



Ministerie van Veiligheid en Justitie

Audit Wpg politie Brabant-Noord

Rapport

Datum
Status

13 december 2011
Definitief

Colofon

Afzendgegevens

Departementale Auditdienst

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

Contactpersonen

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

T 070 370 65 60
wpq@minvenj.nl

Projectnaam

Audit Wet Politiegegevens

Ons kenmerk

DDS/5719710/11

Auteurs

Jacob Hans Kingma MSc
Saskia van Rijn MSc

Inhoud

Colofon 3

1 Assurance Verklaring 6

2 Samenvatting 8

3 Inleiding 17

3.1 Algemeen 17

3.2 Aanleiding 17

3.3 Doelstelling, aard en scope van de opdracht 17

3.4 Afbakening 18

3.5 Normenkader 18

3.6 Beperkingen voor de privacy audit 19

3.7 Onderzoeksmethoden, werkwijze 19

3.8 Doelgroep van het rapport 19

4 Bevindingen 21

4.1 Inleiding 21

4.2 Verantwoordelijke (artikel 1.f) 23

4.3 Kwaliteitsaspecten van politiegegevens (artikel 3 en 4) 24

4.4 Gevoelige gegevens (artikel 5) 25

4.5 Autorisatie (artikel 6) 25

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

4.7 Bewaartermijnen (artikel 14) 28

4.8 Ter beschikking stellen (artikel 15) 30

4.9 Verstrekken (artikel 16/24) 31

4.10 Rechten van betrokkenen (artikel 25/28) 32

4.11 Protocolplicht (artikel 32) 32

4.12 Audits (artikel 33) 33

4.13 Privacy functionaris (artikel 34) 34

4.14 Functionaris Gegevensbescherming 35

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 maand september 2011 is een privacy audit uitgevoerd bij het korps Brabant-Noord.

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 Brabant-Noord.

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 Brabant-Noord, naar de stand van ultimo september 2011, in opzet, bestaan en werking niet volledig heeft voldaan aan de vereisten zoals genoemd in de Wpg.

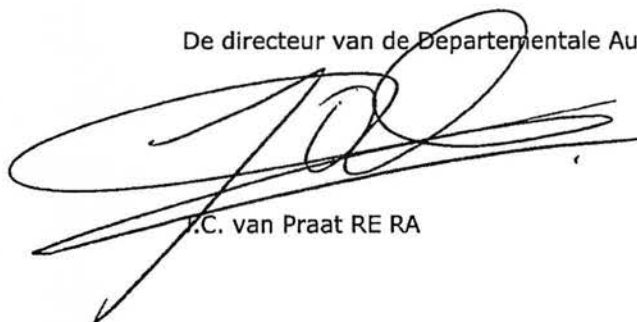
Deze conclusie is onderworpen aan de inherente beperkingen die elders in dit assurance-rapport zijn genoemd.

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

Den Haag, 13 december 2011

De directeur van de Departementale Auditdienst

A handwritten signature in black ink, consisting of several loops and a long horizontal stroke at the bottom.

J.C. van Praat RE RA

2 Samenvatting

Het korps Brabant-Noord heeft veel energie gestoken om in opzet uitvoering te geven aan de Wpg. Op intranet is een uitgebreid document opgenomen met verwijzingen naar diverse procesbeschrijvingen, handreikingen, stroomschema's en wetteksten. Het project Wpg is afgerond en het korps wil de Wpg onlosmakelijk deel uit laten maken van de bedrijfsvoering van de regio. Het korps heeft hiervoor in opzet maatregelen getroffen om dit te borgen. 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	Het mandaat besluit is getekend op 19 januari 2011 door de korpsbeheerder. 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)	De kwaliteitsaspecten zijn opgenomen in het document "WPG implementatie Opsporing Brabant-Noord". Daarnaast is een aparte instructie opgesteld voor blauw op straat. Beide documenten zijn op intranet te vinden. Tijdens presentaties over de WPG is ook aandacht besteedt aan de kwaliteitsaspecten. Hiermee wordt voldaan aan de Wpg.
3.1 t/m 3.3 (8) 4.1 (8)	Noodzakelijkheid (8) Doelbinding Rechtmatigheid Juistheid Volledigheid	Voor artikel 8 verwerkingen zijn procesbeschrijvingen aangetroffen. Met TrueBleu vindt geautomatiseerde controle plaats op de ingevoerde gegevens. Echter het toezicht op de kwaliteit van de ingevoerde gegevens is nog onvoldoende ingeregeld. Hiermee wordt deels voldaan aan de Wpg.
3.1 t/m 3.4 (9) 4.1 (9)	Noodzakelijkheid (9) Doelbinding Rechtmatigheid Herkomst en wijze van verkrijging Juistheid Nauwkeurig Volledigheid	Voor artikel 9 onderzoeken zijn procesbeschrijvingen aangetroffen, deze staan in de Wpg uitleg op het intranet. Hierin is aandacht besteed aan de kwaliteitsaspecten. Op noodzakelijkheid, volledigheid en juistheid vindt collegiale toetsing plaats. Doelbinding moet worden opgenomen in de aanmelding van een onderzoek. Een afschrift hiervan gaat naar de privacyfunctionaris. Rechercheurs moeten informatie waar ze geen toegang tot hebben via de infodesk opvragen.

Norm	Aspect	Bevinding en oordeel
		Infodesk-medewerkers zijn geïnstrueerd voor deze taak. 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	Gezien de bijzondere aard van de werkzaamheden van de CIE en de RID zijn de kwaliteitscriteria goed geborgd. [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] [REDACTED] De CIE heeft een extra waarborg vanwege de toezichthoudende rol van de CIE OvJ. Hiermee wordt voldaan aan de Wpg.
4.3	Beveiliging	BVH, BVO en de mappenstructuur worden beveiligd door middel van autorisaties. In de mappenstructuur is een scheiding aangebracht tussen de verschillende artikelen. [REDACTED] [REDACTED] In geval van schorsing van een persoon wordt diens hoofdaccount afgesloten. Daardoor kan diegene niet meer in de andere systemen van de politie. Echter zijn nog niet alle systemen WPG-proof. Een aantal systemen, waaronder BVH, voldoet niet aan de in de Wpg gestelde bewaartermijnen. Hierdoor ontstaat het risico op onrechtmatig gebruik van politiegegevens. Hiermee wordt deels voldaan aan de Wpg.
Art. 5 Gevoelige gegevens		
	• Gevoelige gegevens	Dit onderwerp is opgenomen in de instructie over de Wpg op intranet. Uit een deelwaarneming van de interne audit is niet gebleken dat gevoelige gegevens vastgelegd worden terwijl dit niet noodzakelijk is. Hiermee wordt voldaan aan de Wpg.
Art. 6, Autorisatie		
	• Korpsautorisatiematrix	Het autorisatiebeleid en de autorisatie matrix zijn conform het landelijk autorisatiemodel en is formeel goedgekeurd door de korpsleiding. Hiermee wordt voldaan aan de Wpg.
	• Aanvraagproces	Een werkinstructie is opgesteld voor aanvraag van autorisaties. Hierbij is onderscheid gemaakt tussen standaard autorisatie gekoppeld aan functies, aanvullende autorisaties en autorisaties van externen. Hiermee wordt voldaan aan de Wpg.
	• Wijziging en verwijdering	Schoning is opgenomen in het autorisatiebeleid Brabant-Noord. Echter kennen de autorisaties nog vervuiling op het gebied van toegewezen bijzondere autorisaties. Het toezicht op de juistheid van

