



Ministerie van Veiligheid en Justitie

Audit Wpg politie Groningen

Rapport

Datum
Status

6 januari 2012
Definitief

Colofon

Afzendgegevens

Departementale Auditdienst

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

Contactpersonen

drs.
drs.
Senior auditors

T
M

Projectnaam

Audit Wet Politiegegevens

Ons kenmerk

DDS/5719704/11

Auteurs

Inhoud

Colofon 3

1 Assurance Verklaring 7

2 Samenvatting 9

3 Inleiding 16

3.1 Algemeen 16

3.2 Aanleiding 16

3.3 Doelstelling, aard en scope van de opdracht 16

3.4 Afbakening 17

3.5 Normenkader 17

3.6 Beperkingen voor de privacy audit 18

3.7 Onderzoeksmethoden en werkwijze 18

3.8 Doelgroep van het rapport 18

4 Bevindingen 19

4.1 Inleiding 19

4.2 Verantwoordelijke (artikel 1.f) 20

4.3 Kwaliteitsaspecten van politiegegevens (artikel 3 en 4) 21

4.4 Gevoelige gegevens (artikel 5) 24

4.5 Autorisatie (artikel 6) 24

4.6 Geautomatiseerd Vergelijken (GV)/In Combinatie Met Elkaar Verwerken (ICMEV)(artikel 11) 27

4.7 Bewaartermijnen (artikel 14) 28

4.8 Ter beschikking stellen (artikel 15) 30

4.9 Verstrekken (artikel 16/24) 32

4.10 Rechten van betrokkenen (artikel 25/28) 34

4.11 Protocolplicht (artikel 32) 35

4.12 Audits (artikel 33) 37

4.13 Privacyfunctionaris (artikel 34) 38

4.14 Functionaris Gegevensbescherming (artikel 36) 38

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 de maanden augustus en september 2011 is een privacy audit uitgevoerd bij het korps Groningen.

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 Groningen.

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

Den Haag, 6 januari 2012

De Directeur van de Departementale Auditdienst

2 Samenvatting

Vanaf augustus 2011 werken de drie noordelijke korpsen samen aan een doorstart van de implementatie van de Wpg. Daartoe hebben zij een gemeenschappelijke werkgroep opgericht met doorzettingsmacht. De werkgroep werkt samen met partners voor het realiseren van de vereiste veranderingen. De in deze rapportage van de Departementale Auditdienst aangegeven manco's en kanttekeningen worden door de werkgroep meegenomen bij het opstellen van een actieplan om de drie korpsen in opzet, bestaan en werking te laten voldoen aan de Wpg.

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 zoals genoemd in 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
Artikel 1.f, Verantwoordelijke			
1.f	Mandaatbesluit		Er is een vigerend mandaatbesluit van 16 november 2010, welke het mandaat regelt, het ondermaat, de volmacht, de subvolmacht en de machtigingen. Hiermee wordt voldaan aan de Wpg.
Artikel 3 en 4, Kwaliteitsaspecten van politiegegevens			
8.1 en 9.1	Onderscheid onderzoek Dagelijkse Politietaken (8) versus Bepaald geval (9)		Het korps heeft criteria voor het verschil tussen artikel 8 versus artikel 9 onderzoeken op intranet staan. Hiermee wordt voldaan aan de Wpg.
3.1 t/m 3.3 (8) 4.1 (8)	Noodzakelijkheid (8) Doelbinding Rechtmatigheid Juistheid Volledigheid		Het korps Groningen gebruikt TrueBlue voor de bewaking van de kwaliteit van een aantal velden in BVH. Binnen het korps zijn Wpg cursussen gegeven. Daarna is het Wpg bewustzijn weggeëbd bij gebrek aan continuïteit in de communicatie. Het korps Groningen heeft de uitrol naar Blauw nog niet afgerond. Binnen het korps wordt een gebrek aan doorzettingsmacht ervaren en er vindt geen monitoring plaats op de uitvoering van de Wpg. Hiermee wordt niet voldaan aan de Wpg.
3.1 t/m 3.4 (9) 4.1 (9)	Noodzakelijkheid (9) Doelbinding Rechtmatigheid Herkomst en wijze van verkrijging		Het rechteproces bevat waarborgen voor deze aspecten. De PDCA-cyclus sluit via het OM en de rechter. Tevens is bij de rechte nu meer aandacht voor de vastlegging van bronnen en hoe informatie uit andere onderzoeken wordt verkregen. Er is een registratiefunctie

Norm	Aspect	Bevinding en oordeel
	Juistheid Nauwkeurig Volledigheid	om toe te zien op de kwaliteit. Hiermee wordt voldaan aan de Wpg.
3.4 (10 en 12) 4.1 (10 en 12)	Noodzakelijkheid (10 en 12) Doelbinding Rechtmatigheid Herkomst en wijze van verkrijging Juistheid Nauwkeurig Volledigheid	De CIE heeft een proceshandboek. De CIE OvJ houdt toezicht. Bij de RID liggen de kwaliteitscriteria al in het doel van de taak vast. Het handboek voor RID ligt ter goedkeuring bij de AIVD. Hiermee wordt voldaan aan de Wpg.
4.3	Beveiliging	De landelijke en regionale informatiesystemen zijn nog niet Wpg-proof. Hiermee wordt niet voldaan aan de Wpg.
Artikel 5, gevoelige gegevens		
	• Gevoelige gegevens	Er zijn geen niet-toegestane gegevensverzamelingen gebaseerd op gevoelige gegevens aangetroffen. Het korps heeft regels voor de omgang met gevoelige gegevens op intranet staan. In de beschikbare artikel 13 protocollen wordt dit onderwerp behandeld. Hiermee wordt voldaan aan de Wpg.
Artikel 6, Autorisatie		
	• Korpsautorisatiematrix	Er is een autorisatietabel SSCN. Hiermee wordt voldaan aan de Wpg.
	• Aanvraagproces	Het aanvraagproces van autorisaties verloopt via SSCN en vtsPN, en is gedocumenteerd. Hiermee wordt voldaan aan de Wpg.
	• Wijziging en verwijdering	Volgens het korps schoont de privacyfunctionaris jaarlijks de autorisaties voor applicaties. Wij zijn van mening dat de privacyfunctionaris een wettelijke taak heeft toezicht uit te oefenen, en dat schonen van autorisaties in dit kader een oneigenlijke taak is. Schoning behoort te worden uitgevoerd als een gedocumenteerd en controleerbaar proces via de lijn. Daarnaast blijkt niet dat er sprake is van een geschoond autorisatiesysteem. Het verwijderproces van autorisaties verloopt via SSCN en vtsPN, en is gedocumenteerd. De rechten op de mapstructuur van de kantoorautomatiseringsomgeving zijn echter minder goed geregeld. Er zijn twee onderzoeken uitgevoerd vanuit Informatiebeveiliging bij de Afdeling Integriteit en bedrijfsveiligheid, gericht op de autorisaties. Deze hebben plaatsgevonden in mei 2009 en februari 2010. In beide rapporten is de conclusie dat het systeem van autorisaties niet voldoet aan de daaraan te stellen normen zoals beschreven in het Basisbeveiligingsniveau Nederlandse Politie (BBNP) en de Wpg. Hiermee wordt niet voldaan aan de Wpg.
	• Autorisatiebeheer CIE en RID	Autorisaties voor medewerkers van de CIE en RID worden toegekend door het hoofd van de CIE respectievelijk

Norm	Aspect		Bevinding en oordeel
			RID. De CIE OvJ heeft het autorisatiebeleid goedgekeurd. Hiermee wordt voldaan aan de Wpg.
32.1.c	Protocollering autorisaties		Binnen SSCN wordt iedere aanvraag voor een mutatie op een autorisatie geregistreerd. Hiermee wordt voldaan aan de Wpg.
32.3 voor 32.1.c	Bewaren protocolgegevens autorisaties		Binnen SSCN wordt iedere aanvraag voor een mutatie op een autorisatie bewaard. Hiermee wordt voldaan aan de Wpg.
Artikel 11, Geautomatiseerd vergelijken en in combinatie met elkaar verwerken			
	• Hanteerbare interpretatie		De begrippen geautomatiseerd vergelijken en in combinatie met elkaar verwerken zijn nog onvoldoende bekend binnen het korps. Hiermee wordt niet voldaan aan de Wpg.
	• Aangewezen functionarissen		De Infodesk is onder andere belast met het in combinatie met elkaar verwerken en geautomatiseerd vergelijken. Ondanks dat er een concept werkinstructie is, zijn de rollen in het kader van de Wpg nog niet daadwerkelijk expliciet belegd. Hiermee wordt deels voldaan aan de Wpg.
11.4	Bevoegd gezag		Doordat in combinatie met elkaar verwerken niet eenduidig is vastgesteld, is het onbekend wanneer het bevoegd gezag moet worden geraadpleegd. Hiermee wordt niet voldaan aan de Wpg.
32.1.d en h	Protocollering 11.1, 11.2, 11.4 en 11.5		Aanvragen die via de Infodesk binnenkomen worden geprotocolleerd. Hiermee wordt voldaan aan de Wpg.
32.3 voor 32.1.d en h	Bewaren protocolgegevens 11.1, 11.2, 11.4 en 11.5		Aanvragen die via de Infodesk binnenkomen worden bewaard. Hiermee wordt voldaan aan de Wpg.
Artikel 14, Bewaartermijnen			
8.2 en 8.3	(8) van 1 tot 5 jaar		Gegevens ouder dan één jaar na eerste vastlegging in BVH worden niet achter schot gezet. Medewerkers gaan er van uit dat de gegevens die ze te zien krijgen ook mogen worden gebruikt voor verdere verwerking. Met name medewerkers op operationeel niveau zijn zich hiervan niet voldoende bewust. Hiermee wordt niet voldaan aan de Wpg.
8.6	(8) verwijderen na 5 jaar		De regels voor de verwijdering van oude artikel 8 gegevens zijn moeilijk uitvoerbaar omdat het handmatig moet gebeuren. Daardoor krijgt het verwijderen en schonen nog onvoldoende prioriteit. Hiermee wordt niet voldaan aan de Wpg.
14.1 (8)	(8) vernietigen na 5 jaar verwijderd		Artikel 8 gegevens worden nog niet op het voorgeschreven moment vernietigd. Hiermee wordt niet voldaan aan de Wpg.
9.4	(9) verwijderen na OH plus ½ jaar		Het opschonen van artikel 9 onderzoeken kan nog verder worden geoptimaliseerd. Hierbij is de ketensamenwerking en specifiek de overdracht van informatie over afgesloten zaken van OM naar de politie een aandachtspunt. Hiermee wordt niet voldaan aan de Wpg.

