



Ministerie van Veiligheid en Justitie

**Audit Wpg politie Noord- en Oost-
Gelderland**
Rapport

Datum
Status

7 december 2011
Definitief

Colofon

Afzendgegevens

Departementale Auditdienst

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

Contactpersoon

I
Senior auditors

T 070 370 65 60
M Wpg@minvenj.nl

Projectnaam

Audit Wet Politiegegevens

Ons kenmerk

DDS 5712393

Auteurs

I

Inhoud

Colofon 3

1 Assuranceverklaring 7

2 Samenvatting 9

3 Inleiding 18

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

4 Bevindingen 21

- 4.1 Inleiding 21
- 4.2 Verantwoordelijke (artikel 1.f) 22
- 4.3 Kwaliteitsaspecten van politiegegevens (art 3 en 4) 22
- 4.4 Gevoelige gegevens (artikel 5) 24
- 4.5 Autorisatie (art 6) 24
- 4.6 Geautomatiseerd Vergelijken/ In Combinatie Met Elkaar Verwerken (art 11) 25
- 4.7 Bewaartermijnen (art 14) 26
- 4.8 Ter beschikking stellen (art 15) 27
- 4.9 Verstrekken (art 16/24) 28
- 4.10 Rechten van betrokkenen (art 25/28) 29
- 4.11 Protocolplicht (art 32) 29
- 4.12 Audits (art 33) 30
- 4.13 Privacy functionaris (art 34) 30
- 4.14 Functionaris Gegevensbescherming (art 36) 31

Den Haag, 7 december 2011

De Directeur van de Departementale Auditdienst

I



1 Assuranceverklaring

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 Noord- en Oost-Gelderland.

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 Noord- en Oost-Gelderland.

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 Noord- en Oost-Gelderland, naar de stand van medio 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 Noord- en Oost-Gelderland te nemen maatregelen. Ook is gebleken dat het korps Noord- en Oost-Gelderland voor het volledig kunnen voldoen aan de Wpg eisen mede afhankelijk is van besluiten die buiten het korps Noord- en Oost-Gelderland 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 Noord- en Oost-Gelderland, is, op grond van artikel 4 lid 1 van de Regeling Periodieke Audit Politiegegevens, verplicht binnen drie maanden een verbeterrapport op te stellen waarin de maatregelen worden beschreven die getroffen zijn ter verbetering van de in de privacy audit geconstateerde tekortkomingen. Op grond van artikel 4 lid 3 dient hercontrole plaats te vinden. Wij adviseren deze hercontrole te laten uitvoeren door de interne audit functie van het korps Noord- en Oost-Gelderland. Het verbeterrapport en de uitgevoerde hercontrole zullen in de navolgende jaren door de privacyauditor worden beoordeeld.

2 Samenvatting

Het korps Noord- en Oost-Gelderland heeft in 2009 een inventarisatie opgemaakt van de meest cruciale activiteiten die het regiokorps uitvoert op het gebied van de Wpg. Na de inventarisatie is gestart met de implementatie van de Wpg. In 2010 is een eindrapport hiervan voorgelegd aan de stuurgroep met de resultaten en met een overzicht van borgingsonderwerpen. In 2011 is er een interne audit uitgevoerd en de resultaten daarvan worden nu opgepakt in het project 'verbetering borging Wpg'. Gesteld kan worden dat het korps Noord- en Oost-Gelderland momenteel met een veelheid aan activiteiten actief bezig is om aan de implementatie van de Wpg gestalte te geven.

Het korps Noord- en Oost-Gelderland heeft een aantal zaken in opzet goed opgepakt, zoals het autorisatiebeheer en een interne audit functie. De korpsleiding toont hiermee en met andere initiërende activiteiten haar aandacht voor de Wpg.

Niettemin voldoet het door ons beschouwde stelsel van maatregelen nog niet in opzet, bestaan en werking aan de vereisten van de Wpg.

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

Criteria:

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

Norm	Aspect	Bevinding en oordeel
Art. 1.f, Verantwoordelijke		
1.f	Mandaatbesluit	Er is een mandaatbesluit en ondermandaatbesluit aanwezig. De verantwoordelijkheden zijn gedelegeerd aan de korpschef en doorgemandeerd aan de districtchefs. 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 geen instructie aangetroffen waarin de criteria voor het onderscheid zijn aangegeven. Vaak begint een zaak in art 8 (BVH) en verandert in loop der tijd in art 9 (BVO) onderzoek. Niet alle art 9 onderzoeken worden vanuit BVH overgezet naar BVO. De systemen faciliteren hierin niet. Het onderscheid is in het begin stadium van een onderzoek lastig te maken. Daarmee is sturing vanuit OM problematisch. Hiermee wordt deels voldaan aan de Wpg.
3.1 t/m 3.3 (8) 4.1 (8)	Noodzakelijkheid (8) Doelbinding Rechtmatigheid Juistheid Volledigheid	Er zijn geen procesbeschrijvingen, procedures of richtlijnen voor het waarborgen van de rechtmatigheid, doelbinding, noodzakelijkheid, volledigheid en juistheid. Lastig vast te stellen of aan criteria wordt voldaan. Er is voorzien in een aantal beheersmaatregelen die er voor moeten zorgen dat aan de criteria wordt

Norm	Aspect	Bevinding en oordeel
		voldaan. De volledigheid en juistheid van gegevens wordt enigszins geborgd door de verplichte invulvelden van BVH. Ook vindt er een check plaats op de persoonsgegevens met het GBA-systeem. Medewerkers hebben via een e-learning module kennis over de Wpg gekregen. In IBT verband is in de zomer een lesblok (1,5 uur) onderricht Wpg gegeven aan alle executieve wapendragenden. Begrippen als integriteit en wettelijk draagvlak voor het verzamelen van gegevens waren onderdeel van een in 2004 gehouden onderzoek en een uitkomst daarvan was dat deze begrippen "zich in de genen van de politie bevinden". Daarnaast worden alle mutaties in het BVH en BVO altijd gelezen, gewogen en gefilterd door een coördinator. Het zelfreinigend vermogen is groot. De risico's dat zich informatie in deze systemen bevindt die niet WPG proof is, wordt laag ingeschat. Daarnaast is voor mutaties in politiegegevens mbt de artikelen 9 en 10 altijd een bevoegd functionaris betrokken. Hiermee wordt deels voldaan aan de Wpg.
3.1 t/m 3.3 (9) 4.1 (9)	Noodzakelijkheid (9) Doelbinding Rechtmatigheid Herkomst en wijze van verkrijging Juistheid Nauwkeurig Volledigheid	Er zijn geen procesbeschrijvingen maar wel werkinstructies voor de medewerkers beschikbaar. Deze staan op Intranet en op de site van PKN. Het is onduidelijk of deze Wpg proof zijn. De medewerkers zijn slechts gedeeltelijk van deze werkinstructies op de hoogte. Juistheid/volledigheid wordt niet automatisch in het systeem gecontroleerd. Medewerkers hebben toegang tot handboeken en werkinstructies voor BVO waarin staat beschreven welke gegevens dienen te worden ingevoerd. Het doel van recherche-onderzoeken wordt vastgelegd in de MRO's. <u>II</u> heeft een overzicht van meldingen en sluitingen van onderzoeken. Bij onduidelijkheden en vragen wordt de <u>II</u> benaderd. Zie ook de laatste alinea van de vorige rubriek. Medewerkers verzamelen aan de nadere kant zoveel mogelijk informatie voor het onderzoek maar houden hierbij geen rekening met het ter zake dienend en niet bovenmatig zijn van informatie. Er is geen middel voor handen om de rechtmatigheid van gegevens te toetsen. Met betrekking tot de herkomst dient dit in het systeem te worden vastgelegd. Hiermee wordt deels voldaan aan de Wpg.
3.4 (9)	Noodzakelijkheid (10 en 12) Doelbinding	Het werkproces van de CIE is beschreven in het landelijk proceshandboek CIE. Dit handboek is Wpg compliant. In de werkprocessen is beschreven hoe

