



Audit Wpg politie Limburg Noord

Rapport

Datum
Status

6 januari 2012
Definitief

Colofon

Afzendgegevens

Departementale Auditdienst

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

Contactpersonen

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

T 070 370 65 60
M wpg@minvenj.nl

Projectnaam

Audit Wet Politiegegevens

Ons kenmerk

DDS/5719693/11

Auteur

drs. D. van Ilpenhof RE CISA

Inhoud

Colofon 3

1 Assurance Verklaring 7

2 Samenvatting 9

3 Inleiding 22

- 3.1 Algemeen 22
- 3.2 Aanleiding 22
- 3.3 Doelstelling, aard en scope van de opdracht 22
- 3.4 Afbakening 23
- 3.5 Normenkader 23
- 3.6 Beperkingen voor de privacy audit 24
- 3.7 Onderzoeksmethoden en werkwijze 24
- 3.8 Doelgroep van het rapport 24

4 Bevindingen 25

- 4.1 Inleiding 25
- 4.2 Verantwoordelijke (artikel 1.f) 26
- 4.3 Kwaliteitsaspecten van politiegegevens (artikel 3 en 4) 26
- 4.4 Gevoelige gegevens (artikel 5) 33
- 4.5 Autorisatie (artikel 6) 34
- 4.6 Geautomatiseerd Vergelijken (GV)/In Combinatie Met Elkaar Verwerken (ICMEV)(artikel 11) 36
- 4.7 Bewaartermijnen (artikel 14) 38
- 4.8 Ter beschikking stellen (artikel 15) 43
- 4.9 Verstrekken (artikel 16/24) 47
- 4.10 Rechten van betrokkenen (artikel 25/28) 52
- 4.11 Protocolplicht (artikel 32) 53
- 4.12 Audits (artikel 33) 54
- 4.13 Privacyfunctionaris (artikel 34) 55
- 4.14 Functionaris Gegevensbescherming (artikel 36) 56

1 Assurance Verklaring

In het jaar 2011 heeft de Departementale Auditdienst (DAD) van het ministerie van Veiligheid en Justitie (VenJ) in opdracht van de landelijke stuurgroep implementatie Wpg, waarin de Directeur-Generaal Politie en het Korpsbeheerders Beraad (KBB) zijn vertegenwoordigd, privacy audits op grond van de Wet politiegegevens (Wpg) uitgevoerd naar de verwerkingen die in de Wpg zijn beschreven bij de politiekorpsen. In 2011 is een privacy audit uitgevoerd bij het korps Limburg-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 Limburg-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 Limburg-Noord, naar de stand van ultimo december 2011, in opzet, bestaan en werking niet volledig heeft voldaan aan de vereisten zoals genoemd in de Wpg.

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

Het oordeel heeft betrekking op de zogenaamde verwerkingen genoemd in de Wpg. Het hierbij gehanteerde normenkader omvat de door het korps Limburg-Noord te nemen maatregelen. Ook is gebleken dat het korps Limburg-Noord voor het volledig kunnen voldoen aan de Wpg eisen mede afhankelijk is van besluiten die buiten het korps Limburg-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 Limburg-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 die hercontrole te laten uitvoeren door de interne auditors van het korps Limburg-Noord. Het verbeterrapport en de uitgevoerde hercontrole zullen in de navolgende jaren door de privacyauditor worden beoordeeld.

Den Haag, 6 januari 2012

De Directeur van de Departementale Auditdienst

A handwritten signature in blue ink, consisting of stylized, overlapping loops and strokes, positioned above a horizontal line.

J.C. van Praat RE RA

2 Samenvatting

Het korps Limburg-Noord heeft een aantal zaken in opzet opgepakt, zoals het onder de aandacht brengen van de kwaliteitsaspecten zoals genoemd in de Wpg. Daarbij is een koppeling gemaakt van deze kwaliteitsaspecten naar de dagelijkse werkzaamheden van de diverse afdelingen van het korps Limburg-Noord. 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.

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

Criteria:

