	In paragraaf 3.3 van het handboek "Verstrekken" staat de procedure omtrent afhandeling van inzageverzoeken van een betrokkene beschreven. Deze procedure is gebaseerd op de landelijke Handreiking Rechten betrokkene (PIWPG, versie 2.0 2009). Burgers kunnen schriftelijk een verzoek met een kopie identiteitsbewijs indienen bij het hoofdbureau. De privacy functionaris neemt alle verzoeken in behandeling. Hiermee wordt voldaan aan de Wpg.
28.1 t/m 28.3	Correctie	Het korps heeft geen richtlijnen beschreven voor verbetering, aanvulling, verwijdering of afscherming van politiegegevens ingeval van feitelijk onjuiste gegevens. Deze taak wordt wel uitgevoerd en is bij de privacy functionaris belegd. Hiermee wordt deels voldaan aan de Wpg.

Norm	Aspect	Bevinding en oordeel
Art. 32, Protocolplicht (32.1.c, d, e, f en h behandeld bij thema's)		
9.2 en 32.1.a	Protocollering doel onderzoek	In de procedure "vastleggen doel art 9" is beschreven waarom en op welke wijze het doel van het onderzoek moet worden vastgelegd. Uit de procedure blijkt dat: 1) de verantwoordelijkheid ligt bij Bevoegd Functionaris, 2) de registratie in applicatie BOSZ dient plaats te vinden en 3) als in applicatie BOSZ geen registratie plaatsvindt dat er een melding bij privacy functionaris gemaakt dient te worden. Hiermee wordt voldaan aan de Wpg.
32.3 voor 32.1.a	Bewaren protocolgegevens doel onderzoek	De protocolgegevens van de doelen artikel 9 onderzoeken worden bewaard in processen verbaal, BOSZ en bij de privacy functionaris. Hiermee wordt voldaan aan de Wpg.
13.4 en 32.1.b	Protocollering Art. 13 gegevensverzameling en	Het korps maakt gebruik van de landelijke protocollen voor schriftelijke vastleggingen als bedoeld in artikel 13, lid 4 van de Wet politiegegevens. Deze worden nog omgeschreven naar de politie Amsterdam-Amstelland. Hiermee wordt deels voldaan aan de Wpg.
32.3 voor 32.1.b	Bewaren protocolgegevens Art. 13 gegevensverzameling en	Vastleggingen van artikel 13 verwerkingen vindt nu plaats in de diverse applicaties van het korps. Er is een document met het overzicht van alle applicaties van Amsterdam-Amstelland waar artikel 13 verwerkingen in voor komen. Het Functioneel beheer heeft toegang tot deze ingevulde sjablonen. Hiermee wordt voldaan aan de Wpg.
32.1.g	Protocollering onrechtmatige handeling	Elk kwartaal heeft de privacy functionaris overleg met informatiebeveiliging en met Bureau Integriteit (BI). BI heeft een overzicht van Wpg-gerelateerde zaken. Er wordt gelogd, maar dit wordt alleen bekeken wanneer er aanleiding toe is. De korpsleiding moet hier dan toestemming ervoor geven. Hiermee wordt voldaan aan de Wpg.
32.3 voor 32.1.g	Bewaren protocolgegevens onrechtmatige handeling	Allé bevragingen worden gelogd en tussen de 3 en 5 jaar bewaard. Hiermee wordt voldaan aan de Wpg.
32.2	Gemeenschappelijke verwerking	Gemeenschappelijke verwerkingen vinden in TGO's plaats. De verantwoordelijkheid ligt bij het korps van de TGO-leider. Voor de andere TGO-leden worden externe autorisaties ultgegeven. Gemeenschappelijke verwerkingen worden niet bij het CBP gemeld omdat de verantwoordelijkheid bij een korps belegd is. Van een gemeenschappelijke verwerking volgens de Wpg is hiermee geen sprake.
Art. 33, Audits		
RPAP 3.1	Interne audit-functie	Er is bij korps Amsterdam-Amstelland een interne auditfunctie. De interne auditor is als RE en RA

Norm	Aspect		Bevinding en oordeel
			ingeschreven in het register. Hiermee wordt voldaan aan de Wpg.
RPAP 3.4	Interne audit-plan		Er is een audit jaarplan 2011. Het jaarplan 2012 is in concept gereed. Hierin is aangegeven dat in 2012 een interne audit gehouden zal worden, waarbij aandacht besteed zal worden aan de bevindingen en aanbevelingen uit externe audit 2011. Hiermee wordt voldaan aan de Wpg.
RPAP 3.6	Interne audit-rapport		De interne auditor heeft in eind 2010 een interne audit naar autorisaties, conform artikel 6 Wpg, uitgevoerd. Van dit onderzoek is op 23 maart 2011 een rapport verschenen. In 2011 heeft er geen interne audit plaatsgevonden, omdat in dat jaar de externe audit stond gepland. Hiermee wordt voldaan aan de Wpg.
Art. 34, Privacy functionaris			
34.1 en 34.4	Benoemd en gemeld		De privacy functionaris is per aanwijzingsbesluit d.d. 9-6-2009 benoemd en aangemeld bij het CBP. Sinds 1 januari 2011 is er een tweede privacy functionaris aangesteld, deze zal nog worden aangemeld bij het CBP. Hiermee wordt voldaan aan de Wpg.
34.2	Overzicht over protocollering		De privacy functionaris kan een overzicht over protocollering van gegevens verkrijgen op basis van informatie uit de organisatie. De privacy functionaris heeft tot nu toe nog geen toetsende rol uitgevoerd. Sinds 1 januari 2011 is er een tweede privacy functionaris bijgekomen. De wens is om in 2012 de rollen te splitsen per PF. Eén privacy functionaris zal dan de adviesrol op zich nemen en de ander de toetsingsrol. Hiermee wordt deels voldaan aan de Wpg.
34.3	Jaarverslag		De Privacy functionaris heeft voor het jaar 2009 een jaarverslag opgesteld. Voor het jaar 2010 is geen jaarverslag opgemaakt, dit jaar wordt meegenomen in komend jaarverslag van 2011. Hiermee wordt deels voldaan aan de Wpg.
Optioneel Art. 36, Functionaris Gegevensbescherming			
36.1 en 36.2	Benoemd		Niet van toepassing. Er is geen Functionaris Gegevensbescherming benoemd.
Wbp 63.3	Gemeld		Niet van toepassing.
Wbp 64.1 t/m 64.4	Toezichthoudende rol		Niet van toepassing.

3 Inleiding

3.1 Algemeen

In opdracht van de landelijke stuurgroep Wpg, waarin de Directeur-Generaal Politie en het KBB zijn vertegenwoordigd, heeft de DAD van het ministerie van VenJ een privacy audit uitgevoerd bij het korps Amsterdam-Amstelland zoals de Korpsbeheerders deze, uit hoofde van de Wpg, twee jaar na inwerkingtreding van de wet dienen te laten uitvoeren (Wpg artikel 33 lid 1).