Norm	Aspect	Bevinding en oordeel
	Rechtsmatigheid Herkomst en wijze van verkrijging Juistheid Nauwkeurig Volledigheid	om te gaan met noodzakelijkheid, doelbinding, rechtsmatigheid en volledigheid. In verband met de aard van de werkzaamheden zijn de kwaliteitscriteria goed ingeregeld. Bij de CIE gebeurt dat door het landelijk proceshandboek CIE en de toezichthoudende rol CIE OvJ. Bij de RID liggen de kwaliteitscriteria al in het doel van de taak vast. Hiermee wordt voldaan aan de Wpg.
4.3	Beveiliging (isolatie)	De landelijke systemen en regionale applicaties zijn nog niet Wpg proof. Een aantal systemen waaronder BVH voldoet niet aan de door de Wpg gestelde bewaartermijnen. Hierdoor is kans op onrechtmatig gebruik. Binnen het korps zijn politiegegevens op basis van een autorisatiesysteem afgeschermd. Tevens is sprake van fysieke beveiliging van de gebouwen in de vorm van toegangssystemen. In het verbeterplan NOG wordt hier aandacht aan besteed. Hiermee wordt deels voldaan aan de Wpg.
Art. 5, Gevoelige gegevens		
	Gevoelige gegevens	Kennis en bewustzijn over opslag en verwerking van gevoelige gegevens is summier aanwezig. Medewerkers "Blauw" zijn niet op de hoogte dat deze gegevens alleen mogen worden opgeslagen indien er noodzaak voor is. Medewerkers Opsporing zijn beperkt op de hoogte hoe om te gaan met gevoelige gegevens. Er worden op dit moment handboeken en instructies in eenvoudige taal gemaakt, er zullen contactpersonen op de operationele eenheden worden aangewezen en er wordt overlegd met de RMT leden hoe deze informatie het best kan worden uitgeleerd aan de medewerkers. Medewerkers CIE leggen alleen gevoelige informatie vast indien hier noodzaak voor is. Hiermee wordt deels voldaan aan de Wpg.
Art. 6, Autorisatie		
	Korpsautorisatiematrix	Het korps hanteert een korpsautorisatiematrix waarin rechten aan functies en taken gekoppeld zijn. Hiermee wordt voldaan aan de Wpg.
	Aanvraagproces	Het handboek autorisaties beschrijft het aanvraagproces. Hiermee wordt voldaan aan de Wpg.
	Wijziging en verwijdering	De autorisatiematrix wordt gevoed met gegevens uit het personeelssysteem Beaufort. Naar aanleiding van een bevinding van het interne auditteam is gedateerd 23-8-2011 een procesbeschrijving opgesteld. Op basis hiervan worden mutaties up-to-date verwerkt, waardoor onterechte autorisaties

Norm	Aspect	Bevinding en oordeel
		voorkomen worden. Systeemeigenaren dienen volgens het handboek autorisaties minimaal twee maal per jaar een controle uit te voeren op de toegekende autorisaties. Dit gebeurt tot op heden niet. Hiermee wordt deels voldaan aan de Wpg.
	• Autorisatiebeheer CIE, RID	Autorisaties CIE worden toegekend door hoofd CIE, waarvan sommige goedgekeurd door OvJ. Autorisaties RID worden toegekend door hoofd RID. Deze processen zijn goed ingeregeld. Hiermee wordt voldaan aan de Wpg
32.1.c	Protocollering autorisaties	Externe aanvragen voor een tijdelijke autorisatie worden geprotocolleerd. De privacyfunctionaris houdt een overzicht bij van de toekenning van artikel 6 autorisaties. De autorisatieverzoeken van lijnchefs voor hun medewerkers, waarop zij hun fiat moet geven. Hiermee wordt voldaan aan de Wpg.
32.3 voor 32.1.c	Bewaren protocolgegevens autorisaties	Protocolgegevens worden conform de richtlijnen bewaard. Hiermee wordt voldaan aan de Wpg.
Art. 11, Geautomatiseerd vergelijken en in combinatie zoeken		
	• Hanteerbare interpretatie	De begrippen zijn slechts bij weinig geïnterviewden bekend. Interpretaties op landelijk niveau en binnen het korps zijn niet vastgelegd; dit bemoeilijkt uniforme toepassing. Hiermee wordt niet voldaan aan de Wpg.
	• Aangewezen functionarissen	De tactische en strategische analisten van de divisie I&I voeren deze activiteiten uit en zijn aangewezen door hun leidinggevenden. Hiermee wordt voldaan aan de Wpg.
11.4	Bevoegd gezag	De tactische en strategische analisten van de divisie I&I voeren deze activiteiten uit en zijn aangewezen door hun leidinggevenden. De aanvraag bij het bevoegd gezag vindt plaats door de eigenaar van het onderzoek, i.e. de bevoegd functionaris. Toestemming van het bevoegd gezag (OM) vindt niet altijd plaats. Hiermee wordt deels voldaan aan de Wpg.
32.1.d 32.1.h	Protocollering 11.1, 11.2, 11.4 en 11.5	Voor artikel 8 zoekslagen is een protocolbeschrijving (waar en hoe te melden) opgesteld. Deze wordt aan de FrontOffice van de Infodesk gestuurd. Procedures GV en ICMEV zijn niet aangetroffen. De analisten bij de divisie I&I, alsmede bij de CIE en RID dragen zorg voor protocollering van de gegevens en de teamchefs zien toe op toepassing en bewaring. Automatisch vergelijken van gegevens ex artn 8 t/m 10 met andere gegevens wordt uitgevoerd door de info coördinatoren van divisie I&I, bijvoorbeeld bij een TGO.

