



Ministerie van Veiligheid en Justitie

Audit Wpg politie Haaglanden

Rapport

Datum
Status

16 december 2011
Definitief

Colofon

Afzendgegevens

Departementale Auditdienst

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

Contactpersonen

drs. D. van Ilpenhof RE CISA
drs. ing. B. Numan RO CIA
senior auditors

T 070 370 65 60
F 070 370 48 47
wpg@minvenj.nl

Projectnaam

Audit Wet Politiegegevens

Ons kenmerk

DDS/5718878/11

Auteurs

drs. ing. C.A. van der Spek RA RO

Inhoud

Colofon 3

1 Assurance Verklaring 7

2 Samenvatting 9

3 Inleiding 17

3.1 Algemeen 17

3.2 Aanleiding 17

3.3 Doelstelling, aard en scope van de opdracht 17

3.4 Afbakening 18

3.5 Normenkader 18

3.6 Beperkingen voor de privacy audit 19

3.7 Onderzoeksmethoden en werkwijze 19

3.8 Doelgroep van het rapport 19

4 Bevindingen 21

4.1 Inleiding 21

4.2 Verantwoordelijke (artikel 1.f) 22

4.3 Kwaliteitsaspecten van politiegegevens (artikel 3 en 4) 23

4.4 Gevoelige gegevens (artikel 5) 26

4.5 Autorisatie (artikel 6) 26

4.6 Geautomatiseerd Vergelijken/In Combinatie Met Elkaar Verwerken (artikel 11) 31

4.7 Bewaartermijnen (artikel 14) 32

4.8 Ter beschikking stellen (artikel 15) 35

4.9 Verstrekken (artikel 16/24) 37

4.10 Rechten van betrokkenen (artikel 25/28) 40

4.11 Protocolplicht (artikel 32) 41

4.12 Audits (artikel 33) 42

4.13 Privacy functionaris (artikel 34) 43

4.14 Functionaris Gegevensbescherming (artikel 36) 43

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 Haaglanden.

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 Haaglanden.

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 Haaglanden, naar de stand van juni 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 Haaglanden te nemen maatregelen. Ook is gebleken dat het korps Haaglanden voor het volledig kunnen voldoen aan de Wpg eisen mede afhankelijk is van besluiten die buiten het korps Haaglanden 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 Haaglanden, 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 die hercontrole te laten uitvoeren door de interne auditfunctie van het korps Haaglanden. Het verbeterrapport en de uitgevoerde hercontrole zullen in de navolgende jaren door de privacyauditor worden beoordeeld.

Den Haag, 16 december 2011

De Directeur van de Departementale Auditdienst

A handwritten signature in blue ink, consisting of a large, stylized 'J' followed by 'C' and 'van Praat' in a cursive script.

J.C. van Praat RE RA

2 Samenvatting

Het korps Haaglanden heeft een aantal zaken in opzet opgepakt, zoals een convenanten databank en een interne audit functie. Er was tijdelijk een derde privacyfunctionaris aangesteld. De korpsleiding toont hiermee en met andere initiërende activiteiten haar aandacht aan 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 tijdens de audit een mandaatbesluit overlegd dat aantoont dat de korpsbeheerder de korpschef mandateert voor de uitvoering van de Wpg. De korpschef mandateert vervolgens uitvoerende taken aan aangewezen functies. Bij het korps Haaglanden is hierdoor Inzichtelijk gemaakt wie de (eind)verantwoordelijkheid draagt voor het implementeren van maatregelen om te voldoen aan de Wpg. Hiermee wordt voldaan aan de Wpg.
Art. 3 en 4, Kwaliteitsaspecten van politiegegevens			
8.1 en 9.1	Onderscheid onderzoek Dagelijkse Politietaken (8) versus Bepaald geval (9)		Er is een instructie gegeven aan de bureauchefs en managementteams om het onderscheid tussen artikel 8 en artikel 9 politiegegevens aan alle wijkbureaus kenbaar te maken. Het aandachtspunt blijft echter het daadwerkelijk gebruik van de aangereikte instrumenten (bijvoorbeeld de Wpg-presentatie) voor het verder informeren van het Blauw en de borging van de aandacht voor de Wpg. Hiermee wordt voldaan aan de Wpg.
3.1 t/m 3.3 (8) 4.1 (8)	Noodzakelijkheid (8) Doelbinding Rechtmatigheid Juistheid Volledigheid		De bevoegde functionarissen, informatie-coördinatoren en de privacyfunctionarissen hebben een Wpg-opleiding gevolgd. Deze functies dienen als vraagbaak voor de rest van het korps. De genoemde functionarissen rollen de Wpg kennis uit naar de medewerkers. De centrale Infodesk toetst impliciet op de aspecten zoals gedefinieerd in artikel 3 en 4 Wpg. De toetsingscriteria zijn niet expliciet gemaakt. Bij twijfel wordt de bevoegde functionaris

Norm	Aspect		Bevinding en oordeel
			geraadpleegd. Hiermee wordt deels voldaan aan de Wpg.
3.1 t/m 3.4 (9) 4.1 (9)	Noodzakelijkheid (9) Doelbinding Rechtmatigheid Herkomst en wijze van verkrijging Juistheid Nauwkeurig Volledigheid		Het rechercheproces bevat waarborgen voor deze kwaliteitsaspecten. De controle op deze criteria sluit via het OM en de rechter. Binnen het proces Opsporing wordt gebruik gemaakt van zowel SUMM-IT als BVO, waarbij de gegevens niet altijd in beide systemen worden geregistreerd. De belangrijkste gegevens staan in BVO, de verwerking vindt vaak plaats in SUMM-IT. Om een volledig beeld te verkrijgen moeten beide systemen worden bevraagd. Volledigheid is daardoor niet structureel geborgd. Door het niet altijd invoeren van 'zachte gegevens' wordt mogelijk niet voldaan aan het volledigheidseisen van artikel 4.1 Wpg. Hiermee wordt deels 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		Het korps heeft een aantal gegevensverzamelingen die worden verwerkt op grond van artikel 10. Bij de CIE gebeurt dit volgens het landelijk proceshandboek CIE en de toezichthoudende rol van de CIE-Officier van Justitie. Bij de RID liggen de kwaliteitscriteria al in het doel van de taak vast. Hiermee wordt voldaan aan de Wpg.
4.3	Beveiliging		De ondersteuning vanuit de IT schiet te kort om geheel te kunnen voldoen aan het aspect 'beveiliging van politiegegevens'. De artikelen 8, 9, 10 en 12 zijn van elkaar geïsoleerd. Er vindt echter geen toetsing plaats op het daadwerkelijke functioneren van de isolatie met name op de informatie aangehouden in de KA-omgeving. Daarnaast zijn nog niet alle systemen Wpg proof. Een aantal systemen, waaronder BVH, voldoet niet aan de in de Wpg gestelde bewaartermijnen. Hierdoor ontstaat het risico op onrechtmatig gebruik van politiegegevens. Hiermee wordt niet voldaan aan Wpg.
Art. 5, Gevoelige Gegevens			
	• Gevoelige gegevens		Er zijn geen niet-toegestane gegevensverzamelingen gebaseerd op gevoelige gegevens aangetroffen. Tevens is in de Wpg-training aandacht besteed aan het omgaan met gevoelige gegevens. Hiermee wordt voldaan aan de Wpg.
Art. 6, Autorisatie			
	• Korpsautorisatiematrix		De Autorisatiematrix BIM / Ploeg Primaire Processen bevat een overzicht van functie specifieke applicaties inclusief kleurcoderingen. De kleurcoderingen dienen als criteria voor toekenning van toegang via functieprofielen tot de applicatie. Hiermee wordt voldaan aan de Wpg.

Norm	Aspect	Bevinding en oordeel
• Aanvraagproces		Conform artikel 6.1 Wpg onderhoudt het korps een systeem van autorisaties dat voldoet aan de vereisten van zorgvuldigheid en evenredigheid. Het aanvraagproces is op hoofdlijnen gedocumenteerd. Met name het vormgeven van het proces voor wijzigingen en verwijderingen vergt nog aandacht. Hiermee wordt deels voldaan aan de Wpg.
• Wijziging en verwijdering		Er is onvoldoende controle op het intrekken van autorisaties bij ontslag, mutaties en beëindiging van tijdelijke inzet. De werking van het proces wijziging en verwijdering is niet geborgd. De autorisaties worden alleen verwijderd bij het wisselen van functies. Hiermee wordt niet voldaan aan de Wpg.
• Autorisatiebeheer CIE en RID.		De autorisaties binnen de CIE zijn goed geregeld. De RID kent een strenge beveiliging en autorisaties. De chef CIE en de chef RID zien streng toe op de autorisaties. Hiermee wordt voldaan aan de Wpg.
32.1.c	Protocollering autorisaties	De belegging van autorisatieafhandeling bij BIM en BIS is conform de Wpg. Echter, bij ontslag wordt soms het gebruik van het 'loopbriefje' niet strikt gehanteerd. De werking van het proces is niet geborgd. Hiermee wordt deels voldaan aan de Wpg.
32.3 voor 32.1.c	Bewaren protocolgegevens autorisaties	Het is niet gebleken dat er een overzicht is van alle schriftelijke vastleggingen van de autorisaties. De papieren autorisatieverzoeken worden niet bewaard. De werking van het proces is niet geborgd. Hiermee wordt niet voldaan aan de Wpg.
Art. 11, Geautomatiseerd vergelijken en in combinatie zoeken		
• Hanteerbare interpretatie		Conform artikel 11 Wpg moet een bevoegde functionaris goedkeuring geven voor de verdere verwerking van gerelateerde gegevens. Er is geen eenduidige interpretatie van GV-ICMEV. De werkwijze en goedkeuring is niet geprotocolleerd, waardoor niet wordt voldaan aan artikel 11 Wpg. Hiermee wordt niet voldaan aan de Wpg.
• Aangewezen functionarissen		Er zijn functionarissen aangewezen voor de uitvoering van artikel 11 Wpg verwerkingen. Hiermee wordt voldaan aan de Wpg.
11.4	Bevoegd gezag	Het proces van goedkeuren van verzoeken voor geautomatiseerd vergelijken en in combinatie zoeken is nog niet uitgewerkt. Hiermee wordt niet voldaan aan de Wpg.
32.1.d en 32.1.h	Protocollering 11.1, 11.2, 11.4 en 11.5	Er is geen inzicht in het werkelijke gebruik van GV-ICMEV. De protocollering is nog niet ingeregeld. Hiermee wordt niet voldaan aan de Wpg.
32.3 voor 32.1.d en 32.1.h	Bewaren protocolgegevens 11.1, 11.2, 11.4 en	Er is geen inzicht in het werkelijke gebruik van GV-ICMEV. De protocollering is nog niet geregeld. De werkwijze en goedkeuring zijn niet