IV
V

III

Norm	Aspect	Bevinding en oordeel
		autorisaties is nog onvoldoende geborgd. Per 1 december 2011 zal de nieuwe werkwijze voor het autoriseren worden ingevoegd in de vorm van de één-loketfunctie. De werkwijze van dit loket is al opgenomen in de werkinstructie. Per 1 januari 2012 maakt vtsPN via Intranet de autorisaties voor alle applicaties en de mappenstructuur realtime zichtbaar en kunnen lijnchefs, privacyfunctionaris en andere geautoriseerden de autorisatielijsten inzien. Hiermee wordt deels voldaan aan de Wpg.
	Autorisatiebeheer CIE en RID	Bij de CIE en de RID zien leidinggevenden zelf toe op autorisaties van eigen medewerkers vanwege de vertrouwelijkheid van informanteninformatie. Functioneel beheer autoriseert alleen na toestemming van het hoofd CIE en RID. Dit is conform een mondelinge afspraak. [REDACTED] Hiermee wordt voldaan aan de Wpg.
32.1.c	Protocollering autorisaties	Functioneel beheer kan overzichten uitdraaien van autorisaties. Autorisaties worden vastgelegd in een Excelbestand. De privacyfunctionaris kan dit overzicht opvragen bij functioneel beheer. Hiermee wordt voldaan aan de Wpg.
32.3 voor 32.1.c	Bewaren protocolgegevens autorisaties	De protocolleringen van autorisaties (van artikel 9 onderzoeken en externen) die via de privacyfunctionaris gaan worden bewaard tot dat de externe audit is afgerond. Echter de aanvragen van bijzondere autorisaties worden niet geregistreerd. De privacyfunctionaris heeft een beperkte steekproef uitgevoerd op de autorisaties en kan pas echt zijn toezichttaak uitvoeren, als het autorisatiebeheer wordt opgeschoond. De autorisatiebeheerder via één loket wordt per 1 december 2011 ingevoerd. Alle mutaties van autorisaties zullen vanaf die datum per persoon worden opgeslagen. Hiermee wordt deels voldaan aan de Wpg.
Art. 11, Geautomatiseerd vergelijken en in combinatie zoeken		
	Hanteerbare interpretatie	Op landelijk niveau bestaat onduidelijkheid over de definitie van geautomatiseerd vergelijken en in combinatie met elkaar verwerken. Het korps heeft wel een invulling gegeven aan de begrippen. De definitie van deze begrippen is opgenomen in de Wpg uitleg op het intranet. Hiermee wordt voldaan aan de Wpg.
	Aangewezen functionarissen	In de werkinstructie op Intranet staat wie welke verwerkingen mag uitvoeren. Deze taak is voornamelijk belegd bij de informatie coördinatoren [REDACTED] Hiermee wordt voldaan aan de Wpg.

III

IV

Norm	Aspect	Bevinding en oordeel
11.4	Bevoegd gezag	Een beperkte groep analisten is geautoriseerd voor in combinatie met elkaar verwerken en zijn hiervoor opgeleid. De aangewezen analisten mogen na toestemming van een OvJ over onderzoeken heen verwerken. Hiermee wordt voldaan aan de Wpg.
32.1.d en 32.1.h	Protocollering 11.1, 11.2, 11.4 en 11,5.	Naar aanleiding van de interne audit is aandacht besteed aan protocollering van geautomatiseerd vergelijken en in combinatie met elkaar verwerken. De werkinstructie is aangepast en opgenomen in de Wpg uitleg op het intranet. Hiermee wordt deels voldaan aan de Wpg.
32.3 voor 32.1.d en 32.1.h	Bewaren protocolgegevens 11.1, 11.2 11.4 en 11,5.	De operationele analyses worden opgeslagen in het betreffende onderzoek. De onderzoeken binnen de afdeling analyse worden op lijsten bijgehouden. De lijsten worden per jaargang opgesteld en bewaard. De privacyfunctionaris heeft geen overzicht van deze type verwerkingen, maar wel toegang tot de registraties in BVO. Hiermee wordt voldaan aan de Wpg.
32.3 voor 32.1.h	Bewaren protocolgegevens 11.5	Protocollering van geautomatiseerd vergelijken en in combinatie met elkaar verwerken wordt bewaard zo lang het onderzoek wordt bewaard. Hiermee wordt voldaan aan de Wpg.
Art. 14, Bewaartermijnen		
8.2 en 8.3	(8) van 1 tot 5 jaar	BVH kan gegevens na één jaar datum eerste verwerking niet achter schot zetten. In de nieuwe release van BVH is dit wel mogelijk. Echter maakt het korps (net als andere korpsen) geen gebruik van deze functionaliteit op landelijk verzoek van de voorzitter van de stuurgroep Wpg. Hiermee wordt niet voldaan aan de Wpg.
8.6	(8) verwijderen na 5 jaar	Gegevens in het oude BPS-systeem zijn tijdig verwijderd. Alleen de infodesk en functioneel beheer hebben toegang tot de verwijderde informatie in BPS. Het BVH bevat nog geen gegevens ouder dan 5 jaar, omdat het systeem pas 3 jaar oud is. De mailboxen bevatten echter nog gegevens ouder dan 5 jaar. Ook de gegevens opgeslagen in de mappenstructuur kent nog oudere gegevens. Hiermee wordt deels voldaan aan de Wpg.
14.1 (8)	(8) vernietigen na 5 jaar verwijderd	Het korps geeft aan dat vernietiging niet plaats vindt conform Wpg. Het korps geeft als reden dat de systemen niet zodanig zijn ingericht dat gegevens afzonderlijk gelabeld kunnen worden en als gevolg daarvan gegevens niet afzonderlijk verwijderd kunnen worden. Daarnaast komen de termijnen van vernietiging volgens de Wpg niet overeen met de verjaringstermijnen van het strafrecht. Aangezien alleen infodesk bij deze gegevens kan en hiervoor geïnstrueerd is, wordt geborgd dat het korps zorgvuldig met deze informatie omgaat.

Norm	Aspect	Bevinding en oordeel
		Hiermee wordt niet voldaan aan de Wpg.
9.4	(9) verwijderen na OH plus ½ jaar	Korpsen zijn afhankelijk van de terugkoppeling over de status van onderzoeken van het OM. Het korps Brabant-Noord handelt proactief door het OM halfjaarlijks een lijst te geven met lopende zaken en te verzoeken hier een terugkoppeling op te geven. Als het OM aangeeft dat een zaak onherroepelijk is, dan wordt de zaak in overleg met de bevoegd functionaris naar de artikel 14 omgeving geplaatst door functioneel beheer. Hiermee wordt voldaan aan de Wpg.
14.1 (9)	(9) vernietigen na 5 jaar verwijderd	Het korps geeft aan dat vernietiging niet plaats vindt conform de Wpg omdat de verjaringstermijnen volgens het wetboek voor strafrecht en de Wpg niet overeenkomen. Hiermee wordt niet voldaan aan de Wpg.
10.6	(10) verwijderen na 5 jaar geen subjectwaardige registratie	Bij de CIE ene de RID worden gegevens op de gezamenlijke harde schijf opgeslagen in jaargangen. Op deze wijze is toezicht op Wpg-termijnen mogelijk. [Redacted text] Hiermee wordt deels voldaan aan de Wpg.
14.1 (10)	(10) vernietigen na 5 jaar verwijderd	Het korps geeft aan dat vernietiging niet plaatsvindt conform de Wpg, omdat de verjaringstermijnen volgens het wetboek voor strafrecht en de Wpg niet overeenkomen. Hiermee wordt niet voldaan aan de Wpg.
14.3	Hernieuwde verwerking	Medewerkers Infodesk (back office) zijn speciaal geïnstrueerd voor hun taak. Hernieuwde verwerking is opgenomen in de procesbeschrijvingen. Hiermee wordt voldaan aan de Wpg.
32.1.e	Protocollering 14.3	Protocollering van artikel 14 lid 3 (hernieuwde verwerking) is niet opgenomen in de procesbeschrijvingen. Wel protocolleren medewerkers van de Infodesk de aanvraag voor, het doel van en de toestemming stemming voor een hernieuwde verwerking. De toestemming komt schriftelijk binnen van de OvJ. Hiermee wordt voldaan aan de Wpg.
32.3 voor 32.1.e	Bewaren protocolgegevens 14.3	Alles wat de Infodesk verstrekt (zowel intern als extern) wordt geprotocolleerd in BVO. De protocolgegevens worden bewaard zo lang de registratie wordt bewaard. Hiermee wordt voldaan aan de Wpg.
12.2	(12) verwijderen na 4	Het omzetten van bruto naar netto informatie