Norm	Aspect		Bevinding en oordeel
14.1 (9)	(9) vernietigen na 5 jaar verwijderd		Doordat het juiste moment van verwijdering niet bekend is, kan niet 5 jaar na verwijdering worden vernietigd. Hiermee wordt niet voldaan aan de Wpg.
10.6	(10) verwijderen na 5 jaar geen subjectwaardige registratie		De CIE OvJ voert periodiek controles uit waarbij ook naar de bewaartermijnen wordt gekeken. Hiermee wordt voldaan aan de Wpg.
14.1 (10)	(10) vernietigen na 5 jaar verwijderd		De CIE OvJ voert periodiek controles uit waarbij ook naar de vernietiging wordt gekeken. Hiermee wordt voldaan aan de Wpg.
14.3	Hernieuwde verwerking		Gegevens worden niet verwijderd, waardoor er geen proces kan worden ingericht voor hernieuwde verwerking in opdracht van het bevoegd gezag. Hiermee wordt niet voldaan aan de Wpg.
32.1.e	Protocollering 14.3		Er is geen proces voor hernieuwde verwerking. Hiermee wordt niet voldaan aan de Wpg.
32.3 voor 32.1.e	Bewaren protocolgegevens 14.3		Er is geen proces voor hernieuwde verwerking. Hiermee wordt niet voldaan aan de Wpg.
12.2	(12) gebruiken tot 4 maanden		De CIE OvJ voert periodiek controles uit waarbij ook naar de bewaartermijnen wordt gekeken. Informatie van informanten wordt binnen een termijn van maximaal 4 maanden verwerkt en netto in een andere omgeving gezet. Dit zit vast in de werkwijze van de CIE. Hiermee wordt voldaan aan de Wpg.
12.6	(12) controleren en vernietigen		Informatie wordt binnen de CIE en RID regelmatig gecontroleerd en geschoond. Bij de RID gebeurt dit elke 5 jaar. Bij de CIE toetst de CIE-OvJ jaarlijks het informantenregister. Hiermee wordt voldaan aan de Wpg.
Artikel 15, Ter beschikking stellen			
• Infodesk voor bevraging			De Infodesk stelt informatie ter beschikking volgens vaste procedures. Een deel van de politiegegevens van het korps Groningen zijn echter opgeslagen in persoonlijke en groepsmappen met een risico op onrechtmatig gebruik en bewaring. Het gebruik van de mappenstructuur binnen Opsporing belemmert de Infodesk met het zoeken en vergelijken met andere onderzoeken. Hierdoor kan informatie ook niet met andere korpsen worden gedeeld. Hiermee wordt niet voldaan aan de Wpg.
• Codering			Coderingen worden gebruikt bij CIE mutaties en voor MRO's. Hiermee wordt voldaan aan de Wpg.
• Aanwijzing Bevoegd Functionaris			Bevoegd functionarissen zijn aangewezen en initieel opgeleid. Hiermee wordt voldaan aan de Wpg.
• Opleiding Bevoegd Functionaris			Bevoegd functionarissen zijn vooral in 2009 opgeleid. Hun kennis van de Wpg is echter deels weggezaakt. Het korps biedt in 2012 een opfriscursus aan.

Norm	Aspect	Bevinding en oordeel
		Hiermee wordt deels voldaan aan de Wpg.
15.2	Weigeringgronden	De weigeringgronden zijn onderwezen aan de bevoegd functionaris. Hiermee wordt voldaan aan de Wpg.
Artikel 16 t/m 24, Verstrekking		
	• Verstrekkingenwijzer (landelijk)	De landelijke verstrekkingenwijzer is tijdens de opleiding voor bevoegd functionaris uitgereikt en is raadpleegbaar op intranet. Hiermee wordt voldaan aan de Wpg.
	• Proces voor convenanten	Nieuwe convenanten, waar nodig inclusief een artikel 20 besluit, worden centraal beoordeeld en, indien akkoord, getekend door de korpsbeheerder. Er is echter nog een inhaalslag gaande op de bestaande convenanten. Hiermee wordt deels voldaan aan de Wpg.
	• Proces voor Artikel 20 Besluiten	Nieuwe artikel 20 besluiten worden centraal beoordeeld en, indien akkoord, getekend door de korpsbeheerder. Er is echter nog een inhaalslag gaande op de bestaande convenanten. Hiermee wordt deels voldaan aan de Wpg.
	• Verstrekkingenschema (regio)	Het korps heeft op het intranet een gegevensbeheerlijst staan met de organisaties waaraan informatie mag worden verstrekt. Hiermee wordt voldaan aan de Wpg.
	• Proces voor geautomatiseerde verstrekking	Naar de mening van het korps vinden er momenteel geen geautomatiseerde verstrekkingen plaats, anders dan de in het Besluit politiegegevens toegestane verstrekkingen, zoals aan RDW bij het invorderen van een kentekenbewijs. Hiermee wordt voldaan aan de Wpg.
7.2	Geheimhouding	Bij het Veiligheidshuis hebben de ketenpartners getekend voor geheimhouding. CIE benadrukt dat de door hen verstrekte gegevens niet verder mogen worden doorverstrekt. Hiermee wordt voldaan aan de Wpg.
32.1.f	Protocollering verstrekking	De Infodesk legt alle verstrekkingen vast. Het verstrekken en het vastleggen van verstrekkingen door andere medewerkers via een I90 in BVH verloopt echter nog niet goed, mede doordat de Wpg in onvoldoende mate wordt begrepen en doordat het vastleggen via een I90 als een administratieve last wordt ervaren. Hiermee wordt niet voldaan aan de Wpg.
32.3 voor 32.1.f	Bewaren protocolgegevens verstrekking	De wel vastgelegde gegevens over verstrekkingen worden bewaard. Hiermee wordt voldaan aan de Wpg.
	• Toezicht door leidinggevenden op verstrekkingen en protocollering	Bij de Infodesk is toezicht door de leidinggevende. Bij andere medewerkers is onvoldoende toezicht op het gebruik van de I90 in BVH. Hiermee wordt niet voldaan aan de Wpg.