Norm	Aspect		Bevinding en oordeel
	11.5		geprotocolleerd. Hierdoor wordt niet voldaan aan de Wpg.
Art. 14, Bewaartermijnen			
8.2 en 8.3	(8) van 1 tot 5 jaar		Er is een procedure om te borgen dat de informatie voldoet aan de bewaartermijnen zoals gesteld in de artikel 8 Wpg. Deze procedure moet nog worden vastgelegd. Er is in de nieuwe release een schoningsmodule in BVH, maar deze staat op landelijk verzoek van de voorzitter van de stuurgroep nog niet aan. Hiermee wordt niet voldaan aan de Wpg.
8.6	(8) verwijderen na 5 jaar		Er is een procedure om te borgen dat de informatie voldoet aan de bewaartermijnen zoals gesteld in de artikel 8 Wpg. De procedure moet nog worden vastgelegd. Hiermee wordt niet voldaan aan de Wpg.
14.1 (8)	(8) vernietigen na 5 jaar verwijderd		Er is geen procedure om te borgen dat de informatie voldoet aan de bewaartermijnen zoals gesteld in de artikel 8 Wpg. De procedure moet nog worden vastgelegd. Hiermee wordt niet voldaan aan de Wpg.
9.4	(9) verwijderen na OH plus ½ jaar		Er is een proces ingericht voor het afmelden van artikel 9 onderzoeken. In 2012 wordt een tool van het korps Hollands-Midden beschikbaar gesteld, waardoor de afmeldingen automatisch plaatsvinden. Hiermee wordt deels voldaan aan de Wpg.
14.1 (9)	(9) vernietigen na 5 jaar verwijderd		Er is een procedure om te borgen dat de informatie voldoet aan de bewaartermijnen zoals gesteld in artikel 9 Wpg. Er is een proces ingericht voor het afmelden van artikel 9 onderzoeken. In 2012 wordt een tool van het korps Hollands-Midden beschikbaar gesteld, waardoor de afmeldingen automatisch plaatsvinden. Er is echter nog geen proces voor het vernietigen na 5 jaar verwijderd. Hiermee wordt niet voldaan aan de Wpg.
10.6	(10) verwijderen na 5 jaar geen subjectwaardige registratie		Twee keer per jaar controleert Officier van Justitie de status van de informant in het systeem. De schoning van het informantenregister gebeurt handmatig. Hiermee wordt voldaan aan de Wpg.
14.1 (10)	(10) vernietigen na 5 jaar verwijderd		De CIE wordt ge-audit door het Ministerie van BZK en de RID staat onder toezicht van AIVD. Twee keer per jaar controleert Officier van Justitie de status van de informant in het systeem. De vernietiging gebeurt handmatig. Hiermee wordt voldaan aan de Wpg.
14.3	Hernieuwde verwerking		Men is op de hoogte dat men voor hernieuwde verwerkingen toestemming moet vragen bij de Officier van Justitie, en bij de meeste medewerkers is bekend dat niet zomaar gegevens van vijf jaar en ouder hiervoor gebruikt mogen worden. De procedure is niet expliciet gemaakt.

Norm	Aspect		Bevinding en oordeel
			Hiermee wordt voldaan aan de Wpg.
32.1.e	Protocollering 14.3		Er is geen procesbeschrijving aanwezig met betrekking tot hernieuwde verwerkingen. Er vindt tevens geen aparte registratie hiervan plaats. Hiermee wordt niet voldaan aan de Wpg.
32.3 voor 32.1.e	Bewaren protocolgegevens 14.3		Er vindt geen protocollering plaats van hernieuwde verwerkingen. Hiermee wordt niet voldaan aan de Wpg.
12.2	(12) verwijderen na 4 maanden		Twee keer per jaar controleert Officier van Justitie de status van informant. De bruto informatie wordt binnen vier maanden netto gemaakt. Hiermee wordt voldaan aan de Wpg.
12.6	(12) controleren en vernietigen		Twee keer per jaar controleert Officier van Justitie de status van informant, schoning gebeurt handmatig. Hiermee wordt voldaan aan de Wpg.
Art. 15, Ter beschikking stellen			
	• Infodesk voor bevraging		De informatieverzoeken worden gericht aan de lokale informatieknooppunten en aan de regionale front-office BRI. Er vindt door de Infodesk geen expliciete toetsing plaats op de aspecten zoals gedefinieerd in artikel 3 en 4 Wpg. Op basis van vertrouwen wordt de informatie ter beschikking gesteld. De infodesk benadert de bevoegde functionaris voor toestemming. Hiermee wordt deels voldaan aan de Wpg.
	• Codering		Het korps heeft geen algeheel proces voor codering van informatie van onderzoeken. Wel toetst de centrale Infodesk impliciet op de aspecten zoals gedefinieerd in art. 3 en 4 Wpg. Hiermee wordt voldaan aan de Wpg.
	• Aanwijzing Bevoegd Functionaris		Het korps heeft bevoegde functionarissen benoemd. Hiermee wordt voldaan aan de Wpg.
	• Opleiding Bevoegd Functionaris		Het korps heeft bevoegde functionarissen Wpg-opleidingen gegeven. Hiermee wordt voldaan aan de Wpg.
15.2	Weigeringsgronden		Niet is vastgesteld of de weigeringsgronden die zijn vastgesteld bij Algemene Maatregelen van Bestuur daadwerkelijk worden uitgevoerd en of er zich buiten deze gronden andere weigeringen hebben plaatsgevonden. Het korps Haaglanden kent een centrale Front Office (Regionale Infodesk) en lokale Infodesks op elk wijkbureau. De toetsing van de kwaliteitscriteria wordt toegepast. Twee medewerkers van Infodesks en alle medewerkers van de Front Office zijn een Wpg-training aangeboden. Daarmee zijn de Infodesk medewerkers geïnformeerd over het toepassen van de kwaliteitscriteria. Hiermee wordt voldaan aan de Wpg.

Norm	Aspect	Bevinding en oordeel
Art. 16 t/m 24, Verstrekking		
• Verstrekkingenwijzer (landelijk)		In opzet voldoet het korps aan de Wpg gezien de aanwezigheid van de landelijke verstrekkingwijzer op intranet. Het ontbreekt echter aan algemene bekendheid voor alle medewerkers waardoor de werking niet kan worden aangetoond. Hierdoor wordt deels voldaan aan de Wpg.
• Proces voor convenanten		Het proces voor artikel 20 besluiten voldoet aan de vereisten vanuit de Wpg. Er is echter geen borging van de naleving op dit proces. Het korps gaat hiervoor een actieplan opstellen. Hiermee wordt deels voldaan aan de Wpg.
• Proces voor Art. 20 Besluiten		Het proces voor convenanten voldoet aan de vereisten vanuit de Wpg. Er is geen borging van de naleving op dit proces. Het korps gaat hiervoor een actieplan opstellen. Hierdoor wordt deels voldaan aan de Wpg.
• Verstrekkingenschema (regio)		Binnen Haaglanden is voor het verstrekken van informatie de zogenaamde ABC-procedure ontwikkeld. Middels deze procedure wordt duidelijk gemaakt onder welke voorwaarden er mag worden verstrekt. Hierdoor wordt voldaan aan de Wpg.
• Proces voor geautomatiseerde verstrekking		Er is inzichtelijk gemaakt welke geautomatiseerde verstrekkingen naar welke partijen plaatsvinden. Toetsing op juridische gronden vindt tevens plaats. Er is echter geen procedure beschikbaar voor de aanvraag van geautomatiseerde verstrekkingen en er kan achteraf niet worden bepaald over welke personen er automatisch is verstrekt. Hierdoor wordt deels voldaan aan de Wpg.
7.2	Geheimhouding	De checklist voor convenanten bevat de attendering op de noodzaak tot geheimhouding bij een verstrekking. Het Blauw is tevens geattendeerd op het belang van het wijzen van de ontvangende partij op de noodzaak tot geheimhouding. Hiermee wordt voldaan aan de Wpg.
32.1.f	Protocollering verstrekking	Slechts een deel van de geïnterviewden is bekend met protocollering d.m.v. I-90 of E 62, dit wordt nog niet door alle medewerkers gebruikt. Het gebruik van een I-90 / en E 62 vertoont wel een stijgende lijn. Dit wordt maandelijks gemonitord per bureau. Op basis van de beschikbare informatie kan niet worden vastgesteld welk bureau informatie verstrekt zoals vastgelegde procedure. Hiermee wordt niet voldaan aan de Wpg.
32.3 voor 32.1.f	Bewaren protocolgegevens verstrekking	De wél ingevulde protocollering wordt bewaard minimaal tot de laatste controle. Hiermee wordt voldaan aan de Wpg.
• Toezicht door leidinggevend op verstrekkingen en protocollering		Toezicht op verstrekkingen bestaat. Toezicht op protocollering is niet effectief gebleken gezien het feit dat niet alle verstrekkingen schriftelijk worden

Norm	Aspect		Bevinding en oordeel
			vastgelegd. Hiermee wordt deels voldaan aan de Wpg.
Art. 25 t/m 31, Rechten van de betrokkene			
25.1	Verzoek om kennisneming		Er is een procesbeschrijving om het inzage-recht van betrokkenen te kunnen afhandelen. Dit proces is conform de Wpg. Er zijn in 2010-2011 geen klachten over de inzagenprocedure binnengekomen. Hiermee wordt voldaan aan de Wpg.
28.1 t/m 28.3	Correctie		Uit de gesprekken blijkt dat correctieverzoeken in behandeling worden genomen. Er hebben zich enkele correctieaanvragen voorgedaan, hier hebben zich geen klachten voorgedaan. Hiermee wordt voldaan aan de Wpg.
Art. 32, Protocolplicht (32.1.c, d, e, f en h behandeld bij thema's)			
9.2 en 32.1.a	Protocollering doel onderzoek		Alle nieuwe onderzoeken moeten worden geregistreerd middels een MRO voordat een onderzoek wordt aangemaakt in BVO. Hiermee wordt voldaan aan de Wpg.
32.3 voor 32.1.a	Bewaren protocolgegevens doel onderzoek		De MRO-formulieren worden vastgelegd en inzichtelijk gemaakt in de applicatie I-BASE. Hiermee wordt voldaan aan de Wpg.
13.4 en 32.1.b	Protocollering Art. 13 gegevensverzameling en		Er vindt geen protocollering van artikel 13 gegevens plaats van de lokale gegevensverzamelingen. De landelijk ter beschikking gestelde gegevens vinden plaats door middel van de landelijke protocollen. Deze heeft het korps echter nog niet definitief vastgesteld, het korps is nu bezig dit actiepoint op te pakken. Hiermee wordt deels voldaan aan de Wpg.
32.3 voor 32.1.b	Bewaren protocolgegevens Art. 13 gegevensverzameling en		Er vindt geen protocollering van artikel 13 gegevens plaats van de lokale gegevensverzamelingen. De landelijk ter beschikking gestelde gegevens vinden plaats door middel van de landelijke protocollen. Deze heeft het korps echter nog niet definitief vastgesteld, het korps is nu bezig dit actiepoint op te pakken. Hiermee wordt deels voldaan aan de Wpg.
32.1.g	Protocollering onrechtmatige handeling		De privacyfunctionaris houdt in een Excel-bestand een overzicht bij van de privacy schendingen die er zich hebben voorgedaan. De privacy functionaris acteert op basis van deze lijst. Hiermee wordt voldaan aan de Wpg.
32.3 voor 32.1.g	Bewaren protocolgegevens onrechtmatige handeling		De privacyfunctionaris houdt in een Excel-bestand een overzicht bij van de privacy schendingen die er zich hebben voorgedaan. Hiermee wordt voldaan aan de Wpg.
32.2	Gemeenschappelijke verwerking		Niet van toepassing. Uit de audit is niet gebleken dat het korps gemeenschappelijke verwerkingen

Norm	Aspect		Bevinding en oordeel
			verricht.
Art. 33, Audits			
RPAP 3.1	Interne audit-functie		Het korps heeft een interne auditfunctie die een interne audit over 2011 heeft uitgevoerd. Hiermee wordt voldaan aan de Wpg.
RPAP 3.4	Interne audit-plan		Er is geen interne audit-plan opgesteld door het Korps Haaglanden. In het Project Initiatie Document staat alleen het voornemen om jaarlijks een deel van het korps te auditen. Hiermee wordt niet voldaan aan de Wpg.
RPAP 3.6	Interne audit-rapport		In 2010 is geen Wpg-audit gehouden. Er is één auditrapport beschikbaar over 2011. De audit is verricht op basis van een gedegen onderzoek. De hieruit volgende aanbevelingen dienen echter terug te komen in actieplannen van het korps en prioritering van de auditactiviteiten in het komend jaar. Hiermee wordt deels voldaan aan de Wpg.
Art. 34, Privacyfunctionaris			
34.1 en 34.4	Benoemd en gemeld		Er zijn twee privacyfunctionarissen aangesteld en gemeld bij het CBP. Hiermee wordt voldaan aan de Wpg.
34.2	Overzicht over protocollering		Er is een overzicht beschikbaar voor 2009 over aangemelde onderzoeken, maar niet over mutaties op autorisaties, vastlegging van verstrekkingen etc. Er zijn nog geen gegevens beschikbaar voor 2010/2011. Hiermee wordt deels voldaan aan de Wpg.
34.3	Jaarverslag		De privacyfunctionaris heeft een jaarverslag opgesteld over 2010, het jaarverslag van 2011 was ten tijde van de audit nog in ontwikkeling. Echter komt de privacyfunctionaris niet voldoende toe aan alle toezichthoudende taken, mede doordat deze ten dele nog moeten worden ingericht en daarmee is het jaarverslag nog niet volledig. 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 Haaglanden 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 uitgevoerd bij het korps Haaglanden in de maanden juni en november 2011.