Norm	Aspect	Bevinding en oordeel
	maanden	gebeurt dagelijks binnen een week. Alleen netto informatie wordt ter beschikking gesteld. Hierdoor wordt de termijn van vier maanden niet overschreden. Hiermee wordt voldaan aan de Wpg.
12.6	(12) controleren en vernietigen	Uit de Interne audit blijkt dat de bewaartermijnen met betrekking tot informanten wordt nageleefd. Halfjaarlijkse controle vindt plaats en gegevens worden na 10 jaar vernietigd. Hiermee wordt voldaan aan de Wpg.
Art. 15, Ter beschikking stellen		
	• Infodesk voor bevraging	Medewerkers infodesk zijn speciaal geïnstrueerd voor hun taak en een procesbeschrijving voor de infodesk is aanwezig. Infodesk vraagt toestemming aan bevoegd functionaris voordat informatie van een onderzoek ter beschikking wordt gesteld. Hiermee wordt voldaan aan de Wpg.
	• Codering	Afspraken over codering is vastgelegd in de procedure beschrijving voor onderzoeken. Middels autorisatie kunnen onderzoeken afgeschermd worden. Een overzicht van coderingen van de lopende artikel 9 onderzoeken is aanwezig. Alle onderzoeken worden opgenomen in de mappenstructuur met een opeenvolgend nummer waardoor de controle goed uitvoerbaar is. Het nummer in de mappenstructuur is gelijk aan het nummer van de BVO registratie. De privacyfunctionaris ziet periodiek toe op de coderingen en ook de functioneel beheerder van opsporing. Hiermee wordt voldaan aan de Wpg.
	• Aanwijzing Bevoegd Functionaris	Middels besluit zijn bevoegd functionarissen aangewezen. Hiermee wordt voldaan aan de Wpg.
	• Opleiding Bevoegd Functionaris	Alle bevoegd functionarissen hebben een opleiding gevolgd tot bevoegd functionaris. De handreiking bevoegd functionaris hebben de functionarissen ter voorbereiding op de opleiding ontvangen. Tijdens de opleiding is de opleider aan de hand van praktijkvoorbeelden en jurisprudentie met de deelnemers aan de slag gegaan. Een omschrijving van de taak van de bevoegd functionaris is ook opgenomen in de Wpg uitleg op het intranet. Hiermee wordt voldaan aan de Wpg.
15.2	Weigeringgronden	Informatie van verschillende regimes is afgeschermd door gebruik van autorisaties. Hierdoor zal informatie opgevraagd moeten worden aan de bevoegd functionaris. Hiermee wordt voldaan aan de Wpg.
Art. 16 t/m 24, Verstrekking		
	• Verstrekkingenwijzer (landelijk)	Brabant-Noord maakt gebruik van de landelijke verstrekkingenwijzer. De afspraak is dat de meeste

Norm	Aspect	Bevinding en oordeel
		verzoeken worden afgewerkt door het backoffice van de infodesk. Daarnaast verlopen verstrekkingen via de meldkamer en DIK. Hiermee wordt voldaan aan de Wpg.
• Proces voor convenanten		Een document genaamd richtlijnen voor convenanten is opgesteld. De bevoegd functionaris is verantwoordelijk voor het opstellen van convenanten. In een opgestelde interne notitie 'verstrekken politiegegevens aan samenwerkingsverbanden' staan de richtlijnen voor het openstellen van een convenant. Deze is raadpleegbaar via de Wpg uitleg op het Intranet. Echter (centraal en) adequaat beheer van convenanten moet nog ingeregeld worden. Hiermee wordt deels voldaan aan de Wpg.
• Proces voor Art. 20 Besluiten		In de procedure voor convenanten is het proces voor artikel 20 besluiten vormgegeven. Hiermee wordt voldaan aan de Wpg.
• Verstrekkingenschema (regio)		Een beleid voor verstrekkingen is opgesteld. Structurele verstrekkingen verlopen via de Infodesk, de Meldkamer en het DIK. De artikel 19 verstrekkingen zijn opgenomen in het basisdocument verstrekkingen. Het korps werkt aan een gedetailleerdere werkinstructie voor dit onderdeel. Hiermee wordt voldaan aan de Wpg.
• Proces voor geautomatiseerde verstrekking		Vanuit de regio vinden geen geautomatiseerde verstrekkingen plaats. Geautomatiseerde verstrekkingen die plaatsvinden verlopen via de vtsPN en zijn wettelijk vastgesteld.
7.2	Geheimhouding	Geheimhouding is opgenomen in de convenanten In de Wpg uitleg op intranet is ook opgenomen dat medewerkers bij verstrekkingen aan derden de geheimhoudingsplicht moeten benadrukken. Hiermee wordt voldaan aan de Wpg.
32.1.f	Protocollering verstrekking	In opzet is beschreven hoe medewerkers verstrekkingen moeten vastleggen. Echter zijn nog niet alle medewerkers bekend met de wijze waarop verstrekkingen geprotocolleerd moeten worden. Hiermee wordt deels voldaan aan de Wpg.
32.3 voor 32.1.f	Bewaren protocolgegevens verstrekking	De protocolleringen van verstrekkingen worden bewaard in de betreffende registratie tot dat de registratie vernietigd is. Hiermee wordt voldaan aan de Wpg.
• Toezicht door leidinggevend op verstrekkingen en protocollering		Voor verschillende verstrekkingen is aangegeven in de Wpg uitleg op intranet welke partij verantwoordelijk is voor welke verstrekkingen. In de interne audit is een steekproef uitgevoerd op de protocollering van verstrekkingen. Echter ervaart blauw op straat weinig sturing op het verstrekken van gegevens. Hiermee wordt deels voldaan aan de Wpg.

Norm	Aspect	Bevinding en oordeel
Art. 25 t/m 31, Rechten van de betrokkene		
25.1	Verzoek om kennisneming	Infodesk handelt verzoeken rechten betrokkenen af. Een procesbeschrijving rechtenbetrokkene is opgesteld. Indien een betrokkene voorkomt in de registraties van onderzoeken (artikel 9) of CIE en RID (artikel 10), moet contact opgenomen worden met bevoegd functionaris. Hiermee wordt voldaan aan de Wpg.
28.1 t/m 28.3	Correctie	Een procesbeschrijving is opgesteld. Ook is opgenomen dat personen of instanties waaraan informatie verstrekt is, ingelicht moeten worden over een wijziging. Hiermee wordt voldaan aan de Wpg.
Art. 32, Protocolplicht (32.1.c, d, e, f en h behandeld bij thema's)		
9.2 en 32.1.a	Protocollering doel onderzoek	De bevoegd functionaris moet een onderzoek aanmelden via aanvraagformulier waar het doel op moet worden vermeld. Doelbinding wordt altijd in BVO vastgelegd. De privacyfunctionaris ontvangt een kopie van de onderzoeksaanvraag. Hiermee wordt voldaan aan de Wpg.
32.3 voor 32.1.a	Bewaren protocolgegevens doel onderzoek	De afschriften van de onderzoeksaanvragen die afgesloten zijn, worden door de privacyfunctionaris bewaard tot dat de externe audit is afgerond. Openstaande onderzoeken blijven ook na de externe audit bewaard. Hiermee wordt voldaan aan de Wpg.
13.4 en 32.1.b	Protocollering Art. 13 gegevensverzameling en	Een overzicht bijhouden van de artikel 13 gegevensverzamelingen (de ondersteunende taken) wordt nog niet gedaan. De privacyfunctionaris geeft aan dat dit ook een lastige taak is omdat veel artikel 13 verwerkingen landelijk geregeld zijn. Het korps was ten tijde van de audit actief bezig met het vastleggen van de locale systemen met artikel 13 verwerkingen. Hiermee wordt deels voldaan aan de Wpg.
32.3 voor 32.1.b	Bewaren protocolgegevens Art. 13 gegevensverzameling en	Een overzicht bewaren van de artikel 13 gegevensverzamelingen (de ondersteunende taken) wordt nog niet gedaan. Het korps was ten tijde van de audit actief bezig met het vastleggen van de locale systemen met artikel 13 verwerkingen. Hiermee wordt deels voldaan aan de Wpg.
32.1.g	Protocollering onrechtmatige handeling	Lijnchefs houden een overzicht bij van onrechtmatige verwerkingen en verstrekken deze jaarlijks aan de privacyfunctionaris voor het jaarverslag. Als er een vermoeden van opzet is van onrechtmatige verwerkingen, zal Bureau Interne Zaken ingeschakeld worden. Hiermee wordt voldaan aan de Wpg.
32.3 voor 32.1.g	Bewaren protocolgegevens onrechtmatige	Protocolgegevens blijven bewaard tot dat de eerstvolgende externe audit is afgerond. Hiermee wordt voldaan aan de Wpg.