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

Norm	Aspect		Bevinding en oordeel
Artikel 1.f, Verantwoordelijke			
1.f	Mandaatbesluit		Er is een mandaatbesluit beschikbaar waarin formeel wordt aangeduid dat de korpsbeheerder zijn mandaat heeft verleend aan de korpschef. De korpschef heeft vervolgens middels een ondermandaat enkele bevoegdheden overgedragen aan anderen binnen het korps. Hiermee wordt voldaan aan de Wpg.
Artikel 3 en 4, Kwaliteitsaspecten van politiegegevens			
8.1 en 9.1	Onderscheid onderzoek Dagelijkse Politietaken (8) versus Bepaald geval (9)		De leidinggevenden, infodeskmedewerkers en de interne auditor en privacyfunctionaris hebben opleidingen over de Wpg gevolgd. Conform het <i>teach-the-teacher-principe</i> is het 'Blauw' verder geïnformeerd over de wet. Op het intranet is een e-learning cursus beschikbaar voor het 'Blauw'. Aan de hand van een organisatiematrix is per functie bepaald welke cursus aan de doelgroep werd aangeboden. Hiermee wordt voldaan aan de Wpg.
3.1 t/m 3.3 (8) 4.1 (8)	Noodzakelijkheid (8) Doelbinding Rechtmatigheid Juistheid Volledigheid		De inhoudelijke kwaliteitscontrole wordt door gegevensbeheer verricht. De juistheid van politiegegevens wordt met behulp van TrueBlue door middel van diverse deelcontroles getoetst. Op elke eenheid is een dagcoördinator aangewezen. Deze persoon controleert de invoeringen in de

Norm	Aspect		Bevinding en oordeel
			systemen waaronder BVH. Bij Bureau Regionale Informatie (BRI) verrichten de medewerkers van gegevensinvoer de correctiewerkzaamheden. Op intranet is een formulier "Aanmelding BVO registratie en WPG VERWERKING" beschikbaar gesteld voor verwerkingen van artikel 8 tot en met 13 Wpg, inclusief een korte uitleg van deze artikelen. Er is onvoldoende aandacht voor gegevensbeheer en voor kwaliteit van gegevens vanwege ontoereikende capaciteit. Dit hangt samen met het wegbezuinigen van driekwart van de afdeling gegevensbeheer. Er vindt geen toetsing wat betreft de noodzakelijkheid van politiegegevens plaats. Hiermee wordt deels voldaan aan de Wpg.
3.1 t/m 3.4 (9) 4.1 (9)	Noodzakelijkheid (9) Doelbinding Rechtmatigheid Herkomst en wijze van verkrijging Juistheid Nauwkeurig Volledigheid		Het rechercheproces bevat waarborgen voor de kwaliteitsaspecten van politiegegevens. De PDCA-cyclus sluit via het OM en de rechter. De rechercheurs zijn zich bewust van het begrip doelbinding. De juistheid en volledigheid van artikel 9 gegevens worden door de operationeel chef van Limburg-Noord en het Openbaar Ministerie (OM) gecontroleerd. De onderzoeksleiding corrigeert op gegevensinvoer en gegevensverzameling. 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		CIE: De CIE handelt conform het landelijke CIE proceshandboek en wordt gecontroleerd door de CIE OvJ. De runners controleren hun eigen informatie. De informatiebeheerder van de CIE controleert de doelbinding van de CIE-gegevens. RID: Bij de RID liggen de kwaliteitscriteria al in het doel van de taak vast. De kwaliteit van de aangeleverde informatie wordt door de RID getoetst. Hiermee wordt voldaan aan de Wpg.
4.3	Beveiliging		BVH, BVO en de mappenstructuur worden beveiligd door middel van autorisaties. Openbare orde- en AIVD-informatie zijn bovendien strikt gescheiden opgeslagen. Wegens tekortkomingen van de software van de systemen BVH en BVO wordt geen onderscheid gemaakt tussen artikel 8 en 9 Wpg-informatie. BVH bevat zowel artikel 8- als artikel 9-informatie. Een aantal systemen, waaronder BVH, voldoet niet aan de in de Wpg gestelde bewaartermijnen. Hierdoor

Norm	Aspect		Bevinding en oordeel
			ontstaat het risico op onrechtmatig gebruik van politiegegevens. Politiegegevens, die niet in BVH en BVO kunnen worden geplaatst, worden opgeslagen binnen de kantoorautomatisering-omgeving. In de mappenstructuur is een scheiding aangebracht tussen de verschillende artikelen. Er is geen standaardproces ingericht voor tijdige schoning van informatie in deze mappenstructuur. Uit de audit is niet gebleken dat het korps Limburg-Noord beleid heeft opgesteld ten aanzien van de kantoorautomatisering, betreffende: • de relaties naar onderzoeken; • gebruiks- en bewaartermijnen en de daaruit voortvloeiende schoningsprocedures. Door het ontbreken van beleid en adequate controle hierop is: • de mappenstructuur divers en niet controleerbaar; • er voor TGO en Zwacri-onderzoeken onzekerheid ten aanzien van de afscherming omdat per district de rechercheurs in elkaars map mogen kijken. De afdelingen RID en CIE zijn fysiek alleen toegankelijk voor medewerkers van deze afdeling. Hiermee wordt niet voldaan aan de Wpg.
Artikel 5, gevoelige gegevens			
	• Gevoelige gegevens		Het team met Zwacri-onderzoeken legt gevoelige gegevens vast indien dat noodzakelijk is. Deze informatie is beperkt toegankelijk. Er zijn geen niet-toegestane gegevensverzamelingen gebaseerd op gevoelige gegevens aangetroffen. Hiermee wordt voldaan aan de Wpg.
Artikel 6, Autorisatie			
	• Korpsautorisatiematrix		De autorisatiematrix was tijdens de audit niet beschikbaar. De standaardprofielen voor een functie ontbreken. Hiermee wordt niet aantoonbaar voldaan aan de vereisten van evenredigheid en zorgvuldigheid en daarmee niet voldaan aan de Wpg.
	• Aanvraagproces		De lijnchefs zijn bevoegd voor het indienen van autorisatieverzoeken. Bij de afwezigheid van een lijnchef, kan een districtschef of divisiechef een verzoek indienen.