3.2 Aanleiding

De 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 korps Haaglanden.

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 juni 2011, van maatregelen en procedures, waarmee het korps

Haaglanden 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)
- Privacyfunctionaris (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 korps. Pas wanneer wij, tijdens het uitvoeren van de audit bij een korps, 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 korps Haaglanden. Dit betekent dat wij geen onderzoek hebben verricht naar door de vtsPN aan het korps Haaglanden geleverde faciliteiten, voor zover de verantwoordelijkheid daarvoor is belegd bij de vtsPN of bij anderen dan het korps Haaglanden.

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 korps Haaglanden en het Openbaar Ministerie, deelwaarnemingen in de procesbeschrijvingen en andersoortige documentatie en deelwaarnemingen in informatiesystemen.

Wij hebben onze werkzaamheden uitgevoerd in de periode van juni 2011 en november 2011.

Het conceptrapport met bevindingen is in juni 2011 besproken met de korpschef van het korps Haaglanden en september 2011 met de korpsbeheerder. 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 J.J. van Aartsen;
- de korpschef Mr. H.P. van Essen;
- de Hoofd Officier van Justitie mr H.C.D. Korvinus
- de Privacy Functionaris [REDACTED];
- de voorzitter van het College Bescherming Persoonsgegevens.

Het rapport mag uitsluitend met toestemming van de korpsbeheerder dan wel de korpschef van het korps Haaglanden aan derden ter beschikking worden gesteld.

¹ Tot aan september 2010 was een derde Privacyfunctionaris aangesteld.

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

4 Bevindingen

4.1 Inleiding

De 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

Het korps Haaglanden heeft de coördinatie omtrent de Wpg voldoende belegd. Zowel de projectleider Wpg, als de privacyfunctionarissen spelen hierbij een belangrijke rol. De privacyfunctionarissen zijn onderdeel van Bureau Integriteit en Security (BIS). Het BIS wordt door geïnterviewden genoemd als een centraal kennis- en informatiepunt, waarbinnen de privacyfunctionarissen als aanspreekpunt optreden.

Algemene aandachtspunten die bij de audit binnen Politie Haaglanden naar voren zijn gekomen, zijn:

- Op de werkvloer is behoefte aan werkinstructies, stroomschema's etc. waarin de regelgeving van de Wpg concreet en helder wordt beschreven. Dit biedt de functionaris handvatten bij het uitvoeren van de dagelijkse werkzaamheden conform de Wpg.
- De toekenning van autorisaties vindt plaats middels een handmatige procedure met kans op fouten. Wij adviseren om hier steekproefsgewijs een controle op uit te voeren. De autorisatie aanpassingen bij functiewisselingen verlopen niet automatisch. Deze procedure verdient daarom nog de nodige aandacht.
- De informatie die wordt aangehouden op de groepsschijven en persoonlijke schijven, die binnen het korps middels de kantoorautomatisering wordt gebruikt, voldoet niet aan de Wpg-vereisten. Wij adviseren het korps om de inrichting van de mappenstructuur te herzien conform de Wpg.

4.1.2

Bekendheid met de Wpg binnen de organisatie

Het korps Haaglanden heeft de bevoegde functionarissen, informatiecoördinatoren en de privacyfunctionarissen een Wpg-opleiding gegeven. Deze functionarissen dienen als vraagbaak voor de rest van het korps. Vanwege de opleidingsdruk binnen het korps is ervoor gekozen om niet iedere individuele medewerker volgens een eenduidige structuur op te leiden over de Wpg.

Wel staat het onderwerp in overleggen op meerdere niveaus op de agenda. Tevens zijn er diverse presentaties voor de medewerkers op alle bureaus aangeboden. Uit interviews blijkt dat in de initiële politieopleiding onvoldoende aandacht wordt geschonken aan het onderwerp Wpg. Hierdoor bestaat het risico dat een deel van het korps onvoldoende kennis heeft van de Wpg.

Het doel van de Wpg, onder voorwaarden delen van informatie, wordt 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 verder toenemen.

De Wpg maakt onderdeel uit van het werkproces en wordt deels ook afgedwongen door het werkproces, maar komt niet als zodanig terug in iedere overweging die wordt gemaakt.

4.1.3

Wpg en de praktijk

De Wpg wordt als multi-interpretabel ervaren. Daardoor zijn er in het land verschillende uitwerkingen.

- Artikel 11: het korps is voor artikel 11, geautomatiseerd vergelijken en in combinatie met elkaar verwerken, continu aan het zoeken naar de grenzen.
- Daarnaast zijn op landelijk niveau weinig regels in de Wpg gekoppeld aan de werkzaamheden van de RID. Dit maakt het voldoen aan de Wpg voor deze afdeling lastig. De RID van het korps Haaglanden heeft daarom zelf een AO-beschrijving opgesteld voor haar afdeling conform de Wpg.
- Doordat momenteel de informatie in drie verschillende informatiesystemen moet worden geregistreerd en vanwege de geringe ondersteuning vanuit de informatiesystemen, is men tijd kwijt met het invullen van BVH en BVO. Derhalve wordt de Wpg als extra last ervaren.
- Schonings- en bewaartermijnen worden soms als knellend ervaren. De functionarissen willen informatie graag langer dan 1 jaar gebruiken. Doordat de informatiesystemen deze informatie na 1 jaar niet achter slot zetten, wordt de informatie in de praktijk ook vaak langer dan 1 jaar gebruikt. Door het gericht zoeken met specifieke 'hit – no hit' resultaten kan langer dan 1 jaar in de gegevensverzameling worden gezocht en heeft men geen last van het 1 jaar schot.
- Het landelijke knelpunt met betrekking tot de registratie van zachte informatie draagt bij aan de toename van de administratieve last. De systemen worden als gebruiksonvriendelijk ervaren. De administratieve last en de gebruiksonvriendelijkheid van de systemen vormen tezamen een belemmering voor het vastleggen van deze informatie. Het gevolg hiervan is dat de informatie in de informatiesystemen onvolledig is en dat de informatie niet kan worden gedeeld.
- Daarnaast wordt tijdens of na afloop van een zaak weinig restinformatie middels een rest proces-verbaal opgeslagen.

4.2 Verantwoordelijke (artikel 1.f)

Mandaatbesluit

Net als onder de 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.

Conform artikel 1f Wpg is door het korps Haaglanden een mandaatbesluit opgesteld waarin formeel wordt aangeduid dat de Korpsbeheerder zijn mandaat geeft aan de korpschef voor het implementeren van maatregelen om te voldoen aan de Wpg.

De korpschef van het korps Haaglanden heeft vervolgens in het 'Besluit Ondermandaat Wet politiegegevens' de betreffende taken en bevoegdheden ondergemandateerd. Per Wpg-artikel is aangegeven aan welke functie het ondermandaat is toegewezen.

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

De projectleider Wpg en de privacyfunctionarissen hebben presentaties opgesteld voor de voorlichtingssessies. De presentaties zijn toegespitst op de Wpg-aspecten waarmee het desbetreffende bureau te maken heeft. De voorlichtingen zijn aangeboden aan alle (19) wijkbureaus, specifiek aan de managementteams en de wijkagenten. Daarbij heeft men het principe van teach-the-teacher gehanteerd.

In deze presentaties heeft men het onderscheid tussen artikel 8 en artikel 9 gegevens op een eenvoudige manier kenbaar proberen te maken. De presentaties wijzen tevens op de kwaliteitsbeginselen inherent aan het politieproces, namelijk de borging van rechtmatigheid, doelbinding etc.

Uit de interviews en de Wpg-presentaties blijkt men de stelregel te hanteren dat onderzoeken die meer dan 72 uur kosten en de inzet van BOB (Bijzonder Opsporings Bevoegdheden)-middelen vereisen, onder artikel 9 worden geschaard.

Een aandachtspunt blijft het daadwerkelijk gebruik van de aangereikte instrumenten (bijvoorbeeld de Wpg-presentatie) voor het verder informeren van het 'Blauw' en de borging van de aandacht voor de Wpg.

Rechtmatigheid

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.

Het korps Haaglanden kent een centrale Front Office (de Regionale Infodesk) en lokale Infodesks op elk wijkbureau. De toetsing van de kwaliteitscriteria (doelbinding, noodzaak etc.) wordt stringenter toegepast bij de Front Office dan bij de lokale Infodesks. Twee medewerkers per lokale infodesks (in totaal ongeveer 40 medewerkers) en alle medewerkers van de Front Office hebben een Wpg-training gevolgd. Daarmee zijn de Infodesk medewerkers geïnformeerd over het toepassen van de kwaliteitscriteria.

Bij de decentrale Infodesks wordt het voldoen aan deze criteria bij de eerste vastlegging van gegevens minder stringenter toegepast. Zij accepteren zonder nadere toetsing de ontvangen informatie. Voor zover het in hun vermogen ligt, zullen zij wel aandacht besteden aan de vereiste criteria, doch de toetsing vanuit die positie is relatief beperkt te noemen.

De decentrale Infodesks toetsen impliciet op de aspecten zoals gedefinieerd in artikel 3 en 4. De toetsingscriteria zijn niet expliciet gemaakt. Bij twijfel wordt de bevoegd functionaris geraadpleegd.

Bij de bijzondere informatie verwerkende afdelingen als de CIE (Criminele Inlichtingen Dienst), OOV (Openbare Orde en Veiligheid) en de RID (Regionale Inlichtingendienst) wordt aan deze aspecten vanwege de aard van hun taakstelling specifiek aandacht besteed. Daarbij is in de opzet het voldoen aan deze criteria,

zeker bij de CIE vanwege de toezichthoudende rol van het OM (de CIE OvJ) en het landelijk gebruik van het proceshandboek CIE, goed verzorgd.

De verstrekingsrapporten (ofwel ter beschikingsstellingsrapporten) worden opgemaakt door de afdeling RID, CIE en OOV in BVH, BVO en I-Base. Alleen OOV werkt in de applicatie I-Base. De informatie wordt ter beschikking gesteld aan andere afdelingen op basis van het need-to-know principe. Daarbij wordt de noodzaak tot informatiedeling bewaakt.