Norm	Aspect	Bevinding en oordeel
	handeling	
32.2	Gemeenschappelijke verwerking	Gemeenschappelijke verwerkingen komen niet voor bij het korps. Bovenregionale zaken worden door een bovenregionaal recherche eenheid uitgevoerd. Ook kan het voorkomen dat medewerkers van een andere regio toegevoegd worden aan een onderzoek van Brabant-Noord. Deze externe medewerker krijgt een autorisatie en valt daarmee onder de verantwoordelijkheid van het korps van de teamleider van het betreffende onderzoek.
Art. 33, Audits		
RPAP 3.1	Interne audit-functie	Het korps heeft een interne auditor Wpg benoemd. Hiermee wordt voldaan aan de Wpg.
RPAP 3.4	Interne audit-plan	De interne audit uitgevoerd in 2011 is conform het opgestelde auditplan uitgevoerd. Door samenvoeging van de korpsen Brabant-Noord met Brabant Zuid-Oost moet een nieuw intern auditplan opgesteld worden. Hiermee wordt deels voldaan aan de Wpg.
RPAP 3.6	Interne audit-rapport	In 2011 is een Interne audit Wpg uitgevoerd en de rapportage is aan ons verstrekt. Hiermee wordt voldaan aan de Wpg.
Art. 34, Privacyfunctionaris		
34.1 en 34.4	Benoemd en gemeld	de privacyfunctionaris is formeel benoemd door de korpsbeheerder en aangemeld bij het CBP. Hiermee wordt voldaan aan de Wpg.
34.2	Overzicht over protocollering	De privacyfunctionaris heeft een overzicht van de artikel 9 onderzoeken. Een overzicht van de artikel 13 gegevensverzamelingen, hernieuwde verwerkingen, geautomatiseerd vergelijken en in combinatie met elkaar verwerken wordt niet bijgehouden door de privacyfunctionaris. Wel zijn vele van deze verwerkingen vastgelegd in de betreffende registratie. Hiermee wordt niet voldaan aan de Wpg.
	Jaarverslag	Over het jaar 2009 en 2010 is een gecombineerd jaarverslag opgesteld. Wegens persoonlijke omstandigheden heeft de privacyfunctionaris zijn toezichtstaak nog niet goed kunnen uitvoeren. Door gebrek aan informatie vanuit de toezichtstaak van de privacyfunctionaris geeft het jaarverslag beperkt inzicht in de uitvoering van de Wpg bij het korps. Hiermee wordt deels voldaan aan de Wpg.
Optioneel Art. 36, Functionaris Gegevensbescherming		
36.1 en 36.2	Benoemd	Het korps heeft geen functionaris gegevensbescherming benoemd.
Wbp 63.3	Gemeld	N.v.t.
Wbp 64.1 t/m 64.4	Toezichthoudende rol	N.v.t.

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 Brabant-Noord 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 Brabant-Noord 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

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

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 politiekorps Brabant-Noord 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 politiekorps. Pas wanneer wij, tijdens het uitvoeren van de audit bij een politiekorps, hebben geconstateerd dat de opzet en het bestaan aan de daaraan te stellen eisen voldoen voeren wij aanvullende werkzaamheden uit om de werking vast te stellen.

3.4 Afbakening

De audit wordt uitgevoerd aan de hand van het normenkader dat wij voor dit doel hebben opgesteld. Het normenkader 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 Brabant-Noord. Dit betekent dat wij geen onderzoek hebben verricht naar door de vtsPN aan het korps Brabant-Noord geleverde faciliteiten, voor zover de verantwoordelijkheid daarvoor is belegd bij de vtsPN of bij anderen dan het korps Brabant-Noord.

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, 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 politiekorps Brabant-Noord en het Openbaar Ministerie, deelwaarnemingen in de procesbeschrijvingen en andersoortige documentatie en deelwaarnemingen in informatiesystemen. Wij hebben onze werkzaamheden uitgevoerd in de periode van 29 augustus tot en met 22 september 2011.

Het conceptrapport met bevindingen is op 10 november 2011 besproken met de korpschef van het korps Brabant-Noord. Op 13 december 2011 is een nieuwe versie voorgelegd aan de korpschef en na zijn goedkeuring is het rapport definitief gemaakt. 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 Korpsbeheerders Beraad is vertegenwoordigd. De stuurgroep wordt voorgezeten door drs. J.J.M. Stikvoort. mr. A.F. Gaastra neemt namens Directeur-Generaal 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 Brabant-Noord; mr. dr. A.G.J.M. Rombouts
- de waarnemend korpschef Brabant-Noord; mr. A.D. Heil
- de fungerend Hoofd Officier van Justitie Brabant-Noord; mr. R.P.H.G. de Beukelaer
- de Privacy Functionaris; [REDACTED]
- de voorzitter van het College Bescherming Persoonsgegevens

I

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

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

4 Bevindingen

4.1 Inleiding

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

4.1.1

Regie en doorzettingsmacht voor de Wpg implementatie

Het korps Brabant-Noord is in 2009 van start gegaan met de implementatie van de Wpg. Uit een vooronderzoek in het kader van de interne audit kwam naar voren, dat de Wpg in opzet onvoldoende was geïmplementeerd binnen het korps. Dit had als oorzaak dat er onder andere te weinig samenhang bestond tussen de verschillende procesbeschrijvingen in relatie tot de Wpg. De interne auditor heeft vervolgens in 2010, gezamenlijk met de afdelingshoofden, de procesbeschrijvingen schematisch volgens de Wpg opgebouwd. Op deze manier is een overzicht tot stand gekomen dat de samenhang creëert tussen alle procesbeschrijvingen en de Wpg.

In 2011 is een interne audit Wpg bij het korps uitgevoerd. Bij alle thema's van de interne audit is zowel de opzet als het bestaan getoetst. Het korps Brabant-Noord heeft aangegeven te wachten met het opvolgen van de aanbevelingen tot de samenvoeging met het korps Brabant Zuid-Oost.

Doormiddel van interviews en documentstudie van de audittrail hebben wij vastgesteld dat we kunnen steunen op de bevindingen die uit de interne audit komen. De medewerkers die de interne audit hebben uitgevoerd zijn kritisch geweest op hun eigen korps en hebben een rapport opgeleverd waar het korps verder mee kan.

Wij merken op dat vanwege omstandigheden de interne auditor gedurende bovenstaand beschreven periode zowel de rol van projectleider als die van de privacyfunctionaris op zich heeft genomen. Dit kan een risico op leveren voor de onafhankelijkheid van de interne auditor. Zie paragraaf 4.12 audits voor meer informatie over de interne audit.

We willen benadrukken dat het korps veel werk heeft verricht aan het bouwen van gedegen procesbeschrijvingen conform de Wpg om aan de implementatie van de Wpg gestalte te geven.

Binnen het korps is een organisatiebeschrijving aanwezig, 'koers naar 2011'. In deze beschrijving zijn onder andere een organogram, taakbeschrijvingen per organisatieonderdeel en de proceseigenaren opgenomen.

In het document 'WPG impact en actie' en in de Wpg map op het intranet is het algemene doel van de Wpg en hoe het korps hier nader invulling aan geeft vastgelegd. De Wpg map bevat een overzicht met hyperlinks naar wetsartikelen, procesbeschrijvingen en werkinstructies op artikelniveau per functionaris. De Wpg map is middels een besluit van de korpsleiding goed gekeurd. Ter introductie zijn

diverse presentaties in managementteams gehouden om de opzet Wpg en het gebruik van deze map toe te lichten.

De korpschef heeft de privacyfunctionaris aangesteld en deze aangemeld bij het CBP. Over het jaar 2010 heeft de privacyfunctionaris een jaarverslag opgesteld. Dit is een gecombineerd verslag van de jaren 2009 en 2010. Door omstandigheden heeft de privacyfunctionaris nog niet alle controle- en toezichttaken uit kunnen voeren zoals deze in de wet zijn vastgelegd. De taken van de privacyfunctionaris zijn wel vastgelegd.

De functies met de rol bevoegd functionaris zijn middels een besluit vastgesteld. De korpsbeheerder heeft een mandaatbesluit vastgesteld. De korpschef heeft een ondermandaat vastgesteld.