De opdracht is beschreven in het document 'Plan van aanpak Audit Wet Politiegegevens' d.d. 08-09-2011 met kenmerk DAD/DDS/2011/5706209. De audit is in 2011 uitgevoerd bij het korps Amsterdam-Amstelland.

3.2 Aanleiding

De nieuwe Wpg, die op 1 januari 2008 in werking is getreden:

- biedt meer armslag voor het gebruik van persoonsgegevens;
- voorziet in mogelijkheden om gegevens, die voor een bepaald doel zijn verwerkt, te gebruiken voor andere doelen;
- biedt meer mogelijkheden voor verstrekking van politiegegevens aan personen en instanties buiten de politiesector;
- voorziet ook in waarborgen voor de burger tegen ongerechtvaardigde inbreuken op diens persoonlijke levenssfeer.

De Wpg schrijft 'de verantwoordelijke' voor om periodiek een privacy audit uit te laten voeren op de naleving van de regels die als gevolg van die wet van toepassing zijn op het verwerken van politiegegevens (artikel 33 lid 1). Tevens dient 'deze verantwoordelijke' tijdig opdracht te verstrekken aan een auditinstelling om de vierjaarlijkse privacy audit uit te voeren.

De DAD is voor 2011 benoemd als de externe auditor voor de audit naar de implementatie van de WPG voor de politie. In opdracht van de stuurgroep voert de DAD de privacy audits uit bij de diverse politieonderdelen conform de Regeling Periodieke Audit Politiegegevens en de Wet Politiegegevens. Dit betekent dat wij opzet, bestaan en waar mogelijk werking in de scope van de audit opnemen.

3.3 Doelstelling, aard en scope van de opdracht

Deze privacy audit heeft tot doel op systematische wijze te toetsen of aan de bepalingen van de Wpg op adequate wijze uitvoering is gegeven ten aanzien van de in de wet genoemde verwerkingen bij het politiekorps Amsterdam-Amstelland.

De privacy audit leidt tot een assurance verklaring met een oordeel over de genoemde doelstelling en over de in dit rapport aangegeven thema's. Daarnaast brengen wij de knelpunten in beeld en voorzien wij elk korps schriftelijk van advies (en overkoepelend de opdrachtgever).

De privacy audit richt zich op de opzet, het bestaan en indien van toepassing de werking, per ultimo december 2011, van maatregelen en procedures, waarmee het

politiekorps Amsterdam-Amstelland beoogt te voldoen aan de beheersdoelstellingen die bij of krachtens de Wpg gelden.

Binnen deze audit richten wij ons (conform de artikelen van de Wpg) op de volgende thema's:

- Noodzakelijkheid, rechtmatigheid en doelbinding (artikel 3)
- Juistheid, volledigheid en beveiliging politiegegevens (artikel 4)
- Gevoelige gegevens (artikel 5)
- Autorisaties (artikel 6)
- Geautomatiseerd vergelijken en in combinatie verwerken (artikel 11)
- Bewaartermijnen (artikel 14)
- Ter beschikking stellen van politiegegevens (artikel 15)
- Verstrekkingen (artikel 16 t/m 24)
- Rechten van betrokkenen (artikel 25 t/m 31)
- Protocolplicht (artikel 32)
- Audits (artikel 33)
- Privacy functionaris (artikel 34)
- Functionaris gegevensbescherming (artikel 36)

Deze audit richt zich op de opzet, het bestaan en waar mogelijk, de werking van de implementatie van de Wpg per politiekorps. Pas wanneer wij, tijdens het uitvoeren van de audit bij een politiekorps, hebben geconstateerd dat de opzet en het bestaan aan de daaraan te stellen eisen voldoen voeren wij aanvullende werkzaamheden uit om de werking vast te stellen.

3.4 Afbakening

De audit wordt uitgevoerd aan de hand van het normenkader dat wij voor dit doel hebben opgesteld. Het normenkader beslaat de 12 thema's uit de Wpg afgezet tegen de relevante wetsartikelen (artikel 8, 9, 10, 12 en 13).

De audit is gericht op bovengenoemde objecten en aspecten voor zover onder verantwoordelijkheid van het politiekorps Amsterdam-Amstelland. Dit betekent dat wij geen onderzoek hebben verricht naar door de vtsPN aan het korps Amsterdam-Amstelland geleverde faciliteiten, voor zover de verantwoordelijkheid daarvoor is belegd bij de vtsPN of bij anderen dan het korps Amsterdam-Amstelland.

3.5 Normenkader

De DAD heeft in het voortraject van deze privacy audit in 2011 een normenkader opgesteld dat is afgestemd met de opdrachtgever.

Dit normenkader voor de privacy audit is afgeleid uit de navolgende documenten:

- Wet politiegegevens, de wet van 21 juli 2007, houdende regels inzake de bescherming van politiegegevens.
- Besluit politiegegevens, besluit van 14 december 2007, houdende bepalingen ter uitvoering van de Wet politiegegevens.
- Regeling periodieke audit politiegegevens, de 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.

3.6 Beperkingen voor de privacy audit

Onze audit is gericht op het geven van een oordeel over het stelsel van maatregelen en procedures met betrekking tot de aangegeven verwerkingen van politiegegevens en de overige genoemde objecten.

Incidentele inbreuken op het stelsel die leiden tot beschadiging van de belangen van individuele personen of het niet naleven van de op de bescherming van persoonsgegevens betrekking hebbende wet- en regelgeving behoeven daarom niet altijd te zijn geconstateerd.

3.7 Onderzoeksmethoden en werkwijze

De privacy audit is uitgevoerd conform de richtlijnen voor het uitvoeren van EDP audits van de Nederlandse Orde van EDP Auditors (NOREA).

Het onderzoek is uitgevoerd door het houden van interviews onder medewerkers en leidinggevenden van het politiekorps Amsterdam-Amstelland en het Openbaar Ministerie, deelwaarnemingen in de procesbeschrijvingen en andersoortige documentatie en deelwaarnemingen in informatiesystemen.

Wij hebben onze werkzaamheden in de vorm van een Quick Scan in de maanden april en mei 2011 uitgevoerd en aanvullende werkzaamheden voor de privacy audit in december 2011 gedaan.

Het eindrapport is met inachtneming van het ontvangen commentaar vastgesteld.

3.8 Doelgroep van het rapport

Het auditrapport is vertrouwelijk en niet bestemd voor het maatschappelijk verkeer.

Wij voeren deze audit uit in opdracht van de stuurgroep waarin het KBB is vertegenwoordigd.