Kwaliteit

De medewerkers maken steeds de afweging welke politiegegevens relevant zijn en muteren alleen deze gegevens. Deze afweging is gebaseerd op de tijd die het kost om de mutatie te maken en of deze informatie van nut kan zijn voor de uitvoering van de politietaak.

Er vindt niet op alle bureaus controle plaats op de kwaliteit van de processen-verbaal. Op mutaties vindt geen controle plaats. Verder is er geen controle op de inhoudelijke registratie van de feiten geconstateerd. De invoercontrole vindt nagenoeg niet plaats wat nadelig voor de kwaliteit van de politiegegevens kan zijn. Er is geconstateerd dat bepaalde 'velden' in de systemen zoals personalia, adressen en huisnummers niet of verkeerd worden ingevoerd. Dit resulteert in dubbele persoonskaarten of het niet kunnen lokaliseren van een incident. In een aantal gevallen is aan bepaalde personen een controlerol toegewezen, maar deze blijken alleen te controleren of een aantal verplichte velden is ingevuld.²

Uit gesprekken blijkt dat wanneer een onjuistheid in de gegevens wordt geconstateerd het onduidelijk is waar dit moet worden gemeld, of men vindt het de moeite niet dit te melden.

Alle medewerkers die geautoriseerd zijn voor BVH hebben hiervoor in 2009 de opleiding gehad. In november 2011 is gestart met de cursus 'verbetering kwaliteit BVH'. Maar controle op de invoer in BVH ontbreekt in de praktijk vaak.

Voor artikel 9 onderzoeken geldt dat de aanmelding geschiedt via een artikel 9/10 aanmeldingsformulier dat naar vtsPN en naar de afdeling BIS wordt gestuurd. De Melding recherche onderzoek (MRO) bevat het aanmeldingsformulier. Na melding zorgt de afdeling BIM voor de toegang tot een BIS-schijf.

In de applicatie VROS worden de subjecten met elkaar gematched. Middels VROS kan worden nagegaan of een onderzoek in een regio is geregistreerd.

Naast BVO wordt gebruik gemaakt van SUMM-IT. Er is een koppeling tussen BVO en SUMM-IT. SUMM-IT wordt gevoed met informatie uit BVO. Dit is geen tweerichtingsverkeer. De informatie ingevoerd in SUMM-IT komt niet direct in BVO terecht. Alleen de meldingen MRO-subjecten worden in BVO teruggemeld door de onderzoeken die in SUMM-IT draaien. Er wordt binnen het korps nog niet (structureel) gewerkt met SUMM-IT. De gegevens worden niet (structureel) geregistreerd in zowel SUMM-IT als in BVO, waardoor deling van gegevens niet volledig plaatsvindt binnen de politieorganisatie. Waarschijnlijk zal begin 2012

² Per 1 maart 2012 zal het systeem TrueBlue in gebruik worden genomen die deze controle kan uitvoeren.
Pagina 24 van 43

SUMM-IT de applicatie BVO vervangen. Met deze vervanging wordt dit probleem opgelost.

De gegevensverzamelingen in SUMM-IT en BVO zijn niet gelijk, waardoor bevragers bij eenzelfde zoekvraag verschillende resultaten kunnen krijgen. Alle subjecten en objecten die belangrijk zijn voor het onderzoek, worden in SUMM-IT en in BVO ingevoerd. Derhalve zal de zoekvraag gericht op deze subjecten en objecten dezelfde uitkomst hebben. Bovendien wordt onderzoeksinformatie op de persoonlijke 'schijven' aangehouden voorafgaand aan de formele start van een onderzoek. De onderdelen van de politie die geen gebruik maken van SUMM-IT beschikken derhalve mogelijk niet over de volledige informatie. Hiermee wordt deels voldaan aan de volledigheidseis conform art. 4.1 Wpg.

Het is niet nodig om alle informatie zowel in BVO als in SUMM-IT te registreren. Bijna alle onderzoeken starten namelijk in BVH. Door het ontbreken van de koppeling met BVO wordt de informatie niet automatisch in BVO of in SUMM-IT ingevoerd. Nu bestaat dus de kans, dat artikel 9 onderzoeken (alleen) in BVH in plaats van BVO staan. Daarbij komt dat op rechtmatigheid én inhoudelijke kwaliteit onvoldoende controle wordt uitgeoefend in BVH. Hiervoor wordt inmiddels de applicatie BOSZ gebruikt. Middels BOSZ kan de status van onderzoeken worden geregistreerd.

Daarnaast zijn nog niet alle systemen Wpg-proof. Een aantal systemen, waaronder BVH, voldoet niet aan de in de Wpg gestelde bewaartermijnen. Hierdoor ontstaat het risico op onrechtmatig gebruik van politiegegevens.

De IT schiet tekort in het labellen van informatie. Daarmee is geen onderscheid te maken tussen artikel 8 en artikel 9 informatie. Er bestaat de mogelijkheid aan informatie een label te hangen, hetzij door een 'label' hetzij door het invullen van een vrij informatieveld. Voor beide artikelen geldt een verschillende bewaartermijn. Op dit moment wordt er één bewaartermijn gehanteerd in BVH, waarmee niet wordt voldaan aan de gestelde bewaartermijn van de Wpg.

Verder blijkt dat medewerkers soms BVO te ingewikkeld vinden waardoor men niet alle informatie registreert. Vooral zogeheten 'zachte informatie' kan hierdoor verloren gaan. Zachte informatie bestaat uit signalen die niet direct strijdig zijn met de wet, maar mogelijk van belang zijn voor de Handhaving of een indicatie geven over een persoon of zijn gedrag. Tevens blijkt de 'zachte informatie' lastig registreerbaar te zijn voor sommige gebruikers van BVH.

De zachte informatie wordt vastgelegd in mutaties. Deze informatie kan niet aan een subject worden gehangen. Door het niet altijd registreren van 'zachte gegevens' wordt mogelijk niet voldaan aan het volledigheidseis van artikel 4.1 Wpg.

Beveiliging

De algemene beveiligingseis van de Wpg is bij de Nederlandse Politie sinds jaar en dag uitgewerkt in de Regeling Informatiebeveiliging Politie (RIP) en het Basis Beveiligingsniveau Nederlandse Politie (BBNP). Op landelijk niveau is men bezig de RIP en de BBNP te actualiseren naar de huidige stand der techniek. Binnen het korps Haaglanden wordt door een werkgroep korpsbreed het integraal beveiligingsbeleid nader uitgewerkt.

Logging

Het systeem BVH biedt verscheidene mogelijkheden voor logging, waarbij automatisering is geleverd om deze logging te lezen. In BVO worden onder andere

de naam, datum, tijd en de mutaties vastgelegd en weergegeven. Deze gegevens zijn in de praktijk nog niet altijd goed te gebruiken, waardoor het ook onduidelijk is hoe lang deze informatie wordt bewaard.

Veelal vindt alleen controle plaats door middel van logging indien er sprake is van het vermoeden van een integriteitsincident.

Fysieke beveiliging

De bureaus zijn allen voorzien van toegangsbeveiliging middels sleutels, het ITRS-toegangssysteem en camerabeveiliging.

Op de wijkbureaus staan soms bij de Infodesk kasten open die niet aan het eind van de werktijd worden afgesloten. Het afsluiten van de kasten is van belang, omdat de Infodesk medewerkers zijn geautoriseerd om meer politiegegevens te verwerken dan een medewerker basispolitiezorg.

Verwerken gegevens buiten BVO

De gegevens die worden verwerkt in de Kantoorautomatisering (KA) worden geregeld op de eigen schijf opgeslagen. Daarnaast wordt ook gebruik gemaakt van de bureauschijf, de ploegschijf en de researchschijf.

De eigen 'schijven' worden niet geschoond conform de geldende bewaartermijnen. Hierdoor wordt niet aan de Wpg voldaan.

4.3.3

Verbeterpunten

Als verbeterpunten zijn te noemen:

- Het aanbieden van praktische handreikingen voor toetsing op de in artikel 3 en 4 genoemde kwaliteitscriteria van de politiegegevens bij binnenkomst van de politieorganisatie.
- Het verder organiseren de toezichtstaak op de kwaliteitscriteria 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

Binnen het korps Haaglanden worden alleen gevoelige gegevens geregistreerd indien dat noodzakelijk is voor uitoefening van de politietaak. Dit uitgangspunt wordt door het hele korps gehanteerd. In de opleiding is aandacht besteed aan het terughoudend (indien onvermijdelijk) registreren van gevoelige gegevens.

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

In 2010 is een centraal gebruikersregister beschikbaar gesteld. Het centraal gebruikersregister is gekoppeld aan het personeelssysteem (SAP). De medewerker krijgt op grond van zijn/haar functie een bepaald gebruikersprofiel toegewezen. Het gebruikersprofiel geeft toegang tot alle applicaties die bij die betreffende functie horen. Binnen het gebruikersprofiel zijn weer verschillende functies mogelijk. Zodra een medewerker een nieuwe functie verkrijgt, veranderen de bevoegdheden tot systemen, autorisaties en de toegang tot een ploegschijf.

De lijn is verantwoordelijk voor de zorg voor de juiste autorisaties. Regelmatig zal worden gecontroleerd of medewerkers ook gebruikmaken van de applicaties waarvoor zij zijn geautoriseerd. Indien een gebruiker feitelijk geen gebruikmaakt van een applicatie, dan kan de autorisatie weer worden ingetrokken. Het toezicht hierop ligt bij de privacyfunctionarissen. De autorisatieverzoeken worden afgehandeld door de afdeling BIM.

Op hoofdlijnen is de basisopzet van het autorisatieproces beschreven met een verwijzing naar een basisprofiel en een applicatieprofiel gebaseerd op een specifieke aanvraag voor een specifiek profiel. De autorisatieprofielen per applicatie zijn onderverdeeld in drie matrices:

- Basisprofiel.
- Profiel voor samenwerkingsverbanden.
- Specifiek profiel waar op basis van de aanvraag autorisaties voor losse applicaties worden verleend.

De Autorisatiematrix BIM / Ploeg Primaire Processen bevat een overzicht van functie specifieke applicaties, inclusief kleurcoderingen voor criteria voor toekenning van toegang via functieprofielen tot de applicatie.

De bureauchefs en hun plaatsvervangers zijn bevoegd te tekenen voor het toekennen van de autorisaties.

Autorisatieproces

Alle autorisatieverzoeken komen bij de afdeling BIM binnen. Het aanvragen van autorisaties vindt plaats door middel van autorisatieformulieren. Het is een handmatige procedure, waarbij autorisaties zijn gekoppeld aan de functie. Het korps werkt aan een digitale procedure.

De (plaatsvervangende) bureauchefs zijn bevoegd voor het (goed)keuren van autorisatieverzoeken. Het korps hanteert gestandaardiseerde formulieren voor afhandeling van autorisatieverzoeken. Deze formulieren worden ondertekend door de chef. Niet-ondertekende formulieren worden door de afdeling BIM niet in behandeling genomen.

Tevens is voor een deel van de applicaties het volgen van een opleiding vereist. De afdeling BIM autoriseert medewerkers voor de digitale cursussen (de zogenaamde E-learning). De afdeling BIM verifieert of een medewerker de cursus succesvol heeft afgerond, voordat het autorisatieverzoek wordt gehonoreerd.

Het intrekken van de autorisaties verloopt niet altijd optimaal. De controle bij uit diensttreden (door middel van het loopbriefje) is niet optimaal en voor verbetering vatbaar.