Norm	Aspect	Bevinding en oordeel
		Hiermee wordt deels voldaan aan de Wpg.
32.3 voor 32.1.d 32.1.h	Bewaren protocolgegevens 11.1, 11.2, 11.4 en 11.5	Voor artikel 8 zoekslagen is een protocolbeschrijving (waar en hoe te melden) opgesteld. Deze wordt aan de FrontOffice van de Infodesk gestuurd. Procedures GV en ICMEV zijn niet aangetroffen. De analisten bij de divisie I&I, alsmede bij de CIE en RID dragen zorg voor protocollering van de gegevens en de teamchefs zien toe op toepassing en bewaring. Automatisch vergelijken van gegevens ex artn 8 t/m 10 met andere gegevens wordt uitgevoerd door de info coördinatoren van divisie I&I, bijvoorbeeld bij een TGO. Hiermee wordt deels voldaan aan de Wpg.
Art. 14, Bewaartermijnen		
8.2 en 8.3	(8) van 1 tot 5 jaar	Er zijn in BVH geen beheersmaatregelen voor de bewaartermijnen. Er is in de nieuwe release een schoningsmodule voor BVH maar deze staat op verzoek van de voorzitter van de landelijk stuurgroep Wpg nog niet aan. Hiermee wordt niet voldaan aan de Wpg.
8.6	(8) verwijderen na 5 jaar	Er is geen proces opgesteld om politiegegevens in BVH en BPS te verwijderen. De gehanteerde applicaties bieden voor dit proces ook geen ondersteuning. Hiermee wordt niet voldaan aan de Wpg.
14.1 (8)	(8) vernietigen na 5 jaar verwijderd	Er is geen proces opgesteld om politiegegevens in BVH te vernietigen. De gehanteerde applicaties bieden voor dit proces ook geen ondersteuning. Politiegegevens worden veelal niet vernietigd. Hiermee wordt niet voldaan aan de Wpg.
9.4	(9) verwijderen na OH plus ½ jaar	Er is geen proces opgesteld om politiegegevens te verwijderen. De gehanteerde applicaties bieden voor dit proces geen ondersteuning. Hiermee wordt niet voldaan aan de Wpg.
14.1 (9)	(9) vernietigen na 5 jaar verwijderd	Er is geen proces opgesteld om politiegegevens te verwijderen. De gehanteerde applicaties bieden voor dit proces geen ondersteuning. Politiegegevens worden niet vernietigd. Hiermee wordt niet voldaan aan de Wpg.
10.6	(10) verwijderen na 5 jaar geen subjectwaardige registratie	Het proceshandboek CIE omvat een hoofdstuk "verwijderen en bewaren van persoonsgegevens". Toezicht door CIE OvJ draagt bij aan naleven van deze bepaling. Hiermee wordt voldaan aan de Wpg
14.1 (10)	(10) vernietigen na 5 jaar verwijderd	Toezicht door CIE OvJ draagt bij aan naleven van deze bepaling. Het proceshandboek CIE omvat een hoofdstuk "verwijderen en bewaren van persoonsgegevens". In de praktijk blijkt het proces onvoldoende te worden nageleefd. Hiermee wordt deels voldaan aan de Wpg.

Norm	Aspect		Bevinding en oordeel
14.3	Hernieuwde verwerking		De bevoegde functionarissen dragen zorgen voor verstrekking van gegevens bij hernieuwde verwerking. Tevens dient het OM dan toestemming te verlenen. De bevoegd functionaris heeft hierin een centrale rol. Niet in alle gevallen wordt de juiste procedure gevolgd. Het handboek bevoegd functionaris dient hierin de weg te wijzen. Hiermee wordt deels voldaan aan de Wpg.
32.1.e	Protocollering 14.3		Zie hernieuwde verwerking. Er is geen procesbeschrijving. Medewerkers Infodesk leggen ook bij hernieuwde verwerking gegevens vast. Hiermee wordt deels voldaan aan de Wpg.
32.3 voor 32.1.e	Bewaren protocolgegevens 14.3		Zie hernieuwde verwerking en protocollering. Bewaring van protocolgegevens vindt dus ook maar deels plaats. Hiermee wordt deels voldaan aan de Wpg.
12.2	(12) verwijderen na 4 maanden		Toezicht door CIE OvJ draagt bij aan naleven van deze bepaling. Hiermee wordt voldaan aan de Wpg.
12.6	(12) controleren en vernietigen		Toezicht door CIE OvJ draagt bij aan naleven van deze bepaling. Hiermee wordt voldaan aan de Wpg.
Art. 15, Ter beschikking stellen			
	• Infodesk voor bevraging		Via een standaard formulier kunnen politiegegevens worden aangevraagd. De coördinator van de frontoffice beoordeelt of de aanvraag aan de eisen voldoet. Bij twijfel wordt navraag gedaan bij de privacyfunctionaris. Hiermee wordt voldaan aan de Wpg.
	• Codering		Wanneer de Infodesk informatie ter beschikking stelt c.q. verstrekt waarvoor de toestemming van een Bevoegd Functionaris nodig is dan wordt het feit dat deze toestemming is verleend in de mail, waarin de informatie ter beschikking wordt gesteld, vermeld. Er wordt niet gewerkt met een aparte codering. Hiermee wordt voldaan aan de Wpg.
	• Aanwijzing Bevoegd Functionaris		Bevoegd functionarissen zijn aangewezen. De aanwijzing is vastgelegd in een regionaal besluit. Hiermee wordt voldaan aan de Wpg.
	• Opleiding Bevoegd Functionaris		De Bevoegd functionarissen hebben in basis een opleiding gekregen aan de politieacademie en middels een zelfstudiemodule beschikbaar op intranet. Er is verder in het korps 4x een bevoegd functionaris cursus gegeven. Met betrekking tot de werking is gebleken dat een gedeelte van de Bevoegd functionarissen behoefte hebben aan een vertaling van de Wpg voor de dagelijkse werktak; handreikingen bevoegd functionaris worden opgesteld. Hiermee wordt deels voldaan aan de Wpg.
15.2	Weigeringsgronden		Infodesk heeft hierin een toetsingsfunctie.

Norm	Aspect	Bevinding en oordeel
		Hiermee wordt voldaan aan de Wpg.
Art. 16 t/m 24, Verstrekking		
• Verstrekkingenwijzer (landelijk)		De verstrekkingenwijzer is bekend. Hiermee wordt voldaan aan de Wpg.
• Proces voor convenanten		Convenanten worden beheerd door de privacyfunctionaris. Er is geen zekerheid over de volledigheid van de convenanten. Centraal beheer is gewenst. Voor zover aanwezig bij de PF, zijn convenanten getoetst op Wpg aspecten, eventueel aangepast en op intranet geplaatst. Er is (nog) geen procesbeschrijving hoe nieuwe convenanten tot stand komen, maar daar wordt door Sturingsondersteuning aan gewerkt. Ook is een beleidsmedewerker opgeleid om hulp te bieden bij het Wpg proof maken van oude en nieuw te maken convenanten. Hiermee wordt deels voldaan aan de Wpg.
• Proces voor Art. 20 Besluiten		Als er nieuwe convenanten worden gemaakt wordt de Wpg (besluit art 20) bij het opstellen van deze convenanten direct meegenomen. Wijzigingen in reeds bestaande convenanten worden in een addendum toegevoegd aan het convenant. Hiermee wordt voldaan aan de Wpg.
• Verstrekkingenschema (regio)		Er wordt een verstrekkingentabel gehanteerd waarin staat vermeld welke stukken aan welke organisaties verstrekt mogen worden. Hiermee wordt voldaan aan de Wpg.
• Proces voor geautomatiseerde verstrekking		Er wordt dagelijks een programma (query) gedraaid over BVH. Op basis van dit programma wordt dagelijks één bestand gemald naar slachtofferhulp met voor hun relevante informatie. Het korps heeft hiermee inzicht in de geautomatiseerde verstrekkingen en de inhoud daarvan. Hiermee wordt voldaan aan de Wpg.
7.2	Geheimhouding	De geheimhoudingsplicht wordt door Infodesk bij verstrekkingen meegenomen. Hiermee wordt voldaan aan de Wpg.
32.1.f	Protocollering verstrekking	Door Infodesk worden verstrekkingen gemuteerd in BVH en BVO. Alle verstrekkingen worden tevens in een outlook bak bewaard. Verstrekkingen door "blauw" worden ten dele geprotocolleerd middels I90. Dit wordt echter als lasten verzwarend beschouwd. Aantallen verstrekkingen I90 uit BVH zijn niet in evenwicht met aantal feitelijk verstrekkingen. Hiermee wordt deels voldaan aan de Wpg.
32.3 voor 32.1.f	Bewaren protocolgegevens verstrekking	Protocolgegevens worden bewaard. De privacyfunctionaris houdt ook een overzicht bij van verstrekkingen met uitzondering van verstrekkingen belang veiligheid staat. Hiermee wordt voldaan aan de Wpg.
• Toezicht door leidinggevend op verstrekkingen en protocollering		Het hoofd Infodesk houdt toezicht op de verstrekkingen.