De stuurgroep wordt voorgezeten door drs. J.J.M. Stikvoort.
mr. A.F. Gaastra neemt namens DG Politie deel aan de stuurgroep.
drs. H.M.F. Bruls neemt namens het KBB deel aan de stuurgroep.

De specifieke doelgroep waarvoor het rapport is bestemd bestaat uit:

- onze opdrachtgever zoals bovengenoemd;
- de korpsbeheerder mr. E.E. van der Laan;
- de korpschef P.J. Aalbersberg;
- de Hoofd Officier van Justitie mr. H.J. Bolhaar;
- de privacy functionaris mr. drs. B.A. Vredendaal;
- de voorzitter van het College Bescherming Persoonsgegevens.

Het rapport mag uitsluitend met toestemming van de korpsbeheerder dan wel de korpschef van politiekorps Amsterdam-Amstelland aan derden ter beschikking worden gesteld.

De opdrachtgever is verantwoordelijk voor de verspreiding, ook binnen de doelgroep, van het rapport.

4 Bevindingen

4.1 Inleiding

De nieuwe Wet Politiegegevens (Wpg), die op 1 januari 2008 in werking is getreden, biedt meer armslag voor het gebruik van persoonsgegevens, voorziet in mogelijkheden om gegevens, die voor een bepaald doel zijn verwerkt, te gebruiken voor andere doelen en biedt meer mogelijkheden voor verstrekking van politiegegevens aan personen en instanties buiten de politiesector. Daarnaast voorziet de nieuwe wet in waarborgen voor de burger tegen ongerechtvaardigde inbreuken op diens persoonlijke levenssfeer.

4.1.1

Regie en doorzettingsmacht voor de Wpg implementatie

Bij het korps Amsterdam-Amstelland vond tijdens het implementatietraject in 2009 en 2010 de sturing van de implementatie van de Wpg plaats vanuit een stuurgroep Wpg met daarin opgenomen een lid van de korpsleiding, alsmede de directeurs van de Dienst Regionale Recherche (DRR) en de Dienst Regionale Informatie (DRI). De dagelijkse coördinatie van de implementatie heeft in 2009 en 2010 plaatsgevonden door het implementatieteam Wpg. Deze heeft in samenwerking met een externe deskundige veel procedures ontwikkeld en bekendheid met Wpg gegenereerd. Op intranet is een aparte pagina aangemaakt met de definitie en alle procedurebeschrijvingen van de Wpg. Na afronding van het project is de verantwoordelijkheid in de lijn belegd. Dit is echter niet actief opgepakt.

4.1.2

Bekendheid met de Wpg binnen de organisatie

Een groot aantal medewerkers heeft opleiding ontvangen in de Wpg. Bevoegde functionarissen zijn aangewezen door de korpsbeheerder en de benoemde privacy functionaris is gemeld aan het CBP. Handboeken voor verstrekkingen en procedures zijn opgesteld en beschikbaar via Intranet. Er is een grote mate van bewustwording gekweekt over betekenis van Wpg binnen de operatie. Er zijn aanjagers, projectcoaches, projectcoördinatoren en poortwachters benoemd die alle hun aandeel leveren bij de toepassing van de Wpg.

Het doel van de Wpg, onder voorwaarden verplicht delen van informatie, wordt echter nog niet algemeen onderschreven in het operationele werkveld binnen het korps. Door zowel top down als bottom-up communicatie, het vastleggen van toepassingen van de Wpg in werkinstructies en het structureel bespreken van vragen c.q. knelpunten van de Wpg tijdens werkoverleggen, zal de bewustwording van de Wpg toenemen.

4.1.3

Wpg en de praktijk

Bij het korps Amsterdam-Amstelland is sprake van een stevige focus op de Wpg. De wijze waarop de schoning van BVH heeft plaats gevonden is op te vatten als een best-practice voor andere regio's en VtsPN. Er is veel werk gemaakt van het Wpg proof maken van convenanten door het centraal te beheren bij het Netwerk en Account Centrum (NAC).

Doordat momenteel de informatie in verschillende informatiesystemen moet worden geregistreerd en vanwege de geringe ondersteuning vanuit de informatiesystemen, wordt de Wpg binnen het korps ervaren als een toename van de administratieve last.

4.2 Verantwoordelijke (artikel 1.f)

Mandaatbesluit

4.2.1

Norm

Net als onder de oude Wet Politierregisters (Wpolr) is ook in de Wpg de korpsbeheerder er verantwoordelijk voor, dat de nodige maatregelen worden getroffen zodat politiegegevens juist, nauwkeurig en proportioneel worden verwerkt en op tijd worden verwijderd.

Bevindingen

Er is een Mandaatbesluit van 17 december 2004, getiteld "Mandaatbesluit Regionale Politiekorps Amsterdam-Amstelland 2005". Hierin wordt aangetoond dat het bevoegd gezag (korpsbeheerder) zijn mandaat verleent aan de korpschef van het regionaal politiekorps Amsterdam-Amstelland. Er is geen specifiek mandaatbesluit voor de Wet Politiegegevens. Volgens de afdeling Juridische Zaken van Politie Amsterdam-Amstelland valt de verantwoordelijkheid voor de Wet Politiegegevens onder het algemene mandaatbesluit.

4.2.2

Verbeterpunten

Als verbeterpunt is te noemen:

- Zorg voor een specifiek mandaatbesluit waaruit de verantwoordelijkheid blijkt voor het implementeren van maatregelen om te voldoen aan de Wpg.

4.3 Kwaliteitsaspecten van politiegegevens (artikel 3 en 4)

4.3.1

Norm

De verwerking van politiegegevens dient op grond van de artikelen 3 en 4 van de Wpg te voldoen aan criteria als rechtmatigheid, doelbinding en noodzakelijkheid (artikel 3) en volledigheid, juistheid en beveiliging (artikel 4).

4.3.2

Bevindingen

Het voldoen aan de bepalingen van de artikelen van de Wpg is een aangelegenheid waarin bijna alle geledingen van de politie zijn betrokken. Niettemin is in het bijzonder van belang dat het zwaartepunt van het voldoen aan deze criteria ligt bij de eerste vastlegging van gegevens. Daarvoor dragen registratie- en gegevensbeheerders de verantwoordelijkheid.

Op intranet van het korps is een instructie "onderscheid art 8/9" d.d. 10-10-2010 opgenomen. Deze instructie is een hulpmiddel om te kunnen bepalen onder welk regime artikel 8 of 9 Wpg-gegevens verwerkt moeten worden. De scheidingslijn tussen beide verwerkingsdoelen is niet eenduidig en biedt de medewerker interpretatieruimte. Om die redenen zijn deze richtlijnen opgesteld.