Op de 'wachtcommandant PC's' waarop NSIS/LIST, OPS en de RDW worden geraadpleegd, wordt soms op andermans of het algemene account gewerkt. Het raadplegen van politiegegevens op de 'wachtcommandant PC's' is voor elke ambtenaar toegestaan gezien de aard van de gegevens.

Inventarisatie autorisaties

Haaglanden heeft nog geen controle uitgevoerd op de rechtmatigheid van alle autorisaties. Het korps is in het proces van het inzichtelijk maken van de huidige autorisaties op de systemen. De autorisaties zijn inzichtelijk gemaakt in de gebruikersregisters op intranet.

Bij het gebruikersregister wordt een beroep gedaan op de eigen verantwoordelijkheid ten aanzien van autorisaties. Na het inloggen wordt een overzicht van alle autorisaties getoond. De bedoeling is dat niet meer van toepassing zijnde autorisaties uit eigen beweging worden beëindigd.

In deze voorgestelde opzet van het gebruikersregister, wordt de eerste bewaking van de evenredigheid van autorisaties belegd bij de individuele medewerker zelf.

Controle steekproeven

Het korps is voornemens om middels steekproeven de benodigde autorisaties te verifiëren. De steekproef zal zich primair richten op de systemen BVH en BVO. Het korps heeft het actieplan nog niet gedocumenteerd.

Een centraal inzicht in de noodzakelijke autorisaties ontbreekt. Het risico bestaat dat de privacyfunctionaris onvoldoende kan controleren op de evenredigheid en zorgvuldigheid van de autorisaties van alle individuele medewerkers. Het korps heeft dit probleem onderkend en is voornemens een actieplan te definiëren om de wenselijke lijst van autorisaties inzichtelijk te maken. Hiermee wordt deels voldaan aan de Wpg.

BVO

Een aanvraag voor een onderzoek wordt middels een MRO ingediend. Zodra deze is goedgekeurd door de afdeling BIS, wordt hiervoor ruimte in BVO aangemaakt. De teamleider kan vervolgens zelf de autorisaties aan zijn medewerkers toekennen. De openheid en transparantie van de onderzoeken in BVO is korpsbreed geregeld. Dit houdt in dat alle politieambtenaren (recherche) op autorisatie niveau 3 of 4 alle onderzoeken in BVO kunnen raadplegen. Voor nadere informatie moet men de bevoegde functionaris benaderen.

De controle op het afmelden van onderzoeken in BVO vindt handmatig plaats door de privacyfunctionaris. In het korps Hollands-Midden is een tool aanwezig om digitaal de afmelding te regelen, deze zal in 2012 ook beschikbaar worden gesteld in het korps Haaglanden.

Autorisaties GENESYS

De voorganger van BVH was GENESYS. Eind 2010 zijn alle autorisaties van de gebruikers ingetrokken waardoor er geen toegang meer is tot dit systeem. Afscherming van de politiegegevens heeft dan ook nog niet plaats gevonden vanwege de overgang naar BVH, maar is geborgd doordat alle autorisaties zijn ingetrokken. Er is nog toegang bij enkele medewerkers van BIS, BIM en bij cold

cases. Via integraal bevragen is door iedereen te zien of er iets staat in GENESYS. Nadat toestemming is verkregen van de afdeling BIS kan informatie worden gebruikt.

BVO en SUMM-IT

Het proces voor autorisatie tot BVO en SUMM-IT is in de huidige opzet toereikend. De politiegegevens worden slechts verwerkt door ambtenaren van de politie die daartoe door de verantwoordelijke zijn geautoriseerd en voor zover de autorisatie strekt.

Uit de interviews blijken enkele incidenten:

- Voor BVO en SUMM-IT zijn er medewerkers die toegang verkrijgen middels een account van een collega. Het gaat hier om tolken die beëdigd zijn en alleen toegang tot de tapmodule hebben op hun eigen toegewezen zaak. Dit geldt ook voor nieuwe medewerkers. Het verkrijgen van de daadwerkelijke toegang duurde dusdanig lang dat het de uitvoering van de politietaak in de weg stond. Hiervoor geldt dat de medewerkers sneller de cursussen moeten volgen (voorwaarde voor toegang tot het systeem) en dat de afdeling HRM en de afdeling BIM de aanvraag en afhandeling sneller moeten verwerken.
- Wanneer een zaak niet is afgemeld hebben alle functionarissen met de toegekende autorisatie voor het onderzoek nog steeds toegang tot de specifieke zaak. De medewerkers van het team krijgen wekelijks nog hits op objecten via de e-mail wanneer de zaak nog niet is afgemeld. Dit wordt gebruikt als signalering dat de zaak nog moet worden afgemeld.

Restinformatie

Het korps Haaglanden heeft een procedure voor het extraheren en voor verdere verwerking van de restinformatie. Deze staat beschreven in de procesbeschrijving Team Grootchalig Optreden. In de praktijk komt het voor dat de tijd om de restinformatie volledig uit te werken te kort is.

Aanmaken onderzoeken in BVO

Standaard wordt voor ieder team/bureau door de functioneel beheerder vijf lege onderzoeken aangemaakt in BVO. De bevoegd functionaris dient op intranet een melding formulier BVO / SUMM-IT in te vullen voor de officiële aanvraag van het onderzoek. Het formulier gaat vervolgens naar de afdeling BIS en de vtsPN. De afdeling BIS verwerkt de aanvraag in I-Base. VtsPN heeft een systeem, expert desk, waarmee de formulieren worden opgehaald door de functioneel beheerders. De functioneel beheerders van het korps Haaglanden vullen aan de hand van het opgehaalde formulier het unieke nummer in BVO in. De bevoegd functionaris/teamleider (autorisatie niveau 7) laat de coördinator autorisaties aan zijn medewerkers van het onderzoek geven (standaard niveau 3, 4 horizontaal). De teamleider kan de informatie delen met andere teamleiders door de informatie te labelen met een ander onderzoek.

- De teamleider vraagt een onderzoek aan en de afdeling BIM maakt een onderzoek aan in BVO. De teamleider legt de handeling soms neer bij de recherche assistent (autorisatie niveau 4). Hiertoe wordt de recherche assistent tijdelijk geautoriseerd op niveau zes. Het autorisatieniveau wordt na afronding van de taak *niet* altijd weer teruggezet van 6 naar 4. Dit gebeurt alleen bij de afdeling BRR en de afdeling BBR. Op deze afdelingen vervult de recherche assistent de rol van registratiebeheerder.
- Er vindt controle plaats op de autorisaties binnen het onderzoeksteam. Deze controle wordt gedaan door de teamleider.

Controle op autorisaties in BVO

De functioneel beheerder heeft vanuit zijn functie de mogelijkheid om op een hoger autorisatieniveau informatie in BVO in te zien. Dit gebeurt dan wel altijd gezamenlijk met de 'eigenaar' van het betreffende onderzoek zodat het 'vier ogen principe' wordt nageleefd.

Toedekken van informatie in BVO

Opmerkelijk is dat de politie automatisch geneigd is om de strafrechtelijke vervolging te borgen en men terughoudend is in het delen van informatie. Om zaken op te lossen is echter informatie nodig en die moet worden vergaard en gedeeld binnen de politie. Vanuit deze optiek is het wenselijk dat er op een eerder moment meer informatie wordt gedeeld.

Een reden voor het toedekken van informatie is dat de angst bestaat dat het onderzoek wellicht door anderen kan worden verstoord doordat de informatie niet goed wordt gebruikt. Om dat tegen te gaan wordt soms het autorisatieniveau voor toegang tot een onderzoek op een hoger autorisatie niveau gesteld, zodat de informatie van subjecten en objecten niet zichtbaar worden voor anderen met een lagere autorisatie. De afdeling BIM ziet hierop toe. Bij signalering van een dergelijke werkwijze wordt de afdeling BBR aangesproken.

I-Base

I-Base is een relationeel systeem, waarmee informatie uit BVO kan worden geïmporteerd. Uit de relationele verbanden wordt een tactisch criminaliteitsbeeld gegenereerd. I-Base is ontstaan omdat MS-notebook grote databestanden niet aankan en hier wel behoefte aan is. In I-Base is het mogelijk om queries te draaien. De individuele mutaties per persoon zijn inzichtelijk in I-Base. De toegang tot I-Base verloopt via de afdeling BIM aan de hand van een aanvraagformulier, dat wordt getoetst. Toestemming wordt pas verleend na goedkeuring.

Conform art. 6.1 Wpg onderhoudt de verantwoordelijke een systeem van autorisaties dat voldoet aan de vereisten van zorgvuldigheid en evenredigheid.

CIE

Voor de CIE is een autorisatiematrix opgesteld. De autorisatieverzoeken tot CIE systemen worden getoetst aan deze autorisatiematrix. De teamchef CIE is zelf verantwoordelijk voor welke functionarissen worden geautoriseerd.

De autorisaties binnen de CIE zijn goed geregeld. Elke CIE medewerker heeft toegang tot de vanuit hun taak noodzakelijke netto informatie en niet tot de bruto informatie. De bruto informatie is die informatie waarvan het niet gewenst is dat deze binnen de politieorganisatie vrij wordt gedeeld. De runners zelf hebben toegang tot de eigen bruto informatie. Dat vormt geen probleem.

Bij de CIE wordt ook de BIS-schijf gehanteerd en onder meer gebruikt voor inzicht in beheerinformatie zoals de voortgang in zaken, aangevraagde tipgelden en managementinformatie. Het is niet mogelijk om deze gegevens af te schermen per individuele CIE medewerker. Hierdoor kunnen alle medewerkers van de CIE bij deze gegevens.

RID

De afdeling RID beschikt over een eigen AO-beschrijving. In deze AO-beschrijving zijn onder andere onderwerpen zoals schoning, archivering en controle vanuit de Wpg voor de RID beschreven. Er wordt gehandeld volgens deze AO.

- Er zijn verschillende autorisatieniveaus voor de mappen bij RID. De runners mogen alleen in hun eigen bron, de analysemedewerkers mogen alleen bij de thema's waar ze aan zijn gekoppeld en de strategisch analist, het hoofd RID en de deelprojectleider RID mag bij alle informatie.
- De informanten worden met een unieke code geregistreerd in het informantenregister. Dit is landelijk bij het NCIE belegd;
- Daarnaast heeft de RID een eigen stand alone netwerk. Bij de RID wordt onder andere het informantenregister bijgehouden;
- Het netwerk van de RID is streng beveiligd, kent strenge autorisaties en de server hiervoor staat op de eigen afdeling.
- Informatie die onder het artikel 10 regime valt wordt vooral door het OOV samen met de RID aangemaakt. De informatie wordt in MS Word verwerkt.

4.5.3

Verbeterpunten

Als verbeterpunten zijn te noemen:

- Het in gebruik nemen van een tool en/of een proces om autorisaties in een geautomatiseerde vorm vast te leggen en te beheren.
- Het realiseren van zicht op autorisaties in de KA omgeving.
- Het hanteren van overzichten waarmee leidinggevend in staat zijn de autorisatie van hun medewerkers te beoordelen.
- Het beschikbaar stellen van tijd voor de juiste verwerking van restinformatie.
- Sturing op het proces voor de wachtcommandant pc ter borging van de herleidbaarheid.
- Schoning van bestaande autorisaties.