Voor het korpsjaarplan 2011 is bewust gekozen om de Wpg niet meer als apart onderwerp in het jaarplan op te nemen. Het project Wpg is afgerond en maakt volgens het korps nu onlosmakelijk deel uit maakt van de bedrijfsvoering van de regio. Om de borging en naleving van de Wpg in de managementcontrolcyclus in te bedden heeft het korps in opzet wel afspraken gemaakt. Uit onze interviews komt wel naar voren dat leidinggevenden twee keer per jaar een checklist Wpg in dienen te vullen. Deze checklisten dienen het management inzicht te verschaffen in hoeverre het korps voldoet aan de bepalingen vanuit de Wpg. Verder maakt het korps gebruik van een dashboard waar ook Wpg onderwerpen in staan. Twee keer per jaar vinden managementgesprekken plaats waar het dashboard ook besproken wordt. De privacyfunctionaris en de interne auditor zijn zich er van bewust dat de borging van de Wpg meer gestalte moet krijgen in de managementcontrolcyclus.

4.1.2

Bekendheid met de Wpg binnen de organisatie

Het merendeel van de medewerkers heeft een Wpg opleiding genoten. Uit de interviews komt naar voren dat de behandelde Wpg-onderwerpen niet altijd goed bijbleven omdat de opleiding een praktische insteek miste. Geïnterviewde geven aan dat ze de Wpg uitleg van de interne auditor (heer [REDACTED]) erg leerzaam vinden.

I

De kennis van de Wpg is nog niet bij iedere politiefunctionaris voldoende aanwezig. Hierdoor is men zich in het dagelijkse werk ook niet altijd bewust van wat de Wpg inhoudt en welke mogelijkheden de Wpg biedt. Functionarissen hebben behoefte aan een periodiek overleg binnen hun afdeling om vragen en knelpunten over de Wpg met elkaar te bespreken. Op dit moment is de Wpg geen structureel agendapunt tijdens afdelingsoverleggen. Uit de interviews komt naar voren dat infodesk hier een uitzondering op is. Deze afdeling kan op dit punt als best practice gezien worden binnen het korps.

De Wpg map op intranet, met daarin de beschreven opzet Wpg, zien wij als een best practice voor andere korpsen. Dit vanwege de volledigheid en vanwege het gemak waarmee de Wpg onderwerpen kunnen worden benaderd (per artikel of per organisatieonderdeel). Leidinggevenden geven aan dat medewerkers op een lager niveau in de organisatie het document niet veel gebruiken. Ze geven aan dat medewerkers het ervaren als een complex document dat niet eenvoudig toepasbaar is in de praktijk. Op de werkvloer hebben medewerkers behoefte aan een eenvoudiger werkinstructie, waarin de regelgeving van de Wpg concreet en helder op één A4 staat beschreven. Dit biedt de functionaris handvatten bij het uitvoeren van de dagelijkse werkzaamheden conform de Wpg.

Bij vragen en onduidelijkheden weten de politiefunctionarissen zowel de privacyfunctionaris als de interne auditor goed te vinden.

4.1.3 *Wpg en de praktijk*

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

Schonings- en bewaartermijnen worden soms als knellend ervaren. Doordat de informatiesystemen deze informatie na één jaar niet achter slot zetten, wordt de informatie in de praktijk ook vaak langer dan één jaar gebruikt. Daarnaast komen de bewaartermijnen volgens de Wpg niet overeen met de termijnen volgens het strafrecht. Hierdoor wordt nog geen uitvoering gegeven aan de vernietigingstermijnen conform de Wpg.

4.1.4 *Verbeterpunten*

- Zorg dat leidinggevenden de instrumenten voor de borging van de Wpg in de P&C-cyclus actief gebruiken.
- Verhoog de Wpg kennis en het bewustzijn in de organisatie bijvoorbeeld door het behandelen van casuïstiek in opleidingen en het verspreiden van promotiemateriaal.
- Laat de Wpg deel uit maken van de verschillende overleggen en behandel daarin eventueel ook best practices, voorbeeld casus en do's en dont's van de Wpg.
- Stel een eenvoudige praktische werkinstructie op voor blauw op straat.

4.2 Verantwoordelijke (artikel 1.f)

Mandaatbesluit

4.2.1 *Norm*

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

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*

Er is een Mandaatbesluit Wet politiegegevens korps Brabant-Noord d.d. 19 januari 2011, waarin wordt aangetoond dat het bevoegd gezag (korpsbeheerder), met terugwerkende kracht tot en met 1 januari 2008, zijn mandaat verleent aan de korpschef van het politiekorps Brabant-Noord. Daarnaast is er ook een Ondermandaatbesluit Wet politiegegevens korps Brabant-Noord d.d. 17 januari 2011, waarin de korpschef van Brabant-Noord ondermandaat verleent aan het hoofd van de Divisie, het District dan wel de proceseigenaren.

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 bijna alle geledingen van de politie zijn betrokken. Het is van belang dat het zwaartepunt om te voldoen aan deze criteria ligt bij de eerste vastlegging van gegevens.

Proces Handhaving

Met betrekking tot artikel 8 informatie *'verwerken van politiegegevens ten behoeve van de dagelijkse politiepraktijk, zoals surveilleren, advisering over preventie, afhandelingen van de verkeersproblematiek, eenvoudig recherchewerk, verlenen van hulp en handhaven van wetten en regels'* zijn procesbeschrijvingen aangetroffen, waarin is opgenomen hoe uitvoering dient gegeven te worden aan deze criteria.

De volledigheid en juistheid van gegevens wordt enigszins geborgd door de verplichte invulvelden van BVH. Ook vindt een check plaats op de persoonsgegevens met het GBA-systeem. Er vindt geen toezicht en sturing plaats op de invoering van informatiegegevens. Wel vindt regelmatig collegiale toetsing plaats bij de invoer op noodzakelijkheid, rechtmatigheid, juistheid en volledigheid. Bij een constatering van onjuiste gegevens worden deze verwijderd.

Aan doelbinding wordt voldaan doordat medewerkers een registratie moeten koppelen aan een incident in BVH. Uit de interne audit komt tevens naar voren dat informatie, ouder dan één jaar na de eerste verwerking, gebruikt wordt voor verdere verwerking. Aan de Wpg termijn van één jaar wordt hiermee niet voldaan.

Proces Opsporing

In artikel 9 Wpg wordt gesproken over het *'gericht verwerken van politiegegevens ten behoeve van een onderzoek met het oog op de handhaving van de rechtsorde in een bepaald geval'*. Hiervoor zijn procesbeschrijvingen aangetroffen waarin is opgenomen hoe uitvoering gegeven dient te worden aan deze criteria.

De doelbinding van informatiegegevens wordt altijd in BVO wordt vastgelegd. Bij de start van een MRO ontvangt de privacyfunctionaris, via een onderzoeksaanvraag, een melding van het onderzoek. Bij het invoeren van gegevens in BVO vindt collegiale toetsing plaats op noodzakelijkheid, rechtmatigheid, juistheid en volledigheid.

Vanuit de controletaak voert de privacyfunctionaris steekproefsgewijs controles uit op de verwerkingen. Wanneer hij onrechtmatige verwerkingen aantreft worden deze teruggekoppeld aan de betreffende persoon. Onrechtmatigheden in verwerkingen worden vaak niet bewust gemaakt, maar komen vaak voort uit onwetendheid.

CIE en RID

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.

De CIE en de RID besteden vanwege de bijzondere aard van hun taken specifiek aandacht aan bovenstaande kwaliteitsaspecten. Daarbij is in opzet voldaan aan deze criteria:

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

III

IV

V

[REDACTED]

[REDACTED]

[REDACTED]

4.3.3**Verbeterpunten**

- Landelijk: Zet informatie, ouder dan één jaar na datum van eerste verwerking, achter schot in de informatiesystemen, zodat deze niet meer zelfstandig gebruikt kan worden voor de verwerking van informatiegegevens.
- Voer sturing en toezicht uit op de invoer van gegevens in BVH ten behoeve van de kwaliteit en informatiedeling.

4.4 Gevoelige gegevens (artikel 5)**4.4.1****Norm**

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

4.4.2**Bevindingen**

In de Wpg uitleg op intranet is het onderwerp gevoelige gegevens opgenomen in diverse documenten, zoals werkinstructies. Tijdens de interne audit is een beperkte deelwaarneming uitgevoerd. Hieruit is gebleken dat geen gevoelige gegevens zijn vastgelegd.