Norm	Aspect	Bevinding en oordeel
		Bij NOG neemt de politie deel aan 3 casusoverleggen in het kader van het Veiligheidshuis (Jeugd, Veelplegers en Huiselijke Geweld). De samenwerking is gebaseerd op de raamregeling Samenwerkingsovereenkomst NOG Veiligheidshuis (met privacy reglement, waarin de informatieverstrekking wordt geregeld). Door de voorzitter van de casusoverleggen (een hoofdinspecteur van politie) wordt onderscheid gemaakt in de verstrekking van informatie aan opsporingsambtenaren en hulpverleners. Schriftelijk krijgen opsporingsambtenaren NAW gegevens en overige relevante informatie; hulpverleners krijgen alleen NAW gegevens. De aanwezigheid van partners (opsporingsambtenaren en hulpverleners) bij de casusoverleggen geschiedt conform de samenwerkingsovereenkomst - hulpverleners dus ook aanwezig. Mondeling gaat er dus wel e.e.a. over tafel. M.a.w. toezicht binnen het Veiligheidshuis is wel geregeld, maar er ligt ingevolge de Wpg nog wel een knelpunt. Hiermee wordt deels voldaan aan de Wpg.
Art. 25 t/m 31, Rechten van de betrokkene		
25.1	Verzoek om kennisgeving	Het implementatie team van de Wpg heeft procedures beschreven en formuleren ontwikkeld ter ondersteuning van het proces rechten van de betrokkene. Er is een stroomschema opgesteld op basis van de Landelijke handreiking. Deze is niet regiospecifiek gemaakt en niet afgestemd op AO van het korps. Wat de werking betreft heeft het interne auditteam vastgesteld dat het proces rechten van de betrokkene grotendeels is geborgd binnen het werkproces van de privacyfunctionaris. Hiermee wordt voldaan aan de Wpg.
28.1 t/m 28.3	Correctie	Door onvoldoende afstemming tussen de privacyfunctionaris en de infodesk medewerker kan het voorkomen dat verzoeken niet juist of niet volledig worden afgehandeld. Hiermee wordt deels 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	De privacyfunctionaris houdt een overzicht bij van de meldingen/sluitingen van onderzoeken. Daarbij wordt met name het doel getoetst. Art 9 onderzoeken worden doorgaans gestart met een MRO. Daarbij worden gegevens vastgelegd in BVO en de overzichten worden bewaard II Hiermee wordt voldaan aan de Wpg.
32.3 voor 32.1.a	Bewaren protocolgegevens doel onderzoek	De privacyfunctionaris heeft de protocolleringsgegevens beschikbaar. Hiermee wordt voldaan aan de Wpg.

Norm	Aspect		Bevinding en oordeel
13.4 en 32.1.b	Protocollering Art. 13 gegevensverzameling en		Gegevens worden in voorkomend geval vastgelegd door de Infodesk. Hiermee wordt voldaan aan de Wpg.
32.3 voor 32.1.b	Bewaren protocolgegevens Art. 13 gegevensverzameling en		De PF houdt van de protocollering overzichtten bij. De privacyfunctionaris heeft de protocolleringsgegevens beschikbaar. Hiermee wordt voldaan aan de Wpg.
32.1.g	Protocollering onrechtmatige handeling		Deze gegevens worden niet geregistreerd. Hiermee wordt niet voldaan aan de Wpg.
32.3 voor 32.1.g	Bewaren protocolgegevens onrechtmatige handeling		Deze gegevens worden niet geregistreerd. Hiermee wordt niet voldaan aan de Wpg.
32.3	Gemeenschappelijke verwerking		Gemeenschappelijke verwerkingen komen niet voor bij het korps.
Art. 33, Audits			
RPAP 3.1	Interne audit-functie		Het korps beschikt over vijf medewerkers van de afdeling Sturingsondersteuning en de Divisie I&I die zijn opgeleid op het gebied van auditing en de Wet politiegegevens. Hiermee wordt voldaan aan de Wpg.
RPAP 3.4	Interne audit-plan		Een auditplan is in de maak Hiermee wordt deels voldaan aan de Wpg.
RPAP 3.6	Interne audit-rapport		Er is een audit onderzoek uitgevoerd Hiermee wordt voldaan aan de Wpg.
Art. 34, Privacyfunctionaris			
34.1 en 34.4	Benoemd en gemeld		Formeel aangesteld door KC en aangemeld bij CBP Hiermee wordt voldaan aan de Wpg.
34.2	Overzicht over protocollering		Grotendeels aanwezig. Hiermee wordt deels voldaan aan de Wpg.
34.3	Jaarverslag		Over 2010 is een jaarverslag opgesteld. Het uitvoeren van de toezichthoudende taak van de privacyfunctionaris krijgt momenteel nog maar beperkt invulling en richt zich in het bijzonder op de borgingsonderwerpen. Hiermee wordt deels voldaan aan de Wpg.
Optioneel Art. 36, Functionaris Gegevensbescherming			
36.1 en 36.2	Benoemd		FGB komt als functie niet voor
Wbp 63.3	Gemeld		FGB komt als functie niet voor
Wbp 64.1 t/m 64.4	Toezichthoudende rol		FGB komt als functie niet voor

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 Noord- en Oost-Gelderland 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 Noord- en Oost-Gelderland 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 (Art. 33:1). 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.

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 Noord- en Oost-Gelderland.

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 maart 2011, van maatregelen en procedures, waarmee het korps Noord- en Oost-Gelderland 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 bestaat uit 12 thema's uit de Wpg afgezet tegen de relevante wetsartikelen (artikel 8, 9, 10, 12 en 13).

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

3.5 Normenkader

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

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

- Wet politiegegevens, de wet van 21 juli 2007, houdende regels inzake de bescherming van politiegegevens.
- Besluit politiegegevens, besluit van 14 december 2007, houdende bepalingen ter uitvoering van de Wet politiegegevens.
- Regeling periodieke audit politiegegevens, de Regeling van de Minister van Justitie, de Minister van Binnenlandse Zaken en de Minister van Defensie van 9 december 2008, nr. 5578598/08, houdende nadere regels ten aanzien van het toezicht op de naleving van de bij of krachtens de Wet politiegegevens gegeven voorschriften.

3.6 Beperkingen voor de privacy audit

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

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

3.7 Onderzoeksmethoden en werkwijze

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

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

Wij hebben onze werkzaamheden uitgevoerd in de periode van 30-08-2011 tot en met 16-09-2011.

Het conceptrapport met bevindingen is op 19 september 2011 besproken met de korpschef van het korps Noord- en Oost-Gelderland en op 03 oktober 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 wvd, J.A. Gerritsen;
- de korpschef mr. A.L.C. Roelofs EMPM;
- de Hoofd Officier van Justitie mr. A.C. Maan;
- de privacyfunctionaris van het korps Noord- en Oost-Gelderland, **I**
- de voorzitter van het College Bescherming Persoonsgegevens.