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

Geautomatiseerd Vergelijken/In Combinatie Met Elkaar Verwerken (GV/ICMEV) wordt toegestaan onder voorwaarde dat een bevoegde functionaris zijn instemming verleent aan het verdere verwerken. Dit maakt dat inzichtelijk dient te zijn in welke functies GV/ICMEV-taken worden uitgevoerd, zodat hier controle op kan worden uitgeoefend. Binnen het korps Haaglanden is geen formele procedure die inregelt welke functies zijn geautoriseerd om geautomatiseerd te vergelijken of in combinatie met elkaar te verwerken. In de interviews wordt gesteld dat middels autorisaties het aantal functies dat geautomatiseerd kan vergelijken of in combinatie met elkaar verwerken onder controle wordt gehouden. Het korps is zich bewust van het ontbreken van procedures omtrent geautomatiseerd vergelijken en in combinatie met elkaar verwerken en heeft als doel gesteld deze procedures in 2012 op te stellen.

Interpretatie art. 11 Wpg

De afdelingen binnen korps gaan verschillend om met de GV-ICMEV-problematiek. Voor informatieanalisten is het toegestaan van deze zoekmogelijkheden gebruik te maken, echter voor deze functies is geen autorisatieproces beschreven. De CIE heeft een specifieke functie aangewezen om dergelijke acties uit te voeren, echter in de praktijk worden dergelijke acties ook door niet-aangewezen functies uitgevoerd.

Het is de front office niet bekend of haar zoekwerkzaamheden zijn geautoriseerd door het bevoegd gezag.

Noot Haaglanden: Elk Korps heeft een eigen interpretatie van artikel 11. Landelijk is afgesproken dat de expertgroep privacy nu met een voorstel komt. In Haaglanden worden alle vormen van zoekslagen verricht binnen het kader van dat doel toegestaan mits de doelstelling is geautoriseerd.

Het korps geeft in interviews aan dat voor 2012 gepland staat om een functie-eenheid te organiseren om alle GV/ICMEV acties uit te voeren en helderheid te creëren in het begrip GV/ICMEV. Er zijn geen richtlijnen opgesteld ten aanzien van GV/ICMEV. Wel is helder dat de mate van privacy impact van invloed is op diepgang van de zoekvraag en is consensus bereikt met het OM van het parket Den Haag over GV/ICMEV bij de CIE.

4.6.3

Verbeterpunten

Als verbeterpunten zijn te noemen:

- Stel procesbeschrijvingen op waarin is aangegeven hoe bij geautomatiseerd vergelijken en in combinatie met elkaar verwerken moet worden gehandeld. Geef daarbij nadrukkelijk de grenzen aan van geautomatiseerd vergelijken en in combinatie met elkaar verwerken.
- Ontwikkel casuïstiek aan de hand waarvan geautomatiseerd vergelijken en in combinatie met elkaar verwerken kan worden besproken.

4.7 Bewaartermijnen (artikel 14)

4.7.1

Norm

Politiegegevens worden vernietigd zodra zij niet langer noodzakelijk zijn voor de uitvoering van de dagelijkse politietaken (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

De Processen Verbaal worden hard copy opgeslagen in de bureaus /(team)kamers. Er wordt onderscheid gemaakt naar artikel 8 en artikel 9 Wpg. Bovendien moet een onderscheid worden gemaakt tussen de papieren dossiers waarbij de dader bekend is dan wel onbekend is, maar de Wpg maakt dit onderscheid niet.

Hierdoor ontstaat een archief waarin een onderscheid kan worden gemaakt tussen de verschillende artikel 8 en 9 dossiers en waarbij bewaartermijnen niet door elkaar lopen. In de papieren dossiers is niet altijd inzichtelijk welke informatie precies wordt bewaard (naast de PV's).

De bekendheid van de bewaartermijnen bij de verschillende bureaus is niet overal even groot. Het korps heeft als insteek dat de expertise omtrent bewaartermijnen geconcentreerd is bij de afdeling Document Informatie Voorziening (DIV). DIV is verantwoordelijk voor de bewaartermijnen, dit is geen verantwoordelijkheid van de bureaus zelf. DIV werkt aan een notitie wijziging bewaartermijnen. Deze is nog niet geheel gereed.

Het korps Haaglanden is zich bewust van de problematiek rondom het hard copy archief en participeert in een expertisegroep om dit te adresseren. Bovendien zijn de decentrale hard copy archieven door de afdeling DIV geïnventariseerd, waarbij de dossiers ouder dan 2 jaar centraal worden gearchiveerd, dus niet meer op de Wijkbureaus.

Een andere kwestie is dat de dossiers door deze gehanteerde methode vrijelijk inzichtelijk blijven voor zoekvragen, zelfs na de gestelde termijnen van 1 jaar (voor artikel 8) en een half jaar na het onherroepelijk moment (voor artikel 9).

Het aanmelden van artikel 9 onderzoeken is procedureel vastgelegd. Dit geldt ook voor de afmelding van onderzoeken. De bewaartermijn hangt af het onherroepelijk vonnis bij een bekende dader. Bij een onbekende dader telt de strafvorderingstermijn.

BVO en SUMM-IT

Artikel 9 Wpg informatie wordt verwerkt in BVO en in SUMM-IT. BVO wordt door vtsPN gehost, waarbij niet kan worden gesteld dat daarmee de verantwoordelijkheid voor een mechanisme wat voorziet in de verwijdering uiterlijk een half jaar na het onherroepelijk moment ook bij vtsPN is belegd. Door een gebrek hieraan dient het korps compenserende maatregelen te nemen om te voldoen aan de Wpg. Dit is een bekend landelijk probleem. Het korps Haaglanden heeft hier nog geen invulling aan gegeven.

Naast BVO wordt ook gebruik gemaakt van SUMM-IT, waardoor tijdelijk een gedeeltelijke dubbele vastlegging ontstaat. De SUMM-IT applicatie wordt nog niet landelijk gehost.

De bewaartermijnen in BVO en SUMM-IT zijn niet ingeregeld. Als een onderzoek tot niets leidt, dan wordt het onderzoek afgemeld bij vtsPN. De privacyfunctionaris houdt een overzicht bij van alle aan- en afmeldingen van artikel 9 Wpg onderzoeken.

Het korps is gestart met de registratie van onderzoeken in I-Base. Vanaf 2009 zijn de onderzoeken geregistreerd in BVO. Alle nieuwe onderzoeken worden sinds begin 2011 in I-Base aangemeld om de afhandeling van de onderzoeken inzichtelijk te maken. Het korps is momenteel bezig onderzoeken van voor 2011 ook in I-Base te verwerken.

Andere applicaties

De politiegegevens worden naast de landelijke applicaties zoals BVH en BVO verwerkt in Microsoft Office applicaties, waardoor de bewaartermijnen zoals gesteld in de Wpg niet worden gewaarborgd. Hierbij moet worden aangetekend dat Microsoft Office applicaties soms worden gebruikt voor de uitvoering van de dagelijkse politietaak. De verzameling aan gegevens die hierdoor ontstaat dient aan procedures te zijn onderworpen.

Er wordt gebruik gemaakt van de lokale I-Base applicatie. In deze applicatie worden verbanden en relaties gelegd tussen personen. Procedures omtrent schoning en bewaartermijnen voor I-BASE ontbreken nog.

Informantenregister

De informanten worden met een unieke code in het informantenregister geregistreerd. De registratie is landelijk bij het NCIE belegd. De RID heeft een eigen stand alone PC waar onder andere het Informantenregister op wordt bijgehouden. Het blijkt dat dit netwerk en de stand alone PC streng zijn beveiligd en van strikte autorisaties zijn voorzien. De server staat op de eigen RID-afdeling en is in eigen beheer.

Hoewel het Informantenregister periodiek wordt gecontroleerd is de schoning van het register nog niet in het systeem ingebouwd. De schoning vindt nu handmatig plaats. Twee maal per jaar neemt de CIE OvJ de status van de informatie over informanten door. Op dat moment wordt beslist of iemand als informant wordt uitgeschreven. Schoning van het informantendossier vindt plaats 10 jaar na de datum van uitschrijving. Dit proces moet nog worden beschreven in de landelijke CIE-expertgroep (artikel 12 Wpg).

Conform artikel 12.6 Wpg worden de politiegegevens vernietigd zodra zij niet langer noodzakelijk zijn voor het doel van de verwerking. Daartoe worden de gegevens elk half jaar gecontroleerd. De gegevens worden vernietigd uiterlijk 10 jaar na datum van laatste verwerking van gegevens (noodzaak).

Bewaartermijnen gegevens Laptops

De laptops worden periodiek geschoond waardoor lokale kopieën op laptops voldoen aan de bewaartermijnen. Hier vindt geen specifieke controle op plaats. De laptops zijn beveiligd middels harddisk encryptie. Er wordt gebruik gemaakt van twee verschillende typen laptops, namelijk:

- de reguliere laptops uitgerust met standaard applicaties en geen toegang tot politiesystemen;
- de doelgroep laptops met toegang tot politiesystemen (via vtsPN). Dit zijn er ongeveer 250.

De laptops worden aangevraagd bij BIM. De afdeling BIM houdt een lijst bij van de beschikbaar gestelde laptops.

Bewaartermijnen artikel 9 gegevens

Het onherroepelijke vonnis is het bepalende moment voor de bewaartermijn van artikel 9 Wpg gegevens bij een bekende dader. De gegevens van onderzoeken die tot niets leiden worden vijf jaar bewaard.

De gegevens van onbekende daders worden bewaard conform de termijn van strafvordering en vervolgens 5 jaar daarna vernietigd.

Het standpunt van het korps Haaglanden is om onderzoeken af te sluiten wanneer 6 maanden niet meer aan een onderzoek is gewerkt is conform artikel 9 Wpg. De redenering is dat de noodzaak hiermee vervalt. De gegevens blijven bij zoekvragen inzichtelijk, waardoor de informatie opvraagbaar blijft. Tevens bestaat de mogelijkheid om een onderzoek opnieuw te openen indien daar aanleiding toe is.

Na afloop van een onderzoek geeft de teamleider (BRR/BBR) aan wanneer het onderzoek moet worden afgemeld. De medewerkers van het onderzoek hebben een half jaar de tijd om de restinformatie over te zetten naar Zwacri-zaken voor de CIE

en RID.

Na een halfjaar worden de BVO registraties dichtgezet. Wanneer er geen afmelding plaatsvindt wordt een onderzoek niet afgesloten.

Aangezien soms informatie wordt opgeslagen op de operationele schijven en geen procedures bestaan voor het verwijderen en vernietigen hiervan is het voldoen aan de bewaartermijnen van de Wpg afhankelijk van de medewerkers. Hierbij dient wederom te worden aangetekend dat in de beschikbaar gestelde systemen geen mogelijkheid bestaat tot het opslaan van bijvoorbeeld films, foto's en andere formulieren (dit kan wel in SUMM-IT), waardoor de politie genoodzaakt is pragmatisch om te gaan met deze problematiek.

4.7.3

Verbeterpunten

- Stel de bewaartermijnen vast voor de diverse gegevensverzamelingen.
- Richt schoningsprocedures in voor de diverse gegevensverzamelingen aangehouden in de kantoorautomatisering en laat deze uitvoeren.

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

Voor de impact van artikel 15 Wpg zijn een aantal maatregelen getroffen bij het korps Haaglanden betreffende het aanwijzen van functionarissen, het reguleren van informatieverzoeken en het opleiden van functionarissen voor afhandeling van informatieverzoeken.