Norm	Aspect	Bevinding en oordeel
Artikel 25 t/m 31, Rechten van de betrokkene		
25.1	Verzoek om kennisneming	De privacyfunctionaris handelt verzoeken af in het kader van de rechten van betrokkenen. Dit is een ongewenste vermenging van functies, aangezien de privacyfunctionaris toezicht dient te houden op dit proces. Hierop komen wij terug bij het onderwerp "Privacyfunctionaris". Niettemin wordt het proces voor de artikelen 25 en 28 goed doorlopen. Hiermee wordt voldaan aan artikel 25 van de Wpg.
28.1 t/m 28.3	Correctie	Zie de toelichting op artikel 25 hierboven. Hiermee wordt ook voldaan aan artikel 28 van de Wpg.
Artikel 32, Protocolplicht (32.1.c, d, e, f en h behandeld bij thema's)		
9.2 en 32.1.a	Protocollering doel onderzoek	Doelbinding conform artikel 9.2 wordt niet altijd op een juiste wijze vastgelegd. De drie noordelijke korpsen hebben plannen BOSZ te implementeren, waarin onder andere het doel van een onderzoek wordt vastgelegd. Hiermee wordt deels voldaan aan de Wpg.
32.3 voor 32.1.a	Bewaren protocolgegevens doel onderzoek	De MRO wordt bewaard in VROS. Hiermee wordt voldaan aan de Wpg.
13.4 en 32.1.b	Protocollering Artikel 13 gegevensverzamelingen	Het korps Groningen beschikt over een aantal protocollen voor Artikel 13 gegevensverzamelingen. Dergelijke protocollen zijn echter nog niet beschikbaar voor alle Artikel 13 gegevensverzamelingen. Hiermee wordt deels voldaan aan de Wpg.
32.3 voor 32.1.b	Bewaren protocolgegevens Artikel 13 gegevensverzamelingen	Het korps Groningen beschikt deels over een Artikel 13 Register. Hiermee wordt deels voldaan aan de Wpg.
32.1.g	Protocollering onrechtmatige handeling	Een overzicht van onrechtmatige verwerkingen ontbreekt. Hiermee wordt niet voldaan aan de Wpg.
32.3 voor 32.1.g	Bewaren protocolgegevens onrechtmatige handeling	Een overzicht van onrechtmatige verwerkingen ontbreekt. Hiermee wordt niet voldaan aan de Wpg.
32.2	Gemeenschappelijke verwerking	Het Shared Service Center Noord (SSCN) is een gemeenschappelijk onderdeel van drie korpsen, waarbij iedere medewerker onder een van de drie korpschefs valt. Door het ontbreken van een landelijke richtlijn voor het positioneren een gemeenschappelijk onderdeel in relatie tot de Wpg, kunnen wij ons vooralsnog geen onderbouwd oordeel vormen over het wel of niet voldoen aan de Wpg. Wij adviseren een nader onderzoek.
Artikel 33, Audits		
RPAP 3.1	Interne audit-functie	Er is geen interne Wpg audit-functie. Hiermee wordt niet voldaan aan de Wpg.
RPAP 3.4	Interne audit-plan	Er is geen intern Wpg audit-plan. Hiermee wordt niet voldaan aan de Wpg.
RPAP 3.6	Interne audit-rapport	Er zijn twee rapporten vanuit informatiebeveiliging, ge-

Norm	Aspect		Bevinding en oordeel
			richt op een uitdraai van de autorisaties. Deze zijn van mei 2009 en februari 2010, en bevatten een negatief oordeel over het systeem van autorisaties. Er is echter geen intern Wpg audit-rapport. Hiermee wordt niet voldaan aan de Wpg.
Artikel 34, Privacyfunctionaris			
34.1 en 34.4	Benoemd en gemeld		De privacyfunctionarissen bij SSCN zijn benoemd en gemeld. Hiermee wordt voldaan aan de Wpg.
34.2	Overzicht over protocollering		De privacyfunctionaris heeft overzichten van de meldingen onderzoeken artikel 9. De privacyfunctionaris heeft echter geen overzichten van mutaties op autorisaties, geen overzicht van geautomatiseerde vergelijkingen, geen overzicht van verstrekkingen en geen overzicht van onrechtmatige verwerkingen. Hiermee wordt niet voldaan aan de Wpg.
34.3	Jaarverslag		Het was de intentie over 2010 één rapport op te stellen voor Groningen, Friesland en Drenthe. Door een veranderende prioriteitstelling in het korps is dit verslag echter niet opgesteld. Daarnaast komt de privacyfunctionaris niet toe aan de toezichthoudende taken. Hiermee wordt niet voldaan aan de Wpg.
Optioneel Artikel 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 Groningen 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 Groningen in de maanden augustus en september 2011.

3.2 Aanleiding

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

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

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

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

3.3 Doelstelling, aard en scope van de opdracht

Doelstelling

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 Groningen.

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 september 2011, van maatregelen en procedures, waarmee het

korps Groningen 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).
- Juisheid, 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 Groningen. Dit betekent dat wij geen onderzoek hebben verricht naar door de vtsPN aan het korps Groningen geleverde faciliteiten, voor zover de verantwoordelijkheid daarvoor is belegd bij de vtsPN of bij anderen dan het korps Groningen.

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 leidinggevendenden van het korps Groningen en het Openbaar Ministerie, deelwaarnemingen in de procesbeschrijvingen en andersoortige documentatie en deelwaarnemingen in informatiesystemen.

Wij hebben onze werkzaamheden uitgevoerd in de periode van augustus 2011 tot en met september 2011.

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. _____;

mr. _____ neemt namens DG Politie deel aan de stuurgroep.

drs. _____ neemt namens het KBB deel aan de stuurgroep.

De specifieke doelgroep waarvoor het rapport is bedoeld bestaat uit:

- Onze opdrachtgever zoals bovengenoemd;
- De korpsbeheerder dr. _____;
- De korpschef mr. _____;
- De Hoofd Officier van Justitie mr. _____;
- De privacyfunctionaris mr. drs. _____;
- De voorzitter van het College Bescherming Persoonsgegevens.

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

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

4 Bevindingen

4.1 Inleiding

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

4.1.1 *Interregionale opstart en Wpg project*

Bij de politiekorpsen Groningen, Friesland en Drenthe is in september 2009 de implementatie in noordelijk verband opgezet op basis van de formule van een interregionaal gecoördineerd en afgestemd, maar per korps zelfstandig en onder eigen regie te doorlopen, proces. De gezamenlijke projectgroep heeft begin 2010 een veelheid aan procesbeschrijvingen opgeleverd. Deze zijn ter goedkeuring voorgelegd aan de respectievelijke korpsleidingen. Binnen het korps Groningen zijn de producten na goedkeuring door de korpsleiding en het strategisch korpsmanagement in april 2011 overgedragen aan de lijn.

Het korps Groningen heeft besloten om informatie- en gegevensbeheer tot strategisch thema te benoemen en hiervoor een Divisie Informatie op te richten. De CIE, RID en RIK vallen onder deze divisie. Binnen het korps Groningen is deze Divisie Informatie aangewezen als verantwoordelijke voor de informatiehuishouding en houdt zich uit dien hoofde bezig met het beheren van informatie. De implementatie van de Wpg moet onder supervisie van deze divisie worden vormgegeven.

In 2010 heeft, als uitvloeisel van de samenvattende eindrapportage van interregionale ambtelijke projectgroep implementatie Wpg, een communicatiecampagne plaatsgevonden. Dit heeft geleid tot een opleving in het bewustzijn van de Wpg. Binnen de regio zijn Wpg cursussen gegeven. Daarna is het Wpg bewustzijn weggebeld bij gebrek aan continuïteit in de communicatie.

Er zijn door ons geen procesbeschrijvingen aangetroffen waarin is opgenomen op welke wijze de zorg voor het voldoen aan de kwaliteitscriteria voor de verwerking van politiegegevens in het kader van artikel 8 en 9 van de Wpg dient plaats te vinden.

Medewerkers van de afdelingen CIE, RID en RIK (Infodesk) van de Divisie Informatie geven aan dat ze volgens de Wpg handelen. Voor de Infodesk geldt dat andere onderdelen van de politie veel verwachten van de Infodesk op het gebied van de Wpg. Binnen het korps wordt de Infodesk gezien als een waarborg voor het juist toepassen van de Wpg.

Voor de CIE hebben wij een proceshandboek CIE ontvangen dat in mei 2011 definitief is gemaakt. Met behulp van een landelijke werkgroep, bestaande uit vertegenwoordigers van verschillende regionale CIE-afdelingen, is de werkwijze van de CIE besproken en beschreven, rekening houdend met wet- en regelgeving, waaronder de Wet Politiegegevens. De werkgroep is verantwoordelijk voor de redactie van het proceshandboek en zijn hierbij ondersteund door medewerkers van de voorziening tot samenwerking Politie Nederland (VtSPN). Voor de RID is ook een landelijk initia-

tief genomen en een concept handboek opgesteld. Dit handboek moet nog door de AIVD worden vastgesteld.

Uit de interviews komt naar voren dat op de werkvloer behoefte is aan vuistregels, voorbeelden, werkinstructies, stroomschema's en andere hulpmiddelen waarin de regelgeving van de Wpg concreet en helder wordt beschreven. Dit zou handvatten moeten bieden bij het uitvoeren van de dagelijkse werkzaamheden conform de Wpg.

- 4.1.2 *Regie en doorzettingsmacht voor de Wpg implementatie*
Volgens de geïnterviewden ontbreekt het aan een kader vanuit de korpsleiding. Daarnaast wordt een gebrek aan doorzettingsmacht ervaren omdat de korpsleiding geen bestuurlijke besluiten neemt ten aanzien van de Wpg. Tenslotte vindt geen monitoring plaats op de uitvoering van de Wpg.

4.2 Verantwoordelijke (artikel 1.f)

Mandaatbesluit

- 4.2.1 *Norm*
Conform artikel 1f Wpg dient een korps een mandaatbesluit op te stellen waarin formeel wordt aangeduid dat de korpsbeheerder zijn mandaat geeft aan de korpschef voor het implementeren van maatregelen om te voldoen aan de Wpg.
- 4.2.2 *Bevindingen*
Er is een vigerend mandaatbesluit van 16 november 2010, welke het mandaat regelt, de ondermaat, de volmacht, de subvolmacht en de machtigingen. Hierin wordt de Wpg expliciet genoemd.
Hiermee wordt voldaan aan Art. 1.f van de Wpg.