Het rapport mag uitsluitend met toestemming van de korpsbeheerder dan wel de korpschef van korps Noord- en Oost-Gelderland ter beschikking worden gesteld.

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

4 Bevindingen

4.1 Inleiding

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

4.1.1

Regie en doorzettingsmacht voor de Wpg implementatie

Binnen het regiokorps Noord- en Oost-Gelderland is men in de loop van 2009 pas echt begonnen aan de implementatie van de Wpg waardoor de implementatie onder grotere tijdsdruk is uitgevoerd. De implementatie van de Wpg heeft daarom op pragmatische wijze plaatsgevonden. Uitgangspunt hierbij was de inventarisatie van de meest cruciale activiteiten die het regiokorps uitvoert. Deze lijst kwam tot stand door actiepunten aangedragen door het landelijk implementatieproject. Voor het belangrijkste deel zijn deze actiepunten ingewonnen uit eigen onderzoek en afkomstig van een zelfde onderzoek dat gelijktijdig plaatsvond in het korps Zaanstreek-Waterland.

Uit de interne audit blijkt dat borging en naleving van de Wpg nog niet is ingebed in de managementcontrolcyclus. Uit onze interviews komt naar voren dat men zich binnen het korps hiervan bewust is en dat dit wordt aangepakt in het project verbetering borging Wpg. Dit blijkt ook uit het plan van aanpak voor dit project.

Algehele aandachtspunten die bij de audit binnen Politie Noord- en Oost-Gelderland naar voren zijn gekomen zijn:

- Het opstellen van procesbeschrijvingen en werkinstructies waarin is aangegeven op welke wijze wordt voldaan aan de eisen van de Wpg.
- Het onvoldoende geborgd zijn van de naleving van bepalingen op het gebied van bewaren en vernietigen van politiegegevens binnen de processen.

4.1.2

Bekendheid met de Wpg binnen de organisatie

Buiten de gestelde normen is in de interne audit en uit onze gesprekken naar voren gekomen dat de kennis van de Wpg nog niet bij iedereen voldoende aanwezig is. Hierdoor is men zich in het dagelijkse werk ook niet altijd bewust wat de Wpg inhoudt en welke mogelijkheden het biedt.

De Bevoegd functionarissen hebben in basis een opleiding gekregen aan de politieacademie en middels een zelfstudiemodule beschikbaar op intranet. Er is verder in het korps 4x een bevoegd functionaris cursus gegeven. Met betrekking tot de werking is gebleken dat een gedeelte van de Bevoegd functionarissen behoefte hebben aan een vertaling van de Wpg voor de dagelijkse werktaken; handreikingen bevoegd functionaris worden opgesteld.

Medewerkers hebben via een e-learning module kennis over de Wpg gekregen. In IBT verband is in de zomer 2011 een lesblok (1,5 uur) onderricht Wpg gegeven aan alle executieve wapendragenden.

4.1.3 *Wpg en de praktijk*

Na de inventarisatie is gestart met de implementatie van de Wpg. In 2010 is een eindrapport hiervan voorgelegd aan de stuurgroep met de resultaten en met een overzicht van borgingsonderwerpen. In 2011 is er een interne audit uitgevoerd en de resultaten daarvan worden nu opgepakt in het project 'verbetering borging Wpg'. Gesteld kan worden dat het korps Noord Oost Gelderland momenteel met een veelheid aan activiteiten actief bezig is om aan de implementatie van de Wpg gestalte te geven.

4.2 Verantwoordelijke (artikel 1.f)

Mandaatbesluit

4.2.1 *Norm*

Net als onder de oude Wet Politieregisters (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 ieder korps 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.

4.2.2 *Bevindingen*

In 2010 is het document 'Korpsbeschrijving politie Noord- en Oost- Gelderland' opgesteld en in 2011 is een nieuw organogram gemaakt. In 2009 is een mandaatbesluit Korpsbeheerder-Korpschef opgesteld waarin verantwoordelijkheden voor de Wpg bij de korpschef zijn belegd. In het ondermandaatbesluit worden deze verantwoordelijkheden door de korpschef bij proceseigenaren belegd.

Met betrekking tot de werking van de mandatering is uit de interne audit gebleken dat er in de praktijk nog niet altijd uitvoering wordt gegeven aan de toebedeelde verantwoordelijkheden.

4.3 Kwaliteitsaspecten van politiegegevens (art 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 (art 3) en volledigheid, juistheid en beveiliging (art 4).

4.3.2 *Bevindingen*

Het voldoen aan de bepalingen van deze artikelen 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. Begrippen als integriteit en wettelijk draagvlak voor het verzamelen van gegevens waren onderdeel van een in 2004 gehouden onderzoek en een uitkomst daarvan was dat deze begrippen "zich in de genen van de politie bevinden". Daarnaast worden alle mutaties in het BVH en BVO altijd gelezen, gewogen en gefilterd door een coördinator. Het zelfreinigend vermogen is gewoon groot. De risico's dat zich informatie in deze systemen bevindt die niet WPG proof is, wordt laag ingeschat. Daarnaast is voor mutaties in politiegegevens mbt de artikelen 9 en 10 altijd een bevoegd functionaris betrokken.

Voor wat betreft het onderscheid onderzoek Dagelijkse Politietask (8) versus Bepaald geval (9) kan het volgende worden vermeld. Vaak begint een zaak in artikel 8 (BVH) en verandert in loop der tijd in een artikel 9 onderzoek. Niet alle art 9 onderzoeken worden vanuit BVH overgezet naar BVO. De systemen faciliteren hierin niet. Het onderscheid is in het begin stadium van een onderzoek lastig te maken. Daarmee is sturing vanuit OM problematisch.

Met betrekking tot artikel 8 informatie *'verwerken van politiegegevens ten behoeve van de dagelijkse politiepraktijk, zoals surveilleren, advisering over preventie, afhandelingen van de verkeersproblematiek, eenvoudig recherchwerk, verlenen van hulp en handhaven van wetten en regels'* zijn geen procesbeschrijvingen aangetroffen waarin is opgenomen op welke wijze de zorg voor het voldoen aan de criteria voor deze informatie dient plaats te vinden. De volledigheid en juistheid van gegevens wordt enigszins geborgd door de verplichte invulvelden van BVH. Ook vindt er een check plaats op de persoonsgegevens met het GBA-systeem. Uit gesprekken komt naar voren dat informatie ten behoeve van de dagelijkse politiepraktijk opgeslagen wordt in privé- en groepsmappen op de kantoorautomatiseringsomgeving. Dit gebeurt bijvoorbeeld omdat mediabestanden niet in de landelijke systemen, zoals BVH, opgehangen kunnen worden. Het risico is hier dat informatie niet kan worden gedeeld.