In deze instructie zijn criteria opgenomen die gelden voor artikel 9. Als een onderzoek niet voldoet aan deze criteria dan kan het onderzoek worden aangemerkt als artikel 8 - verwerking. Medewerkers kunnen de werkinstructies / procedures raadplegen op intranet. Uit de interviews is niet vernomen op welke andere wijze medewerkers op de hoogte worden gesteld van nieuwe of gewijzigde procedures / instructies. In de instructie "onderscheid art 8 en 9" is geen beschrijving van waarborgende maatregelen opgenomen. Uit de interviews is niet af te leiden in hoeverre er op worden toegezien dat onderzoeken ook daadwerkelijk onder het juiste regime worden verwerkt.

Proces handhaving

Met betrekking tot artikel 8 informatie "verwerken van politiegegevens ten behoeve van de dagelijkse politiepraktijk, zoals surveilleren, advisering over preventie, afhandelingen van de verkeersproblematiek, eenvoudig recherchewerk, verlenen van hulp en handhaven van wetten en regels" zijn er een aantal acties ondernomen om de kwaliteitscriteria onder de aandacht te brengen. Er is hieraan aandacht besteed in opleidingen, via een postercampagne en een elektronische briefing voor degenen die de opleiding niet gevolgd hebben. In de elektronische briefing staat bijvoorbeeld het verschil tussen de artikelen uit de Wpg uitgelegd en wordt er extra aandacht besteed aan de kwaliteit van de gegevens. De volledigheid en juistheid van gegevens wordt daarnaast enigszins geborgd door de verplichte invulvelden van BVH.

Uit gesprekken komt naar voren dat informatie ten behoeve van de dagelijkse politiepraktijk opgeslagen wordt in privé- en groepsmappen in de kantoorautomatiseringsomgeving. Dit gebeurt bijvoorbeeld omdat mediabestanden niet in de landelijke systemen, zoals BVH, opgehangen kunnen worden. Het risico is hier dat informatie niet kan worden gedeeld.

Proces opsporing

In artikel 9 Wpg wordt gesproken over het "gericht verwerken van politiegegevens ten behoeve van een onderzoek met het oog op de handhaving van de rechtsorde in een bepaald geval". Op intranet heeft het korps een tweetal procedures opgenomen waarbij aandacht wordt besteed aan een aantal criteria van Wpg te weten procedure "vastleggen doel art 9 (d.d. 30-7-2011)" en het Handboek Bevoegd Functionaris (d.d. 13-12-2010).

In de procedure "vastleggen doel art 9" is beschreven waarom en op welke wijze het doel van het onderzoek moet worden vastgelegd. Uit de procedure blijkt dat:

- De verantwoordelijkheid ligt bij Bevoegd Functionaris.
- De registratie in applicatie BOSZ dient plaats te vinden en als in applicatie BOSZ geen registratie plaatsvindt dat er een melding bij privacy functionaris gemaakt dient te worden.
- In het handboek Bevoegd Functionaris is een aantal taken voor Bevoegd Functionaris beschreven die betrekking hebben op een aantal kwaliteitsaspecten van art 3 en 4 van Wpg zoals:
 - het tijdig aanmelden van het doel van een verwerking zoals bedoeld in art 9 lid 2;
 - het toetsen van voorgenomen doelafwijkend gebruik van politiegegevens;
 - erop toezien dat binnen zijn onderzoek de herkomst en wijze van verkrijging van de gegevens wordt geregistreerd;
 - het afmelden van art 9-verwerking (schonen, ter archivering aanbieden) en de controle of gegevens rechtmatig worden verwerkt (rechtmatige verkrijging, verwerkingstermijn).

Uit de gesprekken komt naar voren dat de kwaliteitscontrole plaatsvindt op de processen verbaal en dat het proces als maatregel van interne controle is opgenomen.

De Infodesk behandelt de aanvragen voor ter beschikking stellen en verstrekkingen. De aanvragen komen via mail binnen. Er zijn werkinstructies en afspraken voor de Infodesk beschikbaar.

CIE en RID

Bij de informatie verwerkte afdelingen als de CIE en de RID worden aan deze aspecten vanwege de bijzondere aard van hun taakstelling specifiek aandacht besteed. Desondanks zijn er voor de CIE en de RID geen procesbeschrijvingen aangetroffen waarin op welke wijze de zorg voor het voldoen aan de criteria voor deze informatie dient plaats te vinden.

Beveiliging

Voor wat betreft beveiliging van gegevens zijn de volgende bijzonderheden geconstateerd:

- Volgens interne audit Wpg "Autorisatie" (rapport d.d. 23-3-2011) wordt geconcludeerd dat de beheersing van Logische Toegangsbeveiliging tot de informatiesystemen bij het korps op essentiële onderdelen als ontoereikend wordt geacht.
- De landelijke systemen BVO en BVH zijn niet wpg-proof.
- De afdeling informatiebeveiliging heeft 32 van 45 panden een certificaat afgegeven gericht op de fysieke toegang tot de gebouwen en cleandesk-policy. Komend jaar zal afdeling Informatiebeveiliging de overige panden in onderzoek betrekken.
- Voor uitgifte van pasjes ten behoeve van fysieke beveiliging is een procedure beschreven (d.d. 15-12-2011). Voor de registratie van pasjes wordt gebruik gemaakt van het systeem Sesam. Uit gesprek is vernomen dat het systeem Sesam mogelijk niet actueel is (vervuld) en dat een periodieke controle tussen het systeem BEAUFORT (soll) en het systeem Sesam (ist) niet plaatsvindt.
- Het korps heeft met VtsPN een Service Level Agreement (SLA) afgesloten. Uit interviews is vernomen dat de SLA en de aanvullende contracten niet voldoen aan de aspecten van Wpg.

Toetsing

Op de naleving van de aspecten van art 3 en 4 van de Wpg houdt de privacy functionaris geen toezicht.

Uit de gesprekken is vernomen dat er geen protocol (werkinstructie) is beschreven waarin wordt aangegeven hoe de teamleiders, hoofden van dienst periodieke controle moet uitvoeren op de uitvoerende werkzaamheden ten aanzien van de Wpg door bijvoorbeeld dit element te bespreken in de werkoverleggen, functioneringsgesprekken en periodiek een PV te controleren.

4.3.3

Verbeterpunten

Als verbeterpunten zijn te noemen:

- Organiseer de toezichtstaak op de kwaliteitsaspecten van politiegegevens.

4.4 Gevoelige gegevens (artikel 5)

4.4.1

Norm

De verwerking van politiegegevens betreffende iemands godsdienst of levensovertuiging, ras, politieke gezindheid, gezondheid, seksuele leven, alsmede persoonsgegevens betreffende het lidmaatschap van een vakvereniging vindt slechts plaats in aanvulling op de verwerking van andere politiegegevens en voor zover dit voor het doel van de verwerking onvermijdelijk is.