4.5 Autorisatie (artikel 6)**4.5.1****Norm**

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

4.5.2 *Bevindingen*

Autorisatieproces

Het korps heeft haar autorisatiebeleid ingericht volgens het landelijke autorisatiebeleid. Brabant-Noord maakt gebruik van een autorisatiematrix waarin per functie een autorisatieprofiel is vastgesteld. Medewerkers krijgen bij indiensttreding een menu aan autorisaties die horen bij een bepaald functieprofiel. Naast deze profielen zijn er mogelijkheden voor de toekenning van extra autorisaties van informatiesystemen en onderzoeksmappen. Een lijnchef moet hiervoor een verzoek indienen bij functioneel beheer. Functioneel beheer beschikt over een lijst met de proceseigenaren. Bij twijfel wordt overleg gevoerd met de privacyfunctionaris en proceseigenaar en vindt toetsing op de noodzaak en rechtmatigheid van de autorisatie plaats. De functioneel beheerder houdt tevens een overzicht van de autorisaties bij. Autorisatieverzoeken voor externe functionarissen worden door de privacyfunctionaris in behandeling genomen. In geval van schorsing van een medewerker wordt diens hoofdaccount afgesloten. Daardoor kan diegene niet meer in de andere systemen van de politie.

Schoning van oudere autorisaties heeft nog niet plaatsgevonden. Brabant-Noord wacht hiermee tot de overgang naar de regio Oost-Brabant. De functie autorisatiebeheerder, zoals genoemd in de interne audit rapportage, was tot op heden nog niet ingevuld omdat Brabant-Noord tot voor kort niet beschikte over voldoende FTE. Per 1 december 2011 zal deze functie wel ingevuld worden en verlopen de autorisaties via één autorisatieloket.

De functioneel beheerder voert steekproefsgewijs op eigen initiatief controles uit op de autorisaties van functionarissen. Als blijkt dat een medewerker uit dienst getreden is worden alle autorisaties verwijderd.

Proces handhaving

De autorisaties voor het proces handhaving worden toegekend op de manier, zoals hierboven beschreven. Alle politieambtenaren met een autorisatie voor BVH kunnen registraties in BVH raadplegen.

Proces Opsporing

De standaard autorisaties voor het proces opsporing worden toegekend op de manier, zoals beschreven onder het autorisatieproces. Daarnaast wordt een onderzoek door een bevoegd functionaris aangemeld via een formulier op intranet. Functioneel beheer ontvangt dit formulier en wijst een map voor het betreffende onderzoek toe in BVO en in de mappenstructuur. De teamleider van het betreffende onderzoek kan vervolgens teamleden autoriseren voor map van het onderzoek. Na afloop van een onderzoek worden de autorisaties op aangeven van de teamleider door de functioneel beheerder verwijderd.

Bij infodesk heeft een selecte groep medewerkers van de Backoffice een hoger autorisatieniveau. Daarmee kunnen deze medewerkers in oudere zaken kijken. Deze medewerkers zijn speciaal geïnstrueerd voor deze taak. Indien informatie verwijderd is, maar nog niet is vernietigd, kan alleen met toestemming van de OvJ informatie ter beschikking gesteld worden voor een nieuw of hernieuwd onderzoek. Daarnaast mag de informatie ingezien worden voor afhandeling van klachten en voor verantwoording.

CIE en RID

De standaard autorisaties voor medewerkers van de CIE en de RID worden toegekend op de manier, zoals beschreven onder het autorisatieproces. 

[REDACTED]

III

4.5.3

Verbeterpunten

- Voer een controle uit op oudere mutaties met betrekking tot autorisaties.
- Zorg voor een structurele controle van de toegekende autorisaties in de functie van een autorisatiebeheerder.

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

4.6.1

Norm

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

Indien politiegegevens in combinatie met elkaar worden verwerkt, worden van die verwerking nader genoemde gegevens vastgelegd (protocolplicht).

4.6.2

Bevindingen

Het geautomatiseerd vergelijken wordt gedaan door alle politiemedewerkers van Brabant-Noord. Doordat de medewerkers in BVH alle informatie ouder dan één jaar na de eerste 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 niet voldoende bewust van dat dit volgens de Wpg niet mag.

Het in combinatie met elkaar verwerken is voornamelijk belegd bij de coördinatoren informatieproces [REDACTED]

[REDACTED] Deze medewerkers zijn opgeleid om deze taak uit te voeren. Uit de interne audit blijkt dat het protocolleren van deze verwerkingen nog niet altijd op uniforme wijze wordt uitgevoerd en in opzet nog moet worden geregeld.

IV

Brabant-Noord heeft op intranet in de map Wpg een instructie staan over wat geautomatiseerd vergelijken en in combinatie met elkaar verwerken is. Daarbij wordt ook aangegeven wat het verschil tussen deze twee termen is.

4.6.3

Verbeterpunten

- Landelijk: Richt systemen zo in dat informatie ouder dan één jaar na eerste verwerking niet tot in detail geraadpleegd kan worden door een onbevoegde politiefunctionaris.
- Maak medewerkers bewust van wat geautomatiseerd vergelijken en in combinatie met elkaar verwerken is en wat de mogelijkheden en grenzen zijn. Dit kan bijvoorbeeld door verwijzing naar de instructie op internet of door het

ontwikkelen van casuïstiek aan de hand waarvan geautomatiseerd vergelijken en in combinatie met elkaar verwerken besproken kan worden..

- Stel een procedure op voor het protocolleren van verwerkingen naar aanleiding van het in combinatie met elkaar verwerken.

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.

Politiegegevens die niet langer noodzakelijk zijn voor het doel van het onderzoek, worden verwijderd, of worden gedurende een periode van maximaal een half jaar verwerkt teneinde te bezien of zij aanleiding geven tot een nieuw onderzoek als bedoeld in artikel 9 of een nieuwe verwerking als bedoeld in artikel 10, en na verloop van deze termijn worden verwijderd.

4.7.2

Bevindingen

Proces Handhaving

Met betrekking tot artikel 8 Wpg is een procedure aangetroffen voor de omgang met bewaartermijnen, maar niet voor de vernietiging van politiegegevens. In algemene zin is wel beschreven welke termijnen gelden voor verwijdering en vernietiging van gegevens.

Het landelijke systeem BVH is niet voorzien van beheersmaatregelen op het gebied van termijnen voor verwijderen en vernietigen van politiegegevens. Het is in BVH niet mogelijk informatie geautomatiseerd na één jaar achter een schot te plaatsen, zodat deze informatie niet meer kan worden geraadpleegd. In de nieuwe release van BVH zou dit wel tot de mogelijkheden behoren; deze release zou Brabant-Noord in week 40 invoeren. Het korps heeft uiteindelijk besloten de nieuwe release niet door te voeren omdat de bewaartermijnen niet overeenkomen met de verjaringstermijnen van het strafrecht. Daarnaast is veel informatie niet meer zichtbaar in de nieuwe release, zoals bijvoorbeeld de maatschappelijke klassen; is iemand verdachte of betrokkene. Het korps geeft aan dat na de invoering van de nieuwe release medewerkers de infodesk en het DIK zullen overbelasten, omdat ze te weinig informatie kunnen zien.

In BVH vinden geen handmatige schoningen plaats. Het korps geeft aan dat dit nog niet nodig is, omdat BVH pas drie jaar oud is en daarom de gegevens in BVH nog geen vijf jaar oud zijn. Het voormalige systeem BPS is wel tijdig geschoond na de termijn van vijf jaar. Deze gegevens worden in de historische omgeving geplaatst waar alleen functioneel beheer en infodesk bij kunnen. De verwijderde gegevens uit BPS worden nog niet vernietigd.

De meldkamer maakt gebruik van het systeem GMS. Gegevens in dit systeem gaan na 5 jaar geautomatiseerd achter schot.

Proces Opsporing

Het landelijke systeem BVO is niet voorzien van beheersmaatregelen op het gebied van termijnen voor verwijderen en vernietigen van politiegegevens. Functioneel beheer kan toezicht houden op de bewaartermijnen in BVO doordat de onderzoeksaanvragen via deze afdeling lopen en functioneel beheer bij aanvang van een onderzoek een label aan het onderzoek mee kan geven. Op deze wijze kan functioneel beheer toezien op termijnen van verjaring. Het OM en functioneel

beheer houden samen een lijst bij met de status van onderzoeken. Als een onderzoek bij het OM is voorgebracht, ontvangt functioneel beheer een terugkoppeling van het OM. Als een onderzoek is verjaard of onherroepelijk is verklaard, worden de betreffende onderzoeken in de artikel 14 omgeving geplaatst. Daarnaast draait functioneel beheer draait jaarlijks een lijst uit met zaken die in aanmerking komen voor afsluiting. In overleg met de teamleider van het onderzoek en verwijdert functioneel beheer de autorisaties van de onderzoeken waarvan de bewaartermijn is verstreken. Op deze wijze kunnen medewerkers niet meer bij de informatie.