In artikel 9 Wpg wordt gesproken over het *'gericht verwerken van politiegegevens ten behoeve van een onderzoek met het oog op de handhaving van de rechtsorde in een bepaald geval'*. Hiervoor zijn geen procesbeschrijvingen aangetroffen waarin is opgenomen op welke wijze de zorg voor het voldoen aan de criteria voor deze gegevens dient plaats te vinden. Op dit gebied zijn wel werkinstructies voor BVO beschikbaar op intranet. Uit de interne audit blijkt dat men niet weet of alle instructies Wpg proof zijn en of er gebruik van wordt gemaakt. Bij onduidelijkheden en vragen wordt de privacy functionaris benaderd. De juistheid en volledigheid van informatie wordt niet automatisch in het systeem gecontroleerd. Het doel van recherche-onderzoeken wordt vastgelegd in de MRO's. **II** een overzicht van meldingen en sluitingen van onderzoeken. De volledigheid van dit overzicht is niet gewaarborgd. Medewerkers verzamelen veelal zoveel mogelijk informatie voor het onderzoek maar houden hierbij geen rekening met de aspecten ter zake dienend en niet bovenmatig. Tevens is er geen middel voor handen om de rechtmatigheid van gegevens te toetsen. Met betrekking tot de herkomst dient dit in het systeem te worden vastgelegd.

Artikel 10 *'verwerken van politiegegevens met het oog op het verkrijgen van inzicht in de betrokkenheid van personen bij bepaalde ernstige bedreigingen van de rechtsorde'* en artikel 12 informatie *'verwerken van politiegegevens met het oog op controle op en het beheer van een informant alsmede de beoordeling en verantwoording van het gebruik van informantgegevens'* wordt vooral verwerkt bij de CIE en de RID. Hier wordt aan de kwaliteitsaspecten, vanwege de bijzondere aard van hun taken, specifiek aandacht besteed. Daarbij is in de opzet voldaan aan deze criteria. Bij de CIE vanwege de toezichthoudende rol van het OM (de CIE OvJ) en het landelijk gebruik van het proceshandboek, regeling CIE en instructie CIE OvJ. De teamchef van de CIE controleert alle inkomende informatie op de kwaliteitsaspecten. Ook de RID maakt gebruik van een proceshandboek specifiek voor het regiokorps. Deze is onlangs opgesteld en gebaseerd op het handboek van regio Zeeland. De ruimtes van de CIE en de RID zijn zowel fysiek als digitaal beveiligd. Binnen de CIE en de RID worden geen gegevens vastgelegd in de kantoorautomatisering. **III**

De Infodesk behandelt de aanvragen voor ter beschikking stellen en verstrekkingen. Zij krijgen de aanvragen binnen via een vaststaand format waar nadrukkelijk naar het doel gevraagd wordt. Voor de medewerkers van de Infodesk zijn procesbeschrijvingen beschikbaar.

De beveiliging (isolatie) van politiegegevens is binnen het korps op basis van een autorisatiesysteem afgeschermd. Tevens is sprake van fysieke beveiliging van de gebouwen in de vorm van toegangssystemen. In BVH worden zowel artikel 8 als 9 gegevens opgeslagen. De landelijke en regionale applicaties zijn nog niet Wpg proof.

4.3.3 *Verbeterpunten*

- Beperk de vastleggingen van politiegegevens in de kantoorautomatisering.
- Stel procesbeschrijvingen op voor art. 8 en art. 9 informatie om de kwaliteitsaspecten te kunnen toetsen.

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*

Uit de interne audit is gebleken dat een groot aantal geïnterviewden niet op de hoogte was van het feit dat gevoelige gegevens alleen opgeslagen mogen worden indien er een noodzaak voor is. Er is slechts een beperkt bewustzijn dat gevoelige gegevens (ras/godsdienst/politieke overtuiging) anders verwerkt moeten worden dan reguliere politiegegevens. Deze gegevens worden veelal niet actief verzameld, maar daar waar zij gevonden worden, worden die meegenomen zonder dat er een onderscheid is in de verwerking. De opmerkingen in het audit rapport hebben er toe geleid dat de verbetering van het bewustzijn en de kennis van de Wpg bij medewerkers als een rode draad door het Verbeterplan/Aktieplan loopt. Medewerkers hebben in IBT verband een instructie Wpg gehad. Er worden op dit moment handboeken en instructies in Jip en Janneke taal gemaakt, er zullen contactpersonen op de operationele eenheden worden aangewezen en er wordt overlegd met de RMT leden hoe deze informatie het best kan worden uitgeleerd aan de medewerkers.

4.4.3 *Verbeterpunten*

Draag zorg voor implementatie van verbetermaatregelen voor de verwerking van gevoelige gegevens.

4.5 Autorisatie (art 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 dient de verantwoordelijke zorg te dragen voor een schriftelijke vastlegging van de toekenning van autorisaties (protocolplicht).

4.5.2 *Bevindingen*

Het handboek autorisatie dat in 2004 is opgesteld is door de komst van de Wpg herzien. Het handboek bevat een duidelijke procesbeschrijving. Regio Noord- en Oost-Gelderland heeft een administratief systeem waarin de autorisaties worden vastgelegd en beheerd. Deze applicatie autoriseert medewerkers op basis van een autorisatiematrix. In de matrix zijn standaard relaties vastgelegd tussen enerzijds functies, organisatieonderdelen en taakaccenten en anderzijds gebruikersrollen of autorisatieniveaus op applicatie en gegevensbronnen. Wijzigingen in autorisaties worden alleen doorgevoerd na schriftelijke toestemming van een leidinggevende. De functies waaraan de autorisaties zijn gekoppeld komen uit het personeelsinformatiesysteem Beaufort. Een voorwaarde voor de juistheid en volledigheid van de autorisaties is dat Beaufort volledige en juiste gegevens moet bevatten van de medewerkers van het korps, inclusief inhuurkrachten en stagiairs. Met het oog hierop is gedateerd 23-8-2011 een procesbeschrijving opgesteld. Belangrijk hierbij is de tijdigheid van aanpassingen in het systeem. Beaufort moet altijd up-to-date zijn. Tweemaal per jaar dienen de systeemeigenaren een controle uit te voeren op de toegekende autorisaties en de resultaten hiervan te rapporteren aan de privacyfunctionaris. Uit de gesprekken is naar voren gekomen dat dit nog niet overal heeft plaatsgevonden. De accreditatie voor toegang tot bepaalde gegevens in de administratie van het autorisatiebeheer wordt geprotocolleerd. Hiermee voldoet het autorisatiesysteem aan de vereisten van zorgvuldigheid en evenredigheid.



Protocolgegevens worden conform de richtlijnen bewaard.

4.5.3 *Verbeterpunten*

- Zorg voor een procedure waarin personeelsmutaties adequaat worden verwerkt, zodat wijzigingen in de autorisaties direct kunnen worden opgepakt.
- Zorg voor een structurele controle van de toegekende autorisaties.

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

4.6.1 *Norm*

Voor het onderzoek kunnen politiegegevens die voor dat onderzoek zijn verwerkt, geautomatiseerd worden vergeleken met andere politiegegevens (GV) 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 (ICMEV), worden van die verwerking nader genoemde gegevens vastgelegd (protocolplicht).

4.6.2 *Bevindingen*

Deze activiteit wordt met name uitgevoerd door algemene analisten bij de divisie Informatie & Intelligence, alsmede door specifieke analisten bij de CIE en RID. Zij dragen ook zorg voor protocollering van de gegevens en de teamchefs zien toe op toepassing en bewaring. Vragen naar de opzet van de verwerking van politiegegevens conform deze richtlijnen worden in het algemeen met grote

omzichtigheid tegemoet getreden. Het is een onderwerp dat slechts bij weinig geïnterviewden bekend lijkt. Waar bekendheid met deze begrippen uit de Wpg aanwezig is, is direct de vraag aan de orde waar de grenzen van GV en ICMEV liggen en op welke wijze daarmee dan in de praktijk moet worden omgegaan. Het verkrijgen van toestemming van het bevoegd gezag (OM) vindt bij ICMEV niet altijd plaats.