4.4.2

Bevindingen

In de "Algemene voorschriften gegevensverwerking Wpg" die te vinden is op het intranet van het korps Amsterdam-Amstelland is een voorschrift opgenomen voor de verwerking van gevoelige gegevens. Hierin wordt beschreven wat gevoelige gegevens zijn en wanneer je ze mag verwerken. Er is ook een richtlijn aanwezig voor de beveiliging van het verwerken van gevoelige gegevens. Deze is terug te vinden in het Handboek Bevoegd functionaris. Binnen het korps Amsterdam-Amstelland geldt dat documenten met gevoelige informatie (welk niet aangeleverd mogen worden aan Blue View) handmatig op autorisatieniveau 6 in BVO worden geplaatst.

4.5 Autorisatie (artikel 6)

4.5.1

Norm

Volgens artikel 6 Wpg is de verantwoordelijke onder meer belast met het voeren van een systeem van autorisaties dat voldoet aan de vereisten van zorgvuldigheid en evenredigheid en wordt zorg gedragen voor een schriftelijke vastlegging van de toekenning van autorisaties (protocolplicht).

4.5.2

Bevindingen

Autorisatieproces

Het korps heeft in 2010 een audit uitgevoerd op autorisaties. Deze audit betrof het beoordelen van de autorisaties van de applicaties BVH, VROS, HKS, PSH-B, NSIS, BOSZ, PAPOS en GMS. Van deze audit is op 23 maart 2011 een rapport verschenen.

Naar aanleiding van de audit zijn acties ondernomen om het autorisatiebeheer te verbeteren. Ten tijde van de Wpg audit was de autorisatiematrix nog in ontwikkeling.

Een procedurebeschrijving voor autorisatiebeheer gericht op het toekennen van autorisaties staat op Intranet. Na ondertekening van de tekenbevoegde controleert de afdeling Autorisaties de aangevraagde autorisaties.

Het wijzigingen en verwijderen van autorisaties verloopt via Beaufort en het verwijderen verloopt via de autorisatieprocedure. Na ondertekening van de tekenbevoegde controleert de afdeling Autorisaties de gewijzigde en verwijderde autorisaties.

De autorisatieformulieren van voor november 2011 worden op papier bewaard. De formulieren van na november 2011 zijn gescanned.

Proces Handhaving

Om met BVH te kunnen werken wordt de medewerker geautoriseerd voor een bepaalde functie zoals generalist, brigadier etc. Elk functie heeft recht op bepaalde schermen in BVH. Per scherm en veld kunnen deze autorisaties op maat worden gemaakt. Autorisatieverzoeken gaan via de leidinggevende naar de beheerders ter controle. Autorisaties in BVH worden toegekend nadat een opleiding BVH is gevolgd.

Proces Opsporing

Autorisaties voor BVO worden verleend op basis van het landelijk autorisatie-model en binnen het korps vastgelegde afspraken aangaande opleidingen. Binnen het korps is het aantal werkzaamheden van het proces "autorisatie aanvragen" verdeeld over functioneel beheer en operationeel beheer. Dit wijkt af van de landelijke benadering. Dit geldt voor het aanvragen van de onderzoeken niet voor autorisatieaanvragen. De reden hiervoor is dat het korps vindt dat het functioneel beheer in feite geen toegang mag hebben tot openbare informatie.

Autorisatieverzoek gaat via leidinggevende aan functioneel beheer BVO. Functioneel beheer BVO maakt voor nieuwe medewerker een account aan en geeft daarbij aan welke menu's (functionaliteiten) de medewerker mag benaderen. Autorisatieniveau 3 (horizontaal) wordt aan een nieuwe medewerker toegekend. Als er een onderzoek van start gaat, zal operationeel beheer vervolgens een onderzoek in BVO aanmaken. Tevens zal zij bij dat onderzoek een registratiebeheerder toewijzen. De betreffende registratiebeheerder autoriseert vervolgens de medewerkers voor het onderzoek.

CIE en RID

Autorisaties voor medewerkers van de CIE worden toegekend door het hoofd van de CIE en zijn plaatsvervanger. De Cie-OvJ heeft de autorisaties bij de CIE goedgekeurd.

Autorisaties voor medewerkers van de RID worden toegekend door het hoofd van de RID. De RID heeft een afgeschermd gedeelte in BVO, daar kunnen andere niet bij.

De CIE en de RID werken in een gesloten afdeling, afgeschermd met speciaal geautoriseerde toegangspassen. Als iemand uit dienst gaat worden de fysieke toegangsrechten en logische toegangsrechten geblokkeerd.

4.5.3

Verbeterpunten

Als verbeterpunt is te noemen:

- Continueer de ontwikkeling van de autorisatiematrix.

4.6 Geautomatiseerd Vergelijken/In Combinatie Met Elkaar Verwerken (artikel 11)

4.6.1

Norm

Voor het onderzoek kunnen politiegegevens die voor dat onderzoek zijn verwerkt, geautomatiseerd worden vergeleken met andere politiegegevens die worden verwerkt op grond van artikel 8 of 9 teneinde vast te stellen of verbanden bestaan tussen de betreffende gegevens. De gerelateerde gegevens kunnen, na instemming van de daartoe bevoegde functionaris, zijnde de leider van het betreffende onderzoek of zijn plaatsvervanger, voor dat onderzoek verder worden verwerkt. Indien politiegegevens in combinatie met elkaar worden verwerkt, worden van die verwerking nader genoemde gegevens vastgelegd (protocolplicht).

4.6.2

Bevindingen

De inhoud van de activiteiten geautomatiseerd vergelijken (GV) en in combinatie met elkaar verwerken (ICMEV) is niet bij veel medewerkers binnen het korps bekend. Waar bekendheid met deze begrippen uit de Wpg wel aanwezig is, komt direct de vraag aan de orde waar de grenzen van GV en ICMEV liggen en op welke wijze daarmee in de praktijk moet worden omgegaan. Het korps Amsterdam-Amstelland heeft daarom samen met het Openbaar Ministerie de twee termen gedefinieerd. De definitie wordt toegelicht in de procedure "Aanvragen opdracht bevoegd gezag tbv in combinatie verwerken", dd 04-10-2010. Er is op intranet ook casuïstiek aanwezig over het verschil tussen de twee termen.

Geautomatiseerd vergelijken (hit/no hit) mag bij een artikel 8 doel zonder toestemming van het bevoegd gezag gedaan worden. Bij in combinatie verwerken moet toestemming verkregen worden van het OM of burgemeester. In de procedure "Aanvragen opdracht bevoegd gezag tbv in combinatie verwerken", dd 04-10-2010 wordt aangegeven welke functionarissen er in combinatie mogen verwerken.