4.3 Kwaliteitsaspecten van politiegegevens (artikel 3 en 4)

4.3.1 Norm

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

4.3.2 Bevindingen

Het voldoen aan de bepalingen van deze artikelen is een aangelegenheid waarin zo ongeveer alle geledingen van de politie zijn betrokken. Hierom is het in het bijzonder van belang dat het zwaartepunt van het voldoen aan deze criteria ligt bij de eerste vastlegging van gegevens.

Het korps heeft de volgende criteria voor het verschil tussen Art. 8 versus Art. 9 onderzoeken op intranet geplaatst:

- Artikel 8 gaat over de verwerking van persoonsgegevens met het oog op de uitvoering van de dagelijks politietaken, ofwel het 'basispolitiewerk'. Een paar voorbeelden hiervan kunnen zijn:
 - Surveillance;
 - Afhandeling van de verkeersproblematiek;
 - Het verlenen van hulp;
 - Het handhaven van wetten en regels;
 - Ook eenvoudige recherche werkzaamheden zoals het onderzoeken van diefstallen en inbraken ('6-uurszaken'), het veilig stellen van sporen en het opnemen van een aangifte van een inbraak, vallen onder een artikel 8 verwerking.
- Een artikel 9 verwerking houdt in dat de Politie overgaat tot een gerichte en omvangrijke verzameling van gegevens over personen, met als doel de rechtsorde te herstellen of schendingen daarvan te voorkomen. Waar het in deze gevallen om gaat is dat de politie, naar aanleiding van een naar tijd beperkte gebeurtenis of situatie dan wel een serie van gebeurtenissen, over gaat tot gerichte en omvangrijke gegevensverzameling over personen. Een paar voorbeelden hiervan kunnen zijn:
 - een opsporingsonderzoek (er is bijvoorbeeld een moord gepleegd);
 - een verkennend onderzoek (er is veel drugsmisdaad in een bepaald gebiedesignaleerd, of de aanpak van de overlast bij een school of coffeeshop);
 - een landelijke coördinatieonderzoeken (bijvoorbeeld landelijke verkiezingen);
 - het bewaken en beveiligen van personen;
 - als ten aanzien van een veelpleger een dossier wordt opgemaakt ten behoeve van de verdere aanpak, is er vaak sprake van een artikel 9 verwerking.
- Binnen regio-Noord is afgesproken dat ten minste deze zaken een artikel 9 verwerking zijn:
 - Binnen tactische opsporing, TGO / SGO is er altijd sprake van een artikel 9 onderzoek;
 - Als er BOB aanvraag is gedaan, met uitzondering van het alleen opvragen van informatie / beelden (artikel 126 n t/m ni Wetboek van Strafvordering);
 - Als de onderzoeksduur de termijn van 5 dagen overschrijdt, of als de verwachting is dat de termijn van 5 dagen wordt overschreden.

Uit de audit is gebleken dat doelbinding een lastig begrip is. Daarnaast is het ook niet altijd even makkelijk te bepalen wanneer politiegegevens relevant zijn. Verder is aangegeven dat de vastleggingen in BVO en BVH onvolledig zijn. Dit is onder meer te wijten aan de administratieve last voor het vastleggen en het ontbreken van koppelingen tussen applicaties. De moeilijkheid van doelbinding blijkt onder meer bij het verzamelen van gegevens over hangjongeren zonder dat een overtreding

ding is geconstateerd. In dit geval is er geen sprake van doelbinding. Aangegeven wordt dat deze gegevens later wel van belang kunnen zijn bij het opsporen van strafbare feiten.

De CIE besteedt specifieke aandacht aan de kwaliteitsaspecten van politiegegevens. Deze aandacht heeft ook te maken met de bijzondere aard van hun taakstelling. In opzet voldoet de CIE aan de kwaliteitscriteria. Verder is de toezichthoudende rol van het OM een goede waarborg. De CIE OvJ ziet toe op rechtmatigheid, juistheid, volledigheid van informatie. De CIE OvJ ziet toe op naleving van de Wpg bij alle artikel 12 processen-verbaal.

Vanwege de bijzondere aard van de taakstelling van de RID, gaat de RID zorgvuldig om met politiegegevens. Bij de RID hebben wij de opzet door het ontbreken van een handboek niet vast kunnen stellen. De RID wacht, zoals eerder aangegeven, op het landelijk definitief vast te stellen handboek. Ook een toezichthoudende taak door een onafhankelijk orgaan als een OvJ, ontbreekt bij de RID. Wel vindt toezicht plaats op de uitvoering door hoofd RID in afstemming met de korpschef. Verder wordt informatie van de RID in principe niet gebruikt in een strafzaak. Als een informant nuttige informatie heeft voor de CIE, dan wordt de CIE OvJ erbij gehaald om te borgen dat een OvJ bij de zaak wordt betrokken.

Voor het runnen van informanten maakt de RID gebruik van checklisten, deze moeten de volledigheid en rechtmatigheid van de informatie borgen. Daarnaast moeten runners gecertificeerd zijn om informanten te mogen runnen. Ook wordt de betrouwbaarheid van de verkregen informatie bepaald voordat de informatie in de netto-omgeving komt. Door het veredelen van de bronnen kan de RID een inschatting maken van de betrouwbaarheid van de verkregen informatie.

Uit de interviews komt naar voren dat de Wpg een onderwerp is dat binnen de Infodesk aandacht krijgt. Met regelmaat vinden interne overleggen plaats waar praktijkcases worden behandeld. Medewerkers vragen zich dagelijks af wat wel en niet mag in het kader van de Wpg. De Infodesk is zich er van bewust dat de informatiesystemen BVO en BVH niet Wpg-proof zijn. De Infodesk ziet daarom toe op de rechtmatigheid bij verstrekkingen en ter beschikking stellen van informatie.

Bij de recherche is sinds kort een registratie-functionaris vrijgemaakt om toe te zien op de kwaliteit van vastleggingen. Aangegeven is dat deze werkwijze de kwaliteit van vastleggingen heeft verbeterd. Hiermee laat het korps zien dat zij aandacht besteden aan de vastlegging.

De volgende beheersmaatregelen zijn geïmplementeerd, gericht op het voldoen aan deze criteria:

- Een security beleidsplan, waarin de kwaliteit van gegevens aandacht krijgt, is opgesteld door de drie samenwerkende noordelijke korpsen;
- Een aantal procedures en checklisten is opgesteld om volledigheid en juistheid te waarborgen;
- Een aantal leidinggevenden bespreekt de onderwerpen van de Wpg tijdens interne overleggen;
- Registratiesystemen zoals BVH en BVO dwingen via de workflow bepaalde vastleggingen af. Op deze wijze wordt bijvoorbeeld volledigheid nagestreefd, zoals voor de MRO bij BVO;
- Bij de recherche is er aandacht voor vastlegging van bronnen en hoe informatie uit andere onderzoeken is verkregen;
- Bij de recherche is de registratie-functie in het leven geroepen om toe te zien op de kwaliteit van vastleggingen;

- Wpg-posters zijn opgehangen om medewerkers te informeren over de Wpg;
- Op het intranet van het korps staat informatie over de Wpg.

Kwaliteitsbewaking met TrueBlue in BVH

Het korps Groningen gebruikt het scanhulpmiddel TrueBlue voor de bewaking van de kwaliteit van een aantal velden in BVH. Landelijk is er een lijst met kennisregels opgemaakt, die elk korps naar behoefte in BVH kan activeren. Door het korps Groningen worden geen eigen kennisregels gemaakt. De beschikbare kennisregels zijn gedocumenteerd.

Informatievoorziening

De landelijke systemen, zoals onder andere BVH en BVO, en de regionale systemen zijn niet voorzien van beheersmaatregelen op het gebied van termijnen voor verwijderen en vernietigen van politiegegevens. De regels voor de verwijdering van oude gegevens zijn moeilijk uitvoerbaar omdat het handmatig moet gebeuren.

4.3.3

Oordeel over artikel 3 en 4

Het korps heeft de criteria voor het verschil tussen Art. 8 versus Art. 9 onderzoeken op intranet geplaatst.

Hiermee wordt voldaan aan de Wpg.

Het korps Groningen gebruikt TrueBlue voor de bewaking van de kwaliteit van een aantal velden in BVH.

Er zijn Wpg cursussen gegeven. Daarna is het Wpg bewustzijn weggeëbd bij gebrek aan continuïteit in de communicatie.

Het korps Groningen heeft de uitrol naar Blauw nog niet afgerond.

Er wordt een gebrek aan doorzettingsmacht ervaren en er vindt geen monitoring plaats op de uitvoering van de Wpg.

Hiermee wordt niet voldaan aan de Wpg.

Het procesproces bevat waarborgen voor deze aspecten. De PDCA-cyclus sluit via het OM en de rechter.

Tevens is bij de recherche nu meer aandacht voor de vastlegging van bronnen en hoe informatie uit andere onderzoeken wordt verkregen. Er is een registratiefunctie om toe te zien op de kwaliteit.