Bij de recherche wordt gebruik gemaakt van het systeem DRS. Gegevens in DRS worden niet vernietigd, schoning vindt slechts handmatig plaats. Het OM ziet niet toe op naleving van de WPG met betrekking tot gegevens in DRS. Op de back-up server staan complete images van gegevens. Schoning van de back-up server vindt echter niet plaats. Ook het systeem TRIS is niet WPG-proof.

Uit de interviews komt naar voren dat rechercheurs niet geautoriseerd zijn om te kunnen zoeken in oudere zaken, maar dat wel graag willen. Ze denken dat door hun inhoudelijke betrokkenheid ze meer informatie uit oudere informatie kunnen halen dan de infodesk. Hoewel niet alle medewerkers even content zijn met de situatie, blijkt hieruit wel dat op dit punt conform Wpg gehandeld wordt.

Met het oog op bewaartermijnen en vernietiging voldoet Brabant-Noord in opzet niet aan de eisen die de Wpg stelt. Doordat de infodesk wel kijkt naar de bewaartermijnen bij het verstrekken van informatie en de CIE hier ook rekening mee houdt bij het opstellen van een proces verbaal, wordt geprobeerd het risico van onrechtmatig gebruik beperkt te houden.

CIE en RID

[REDACTED] III

Kantooromgeving

Controle op de bewaartermijnen van gegevens in de kantoorautomatisering is nog onvoldoende en vernietiging vindt hier niet plaats. Informatie ten behoeve van de dagelijkse politiepraktijk wordt opgeslagen in de mappen op de O-schijf. Dit betreffen bijvoorbeeld aantekeningen van blauw op straat en mediabestanden die medewerkers niet in BVH kunnen opslaan. De mappenstructuur is zondanig ingedeeld dat met jaargangen wordt gewerkt, waardoor toezicht op schoning mogelijk is. In opzet is een procedure geregeld om overzicht te houden op wat in de kantoorautomatisering staat. In bestaan kan het voorkomen dat operationele zaken nog op de J-schijf staan, de schijf voor bedrijfsvoering.

Uit de interviews komt naar voren dat verschillende afdelingen en ook het veiligheidshuis de gegevens in de gezamenlijke mappenstructuur niet schonen. Een uitzondering hierop vormt de infodesk. Het Hoofd infodesk ziet toe op

schoning van deze mappen. Dit kan in het korps als een best practice op dit gebied worden aangemerkt.

De outlook-mailboxen vereisen hier bijzondere aandacht. Verzonden mails met bijvoorbeeld verstrekkingen worden niet geschoond. Uit de gesprekken is naar voren gekomen dat de kennis van de bewaartermijnen en vernietiging niet bij iedereen aanwezig is.

4.7.3

Verbeterpunten

- Landelijk: Zorg dat informatie, ouder dan één jaar na de eerste verwerking, in BVH niet meer te raadplegen is door een onbevoegde politiefunctionaris.
- Landelijk: geef prioriteit aan het inrichten van beheersmaatregelen voor verwijdering en vernietiging in de systemen BVH en BVO.
- Landelijk: afstemmen van bewaartermijnen en vernietigingstermijnen volgens de Wpg met de termijnen volgens het strafrecht.
- Beperk vastleggingen van politiegegevens in de kantoorautomatisering en zie toe op de uitvoering van vastlegging conform interne afspraken.
- Verrijk de procesbeschrijving voor omgang met bewaartermijn en vernietiging van politiegegevens. Denk hierbij ook aan de informatie in de mailboxen en in de kantoorautomatisering. Maak ook duidelijk wie voor welke handeling verantwoordelijk is en zie toe op de uitvoering van schoningen.

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

In de vorige paragraaf is aangegeven dat het voldoen aan de bewaartermijnen van de WPG problemen oplevert. Het gevolg is dat informatie onterecht ter beschikking wordt gesteld aan onbevoegde medewerkers. Daarnaast wijken politiemedewerkers uit naar de mappenstructuur in de KA-omgeving. Deze werkwijze vormt een risico voor het delen van politiegegevens, omdat het zoeken naar informatie lastiger is.

De CIE en de RID zijn beide strikt in het vastleggen van het ter beschikking stellen van politiegegevens. Bij de CIE is een extra waarborg dat de CIE OvJ toezicht houdt.

De gegevens vastgelegd door de meldkamer in GMS worden geautomatiseerd ter beschikking gesteld in BVH. De meldkamermedewerkers voorzien collega's op straat ter ondersteuning ook rechtstreeks van informatie. Als de informatieverzoeker meer informatie wil hebben dan de meldkamermedewerkers kan inzien, wordt diegene doorverwezen naar de infodesk. Voor het ter beschikking stellen van telefoongesprekken is een aanvraagformulier en procedure opgesteld.

Middels autorisatie kunnen onderzoeken afgeschermd worden. Afspraken over codering van onderzoeken is vastgelegd in de procedure beschrijving voor opsporing. De privacyfunctionaris heeft een overzicht van de lopende artikel 9 onderzoeken.

De infodesk vervult een belangrijke rol binnen de politie als het gaat om het verstrekken van politiegegevens. Alle informatieverzoeken en verstrekking worden in BVO vastgelegd in een aparte infodeskregistratie die in BVO zit. De infodesk is opgesplitst in een Frontoffice en Backoffice met elk gespecialiseerde medewerkers. Bij de infodesk zijn nog niet alle procesbeschrijvingen uitgewerkt. Bij de infodesk wordt geprobeerd om de bewustwording van de WPG bij medewerkers te vergroten door WPG-onderwerpen bespreekbaar te maken tijdens de maandelijkse afdelingsoverleggen en jaarlijkse functioneringsgesprekken. Deze werkwijze is ook conform de afspraken van het korps en is ook als onderwerp opgenomen in de checklist.

4.8.3

Verbeterpunten

- Laat andere afdelingen het voorbeeld van de infodesk volgen op het gebied van bewustwording.
- Heb aandacht voor in de kantoorautomatiseringsomgeving vastgelegde gegevens bij het ter beschikking stellen van politiegegevens.

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

Verstrekkingen verlopen bij Brabant-Noord op meerdere manieren via de infodesk, DIK en de meldkamer. De infodesk verstrekt alleen informatie via een beveiligde emailverbinding of per aangetekende post. Infodeskmedewerkers maken gebruik van een verstrekkingwijzer. Hierin staat duidelijk aangegeven en gecategoriseerd welke informatie aan wie verstrekt mag worden. Alle informatieverzoeken en verstrekkingen worden vastgelegd in BVO. Ook de structurele verstrekkingen aan instanties artikel 18 verlopen via de infodesk en worden vastgelegd.

De meldkamer kan alleen informatie verstrekken die medewerkers kunnen opzoeken in de systemen die ze kunnen raadplegen. De meldkamer heeft een matrix opgesteld waarin staat welke informatieverzoeken van welke spelers binnen kunnen komen. De matrix heeft nog geen landelijke goedkeuring omdat er nog discussie is of de matrix WPG-proof is. Alle informatieverzoeken en verstrekkingen worden in GMS vastgelegd.

Ook blauw op straat verstrekt informatie aan derden. Daarbij moet een agent zelf de inschatting maken welke informatie verstrekt kan worden. Uit de interviews komt naar voren dat politiefunctionarissen te weinig gestuurd worden op het verstrekken van informatie.

Verder zijn er verschillende overlegvormen waar informatie verstrekt wordt. Brabant-Noord heeft er voor gekozen om een koepelbesluit op te stellen, omdat zij het niet werkbaar vinden om voor alle overlegvormen een apart besluit op te stellen.

Voor het protocolleren van verstrekkingen wordt nauwelijks gebruik gemaakt het I90 formulier. Wel wordt in het systeem de aanduiding maatschappelijke klasse I90 vastgelegd. Verstrekkingen worden op andere manieren geprotocolleerd, door bijvoorbeeld mutaties, verslagen en brieven om het voor de medewerkers werkbaar te houden. Het korps voldoet aan de protocolplicht door gebruik te maken van andere formulieren die in de systemen gemaakt en opgeslagen worden. Sommige functionarissen zijn niet voldoende bekend met de protocolplicht.