De aanvragen worden via vaststaand formulier vastgelegd in het onderzoeksdossier. Er is een aparte procedure beschrijving voor artikel 11.5 verwerkingen (andere gegevens), "Onderkennen en aanmelden art. 11.5 verwerking". Artikel 11.5 verwerkingen moeten bij de privacy functionaris worden aangemeld.

Door de procesbeschrijvingen en casuïstiek zijn de termen goed gedefinieerd. Er is echter nog geen toetsing op de uitvoering hiervan.

4.6.3

Verbeterpunt

Als verbeterpunt is te noemen:

- Zorg voor een toezichthoudende rol van de privacy functionaris, zodat blijkt of het korps volgens de definitie werkt.

4.7 Bewaartermijnen (artikel 14)

4.7.1

Norm

Politiegegevens worden vernietigd zodra zij niet langer noodzakelijk zijn voor de uitvoering van de dagelijkse politietaak (artikel 8) en worden in ieder geval uiterlijk vijf jaar na de datum van eerste verwerking verwijderd. De politiegegevens die niet langer noodzakelijk zijn voor het doel van het onderzoek, worden verwijderd, of worden gedurende een periode van maximaal een half jaar verwerkt teneinde te bezien of zij aanleiding geven tot een nieuw onderzoek als bedoeld in artikel 9 of een nieuwe verwerking als bedoeld in artikel 10, en na verloop van deze termijn worden verwijderd.

4.7.2

Bevindingen

Proces Handhaving

Bij het korps Amsterdam-Amstelland is inmiddels voor BVH een nieuwe release 1.2.2. geïmplementeerd. In deze release is de WPG-beslotenheid doorgevoerd. De wijzigingen zijn het handboek WPG in BVH (versie 1.0, 9-8-2011) beschreven. Met deze release van BVH worden 2 hoofdaspecten nagestreefd:

- taakgebonden toegang tot registraties d.m.v. autorisaties en
- het voorkomen van onrechtmatige verwerking van verouderde politiegegevens.

Registraties tot 1 jaar zijn gedurende het 1e jaar vrij toegankelijk. Registraties van 1 tot 5 jaar oud (Wpg-afgeschermd) zijn niet langer voor alle BVH-gebruikers toegankelijk. Beperkte groepen gebruikers kunnen bij de registratie, de zogenaamde Poortwachters.

Registraties ouder dan vijf jaar (WPG-bewaard) zijn in die periode alleen ter afhandeling van klachten en verantwoording van verrichtingen nog beschikbaar. In bijzondere omstandigheden mogen, wanneer daartoe noodzakelijk blijkt, de gegevens op last van een bevoegd gezag weer herbruikt worden ten behoeve van artikel 9 en of 10. Om onrechtmatige verwerking te voorkomen worden registraties ouder dan 10 jaar uit BVH verwijderd, mits deze niet langer noodzakelijk zijn met het oog op het maatschappelijk belang.

Er is een procedure Hernieuwd Verwerken (01-10-2010, versie 1.4) aanwezig. Deze is bestemd voor alle medewerkers werkzaam binnen Handhaving en Opsporing en staat op intranet. Volgens de procedure geeft de Bevoegd functionaris toestemming om een aanvraag tot hernieuwing in te dienen. Daarna wordt er contact opgenomen met het bevoegd gezag (OM). De hernieuwde gegevens worden vastgelegd in BVH en de Poortwachters registreren de hernieuwde verwerking.

Kantooromgeving

Het korps heeft een instructie "inrichting groepsmappen" d.d. 21-9-2010 (versie 1.0) opgesteld. Deze instructie is een hulpmiddel om de groepsmappen waarin politiegegevens worden opgeslagen (als word en Excel-documenten) volgens de richtlijnen van de Wpg in te richten. Als de instructie opgevolgd wordt, dan zullen wettelijke voorwaarden opgelegd in de Wpg, bijvoorbeeld de bewaartermijnen, gehandhaafd kunnen worden. In deze instructie is alleen rekening gehouden met gegevens in het kader van artikel 8 en 9 verwerkingen, Bewaartermijnen van artikel 10, 12 en 13 worden hierin niet meegenomen.

De doelstelling van het korps is om geen projectdocumentatie in een eigen groepsmap op te nemen. Alle informatie dient in BVH, BVO en Summ-It te zijn geregistreerd. Om dit te kunnen bewerkstellingen zal binnen het korps een schoningsslag op de groepsmappen plaatsvinden. Overwogen wordt om,

als alle groepsmappen waarin projectdocumentatie zijn opgenomen, leeg zijn, de rechten voor groepsmappen in te trekken.

Proces Opsporing

Schoning voor het opsporingsproces is moeilijk te realiseren. Een zaak wordt in VSO (Voortschrijdend overzicht) gesloten / dichtgezet (status) als het procesverbaal naar Justitie is gestuurd. Daarna kan de afwikkeling van artikel 9 verwerkingen pas plaatsvinden als vanuit het OM een afloopbericht komt. Als deze melding is doorgegeven en verwerkt, dan mag een artikel 9 verwerking nog 6 maanden actief blijven, voordat deze achter slot gezet wordt. Als de afloopberichten binnen komen dan wordt het autorisatieniveau van de medewerkers op 0 gezet en de superregistratie eraf gehaald. Er wordt nog geen informatie vernietigd in BVO.

Informantenregister

Informatie wordt binnen een termijn van een week (wettelijk: maximaal 4 maanden) verwerkt en van BVO-bruto in BVO-netto gezet. Dit zit verankerd in de werkwijze van de CIE.

Informatie wordt binnen de CIE en de RID regelmatig gecontroleerd en handmatig geschoond, automatisch is niet mogelijk in BVO. Bij de CIE toetst de CIE-OvJ jaarlijks het informantenregister en bij de RID gebeurt dit door een operationeel analist.

4.7.3

Verbeterpunten

Als verbeterpunt is te noemen:

- Zorg voor naleving van de bewaartermijnen in de landelijke applicaties en de kantoorautomatisering.

4.8 Ter beschikking stellen (artikel 15)

4.8.1

Norm

De verantwoordelijke stelt politiegegevens ter beschikking aan personen die door hemzelf dan wel door een andere verantwoordelijke zijn geautoriseerd voor de verwerking van politiegegevens, voor zover zij deze behoeven voor de uitvoering van hun taak.

4.8.2

Bevindingen

De Infodesk heeft een procedure voor ter beschikking stellen en verstrekken. De infodesk behandelt alleen verzoeken die via de mail binnenkomen en benadert de bevoegd functionaris bij binnen gekomen aanvragen. De Infodesk geeft geen ongevraagde informatie af en beoordeelt ook de noodzaak van de verzoeken.