Hiermee wordt voldaan aan de Wpg.

De CIE heeft een proceshandboek. De CIE OvJ houdt toezicht.

Bij de RID liggen de kwaliteitscriteria al in het doel van de taak vast. Het handboek voor RID ligt ter goedkeuring bij de AIVD.

Hiermee wordt voldaan aan de Wpg.

De landelijke en regionale informatiesystemen zijn nog niet Wpg-proof.

Hiermee wordt niet voldaan aan de Wpg.

4.4 Gevoelige gegevens (artikel 5)

4.4.1 Norm

Artikel 5. 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

Er zijn geen niet-toegestane gegevensverzamelingen gebaseerd op gevoelige gegevens aangetroffen.

Het korps heeft procedurele regels voor de omgang met gevoelige gegevens op intranet (PING) staan. Hierin is vastgelegd dat medewerkers van Politie Groningen gevoelige gegevens alleen mogen vastleggen als dat onvermijdelijk is voor het uitvoeren van de politietaak.

In de binnen het korps Groningen beschikbare artikel 13 protocollen wordt dit onderwerp behandeld en waar nodig toegelicht.

Hiermee wordt voldaan aan artikel 5 van de Wpg.

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

Er is een autorisatietabel van het Shared Service Centrum Noord (SSCN). Deze autorisatiematrix bevat de belangrijkste rollen binnen een korps en geeft initieel aan welke bevoegdheden in de basisvoorzieningen BVCM, BVH en BVO worden gekoppeld aan een rol, evenals autorisaties in andere systemen zoals GMS. Bij veel rollen heeft een medewerker actief toegang tot bijvoorbeeld BVH en BVO van het eigen korps, en mag raadplegen in de overeenkomstige basisvoorziening van de andere twee korpsen.

Het autorisatieproces in het korps Groningen wordt gezamenlijk uitgevoerd door het politiekorps, het SSCN en de vtsPN. Het beheer vindt plaats op basis van een procesbeschrijving voor autorisatiebeheer. Er is een procedure die de toekenning van autorisaties beschrijft. De privacyfunctionaris schoont jaarlijks de autorisaties voor applicaties.

De rechten op de mappenstructuur van de kantoorautomatiseringsomgeving zijn minder goed geregeld. Een uitzondering hierop zijn de MRO waardige onderzoeken in BVO. Functioneel beheer maakt bij ontvangst van een aanvraagformulier voor een MRO direct een map aan voor het betreffende onderzoek op de I-schijf. De gegevensbeheerder van een onderzoek kan andere teamleden vervolgens autoriseren voor deze map.

De CIE OvJ heeft een rol in het toetsen van de autorisaties van de CIE. Er bestaat op dit moment een proces waarbij de autorisaties van de CIE-medewerkers worden voorgelegd bij de OvJ. Dit proces is echter niet beschreven.

Er zijn twee onderzoeken uitgevoerd vanuit Informatiebeveiliging bij de Afdeling Integriteit en bedrijfsveiligheid, gericht op de autorisaties. Deze hebben plaatsgevonden in mei 2009 en februari 2010. In beide rapporten is de conclusie dat het systeem van autorisaties niet voldoet aan de daaraan te stellen normen zoals beschreven in het Basisbeveiligingsniveau Nederlandse Politie (BBNP) en de Wpg.

Het eerste rapport is "Interne audit van de autorisaties", Afdeling Integriteit en bedrijfsveiligheid, Informatiebeveiliging, mei 2009. Hierin wordt een telling beschreven van de autorisaties in 5 applicaties, namelijk BPS-PCS, HKS, BVO, GRN en BVH. Deze autorisaties zijn vergeleken met de medewerkers die in 2009 dienst zijn. Het rapport trekt een tweetal conclusies:

- vtsPN-NO is niet in staat de door Politie Groningen opgevraagde lijsten met gebruikers voor alle systemen volledig en betrouwbaar op te leveren. Daardoor moest het onderzoek worden beperkt tot de vijf voornoemde applicaties en kon geen onderzoek worden gedaan naar autorisaties in de kantooromgeving (mappen), BlueView en Corsa. Dit staat op blz. 3 van dat rapport;
- Van de in totaal 5.249 autorisaties zijn er 2.920 (56%) rechtmatig en 2.394 (44%) onrechtmatig, namelijk van personen die niet in 2009 voor Politie Groningen werkzaam zijn. Dit staat op blz. 4 van dat rapport

Het onderzoek naar autorisaties is opnieuw uitgevoerd in februari 2010. Het rapport is "Interne audit van het systeem van autorisaties 2010", Afdeling Integriteit en bedrijfsveiligheid, Informatiebeveiliging. Hierbij zijn de autorisaties beschouwd in BPS-PCS, Ping, BVO, HKS, Kantoorautomatisering, BlueView, BVH, Corsa, BVCM, Beaufort en SmartStream. Het rapport trekt een tweetal conclusies:

- De onderzoeker stelt vast dat Politie Groningen niet kan aantonen wie er toegang heeft gehad tot de politiegegevens, dus ook niet of er sprake is van onrechtmatige toegang tot die politiegegevens. Dit staat op blz. 3 van dat rapport;
- Van de in totaal 14.176 autorisaties zijn er 10.764 (76%) rechtmatig en 3.415 (24%) onrechtmatig, namelijk van personen die niet in 2010 voor Politie Groningen werkzaam zijn. Dit staat op blz. 5 van dat rapport.

Geïmplementeerde beheersmaatregelen zijn:

- Er is een SSCN brede autorisatieprocedure, waarin ook de registratie wordt geadresseerd;
- De chef is verantwoordelijk voor het aanvragen van autorisaties;
- Voor wat betreft BVO krijgt de functioneel beheerder een lijst met ontslagen medewerkers vanuit het personeelssysteem;
- Een BVO-account wordt na een periode van geen activiteit na 3 maanden gelockt, na 6 maanden geblokkeerd en na een jaar verwijderd;
- Hoofd CIE en Hoofd RID houden zelf toezicht op autorisaties en zien ook toe op het verwijderen van autorisaties bij uitdiensttreding;
- De RID werkt met een sleutelijst voor het betreden van de afdeling;
- Voordat medewerkers voor BVH, BVO en BlueView worden geautoriseerd, moeten zij eerst een opleiding succesvol afronden voor het betreffende systeem;
- Het Veiligheidshuis zit in een locatie van het OM en maakt gebruik van de infrastructuur en beveiliging van dit pand. De Hoofd OvJ kent de autorisaties toe aan medewerkers van het Veiligheidshuis.

4.5.3 *Oordeel over het autorisatieproces*

De korpsautorisatiematrix is ingericht zoals redelijkerwijs kan worden verwacht en geeft tevens weer op welke wijze rollen binnen de drie korpsen samenwerken bij toegang tot de applicaties.

Hiermee voldoet het korps voor de autorisatiematrix aan de Wpg.

Het aanvraagproces van autorisaties verloopt via SSCN en vtsPN, en is gedocumenteerd.

Er zijn echter twee onderzoeken uitgevoerd vanuit Informatiebeveiliging bij de Afdeling Integriteit en bedrijfsveiligheid, gericht op de autorisaties. Deze hebben plaatsgevonden in mei 2009 en februari 2010. In beide rapporten is de conclusie dat het systeem van autorisaties niet voldoet aan de daaraan te stellen normen zoals beschreven in het Basisbeveiligingsniveau Nederlandse Politie (BBNP) en de Wpg.

Het verwijderproces van autorisaties verloopt via SSCN en vtsPN, en is gedocumenteerd. De rechten op de mappenstructuur van de kantoorautomatiseringsomgeving zijn echter minder goed geregeld.

Hiermee voldoet het korps voor aanvragen en verwijderen niet aan de Wpg.

De privacyfunctionaris schoont jaarlijks de autorisaties voor applicaties. Wij zijn van mening dat de privacyfunctionaris een wettelijke taak heeft toezicht uit te oefenen, en schonen van autorisaties in dit kader een oneigenlijke taak is. Schoning behoort te worden uitgevoerd als een gedocumenteerd en controleerbaar proces via de lijn. Hiermee wordt voor schoning niet voldaan aan de Wpg.

Autorisaties voor medewerkers van de CIE en RID worden toegekend door het hoofd van de CIE respectievelijk RID. De CIE OvJ heeft het autorisatiebeleid goedgekeurd. Hiermee wordt voldaan aan de Wpg.

Binnen SSCN wordt iedere aanvraag voor een mutatie op een autorisatie geregistreerd en bewaard.

Hiermee wordt voldaan aan de Wpg.

4.6 Geautomatiseerd Vergelijken (GV)/In Combinatie Met Elkaar Verwerken (ICMEV)(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 bevoegd functionaris- zijnde de leider van het betreffende onderzoek of zijn plaatsvervanger, voor dat onderzoek verder worden verwerkt. Indien politiegegevens in combinatie met elkaar worden verwerkt, worden van die verwerking nader genoemde gegevens vastgelegd (protocolplicht).