Het veiligheidshuis maakt bij elke verstrekking niet gebruik van de I90 formulieren om dubbele lasten te voorkomen. Het veiligheidshuis legt verstrekte informatie vast in notulen in de mappenstructuur op de O-schijf. In de notulen staan unieke codes van de behandelde personen en op deze wijze is na te gaan aan wie wanneer welke informatie verstrekt is.

4.9.3

Verbeterpunten

- Zorg dat de organisatie goed bekend is met de protocolplicht bij verstrekkingen en hoe dit moet worden vastgelegd.
- 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 (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

Per oktober 2011 zal de Backoffice van de infodesk verzoeken van betrokkenen afhandelen, omdat zij in meerdere systemen kan kijken. De medewerkers van de Backoffice hebben hier een opleiding voor gehad en weten bij twijfel de privacyfunctionaris te vinden. Het korps heeft een procesbeschrijving opgesteld voor het afhandelen van rechten betrokkenen. Hierin is ook opgenomen dat na het wijzigen of verwijderen van gegevens de personen of instanties, die de betreffende informatie hebben ontvangen, hiervan op de hoogte gesteld worden.

Het is nog niet mogelijk om een lijst uit te draaien met verstrekkingen. Als een betrokkene inzage wil, is het wel mogelijk om in het systeem na te gaan welke informatie aan wie verstrekt is. Uit de interne audit blijkt dat het korps voldoet aan de wettelijke termijnen.

4.10.3

Verbeterpunten

- Zorg dat de organisatie goed bekend is met de nieuwe werkwijze omgang rechten betrokkene.

4.11 Protocolplicht (artikel 32)

4.11.1

Norm

De verantwoordelijke draagt zorg voor de schriftelijke vastlegging van:

- de doelen van artikel 9 onderzoeken;

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

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

4.11.2 *Bevindingen*

Bij het verstrekken van politiegegevens wordt niet altijd gebruik gemaakt van de I90-formulieren, maar wel van de I90 aanduiding in het systeem. De verstrekkingen worden op verschillende wijze geprotocolleerd zoals eerder aangegeven. Het is nog niet voor alle medewerkers duidelijk wanneer en hoe geprotocolleerd moet worden bij verstrekkingen. De meldkamer en infodesk leggen in GMS of BVO vast welke informatie aan wie ter beschikking gesteld of verstrekt is.

Doordat de loggingserver landelijk is gesaneerd, kan er geen toezicht worden uitgevoerd op naleving van de Wpg op dit punt. Bij eventuele gevoelige zaken bestaat wel de mogelijkheid om loggingdata bij het vtsPN op te vragen.

De privacyfunctionaris heeft een overzicht van de artikel 9 onderzoeken. Een overzicht van de artikel 13 gegevensverzamelingen, hernieuwde verwerkingen, geautomatiseerde vergelijkingen en in combinatie met elkaar verwerkingen wordt niet bijgehouden door de privacyfunctionaris. Wel zijn vele van deze verwerkingen vastgelegd in de betreffende registratie.

De gegevens die geprotocolleerd worden, worden in ieder geval bewaard tot de datum waarop de externe audit is afgerond.

4.11.3 *Verbeterpunten*

- Zorg dat de organisatie goed bekend is met de protocolplicht en hoe hier uitvoering aan gegeven kan worden. Dit geldt met name voor verstrekkingen.
- Activeer de loggingserver zodat de toezichttaak Wpg uitgevoerd kan worden.

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*

De interne audit is in 2011 in de periode van april 2011 tot augustus 2011 uitgevoerd bij Brabant-Noord. De interne auditor heeft gebruik gemaakt van de handreiking normering wet politiegegevens. De auditors hebben de vragen van de handreiking omgebouwd tot praktische vragen die aansluiten op de praktijk van de geïnterviewde politiemedewerkers. De interne auditors hebben een kritisch rapport opgesteld dat inzicht verschaft in de knelpunten in de uitvoering van de Wpg.

Een belangrijk punt in de uitvoering van de audit is dat de auditor drie rollen op zich heeft genomen tijdens de implementatie van de Wpg. De interne auditor was betrokken bij het opstellen van de opzet implementatie Wpg en heeft taken van de privacyfunctionaris op zich genomen. Hierdoor kunnen vraagtekens gezet worden bij de objectiviteit van de interne auditor. Wel willen we benadrukken dat de toewijding van de interne auditor voor de Wpg, van belangrijke waarde is geweest voor de implementatie van de Wpg binnen het korps.

Om de objectiviteit te borgen is de audit in nauwe samenwerking met de andere interne auditor binnen het korps uitgevoerd, deze auditor is niet aangewezen als interne auditor voor de Wpg. Deze functionaris heeft wel een belangrijk aandeel gehad in het houden van interviews en het opstellen van het rapport. Tijdens de interviews hebben ook drie andere functionarissen meegewerkt. Bij de afname van de interviews was in ieder geval één auditor aanwezig.

De interne auditors vallen onder de afdeling Sturing. Het korps heeft een jaarplanning opgesteld voor de interne audits waarbij alle afdelingen na 4 jaar geaudit moeten zijn. Door de samenvoeging met Brabant Zuid-Oost is de planning nog niet zeker.

4.12.3

Verbeterpunten

- Zorg dat de interne auditor afstand neemt van de taak van privacyfunctionaris om objectiviteit tijdens audits te waarborgen.

4.13 Privacy functionaris (artikel 34)

4.13.1

Norm

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

4.13.2

Bevindingen

Brabant-Noord heeft de heer [REDACTED] benoemt als privacyfunctionaris. De heer [REDACTED] is aangemeld bij het CBP. Wegens persoonlijke omstandigheden heeft de privacyfunctionaris zijn toezichtstaak nog niet goed kunnen uitvoeren. De privacyfunctionaris heeft alleen de reguliere autorisaties gekregen en listrechten. Met de listrechten is het mogelijk om de mappenstructuur in te zien en wie toegang heeft tot deze mappen, maar welke documenten in de mappen staan is niet zichtbaar. Indien hij voor toezicht of controle toegang nodig heeft tot informatie buiten zijn autorisatie, dan vraagt hij een medewerker met de juiste autorisatie om mee te kijken in het systeem. Indien deze werkwijze problemen oplevert, dan wordt de privacyfunctionaris als nog de geautoriseerd.

I

De privacyfunctionaris voert onder andere de volgende taken uit:

- toetsen van autorisaties voor externen op noodzaak en rechtmatigheid. Functioneel beheer ondersteunen bij afwijkende autorisatieaanvragen. Functioneel beheer houdt een lijst bij van autorisaties en de privacyfunctionaris kan deze opvragen. Deze lijst wordt door de privacyfunctionaris geaccordeerd.
- bijhouden van een overzicht van de meldingen en sluitingen van onderzoeken ex artikel 9. Deze informatie komt van functioneel beheer.
- uitvoeren van toezichtstaak en terugkoppelen van incidenten.
- beantwoorden van Wpg gerelateerde vragen en geven van advies.

- een privacyjaarverslag opstellen.

Een overzicht bijhouden van de gegevens krachtens artikel 13 met betrekking tot de ondersteunende taken wordt nog niet gedaan. De privacyfunctionaris geeft aan dat dit ook een lastige taak is omdat veel artikel 13 verwerkingen landelijk geregeld zijn.

Voor het jaarverslag ontvangt de privacyfunctionaris jaarlijks van de Lijnchefs een overzicht van onrechtmatige verwerkingen. Als er een vermoeden van opzet is van onrechtmatige verwerkingen, zal Bureau Interne Zaken ingeschakeld worden. Alleen als er aanleiding toe is zal de logging bekeken worden door de vtsPN of het betreffende korps, omdat dit een intensieve klus is.

De privacyfunctionaris geeft aan dat elk korps een privacyfunctionaris heeft en dat deze functionarissen de Wpg verschillend interpreteren binnen het korps. Het risico bestaat dat landelijk niet uniform wordt gewerkt. Een landelijke strakkere sturing op de functie van privacyfunctionaris is wenselijk.

4.13.3

Verbeterpunten

- Borg de toezichthoudende taak van de privacyfunctionaris, zoals in de Wpg benoemd.
- Landelijk: draag zorg voor een uniforme benadering van de functie van de privacyfunctionaris.

4.14 Functionaris Gegevensbescherming

Het korps Brabant-Noord heeft geen functionaris Gegevensbescherming.