De Infodesk stelt alleen informatie uit artikel 8 en artikel 13 ter beschikking. Bij opsporingsinformatie wordt de aanvrager doorverwezen naar de bevoegd functionaris. Codering wordt daarom alleen gebruikt bij embargo-onderzoeken en CIE-informatie. Hier zijn richtlijnen voor opgesteld.

Het korps heeft een "aanwijzingsbesluit bevoegde functionarissen op grond van de WPG", die met terugwerkende kracht vanaf 1 januari 2008 geldig is en getekend is door de plaatsvervangend korpsbeheerder. De bevoegd functionarissen hebben een training gehad, waarbij het Handboek Bevoegd functionaris d.d. 13-12-2010 (versie 122) het trainingsmateriaal was. In het Handboek Bevoegd functionaris d.d. 13-12-

2010 (versie 1,2) staan in paragraaf 4.4 criteria beschreven op basis waarvan een bevoegd functionaris mag weigeren om informatie ter beschikking te stellen.

4.9 Verstrekken (artikel 16/24)

4.9.1

Norm

Paragraaf 3 van de Wpg omvat de artikelen waarin verstrekkingen van politiegegevens aan anderen dan de politie en de Marechaussee worden geregeld. In de artikelen 16 t/m 24 worden deze verstrekkingen nader uitgewerkt. Artikel 20 regelt de omstandigheden en voorwaarden voor de verstrekkingen aan derden structureel voor samenwerkingsverbanden.

4.9.2

Bevindingen

De laatste jaren heeft de informatieverstrekking vanuit het korps aan partijen buiten de politie een sterke vlucht genomen. Het aantal informatie-aanvragen is sterk gegroeid.

Er is een landelijke verstrekkingwijzer, deze is uitgedeeld binnen het korps en is digitaal beschikbaar op intranet. Op intranet staan veel procedures met betrekking tot het verstrekken. Zoals de algemene procedure verstrekken (versie 0.96, 13-07-2010), de procedure artikel 19-verstrekking (versie 0.9, 13-07-2010) en de Alfabetische verkorte verstrekkingentabel (versie 01-09-2009).

De infodesk heeft voor elke ketenpartner een protocol beschreven. Dit protocol bestaat uit een beschrijving van de ketenpartner in relatie tot het opvragen van informatie. Daarin is beschreven welke functionaris van de ketenpartner bevoegd is om informatie op te vragen. In het protocol zijn twee werkinstructies opgenomen:

- welke informatie mag ter beschikking worden gesteld of verstrekt en
- hoe moet deze worden vastgelegd.

Volgens het Inrichtingsvoorstel Verstrekkingen ligt vast wie aan wie mag verstrekken. Dit is te vinden via intranet.

Binnen het korps bestaat inzicht in het proces voor "Geautomatiseerd verstrekken". Dit is opgenomen in een memo.

In het "Handboek verstrekken" en het "Handboek Bevoegd Functionaris" komt de geheimhoudingsplicht naar voren. Dit moet worden opgenomen in de convenanten. Vastlegging verstrekkingen gebeurt bij de Infodesk conform werkwijze ter beschikking stellen. Daarnaast moeten conform de protocolplicht de losse verstrekkingen eveneens worden geadministreerd. Dit laatste dient plaats te vinden volgens de procedure "administreren verstrekkingen". Deze procedure is in het "Handboek verstrekkingen" opgenomen als bijlage 6 paragraaf 8.6.

De protocolgegevens worden via de i90-formulieren in BVH bewaard, conform de bewaartermijnen van BVH. De losse verstrekkingen worden door de privacy functionaris bewaard. De privacy functionaris kan een totaaloverzicht van de verstrekkingen krijgen. De privacy functionaris voert echter geen toetsing op de vastlegging van verstrekkingen uit.

Convenanten

Het korps Amsterdam-Amstelland heeft het proces voor convenanten centraal belegd bij het Netwerk en Account Centrum (NAC). Het NAC geeft overzicht en inzicht in de convenanten, partners en bevoegd functionarissen. Het NAC ontwikkelt beleid en hulpmiddelen voor het opstellen en afsluiten van convenanten, maar is niet verantwoordelijk voor verstrekkingen en heeft daarin geen toezichhoudende

rol. Wel heeft het NAC een toezichthoudende rol bij de totstandkoming van een nieuw convenant. Alle actieve, goede en geldige convenanten zijn in 2011 bekeken en voor goedkeuring voorgelegd aan de korpschef. De goede convenanten zijn, naast met de eigen privacy functionaris, ook met de privacy functionarissen van het Openbaar Ministerie en Openbaar Bestuur gedeeld. Na 2009 zijn nieuwe convenanten volgens het modelconvenant opgesteld, deze hoeven dus niet opnieuw door de driehoek bekrachtigd te worden en zijn Wpg-proof. De richtlijn voor het verstrekken en afsluiten van convenanten staat op intranet. Er is een procedure voor artikel 20 besluiten beschreven op intranet. Dit proces verloopt ook via het convenantenloket (NAC).

4.9.3

Verbeterpunten

Als verbeterpunt is te noemen:

- Zorg voor een toezichthoudende rol van de privacy functionaris op de verstrekkingen.

4.10 Rechten van betrokkenen (artikel 25/28)

4.10.1

Norm

De verantwoordelijke deelt een ieder op diens schriftelijk verzoek binnen zes weken mede of, en zo ja welke, deze persoon betreffende politiegegevens zijn vastgelegd.

4.10.2

Bevindingen

In paragraaf 3.3 van het handboek "Verstrekken" staat de procedure omtrent afhandeling van inzageverzoeken van een betrokkene beschreven.

Burgers kunnen schriftelijk een verzoek met een kopie identiteitsbewijs indienen bij het hoofdbureau. De privacy functionaris neemt alle verzoeken in behandeling.

Het korps heeft geen richtlijnen beschreven voor verbetering, aanvulling, verwijdering of afscherming van politiegegevens ingeval van feitelijk onjuiste gegevens. Deze taak wordt uitgevoerd door de privacy functionaris.

4.10.3

Verbeterpunten

Als verbeterpunt is te noemen:

- Stel richtlijnen op voor verbetering, aanvulling, verwijdering of afscherming van politiegegevens ingeval van feitelijk onjuiste gegevens.

4.11 Protocolplicht (artikel 32)

4.11.1

Norm

De verantwoordelijke draagt zorg voor de schriftelijke vastlegging van:

- de doelen van artikel 9 onderzoeken;
- gegevens die op grond van ondersteunende taken worden vastgelegd (artikel 13);
- de toekenning van autorisaties;
- de geautomatiseerde vergelijking of het in combinatie met elkaar verwerken van politiegegevens;
- de geautomatiseerde vergelijking van gegevens met openbare bronnen;
- de hernieuwde verwerking van politiegegevens op grond van artikel 9 of 10;
- de verstrekking van politiegegevens;
- signalen van onbevoegde of onrechtmatige verwerkingen.