4.6.2 Bevindingen

De begrippen geautomatiseerd vergelijken en in combinatie met elkaar verwerken zijn nog onvoldoende bekend binnen het korps. Hierdoor bestaat het risico dat medewerkers ruimer verwerken dan de Wpg toestaat. Doordat de medewerkers in BVH alle informatie ouder dan één jaar na de laatste verwerking kunnen raadplegen, bestaat het risico dat geautomatiseerd vergelijken niet conform Wpg verloopt. Medewerkers gaan er van uit dat ze de informatie die ze te zien krijgen door middel van een zoekopdracht ook mogen gebruiken. Medewerkers zijn zich onvoldoende bewust dat dit volgens de Wpg niet mag.

De Infodesk is onder andere belast met het in combinatie met elkaar verwerken en geautomatiseerd vergelijken. Bij de Infodesk zijn enkele medewerkers geautoriseerd voor Blueview. Nieuwe inzichten verkregen vanuit verschillende bronsystemen worden vastgelegd.

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

- Het werkproces Infodesk is beschreven. De status van deze werkinstructie is echter nog steeds concept.
- De CIE legt de bronnen vast bij opdracht tot analyse.
- De RID volgt in deze eveneens een stringente vastlegging van bronnen.

4.6.3 Oordeel over artikel 11

De begrippen geautomatiseerd vergelijken en in combinatie met elkaar verwerken zijn nog onvoldoende bekend binnen het korps.

Hiermee wordt niet voldaan aan artikel 11.1, 11.2, 11.4 en 11.5 van de Wpg.

De Infodesk is onder andere belast met het in combinatie met elkaar verwerken en geautomatiseerd vergelijken. Ondanks dat er een concept werkinstructie is, zijn de rollen in het kader van de Wpg nog niet daadwerkelijk expliciet belegd. Hiermee wordt deels voldaan aan de Wpg.

Doordat in combinatie met elkaar verwerken niet eenduidig is vastgesteld, is het onbekend wanneer het bevoegd gezag moet worden geraadpleegd. Hiermee wordt niet voldaan aan artikel 11.4 van de Wpg.

Doordat het vergelijken van politiegegevens met andere dan politiegegevens volgens artikel 11.5 niet eenduidig is omschreven, is het onbekend welke handelingen onder dit artikellid vallen.

Hiermee wordt niet voldaan aan artikel 11.5 van de Wpg.

Aanvragen die via de Infodesk binnenkomen worden geprotocolleerd.
Hiermee wordt voldaan aan artikel 32.1.d van de Wpg voor de protocollering.

4.7 Bewaartermijnen (artikel 14)

4.7.1 Norm

Politiegegevens worden vernietigd zodra zij niet langer noodzakelijk zijn voor de uitvoering van de dagelijkse politietaak (artikel 8) en worden in ieder geval uiterlijk vijf jaar na de datum van eerste verwerking verwijderd. De politiegegevens die niet langer noodzakelijk zijn voor het doel van het onderzoek, worden verwijderd, of 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 landelijke informatie systemen zijn niet Wpg proof. Daardoor is uitvoering geven aan bepaalde Wpg-eisen onmogelijk zonder sterke toename van de administratieve last. Zo is bijvoorbeeld bij het gebruik en opschoning van BVH het niet kunnen onderscheiden van de artikelen 8 en 9 Wpg een knelpunt. Ook het ontbreken van een koppeling tussen BVH en BVO wordt als knellend ervaren.

Gegevens ouder dan één jaar na eerste vastlegging in BVH worden niet achter schot gezet. Medewerkers gaan er van uit dat de gegevens die ze te zien krijgen ook mogen worden gebruikt voor verdere verwerking. Met name medewerkers op operationeel niveau zijn zich hiervan niet voldoende bewust.

De werkbaarheid van de bewaartermijnen in Wpg levert een divers beeld. Sommige functionarissen geven aan oude informatie onbruikbaar te achten, anderen geven aan groot belang te hechten aan alle informatie die ooit is verzameld.

De regels voor de verwijdering van oude gegevens zijn duidelijk bij de leidinggevendenden. Echter in de praktijk zijn ze moeilijk uitvoerbaar omdat het verwijderen handmatig moet gebeuren. Daardoor krijgt het verwijderen en schonen nog onvoldoende prioriteit. Ook is niet voor iedereen helder wie verantwoordelijk is voor deze activiteiten.

Het opschonen van artikel 9 onderzoeken kan nog verder worden geoptimaliseerd. Hierbij is de ketensamenwerking en specifiek de overdracht van informatie over afgesloten zaken van OM naar de politie een aandachtspunt. Het OM heeft inzicht in de wijze van afdoening van zaken en moet dit delen met de politie om aan te geven wanneer WPG verwijderingstermijnen gaan lopen

Geïmplementeerde beheersmaatregelen zijn onder meer:

- Binnen het kantoor zijn Wpg-posters met informatie over bewaartermijnen opgehangen;
- Medewerkers van de Infodesk zien toe op bewaartermijnen bij verstrekken van informatie;
- CIE OvJ voert periodiek controles uit waarbij ook naar de bewaartermijnen wordt gekeken.

4.7.3 Oordeel over bewaartermijnen voor artikel 8

Gegevens ouder dan één jaar na eerste vastlegging in BVH worden niet achter schot gezet. Medewerkers gaan er van uit dat de gegevens die ze te zien krijgen ook mo-

gen worden gebruikt voor verdere verwerking. Met name medewerkers op operationeel niveau zijn zich hiervan niet voldoende bewust.

De regels voor de verwijdering van oude artikel 8 gegevens zijn moeilijk uitvoerbaar omdat het handmatig moet gebeuren. Daardoor krijgt het verwijderen en schonen nog onvoldoende prioriteit.

Artikel 8 gegevens worden nog niet op het voorgeschreven moment vernietigd.

Hiermee wordt niet voldaan aan de artikelen 8.2, 8.3, 8.6 en 14.1 van de Wpg.

4.7.4 *Oordeel over bewaartermijnen voor artikel 9*

Het opschonen van artikel 9 onderzoeken kan nog verder worden geoptimaliseerd. Hierbij is de ketensamenwerking en specifiek de overdracht van informatie over afgesloten zaken van OM naar de politie een aandachtspunt.

Doordat het juiste moment van verwijdering niet bekend is, kan niet 5 jaar na verwijdering worden vernietigd.

Hiermee wordt niet voldaan aan de artikelen 9.4 en 14.1 van de Wpg.

4.7.5 *Oordeel over de bewaartermijnen voor artikel 10 en 12*

Bij de CIE voert de OvJ periodiek controles uit waarbij ook naar de bewaartermijnen wordt gekeken. Informatie van informanten wordt binnen een termijn van maximaal 4 maanden verwerkt en netto in een andere omgeving gezet. Dit zit vast in de werkwijze van de CIE.

Informatie wordt binnen de CIE en RID regelmatig gecontroleerd en geschoond. Bij de RID gebeurt dit elke 5 jaar. Bij de CIE toetst de CIE-OvJ jaarlijks het informantenregister.

Hiermee wordt voldaan aan de artikelen 10.6, 12.2, 12.6 en 14.1 (voor artikel 10 en 12 gegevens) van de Wpg.

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 het realiseren van artikel 15 Wpg is een aantal maatregelen getroffen bij Politie Groningen.

De Infodesk valt onder de divisie Informatie. Deze Infodesk stelt informatie ter beschikking volgens vaste procedures. Op andere niveaus in het korps bestaat minder structuur in de informatie-uitwisseling. Er is aangegeven dat sommige medewerkers gebruik maken van informatie die volgens de Wpg had moeten worden verwijderd. Dit is moeilijk te voorkomen als de informatie niet wordt afgeschermd in de systemen. Ook het protocolleren van het ter beschikking stellen van informatie is een aandachtspunt. Uit de audit komt naar voren dat leidinggevend niet altijd goed zicht hebben op welke informatie ter beschikking wordt gesteld.

Bij CIE- en MRO-mutaties maakt men gebruik van de coderingen 00, 01 en 11. De door het korps gehanteerde omschrijving is:

- 00= niet operationeel te gebruiken;
- 01= slechts te gebruiken na overleg met de CIE;
- 11=operationeel te gebruiken.

Informatie van onderzoeken wordt soms door rechercheurs bij Politie Groningen, naast BVO en BVH, ook in eigen persoonlijke en groepsmappen vastgelegd. Daardoor ontstaat een risico op onrechtmatig gebruik en bewaring. Daarnaast is dit niet bevorderlijk voor het delen van informatie. Met name restinformatie wordt niet gedeeld, omdat dit nauwelijks in BVO wordt vastgelegd.

In Bijlage 1.8 "Functies die aansluiten bij de werkprocessen/Opleiding en instructie" bij het implementatierapport van de "Interregionale projectgroep implementatie wet politiegegevens Drenthe, Fryslân en Groningen" van 1 november 2009 staat dat in Groningen (per regio) 25 bevoegde functionarissen zijn aangewezen, namelijk de unitchefs recherche, de chefs RID en CIE en de chefs districtsondersteuning. Bij navraag hebben wij vernomen dat er in totaal 75 bevoegd functionarissen zijn, die in 2009 een verplichte opleiding hebben gevolgd. Daarna zijn enkele nieuwe bevoegd functionarissen opgeleid. In de cursus is onder andere aandacht besteed aan de weigeringsgronden conform artikel 15.2.