Bevoegd Functionarissen

Begin 2009 is in het korps een begin gemaakt met het opleiden van de bevoegde functionarissen. De bevoegde functionaris is een nieuw fenomeen (artikel 9 lid 3 Wpg). De bevoegde functionaris geeft toestemming voor het uitwisselen van gegevens tussen rechercheonderzoeken, voor het verstrekken van Zwacri-gegevens (CIE) en voor Openbare Orde-gegevens (RID) voor andere politietaken/onderzoeken.

De functie bevoegde functionaris is dusdanig gepositioneerd binnen het korps Haaglanden dat deze automatisch vragen krijgt toebedeeld. Als bevoegde functionarissen zijn de chefs opsporing, ploegchefs opsporing, teamchefs en hoofden informatie en bedrijfsvoering aangewezen. Vanuit die rol neemt men beslissingen, waarbij de Wpg-vereisten worden meegewogen.

In 2009 hebben er zeven opleidingen plaatsgevonden in het opleidingscentrum in Den Haag. De opleidingen zijn gegeven door het Politievormingscentrum. Inmiddels zijn bijna alle bevoegde functionarissen aangesteld en is de procedure aanstelling bevoegde functionaris geborgd bij bureau HRM – services. Tevens is op intranet een lijst beschikbaar gesteld met alle bevoegde functionarissen binnen het korps Haaglanden.

Op intranet van het korps Haaglanden staat een beschrijving 'Handreiking bevoegd functionaris' over de rollen van bevoegde functionarissen en de aangewezen functies die als bevoegde functionaris dienen.

Opleidingen

De opleidingen voor BVH, BVO en BVCM hebben een dusdanige impact gehad op de beschikbare tijd en middelen, dat algemene Wpg opleidingen niet mogelijk waren. Alleen de sleutelfiguren, zoals de bevoegde functionaris, hebben een Wpg-opleiding gekregen.

- Er zijn zeven opleidingen voor bevoegde functionarissen gegeven, en vijf opleidingen voor infomedewerkers. Er waren twee workshops voor medewerkers die regelmatig samenwerkingsovereenkomsten opstellen met partners van het korps Haaglanden.
- Daarnaast zijn er ongeveer 20 Wpg-voorlichtingen geweest voor de kerninstructeurs BVH. Verder zijn er 2 instructiebijeenkomsten voor HKD-medewerkers georganiseerd. Ook zijn alle wijkbureaus bezocht waar tijdens het managementteamoverleg en het wijkagentenoverleg een presentatie over de Wpg en het gebruik daarvan is gegeven. Dit betrof 28 voorlichtingen in 2009. Op verzoek zijn er ook andere specifieke presentaties gegeven bij ondersteunende bureaus. In de Wpg-opleiding hebben ook enkele medewerkers van het parket Den Haag geparticipeerd.
- Ook bij BRI zijn voorbereidingen voor de Wpg getroffen en zijn opleidingen voor de bevoegde functionarissen verzorgd. De Privacyfunctionarissen hebben hierbij ook voorlichting gegeven.

Werking privacyfunctionaris

De privacyfunctionarissen behandelen dagelijks, zowel telefonisch als per e-mail, vragen van collega's over hoe men dient te handelen in bepaalde situaties waar het verstrekkingen betreft. Daarnaast beantwoorden ze ook vragen van burgers met betrekking tot inzageverzoeken. Hun adviezen worden zowel mondeling als schriftelijk uitgebracht. Verder hebben zij een controle-, toezichts- en voorlichtingsfunctie. Jaarlijks brengen zij een verslag uit van hun werkzaamheden.

De kennis bij de geïnterviewden over wanneer aan wie politiegegevens mogen worden verstrekt, is voor verbetering vatbaar. Dit lijkt er de reden van te zijn dat de geïnterviewden aangeven dat zij, bij twijfel, liever geen politiegegevens verstrekken.

Infodesk

Binnen het korps Haaglanden is een centrale Infodesk, het Regionaal Informatie Knooppunt (RIK). Het RIK is onderdeel van het BRI.

De informatieverzoeken worden gericht aan de informatieknooppunten van de wijkbureaus en de front office BRI (RIK). Deze zorgen voor de verdere verwerking en deling van de informatieverzoeken. De informatieverzoeken front office worden vastgelegd in de BVO-infodeskmodule. In 2009 betrof dit ruim 19.000 verzoeken.

Informatie delen

Ieder wijkbureau heeft een lokaal informatie knooppunt (LIK). Daar worden de lokale vragen uitgezet.

In de informatie organisatie wordt er veel gewerkt met BVH en Amazone. Een doelgroep kan worden gezocht in Amazone (satelliet van BVH). Amazone biedt de mogelijkheid tot het abonneren op een deel van de informatie, ontsloten middels het toekennen van abonnementen op doelgroepen. Een abonnement is op

persoonsniveau beschikbaar te stellen. Tevens is het mogelijk dit aan derde partijen ter beschikking te stellen. De informatiestroom verloopt via Amazone.

Ter beschikking stelling en isoleren van informatiedragers:

De meeste informatie wordt digitaal verstrekt en/of beschikbaar gesteld. Als er een verstrekking of ter beschikking stelling plaatsvindt, dient ook het vervoer plaats te vinden op een veilige manier.

Politiegegevens op persoonlijke schijven

In de huidige situatie worden naast BVO ook politiegegevens op de eigen researchewerkomgeving, de BIS-schijven, opgeslagen. Een team kan een schijf aanvragen om informatie voor een onderzoek op te slaan. Het nadeel van de BIS schijven is dat die informatie verder niet kan worden gedeeld met anderen die deze informatie nodig hebben voor de uitvoering van hun taak.

4.8.3

Verbeterpunten

- Stimuleer waar dat nuttig en noodzakelijk is, centrale afhandeling van het ter beschikking stellen van politiegegevens door de regionale Infodesk.
- Zorg voor bewustwording en kennis over het proces van ter beschikking stellen door de Infodesks.
- Heb aandacht voor in de kantoorautomatiseringsomgeving vastgelegde gegevens bij het ter beschikking stellen van politiegegevens.
- Afschaffen BIS schijven.

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

Verstrekkingenwijzer (landelijk)

De landelijke verstrekkingwijzer kan dienen als onderliggende documentatie om deels invulling te geven aan artikel 16 t/m 24 Wpg. De centraal opgestelde procesbeschrijving geeft weer welke informatie aan welke partijen mag worden verstrekt. Het korps Haaglanden maakt weliswaar gebruik van de landelijke verstrekkingwijzer op intranet, maar deze is nog niet bij iedereen binnen het korps bekend.

Nog niet iedereen is op de hoogte van de protocolplicht waarbij een I-90 / E 62 melding moet worden opgemaakt bij het verstrekken van politiegegevens. Uit de BIS-overzichten van deze I-90-/ E 62 meldingen blijkt dat dit laatste onvoldoende plaatsvindt. Wel is er al een toename van het aantal I-90-/ E 62-meldingen zichtbaar. Er vindt maandelijks monitoring plaats op bureauniveau.

Artikel 19 Wpg verstrekkingen

In 2009 zijn er diverse incidentele verzoeken om informatie afgehandeld conform artikel 19 Wpg. Het betrof onder andere verzoeken om informatie van gemeenten, verzekeringsmaatschappijen en woningbouwverenigingen. Deze verzoeken zijn door de wijkbureaus individueel afgehandeld. Echter, men is er zich niet altijd van bewust dat bij afwezigheid van een convenant men te maken kan hebben met artikel 19

Wpg, namelijk de incidentele verstrekkingen. De beslissing al dan niet te verstrekken is voorbehouden aan de Officier van Justitie of de bureauchef.

Er is een incident geconstateerd waarbij er artikel 19 informatie is verstrekt zonder medeweten van de betreffende chef. Vastgesteld is dat artikel 19 en 20 Wpg verstrekkingen niet altijd op de juiste manier worden toegepast.

Convenantendatabank

In 2009 is een convenantendatabank op intranet geplaatst waardoor inzichtelijk wordt gemaakt wat met de partners is afgesproken over structurele informatieverstrekkingen. Ook zijn in 2009, 2010 en 2011 de beleidsmedewerkers bijgeschoold over de (on)mogelijkheden om informatie, onder de aanwezigheid van convenanten met partners, te verstrekken.

Hoewel er een convenantendatabank op intranet beschikbaar is, blijkt men voor verstrekkingen dit niet altijd te controleren. De geïnterviewden gaan er vanuit dat er een convenant aanwezig is, zonder dit te controleren.

Overzicht convenanten Korps Haaglanden

Het korps Haaglanden heeft alleen een getekend convenant om informatie uit te wisselen met betrekking tot Schoolveiligheid.

Regionale Convenanten

- Voor regionale samenwerkingsverbanden is een start gemaakt met het opstellen van convenanten. Dit zijn onder andere de volgende convenanten: Veiligheidshuis, RIEC, Huiselijk Geweld, voetbalconvenant 2010-2011, convenant zorginstellingen, zwembadprotocol, convenant woonoverlast Den Haag, collectieve briefing binnenstad DH, collectieve briefing Leidschenhage, regionaal convenant hennep, aanpak huisjesmelkers, informatie-uitwisseling jeugd Westland, overlast wijk Buitenhof en regionaal schoolveiligheid.
- In het Veiligheidshuis wordt het probleem van de veelplegers aangepakt door de politie, het OM, reclassering, jeugdzorg en andere maatschappelijke geledingen;
- Vanwege de nieuwe groepen die in het Veiligheidshuis worden besproken, is het bestaande convenant verouderd. BIS stelt in samenwerking met het Veiligheidshuis een nieuw convenant op.

Proces voor artikel 20 besluiten

Er is een vast proces voor nieuwe convenanten. Een nieuw convenant moet altijd via de privacyfunctionaris, staf korpsdirectie/korpsjuristen en bureauchef naar de betreffende adjunct-directeur. De adjunct-directeur bepaalt of het convenant ook nog aan OKD en/of driehoek moet worden aangeboden. Dit proces is niet beschreven.

Het korps is in 2009 begonnen met het inventariseren van de huidige convenanten, de status van de convenanten en de inhoud van convenanten. Daartoe is een 'checklist Wpg samenwerkingsverband' opgesteld. De checklist is in lijn met de vereisten vanuit de Wpg.

De checklist bevat geen strikte procesbeschrijving, maar bevat voldoende handvatten voor het opdoen van convenanten en artikel 20 Wpg Besluiten. De bevoegde functionaris ziet toe op de geldigheid van de convenanten.

Verstrekkingenschema (regionaal)

Binnen Haaglanden is voor het verstrekken van informatie de ABC-procedure ontwikkeld:

- Algemene verstrekkingen waarvoor een wettelijke basis geldt (artikel 18 Wpg).
- Bevoegd gezag, betreffende incidentele verstrekkingen (artikel 19 Wpg).
- Convenanten, betreffende structurele verstrekkingen (artikel 20 Wpg).

Op grond van deze procedure wordt bepaald of op basis van A, B of C informatie wordt verstrekt. Tijdens de presentaties en in de interne communicatie is deze procedure steeds toegelicht. Daarbij is ook ingegaan op het vastleggen, het protocolleren van deze verstrekking in BVH via de I-90 procedure en sinds 2011 ook voor de E 62 procedure. Ook is deze procedure gepubliceerd in Korpskrant Haaglanden (nr. 11, 2009).