Het geautomatiseerd vergelijken van politiegegevens die worden verwerkt op grond van artikel 8, 9 of 10 met andere politiegegevens wordt uitgevoerd door de info coördinatoren van divisie I&I, bijvoorbeeld bij een TGO. Zij dragen ook zorg voor protocollering van de gegevens.

4.6.3

Verbeterpunten

- Stel procesbeschrijvingen op waarin is aangegeven hoe bij GV en ICMEV moet worden gehandeld.
- Ontwikkel casuïstiek voor het geautomatiseerd vergelijken en in combinatie met elkaar verwerken van politiegegevens.

4.7 Bewaartermijnen (art 14)

4.7.1

Norm

Politiegegevens worden vernietigd zodra zij niet langer noodzakelijk zijn voor de uitvoering van de dagelijkse politietaak (art 8) en worden in ieder geval uiterlijk vijf jaar na de datum van eerste verwerking verwijderd.

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 landelijke systemen zoals BPS, BVH en BVO zijn niet voorzien van beheersmaatregelen op het gebied van termijnen voor verwijderen en vernietigen van politiegegevens. Het is in BVH en BPS niet mogelijk informatie na bijvoorbeeld 1 jaar achter een schot te plaatsen zodat deze informatie niet meer kan worden geraadpleegd. Ook vinden er geen handmatige verwijderingen plaats. In de nieuwe release van BVH zou dit wel tot de mogelijkheden behoren; deze release wordt volgens planning in week 43 bij Noord- en Oost-Gelderland ingevoerd. In BVO worden registraties gesloten en dan worden de autorisaties op nul gezet zodat men niet meer bij de informatie kan. Er is hier echter geen sprake van vernietiging. Er is met betrekking tot artikel 8 en 9 Wpg geen procedure aangetroffen voor de omgang met bewaartermijnen en vernietiging van politiegegevens. Nader onderzoek naar het Wpg proof zijn van BVH en BVO is noodzakelijk. Gegevens die in de kantoorautomatisering zijn opgeslagen vallen helemaal buiten beeld. Controle op de bewaartermijnen en vernietiging vindt hierop niet plaats. Er is geen totaaloverzicht van wat er in die omgeving is opgeslagen. De outlook-mailboxen vereisen hier bijzondere aandacht, verzonden mails, met bijvoorbeeld verstrekkingen, worden waarschijnlijk niet geschoond. Uit de gesprekken is wel naar voren gekomen dat de kennis van de bewaartermijnen en vernietiging vaak wel aanwezig is.

In het handboek CIE en RID (artikel 10 Wpg) is wel aandacht geschonken aan deze onderwerpen. In de interne audit zijn deze documenten inhoudelijk beoordeeld en aangegeven is dat het handboek CIE onvoldoende waarborgen bevat voor het

naleven van wettelijke bepalingen op het gebied van verwijderen, bewaren en vernietigen van politiegegevens.

Binnen de recherche is aangegeven dat bij het kopiëren van gegevens van digitale gegevensdragers, zoals smartphones en tablets, de gegevens na gebruik niet worden vernietigd. Alle in beslag genomen gegevensdragers worden na de beslissing van de officier van Justitie teruggegeven. Het Openbaar Ministerie geeft vaak geen signaal als een onderzoek tot een onherroepelijk vonnis heeft geleid. Hierdoor ontstaan overvolle kasten en schijven. Alleen uit ruimtebesparende motieven wordt een enkele keer gegevens verwijderd of vernietigd.

De bevoegde functionarissen dragen zorgen voor verstrekking van gegevens bij hernieuwde verwerking. Tevens dient het OM dan toestemming te verlenen. De bevoegd functionaris heeft hierin een centrale rol. Niet in alle gevallen wordt de juiste procedure gevolgd. Het handboek bevoegd functionaris dient hierin de weg te wijzen.

Hierdoor wordt in opzet niet volledig voldaan aan de eisen die de Wpg stelt aan bewaartermijnen en vernietiging.

4.7.3

Verbeterpunten

- Voer controle uit op de gegevens in de kantoorautomatisering.
- Houd beheersmaatregelen voor verwijdering en vernietiging in de systemen BVH en BVO landelijk op de agenda.
- Pas het handboek CIE aan op het gebied van wettelijke bepalingen voor verwijderen, bewaren en vernietigen van politiegegevens.
- Ontwerp een procedure waarin gebruikte gegevens afkomstig van in beslag genomen gegevensdragers na gebruik kunnen worden vernietigd.

4.8 Ter beschikking stellen (art 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

Bij het ter beschikking stellen van politiegegevens wordt gebruik gemaakt van een standaard formulier. Deze formulieren worden verstuurd naar de Infodesk bij Divisie I&I, die ze verder afhandelt. Het werkproces van de Infodesk is beschreven.

Aangegeven is dat in de praktijk nog niet alles via I&I verloopt en dat nog veel formulieren terecht komen bij de privacyfunctionaris. De CIE en de RID zijn beide strikt in het vastleggen van het ter beschikking stellen van gegevens. Bij de CIE is een extra waarborg dat de CIE-OvJ toezicht houdt.

Wanneer de Infodesk informatie ter beschikking stelt c.q. verstrekt waarvoor de toestemming van een Bevoegd Functionaris nodig is dan wordt het feit dat deze toestemming is verleend in de mail, waarin de informatie ter beschikking wordt gesteld, vermeld. Er wordt niet gewerkt met een aparte codering. Het verstrekken van dit soort informatie gebeurt (vrijwel) niet.

4.8.3

Verbeterpunten

- Stimuleer centrale afhandeling van het ter beschikking stellen van politiegegevens door de Infodesk.

- Zorg voor bewustwording en kennis over het proces van ter beschikking stellen door de Infodesk, medewerkers moeten automatisch de Infodesk kunnen vinden in plaats van de privacyfunctionaris.

4.9 Verstrekken (art 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

Verstrekkingen verlopen bij het regiokorps via de Infodesk bij divisie I&I. Voor zover verstrekkingen onder afgesloten convenanten vallen, wordt een verstrekkingen tabel gehanteerd waarin staat vermeld welke stukken aan welke organisaties verstrekt mogen worden. Alle verstrekkingen gaan via de (beveiligde) mail en worden in de computer in een gezamenlijke bak bewaard (Outlook). De verstrekkingen worden gemuteerd in BVH en BVO zodat steeds duidelijk is wat er verstrekt is.

Van de overige verstrekkingen moet een vastlegging worden gemaakt zoals een I90 formulier bij een BVH verstrekking of een vastlegging in het werkjournaal bij verstrekkingen afkomstig uit BVO of andere politie systemen. Aangegeven is dat deze aantallen vastleggingen niet in evenwicht zijn met de feitelijk gedane verstrekkingen.

De RID levert de verstrekkingenrapporten bij de Infodesk aan per mail.

Aandachtspunt hierbij is dat de verstrekkingenrapporten in de verzonden items van de mailbox blijven staan. Als schoning achterwege blijft, dreigt het risico van overschrijding van de bewaartermijnen.