Wij hebben vernomen dat door het achterblijven van de ICT de Wpg-kennis van de bevoegd functionarissen is weggezaakt. Er zijn geen herhalingscursussen of opfriscursussen geweest in 2010 en 2011. Het korps heeft besloten in 2012 een opfriscursus van een dag aan te bieden.

Geïmplementeerde beheersmaatregelen zijn onder meer:

- CIE stelt alleen gegevens ter beschikking via een proces-verbaal verloopt na toestemming te hebben verkregen van de CIE OvJ;
- RID gaat zorgvuldig om met het ter beschikking stellen van informatie. Zie ook het thema verstrekkingen. Hoofd RID ziet toe op de omzetting van bruto naar netto informatie;

- Iedereen die voor BVO is geautoriseerd kan zien als iemand een object is van onderzoek, maar niet de specifieke informatie. Voor specifieke informatie is toestemming nodig van de teamleider van dat onderzoek.

4.8.3

Oordeel over ter beschikking stellen

De Infodesk stelt informatie ter beschikking volgens vaste procedures.

Een deel van de politiegegevens van het korps Groningen zijn echter opgeslagen in persoonlijke en groepsmappen met een risico op onrechtmatig gebruik en bewaring. Het gebruik van de mappenstructuur binnen Opsporing belemmert de Infodesk met het zoeken en vergelijken met andere onderzoeken. Hierdoor kan informatie ook niet met andere korpsen worden gedeeld.

Van het opnemen van restinformatie in het Zwacri register of het aanmaken van een nieuwe registratie wordt maar zeer incidenteel gebruik gemaakt. Voor hernieuwd gebruik van informatie is geen structuur aanwezig.

Hiermee wordt niet voldaan aan de Wpg.

Bij CIE- en MRO-mutaties maakt men gebruik van de coderingen 00, 01 en 11.

Hiermee wordt voldaan aan de Wpg.

De 75 bevoegd functionarissen hebben in 2009 een verplichte opleiding gevolgd.

Daarna zijn enkele nieuwe bevoegd functionarissen opgeleid. Door het achterblijven van de ICT is hun kennis weggezaakt. Er zijn geen herhalingscursussen of opfriscursussen geweest in 2010 en 2011. Het korps heeft besloten in 2012 een opfriscursus van een dag aan te bieden.

Hiermee wordt deels voldaan aan de Wpg.

In de cursus voor de bevoegd functionarissen is onder andere aandacht besteed aan de weigeringsgronden conform artikel 15.2.

Hiermee wordt voldaan aan de Wpg.

4.9 Verstrekken (artikel 16/24)

4.9.1 Norm

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

4.9.2 Bevindingen

De landelijke verstrekkingenwijzer is tijdens de opleiding voor bevoegd functionaris uitgereikt en is raadpleegbaar op intranet. Er is geen regionaal verstrekkingenschema. Het korps heeft op het intranet een gegevensbeheerlijst staan met de organisaties waaraan informatie mag worden verstrekt.

In het geval van het Veiligheidshuis is met de ketenpartners een convenant met een artikel-20 besluit opgesteld. Alle ketenpartners hebben getekend voor geheimhouding. Notulen en afspraken worden in JCO-support en of in VIS-2 vastgelegd.

Op intranet staat een gegevensbeheerlijst met de organisaties waaraan informatie mag worden verstrekt.

Nieuwe convenanten, waar nodig inclusief een artikel 20 besluit, worden door een lijnchef opgesteld. Deze stukken worden ter correctie aangeboden aan de privacyfunctionaris of de Juridische Dienst. Indien akkoord word het besluit getekend door de korpsbeheerder. Er is een inhaalslag gaande op de bestaande convenanten.

Naar de mening van het korps vinden er momenteel geen geautomatiseerde verstrekkingen plaats, anders dan de in het Besluit politiegegevens toegestane verstrekkingen, zoals aan RDW bij het invorderen van een kentekenbewijs. Sinds kort is Amazon in gebruik. Deze applicatie wordt op het moment van ons onderzoek pas gebruikt voor drie items. Het is nog niet bekend of Amazon in de toekomst zal worden gebruikt voor geautomatiseerde verstrekking. Volgens de functioneel beheerder en de proceseigenaar is dat nu nog niet het geval.

De meeste verstrekkingen van politiegegevens lopen via de Infodesk. Bij deze afdeling is vastgelegd in de procedures dat alle verstrekkingen moeten worden geregistreerd. Alleen het verstrekken van gegevens afkomstig uit algemene bronnen, zoals vanuit RDW en GBA, wordt niet vastgelegd omdat deze systemen breed raadpleegbaar zijn.

Het vastleggen van verstrekkingen middels een I90-formulier kent nog veel onduidelijkheid bij medewerkers. Medewerkers zijn zich onvoldoende bewust op welke wijze verstrekkingen moeten worden geprotocolleerd en zien dit als een administratieve last. Het korps beschikt over een rapport van de Mystery Guest, waaruit blijkt dat veel medewerkers nog erg terughoudend zijn met het verstrekken van politiegegevens. Naar de mening van het korps is dit mogelijk een na-ijleffect van de Wpolr. Uit de rapportage blijkt dat veelal geen informatie wordt verstrekt en vaak wordt verwezen naar de privacyfunctionaris.

CIE verstrekt alleen informatie met toestemming van CIE OvJ. Verder wordt vanuit CIE benadrukt dat door hen verstrekte en ter beschikking gestelde informatie niet zonder overleg mag worden doorverstrekt.

4.9.3

Oordeel over verstrekkingen

De landelijke verstrekkingenwijzer is tijdens de opleiding voor bevoegd functionaris uitgereikt en is raadpleegbaar op intranet. Het korps heeft op het intranet tevens een gegevensbeheerlijst staan met de organisaties waaraan informatie mag worden verstrekt.

Hiermee wordt voldaan aan de Wpg.

Bij het Veiligheidshuis hebben de ketenpartners getekend voor geheimhouding. CIE benadrukt dat de door hen verstrekte gegevens niet verder mogen worden doorverstrekt.

Hiermee wordt voldaan aan de Wpg.

Nieuwe convenanten, waar nodig inclusief een artikel 20 besluit, worden centraal beoordeeld en, indien akkoord, getekend door de korpsbeheerder. Er is een inhaalslag gaande op de bestaande convenanten.

Hiermee wordt deels voldaan aan de Wpg.

Naar de mening van het korps vinden er momenteel geen geautomatiseerde verstrekkingen plaats, anders dan de in het Besluit politiegegevens toegestane verstrekkingen, zoals aan RDW bij het invorderen van een kentekenbewijs.

Hiermee wordt voldaan aan de Wpg.

De Infodesk legt alle verstrekkingen vast. Het verstrekken en het vastleggen van verstrekkingen door andere medewerkers via een I90 in BVH verloopt echter nog niet goed, mede doordat de Wpg in onvoldoende mate wordt begrepen en doordat het vastleggen via een I90 als een administratieve last wordt ervaren.

Hiermee wordt niet voldaan aan de Wpg.

De wel vastgelegde gegevens over verstrekkingen worden bewaard.

Hiermee wordt voldaan aan de Wpg.

Bij de Infodesk is toezicht door de leidinggevende. Bij andere medewerkers is onvoldoende toezicht op het gebruik van de I90 in BVH.

Hiermee wordt niet voldaan aan de 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*

Verzoeken in het kader van de rechten van betrokkenen verlopen via de privacyfunctionaris. In 2010 zijn er voor de Politie Groningen ongeveer 200 verzoeken in het kader van artikel 25 behandeld door de privacyfunctionaris.

4.10.3 *Oordeel over rechten van betrokkenen*

De privacyfunctionaris handelt verzoeken af in het kader van de rechten van betrokkenen. Dit is een ongewenste vermenging van functies, aangezien de privacyfunctionaris toezicht dient te houden op dit proces. Hierop komen wij terug bij het onderwerp "Privacyfunctionaris".

Niettemin wordt het proces voor de artikelen 25 en 28 goed doorlopen. Hiermee wordt voldaan aan de artikelen 25 en 28 van de Wpg.

4.11 Protocolplicht (artikel 32)

4.11.1 Norm

De verantwoordelijke draagt zorg voor de schriftelijke vastlegging van:

- a. de doelen van Art. 9 onderzoeken;
- b. gegevens die op grond van ondersteunende taken worden vastgelegd (Art. 13.4);
- c. de toekenning van autorisaties (Art. 6);
- d. de geautomatiseerde vergelijking of het in combinatie met elkaar verwerken van politiegegevens (Art. 8.3 en 11.1, 11.2 en 11.4);
- e. de hernieuwde verwerking van politiegegevens op grond van Art. 9 of 10 (Art. 14.3);
- f. de verstrekking van politiegegevens (Paragraaf 3);
- g. signalen van onbevoegde of onrechtmatige verwerkingen;
- h. de geautomatiseerde vergelijking van gegevens met openbare bronnen (Art. 11.5).