Proces voor geautomatiseerde verstrekking

Automatische verstrekking zonder tussenkomst van een persoon zijn inzichtelijk voor de privacyfunctionaris. Van deze geautomatiseerde verstrekkingen is een lijst bijgehouden. Aan welke partijen automatisch wordt verstrekt is inzichtelijk. Er vinden automatische verstrekking plaats naar:

- het Veiligheidshuis
- 'Hoe veilig is mijn wijk'
- Rijkswaterstaat (met betrekking tot aanrijdingsgegevens)
- Slachtofferhulp Nederland

Er is echter geen procedure opgesteld voor de aanvraag van een nieuwe geautomatiseerde verstrekking, maar wanneer een aanvraag wordt ingediend, wordt deze wel getoetst op de juridische grondslag.

Er vindt geen protocollering plaats van geautomatiseerde verstrekking zodat nog niet achteraf is te bepalen over welke personen geautomatiseerde politiegegevens zijn verstrekt.

Geheimhouding verstrekking informatie

De checklist voor convenanten bevat het attenderen op de noodzaak tot geheimhouding bij een verstrekking. Het Blauw is tevens geattendeerd op het belang van het wijzen op de noodzaak tot geheimhouding.

Protocollering verstrekking

De incidentele protocollering van het verstrekken van politiegegevens vindt plaats door middel van I-90 en E 62 formulieren. Men geeft aan dat BVH pas in december 2009 volledig is geïmplementeerd, waardoor de controles op het gebruik van I-90 formulieren pas in 2010 hebben kunnen plaatsvinden.

Bij het korps Haaglanden is niet overal bekend dat eventuele verstrekkingen dienen te worden vastgelegd. Ook blijkt uit de BIS-overzichten dat het invullen van de I-90 / E 62 formulieren nog niet structureel plaatsvindt. Het gebruik van de I-90 / E 62 formulieren vertoont wel een stijgende lijn.

Bewaren protocolgegevens verstrekking

De geprotocolleerde verstrekkingen worden bewaard binnen BVH en minimaal gedurende 1 jaar bewaard.

Toezicht leidinggevenden op verstrekkingen en protocollering

Alle medewerkers die geautoriseerd zijn voor BVH kunnen politiegegevens verstrekken. Informatieverstrekking wordt in sommige gevallen geweigerd. Er is geen direct toezicht van de leidinggevenden. De privacyfunctionaris ziet toe op de verstrekkingen en de protocollering daarvan. De privacyfunctionaris heeft onlangs een steekproef gedaan op een aantal geregistreerde verstrekkingen. Bij

geconstateerde kwalitatieve tekortkomingen heeft de privacyfunctionaris een terugkoppeling gegeven aan de medewerker die informatie heeft verstrekt.

4.9.3

Verbeterpunten

Beheersmaatregelen die zijn gericht op het voldoen aan deze criteria en die in dit kader kunnen worden genoemd, zijn onder meer:

- Zorg voor beheersmaatregelen die gericht zijn op een volledige registratie van verstrekkingen door middel van I-90 / E 62 uit BVH en andere vastleggingen in BVO.
- Zorg voor een actieplan inclusief toekenning van mensen en middelen voor de opschoning van de convenanten en een adequaat en centraal beheer.
- Zorg dat de inhoud van de convenanten bekend is en maak medewerkers ervan bewust dat politiegegevens alleen mogen worden verstrekt als dit gebeurt voor de doeleinden zoals genoemd in artikel 20 WPG.

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

Inzagerecht

Er is een procesbeschrijving inzake het verstrekken van gegevens aan burgers uit hoofde van het inzagerecht beschikbaar op het intranet. Binnen het korps is in 2008 een nieuwe inzageprocedure opgesteld waarbij het Bureau Integriteit en Security (BIS) alle verzoeken coördineert en behandelt. In alle Wpg-voorlichtingen op de bureaus wordt deze procedure uitgelegd.

In het jaarverslag van 2009 wordt aangegeven dat ongeveer 90 % van de inzageverzoeken informatie uit artikel 8 en artikel 13 Wpg betreft. De overige 10 % van de inzageverzoeken betreft artikel 9 en artikel 10 Wpg onderzoeken. De verzoeken tot inzage in rechercheonderzoeken (artikel 9 en 10 Wpg) worden door de privacyfunctionaris persoonlijk begeleid.

In 2008 hebben er in totaal 267 inzage/verstrekkingverzoeken plaatsgevonden. In 2009 is dit gestegen tot 367 verzoeken. Alle verzoeken zijn binnen de wettelijke termijn afgerond. Indien noodzakelijk, bijvoorbeeld bij voorlopige voorziening, krijgt men binnen 48 uur al inzicht in de informatie.

Recht op correctie

Er zijn enkele verzoeken voor correcties geweest en deze worden door de privacyfunctionaris gedocumenteerd. Er hebben zich geen klachten voorgedaan.

Mededeling van verbetering, aanvulling, verwijdering of afscherming

Binnen het korps Haaglanden is niet algemeen bekend dat de verplichting bestaat om op grond van artikel 30 Wpg eventuele wijzigingen in de politiegegevens door te geven aan de verzoeker gedurende 1 jaar na de verstrekking.

4.10.3

Verbeterpunt

- Zie toe op en rapporteer over verbetering, aanvulling en verwijdering van politiegegevens.

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, tenminste 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.

Protocollering doel onderzoek

In 2008 zijn er in 9 maanden 215 artikel 9 Wpg onderzoeken aangemeld en 26 art 9 Wpg onderzoeken afgemeld. In 2009 is dit aantal gestegen tot 322 aanmeldingen en 119 afmeldingen (26 afmeldingen betroffen in 2008 geopende onderzoeken en 93 afmeldingen betroffen in 2009 geopende en afgeronde onderzoeken). Hiervoor is door Bureau informatiemanagement (BIM) een applicatie gemaakt, die automatisch na melding van het onderzoek de aanmelding in de BVO verzorgt. De controle van de aan- en afmeldingen vindt plaats door de privacyfunctionaris.

In de sturingscyclus wordt viermaandelijks een overzicht gepresenteerd, waarbij het aantal meldingen art 9 Wpg en BVO-meldingen vermeld staat. Het aantal meldingen wordt regelmatig besproken met bureauchefs en de directie. Op deze wijze is er inzicht en controle op verwerking en opslag van opsporingsgegevens. Daarnaast wordt regelmatig bekeken of de onderzoeken ook geheel in BVO worden verwerkt.

Protocollering CIE

Binnen de CIE wordt gewerkt volgens een protocol dat door vijf grote korpsen is opgesteld. In dit protocol zijn de CIE-werkprocessen geüniformeerd.

Bewaren protocolgegevens doel onderzoek

Middels I-Base worden de doelen van onderzoeken vastgelegd en inzichtelijk gemaakt voor de privacyfunctionaris. Alle nieuwe onderzoeken moeten worden geregistreerd middels een MRO voordat een onderzoek wordt aangemaakt in BVO.

Een overzicht van de artikel 9 Wpg aan- en afmeldingen wordt aangehouden. Er is een achterstand ontstaan dit jaar, omdat er een tijd lang geen toegang was tot I-Base, waarin de registraties plaatsvinden. De achterstand is op dit moment 100 afmeldingen (periode maart en juli tot en met november 2011). De aanmeldingen zijn verwerkt tot en met 6 november 2011.

In het Excel bestand zijn de afgemelde onderzoeken gemarkeerd.

Protocollering artikel 13 gegevensverzameling

Het korps Haaglanden heeft een interpretatie van artikel 13 gegevensverzamelingen en op basis hiervan zijn er geen lokale artikel 13 gegevensverzamelingen aanwezig bij het korps. Deze zijn geschaard onder artikel 10 Wpg. Als argumentatie voor deze constructie wordt gesteld dat de aard van de gegevens zich niet lenen voor een artikel 13 Wpg markering. Het gaat hierbij niet om de relatief soort onschuldige gegevens zoals bedoeld in artikel 13 Wpg.

De protocollering van landelijke artikel 13 Wpg gegevens wordt gedaan aan de hand van landelijke protocollen. Deze heeft het korps echter nog niet definitief vastgesteld, het korps is nu bezig dit actiepunt op te pakken. Derhalve vindt er geen protocollering van artikel 13 gegevens plaats van de lokale gegevensverzamelingen.

Protocollering onrechtmatige handeling

De privacyfunctionaris houdt in een Excel-bestand een overzicht bij van de privacyschendingen die er zich hebben voorgedaan. Er blijken in 2011 120 schendingen te zijn geconstateerd, en deze zijn vastgelegd in het betreffende overzicht.

Deze vastlegging wordt bij Haaglanden ten minste bewaard tot en met de volgende uit te voeren audit.

Hernieuwde verwerkingen

Binnen het korps Haaglanden is bekend dat men toestemming voor dit soort verwerkingen dient te verkrijgen van het bevoegd gezag, in dit geval de Officier van Justitie. Daarbij is tevens bekend dat men niet zomaar gebruik mag maken van gegevens van vijf jaar en ouder.

Er is geen procesbeschrijving aanwezig en er is geen aparte registratie (protocollering) voor hernieuwde verwerkingen. Protocollering vindt derhalve niet plaats.

Gemeenschappelijke verwerking

Niet van toepassing. Uit de audit is niet gebleken dat samen met het korps Haaglanden gemeenschappelijke verwerkingen plaatsvinden.

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

Interne audit functie

Bij het Korps Haaglanden is een interne auditor aangewezen. De enige Wpg audit bij het Korps Haaglanden dateert uit 2011. Het voornemen is om dit jaarlijks te herhalen.

Interne audit plan

Er is geen auditplan, maar slechts een voornemen om jaarlijks een Wpg audit uit te voeren.

Interne audit rapport

Aan de hand van het rapport van 2011 is vastgesteld dat de gevolgde werkwijze is beschreven, de resultaten van de privacy audit zijn beschreven en het oordeel en de aanbevelingen zijn opgesteld.

4.12.3

Verbeterpunten

- Richt een vaktechnisch verantwoorde en meerjarig gerichte audit in.
- Stel een auditdossier op.

4.13 Privacy functionaris (artikel 34)

4.13.1

Norm

De privacyfunctionaris 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

Benoeming en melding

Uit de stukken blijkt dat er in 2009 twee privacyfunctionarissen zijn aangewezen. Beide privacyfunctionarissen zijn bij het bureau Integriteit en Security (BIS) werkzaam. Tussen november 2009 en juli 2010 is een extra privacyfunctionaris aangesteld door de directie om de werkzaamheden van de Wpg te begeleiden.

Alle privacyfunctionarissen zijn formeel benoemd en aangewezen, alsmede aangemeld bij het College Bescherming Persoonsgegevens.

De privacyfunctionarissen hebben drie keer per jaar in het kader van managementsturingscyclus overleg met de directeur Opsporing & Informatie over hun werkzaamheden en de voortgang daarvan.

Opleiding

Twee privacyfunctionarissen hebben in 2009 de speciale, door de PIWPG georganiseerde, opleiding privacyfunctionarissen en de Wpg gevolgd.

Protocollering

In de sturingscyclus wordt viermaandelijks een overzicht gepresenteerd, waarbij het aantal meldingen van artikel 9 Wpg en BVO-meldingen staat vermeld. Het aantal meldingen wordt regelmatig besproken met bureauchefs en de directie. Op deze wijze is er inzicht in en controle op de verwerking en opslag van opsporingsgegevens. Daarnaast wordt regelmatig bekeken of de onderzoeken ook geheel in BVO worden verwerkt.

Jaarverslag

Jaarlijks wordt door de privacyfunctionaris een jaarverslag opgesteld. Het verslag over 2010 is ter beschikking gesteld. Aan het verslag over 2011 wordt momenteel gewerkt.

4.14 Functionaris Gegevensbescherming (artikel 36)

De Functionaris Gegevensbescherming bestaat niet als functie bij het korps Haaglanden.