Voor de structurele verstrekkingen aan samenwerkingsverbanden is er onderscheid te maken in algemene en Wpg convenanten. Voor het traceren van convenanten is er een oproep geweest aan de districtscheffs om deze aan te leveren aan de privacyfunctionaris. In eerste instantie kwam hierop weinig respons. De convenanten die zijn aangeleverd, zijn getoetst op de Wpg en waar nodig aangepast en op intranet geplaatst. Inmiddels weten de mensen de privacyfunctionaris te vinden als het om dit onderwerp gaat. Convenanten worden momenteel beheerd door de privacyfunctionaris. Vanwege deze ontstaansgeschiedenis bestaat er momenteel nog geen zekerheid over de volledigheid van de convenanten. Er is (nog) geen procesbeschrijving hoe nieuwe convenanten tot stand komen, maar daar wordt door Sturingsondersteuning aan gewerkt. Ook is een beleidsmedewerker opgeleid om hulp te bieden bij het WPG proof maken van oude en nieuw te maken convenanten. Als er nieuwe convenanten worden gemaakt, wordt de Wpg (besluit art 20) bij het opstellen van deze convenanten direct meegenomen. Wijzigingen in reeds bestaande convenanten worden in een addendum toegevoegd aan het convenant.

Voor wat betreft de geautomatiseerde verstrekkingen wordt er dagelijks een programma (query) gedraaid over BVH. Op basis van dit programma wordt dagelijks één bestand gemaild naar slachtofferhulp met voor hun relevante informatie. Het korps heeft hiermee inzicht in de geautomatiseerde verstrekkingen en de inhoud daarvan.

In NOG neemt de politie deel aan 3 casusoverleggen in het kader van het Veiligheidshuis (Jeugd, Veelplegers en Huiselijke Geweld). De samenwerking is gebaseerd op de raamregeling Samenwerkingsovereenkomst NOG Veiligheidshuis (met

privacy reglement, waarin de informatieverstrekking wordt geregeld). Door de voorzitter van de casusoverleggen (een hoofdinspecteur van politie) wordt onderscheid gemaakt in de verstrekking van informatie aan opsporingsambtenaren en hulpverleners. Schriftelijk krijgen opsporings-ambtenaren NAW gegevens en overige relevante informatie; hulpverleners krijgen alleen NAW gegevens. De aanwezigheid van partners (opsporingsambtenaren en hulpverleners) bij de casusoverleggen geschiedt conform de samenwerkingsovereenkomst - hulpverleners dus ook aanwezig. Mondeling gaat er dus wel e.e.a. over tafel. M.a.w. toezicht binnen het Veiligheidshuis is wel geregeld, maar er ligt ingevolge de Wpg nog wel een knelpunt.

4.9.3 *Verbeterpunten*

- Zorg voor beheersmaatregelen die gericht zijn op een volledige registratie van verstrekkingen door middel van I90 formulieren en andere vastleggingen.
- Controleer of verzonden verstrekkingen in de mailbox RID en Infodesk tijdig worden geschoond.
- Zorg voor een adequaat en centraal beheer van convenanten.

4.10 Rechten van betrokkenen (art 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*

Er is een landelijke handreiking rechten betrokkenen opgesteld. Deze is gebruikt in het project implementatie Wpg binnen regiokorps Noord- en Oost-Gelderland. Het implementatie team van de Wpg heeft procedures beschreven en formulieren ontwikkeld ter ondersteuning van het proces rechten van de betrokkene. Er is een stroomschema opgesteld op basis van de Landelijke handreiking. In de eindrapportage van dit project heeft de implementatie van het artikel de status AF gekregen. Echter uit de interne audit blijkt dat de procedures uit de landelijke handreiking niet specifiek zijn gemaakt en ook niet zijn afgestemd op de administratieve organisatie van het korps.

4.10.3 *Verbeterpunt*

- Maak de landelijke handreiking specifiek en stem deze af op de administratieve organisatie van het korps.

4.11 Protocolplicht (art 32)

4.11.1 *Norm*

De verantwoordelijke draagt zorg voor de schriftelijke vastlegging van:

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

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

4.11.2 *Bevindingen*

Volgens het privacyjaarverslag 2009-2010 heeft de privacyfunctionaris een overzicht van alle protocolgegevens. Dit is nodig om de toezichthoudende en adviserende taak uit te voeren. De privacyfunctionaris houdt van een aantal protocol verplichtingen overzichten bij.

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

4.12 Audits (art 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 het korps Noord- en Oost-Gelderland is in de periode maart tot en met juni 2011 een interne audit uitgevoerd, die als verdienstelijk kan worden gekwalificeerd en heel praktisch is gericht op het zicht krijgen op bestaande knelpunten in de uitvoering van de Wpg. De audit is uitgevoerd in opdracht van de korpschef na goedkeuring van het opgestelde plan van aanpak. Het interne auditteam bestaat uit 5 medewerkers van de afdeling Sturingsondersteuning en de Divisie Informatie & Intelligence. Zij hebben een training gevolgd op het gebied van auditing en de Wpg. In de interne audit is niet naar alle artikelen van de Wpg gekeken. Op basis van een risicoanalyse zijn de artikelen bepaald. Men is nu bezig een auditplanning voor de komende jaren op te stellen, waarbij er jaarlijks een audit plaats vindt. Na vier jaar zijn op deze wijze alle artikelen van de Wpg aan bod gekomen.

4.12.3 *Verbeterpunten*

- Houd bij de interne meerjaren auditplanning rekening met de opvolging van de aanbevelingen uit de voorgaande audits.
- Zorg voor een structurele borging van de interne auditfunctie. Borg hierbij ook de vaktechnische kennis, bijvoorbeeld door het aanbieden van een interne audit opleiding.

4.13 Privacy functionaris (art 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*

De privacyfunctionaris is formeel aangesteld door de korpschef en aangemeld bij het CBP. De privacyfunctionaris voert o.a. de volgende taken uit:

- Een overzicht bijhouden van de toekenning van artikel 6 autorisaties; de autorisatieverzoeken van lijnchefs voor hun medewerkers, waarop zij het fiat moet geven.

- Een overzicht bijhouden van de meldingen/sluitingen van onderzoeken ex artikel 9, daarbij wordt met name het doel getoetst.
- Een overzicht bijhouden van de gegevens krachtens artikel 13 Wpg m.b.t. ondersteunende taken).
- Een overzicht bijhouden van de gegevens krachtens artikel 25 Wpg i.v.m. art.4 BPG (= recht van betrokkenen).
- Een overzicht bijhouden van incidentele verstrekkingen.
- Een privacyjaarverslag opstellen.
- Wpg- en de Wob-verzoeken zijn bij de privacy functionaris belegd.

Het uitvoeren van de toezichthoudende taak van de privacyfunctionaris krijgt om informatie. Tijd om daadwerkelijk toezichthoudende activiteiten uit te voeren in het veld is er daardoor niet.

De functiebeschrijving van de privacyfunctionaris was gericht op de Wet Politiregisters. In het nieuwe functiehuis wordt wel gesproken over de aanstelling conform artikel 34 Wpg, maar over de inhoud van het werk wordt niets vermeld.

4.13.3

Verbeterpunten

- Borg de toezichthoudende taak van de privacyfunctionaris, zoals in de Wpg benoemd.

4.14 Functionaris Gegevensbescherming (art 36)

Het korps Noord- en Oost-Gelderland heeft geen functionaris Gegevensbescherming.