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

4.11.2 Bevindingen

Een deel van de protocolplicht zit verweven in meerdere artikelen van de Wpg, bijvoorbeeld autorisaties en verstrekkingen. Zie daarvoor de bevindingen bij de eerder genoemde artikelen.

Artikel 32.1.a

Een onderzoek conform Art. 9 wordt verwerkt in BVO, BVH of de mappenstructuur. Bij het starten van een onderzoek wordt een Melding Recherche Onderzoek (MRO) verstuurd naar de landelijke verwijsindex VROS, onder beheer van KLPD. Een overzicht van de meldingen is in een map geplaatst in de omgeving van de kantoorautomatisering, welke toegankelijk is voor de privacyfunctionaris. Een kopie van deze lijst over de periode 2010 en 2011 is aan ons overlegd.

Artikel 32.1.b

Wij hebben het Artikel 13 Register met de landelijke en regionale artikel 13 applicaties opgevraagd, inclusief doel etc. conform artikel 13.4. Het korps heeft daarop informatie verstrekt over een aantal applicaties voor artikel 13, namelijk voor:

- FOIS;
- PAPOS;
- VRIS;
- VROS;
- HKS;
- VERONA;
- Observatieteam (OT);
- Team Politieonderhandelaars;
- Arrestatie Ondersteuning Eenheid (AOE).

Artikel 32.1.g

Een overzicht van onrechtmatige verwerkingen ontbreekt.

4.11.3 *Oordeel over protocolplicht*

Bij het starten van een onderzoek wordt een Melding Recherche Onderzoek (MRO) verstuurd naar de landelijke verwijsindex VROS, onder beheer van KLPD. Er is een overzicht van deze meldingen beschikbaar voor de privacyfunctionaris.

Doelbinding conform artikel 9.2 wordt niet altijd op de juiste wijze vastgelegd. De drie noordelijke korpsen hebben plannen BOSZ te implementeren, waarin onder andere het doel van een onderzoek wordt vastgelegd.

Hiermee wordt deels voldaan aan artikel 9.2 en 32.1.a van de Wpg.

Het korps Groningen beschikt over een aantal protocollen voor Artikel 13 gegevensverzamelingen. Dergelijke protocollen zijn echter nog niet beschikbaar voor alle Artikel 13 gegevensverzamelingen.

Hiermee wordt deels voldaan aan de artikelen 13.4 en 32.1.b van de Wpg.

Een overzicht van onrechtmatige verwerkingen ontbreekt.

Hiermee wordt niet voldaan aan artikel 32.1.g van de Wpg.

4.11.4 *Bevinding gemeenschappelijke verwerking*

Het Shared Service Center Noord (SSCN) is een gemeenschappelijk onderdeel van drie korpsen. De processen, lokale infrastructuur en lokale gegevensverzamelingen worden gedeeld tussen medewerkers van deze drie korpsen. In de stukken hebben wij geen bevestiging kunnen vinden dat wordt voldaan aan artikel 32.2 Wpg, namelijk dat een verantwoordelijke is aangewezen en dat deze het SSCN als een gemeenschappelijke verwerking heeft gemeld bij het CBP.

Navraag bij het korps leverde het volgende antwoord: "Directie SSCN: De drie korpsleidingen zijn verantwoordelijk, het is niet een zelfstandige entiteit. De medewerkers zijn in dienst van een van de drie korpsen. De privacy functionaris is bijvoorbeeld ondergebracht bij de JD van SSC, maar valt onder korps Groningen en is ook als zodanig aangemeld bij CBP."

Vervolgens is door het korps meegedeeld: "In SSCN zijn een aantal ondersteunende werkzaamheden samengevoegd, zoals de salaris- en personeelsadministratie, de juridische dienst en de facilitaire dienst. Ook de forensisch-technische recherche en enkele recherche specialiteiten zijn samengevoegd, waaronder de digitale recherche en de financiële recherche. Feitelijk zijn deze ondersteunend aan de drie korpsen. Wanneer er sprake zou zijn van een gemeenschappelijke verwerking zal deze niet plaatsvinden onder de verantwoordelijkheid van de SSCN, maar onder verantwoordelijkheid van een korps."

4.11.5 *Oordeel over gemeenschappelijke verwerking*

SSCN is een gemeenschappelijke activiteit van drie korpsen, waarbij iedere medewerker onder een van de drie korpschefs valt. Door het ontbreken van een landelijke richtlijn voor het positioneren een gemeenschappelijk onderdeel in relatie tot de Wpg, kunnen wij ons vooralsnog geen onderbouwd oordeel vormen over het wel of niet voldoen aan de Wpg.

Wij adviseren nader onderzoek, zowel landelijk om tot een richtlijn te komen over het positioneren van een gemeenschappelijke activiteit, als regionaal om de informatiestromen binnen SSCN in beeld te brengen en aan de Wpg te toetsen.

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

Binnen de regio Groningen was het de bedoeling om een jaar na de implementatie gezamenlijk een interne Wpg audit te starten om de balans op te kunnen maken. Hiervoor was binnen het korps Groningen al iemand benoemd. De interne Wpg audit is echter nooit gestart omdat de implementatie van de Wpg niet van de grond is gekomen. Op het moment dat er sprake was dat een externe audit zou worden uitgevoerd heeft de korpsleiding ervoor gekozen de inspanningen niet te richten op de interne audit maar op de externe audit.

Er zijn wel twee onderzoeken uitgevoerd vanuit Informatiebeveiliging bij de Afdeling Integriteit en bedrijfsveiligheid, gericht op de autorisaties. Deze hebben plaatsgevonden in mei 2009 en februari 2010. In beide rapporten is de conclusie dat het systeem van autorisaties niet voldoet aan de daaraan te stellen normen zoals beschreven in het Basisbeveiligingsniveau Nederlandse Politie (BBNP) en de Wpg.

4.12.3 Oordeel over interne audit

Er is geen interne Wpg audit functie, geen intern Wpg audit plan en geen interne Wpg audit rapportage.

Hiermee wordt niet voldaan aan de artikelen 3.1, 3.4 en 3.6 van de Regeling Periodieke Audit Politiegegevens (RPAP).

4.13 Privacyfunctionaris (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

Op 3 maart 2009 heeft de korpsbeheerder Groningen aan CBP de benoeming van de privacyfunctionaris gemeld, en daarbij gesteld dat deze functie niet strikt conform de handreikingen Wpg wordt ingericht. De Politie Groningen kiest voor een multifunctionele invulling van deze wettelijk voorgeschreven taak, en combineert dit met andere juridische taken zoals voor de WOB en BIBOB, primaire ondersteuner van het hoofd van de Divisie Informatie etc.

De privacyfunctionaris voert geen toezichthoudende taken uit. Er is een overzicht van meldingen onderzoeken artikel 9, welke aan ons is overlegd en die toegankelijk is voor de privacyfunctionaris. Er is tevens een zestal protocollen voor de artikel 13 gegevensverzamelingen. Er is echter geen overzicht van mutaties op autorisaties, geen overzicht van geautomatiseerde vergelijkingen, geen overzicht van verstrekkingen en geen overzicht van onrechtmatige verwerkingen.

De privacyfunctionaris is betrokken bij het afhandelen van verzoeken in het kader van de rechten van betrokkenen en eventuele daarmee samenhangende correcties conform de artikelen 25 en 28. In 2010 zijn er voor de Politie Groningen ongeveer 200 verzoeken in het kader van artikel 25 behandeld door de privacyfunctionaris.

Over 2010 is geen jaarverslag beschikbaar. Het was de intentie één rapport op te stellen voor Groningen, Friesland en Drenthe. Door een veranderende prioriteitstelling in het korps is dit verslag echter niet opgesteld. Hiermee wordt niet voldaan aan de Wpg voor wat betreft de toezichthoudende en de signalerende rol.

Medewerkers van het korps Groningen weten de privacyfunctionaris wel te vinden als zij vragen hebben over de Wpg. De privacyfunctionaris acteert als Wpg-loket en heeft vooral een uitvoerende en adviserende rol.

Er wordt voldaan aan de eis vanuit de Wpg dat er een privacyfunctionaris moet zijn, maar de invulling van deze taak is niet in overeenstemming met de Wpg.

4.14 Functionaris Gegevensbescherming (artikel 36)

4.14.1 Bevindingen

De functionaris gegevensbescherming bestaat niet als functie bij Politie Groningen. Aangegeven is dat Politie Groningen van mening is dat de functionaris gegevensbescherming geen toegevoegde waarde heeft ten opzichte van de privacyfunctionaris. Wel heeft het korps een functionaris die zich bezig houdt met informatiebeveiliging en privacybescherming. Deze medewerker geeft zelf aan dat de taken die hij uitvoert deels goed aansluiten op het profiel van de functionaris gegevensbescherming. De Wpg is volgens deze medewerker echter nog onvoldoende duidelijk om een praktische invulling te kunnen geven aan de functie. Informatiemanagement is een breed begrip en de Wpg is daar niet specifiek genoeg in.