Deze gegevens worden bewaard, ten minste tot de datum waarop de laatste controle (audit) is verricht.

4.11.2

Bevindingen

De protocolplicht houdt in dat het korps middels schriftelijke vastlegging verantwoording aflegt over de wijze waarop zij omgaat met privacy gevoelige gegevens.

Op intranet heeft het korps een tweetal procedures opgenomen waarbij aandacht wordt besteed aan een aantal criteria van Wpg te weten procedure "vastleggen doel art 9 (d.d. 30-7-2011)" en het Handboek Bevoegd Functionaris (d.d. 13-12-2010). In de procedure "vastleggen doel art 9" is beschreven waarom en op welke wijze het doel van het onderzoek moet worden vastgelegd. Uit de procedure blijkt dat de verantwoordelijkheid ligt bij Bevoegd Functionaris;

- de registratie in applicatie BOSZ dient plaats te vinden en
- als in applicatie BOSZ geen registratie plaatsvindt dat er een melding bij de privacy functionaris gemaakt dient te worden.

In het handboek Bevoegd Functionaris is een aantal taken voor Bevoegd Functionaris beschreven die betrekking hebben op een aantal kwaliteitsaspecten van artikel 3 en 4 van Wpg zoals:

- het tijdig aanmelden van het doel van een verwerking zoals bedoeld in art 9 lid 2;
- het autoriseren van personen voor de verwerking van politiegegevens ten behoeve van onderzoeken met het oog op handhaving van het rechtsorde;
- het toetsen van voorgenomen doelafwijkend gebruik van politiegegevens;
- erop toezien dat binnen zijn onderzoek de herkomst en wijze van verkrijging van de gegevens wordt geregistreerd;
- het afmelden van art 9-verwerking (schonen, ter archivering aanbieden) en
- de controle of gegevens rechtmatig worden verwerkt (rechtmatige verkrijging, verwerkingstermijn).

Uit de interne audit op autorisaties blijkt dat door het ontbreken van een goed toegankelijke vastlegging van geaccordeerde autorisatie aanvragen, van gerealiseerd autorisaties, van een goed beschrijving van de verschillende autorisatie rollen en van de politiewerkzaamheden waarvoor de autorisatie rollen nodig zijn, controle op bestaande autorisatie niet mogelijk is.

Het korps maakt gebruik van de landelijke protocollen voor schriftelijke vastleggingen als bedoeld in artikel 13, lid 4 van de Wet politiegegevens. Deze worden nog omgeschreven naar de politie Amsterdam-Amstelland. Vastleggingen van artikel 13 verwerkingen vindt nu plaats in de diverse applicaties van het korps. Er is een document met het overzicht van alle applicaties van Amsterdam-Amstelland waar artikel 13 verwerkingen in voor komen. Afdeling Functioneel Beheer heeft toegang tot deze ingevulde sjablonen.

Elk kwartaal heeft de privacy functionaris overleg met informatiebeveiliging en met Bureau Integriteit (BI). BI heeft een overzicht van Wpg-gerelateerde zaken. Er wordt gelogd, maar dit wordt alleen bekeken wanneer er aanleiding is. De korpsleiding moet hier dan toestemming ervoor geven. Alle bevestigingen worden gelogd en tussen de 3 en 5 jaar bewaard.

Gemeenschappelijke verwerkingen vinden in TGO's plaats. De verantwoordelijkheid ligt bij het korps van de TGO-leider. Voor de andere TGO-leden worden externe autorisaties uitgegeven. Gemeenschappelijke verwerkingen worden niet bij het CBP

gemeld omdat de verantwoordelijkheid bij een korps belegd is. Van een gemeenschappelijke verwerking volgens de Wpg is hiermee geen sprake.

4.11.3

Verbeterpunten

Als verbeterpunt is te noemen:

- Zorg voor een protocollering in het autorisatie proces.

4.12 Audits (artikel 33)

4.12.1

Norm

Bij regeling van Onze Ministers kan bepaald worden dat ter voorbereiding op de controle, bedoeld in het eerste lid, interne audits plaatsvinden en kunnen regels worden gesteld over de wijze waarop deze audits worden verricht.

4.12.2

Bevindingen

Het korps Amsterdam-Amstelland beschikt over een interne auditfunctie. De interne (EDP-)auditor heeft in eind 2010 een interne audit naar autorisaties uitgevoerd. Van dit onderzoek is op 23 maart 2011 een rapport verschenen. In 2011 heeft er geen interne audit plaatsgevonden, omdat in dat jaar een externe audit stond gepland. Het voorgaande is beschreven in het jaarplan 2011. Het jaarplan 2012 is in concept gereed. Hierin is aangegeven dat in 2012 een interne audit gehouden zal worden, waarbij aandacht besteed zal worden aan de bevindingen en aanbevelingen uit externe audit 2011.

4.13 Privacy functionaris (artikel 34)

4.13.1

Norm

De privacy functionaris ziet namens de verantwoordelijke toe op de verwerking van politiegegevens overeenkomstig het bij of krachtens de wet bepaalde en dient de verantwoordelijke van advies.

4.13.2

Bevindingen

De privacy functionaris is middels Aanwijzingsbesluit privacy functionaris d.d. 9-6-2009 formeel aangewezen door de korpsbeheerder. De privacy functionaris is op 9-6-2009 aangemeld bij het CPB. Er is een ontvangstbevestiging van het CBP per fax verkregen op 12-12-2011. Op deze fax staat aangegeven dat het CBP de brief en aanwijzingsbesluit heeft ontvangen op 11-6-2009.

De privacy functionaris houdt zich met name bezig met inzageverzoeken en de adviesrol. Het is voor de privacy functionaris mogelijk om, op basis van informatie geleverd door andere organisatieonderdelen, een overzicht te verkrijgen over de protocollering van gegevens. De toezichtstaken zijn echter nog niet ingevuld. Sinds 1 januari 2011 is er een tweede privacy functionaris benoemd. De eerste privacy functionaris heeft deze gedurende 2011 opgeleid in de privacy wetgeving. De wens is om in 2012 de rollen over de twee functionarissen te verdelen. De eerste privacy functionaris zal zich dan richten op de adviesrol en de tweede op de toetsingsrol.

De privacy functionaris heeft voor het jaar 2009 een jaarverslag opgesteld. Voor het jaar 2010 is geen jaarverslag opgemaakt, dit jaar wordt meegenomen in komend jaarverslag van 2011.

4.13.3 *Verbeterpunt*

Borg de toezichthoudende taak van de privacy functionaris, zoals in de Wpg benoemd.

4.14 Functionaris Gegevensbescherming (artikel 36)

De Functionaris Gegevensbescherming bestaat niet als functie bij het korps Amsterdam-Amstelland.