Norm	Aspect	Bevinding en oordeel
		De autorisatieverzoeken worden volgens een beschreven procedure ingediend middels de functionele mailbox van vtsPN en vervolgens geregistreerd in de applicatie Expertdesk. Er is een procedure voor tijdelijke (student)autorisaties en autorisatiemutaties als gevolg van schorsingen en wijzigingen. De aanvraagprocessen zijn tevens vastgelegd in process flows. Hiermee wordt voldaan aan de Wpg.
	• Wijziging en verwijdering	De autorisatiematrix is niet inzichtelijk voor het korps. Hierdoor kunnen de verantwoordelijken de zorgvuldigheid en evenredigheid van de verleende autorisaties niet toetsen. Hiermee wordt niet voldaan aan de Wpg.
	• Autorisatiebeheer CIE en RID	De chef CIE en RID zijn bevoegd om personen te autoriseren. De functioneel beheerder voert deze mutaties uit conform het landelijk autorisatiemodel. Binnen de Zwacri-omgeving is het de onderzoeksleider in de rol van bevoegde functionaris die bepaalt wie wordt geautoriseerd. Hiermee wordt voldaan aan de Wpg.
32.1.c	Protocollering autorisaties	De privacyfunctionaris heeft een overzicht van de externe autorisaties en toetst deze halfjaarlijks. Protocolleringen van de autorisatieverzoeken vindt plaats via gebruik van de functionele mailbox van vtsPN en daaropvolgende registratie in de applicatie Expertdesk. Hiermee wordt voldaan aan de Wpg.
32.3 voor 32.1.c	Bewaren protocolgegevens autorisaties	De protocolgegevens vastgelegd door middel van Expertdesk worden bewaard bij O&I en zijn op te vragen door de privacyfunctionaris. Uitgegeven autorisaties worden vastgelegd aan de hand van ingestuurde autorisatieformulieren. Er is geen bewaartermijn vastgesteld, echter, er wordt niets vernietigd. Hiermee wordt voldaan aan de Wpg.
Artikel 11, Geautomatiseerd vergelijken en in combinatie zoeken		
	• Hanteerbare interpretatie	Definities voor geautomatiseerd vergelijken en in combinatie zoeken ontbreken op landelijk en op korpsniveau. Bij gebrek aan een definitie hanteert Limburg-Noord

Norm	Aspect		Bevinding en oordeel
			een gedocumenteerd proces: Een analyse wordt verricht op verzoek van de bevoegde functionaris van de betreffende afdeling of door de Officier van Justitie van het betreffende onderzoek. Het geautomatiseerd vergelijken of het in combinatie zoeken van enkel politiegegevens mag slechts plaatsvinden na verkregen toestemming van het bevoegde gezag. Hiermee wordt deels voldaan aan de Wpg.
	Aangewezen functionarissen		Het geautomatiseerd vergelijken / in combinatie met elkaar verwerken gebeurt door Bureau Regionale Informatievoorziening (BRI). De informatie coördinatoren en misdaadanalisten van het BRI zijn als functionarissen aangewezen voor deze handelingen. Hiermee wordt voldaan aan de Wpg.
11.4	Bevoegde gezag		Het bevoegde gezag bij de Regionale Inlichtingen Dienst is belegd bij de verschillende burgemeesters binnen de regio. Voor artikel 11.4 zoekacties dient toestemming te worden gevraagd aan het bevoegde gezag. Het bevoegde gezag bij de CIE is belegd bij de CIE Officier van Justitie. Hiermee wordt voldaan aan de Wpg.
32.1.d en 32.1.h	Protocollering 11.1, 11.2, 11.4 en 11.5		Artikel 11 Wpg zoekacties worden bij het korps Limburg-Noord niet of nauwelijks geprotocolleerd. In een enkel geval blijkt de toestemming van het bevoegde gezag te zijn geregistreerd in het zaaksjournaal. De zoekacties op grond van artikel 11.5 Wpg worden tevens niet vastgelegd, blijkende uit het jaarverslag van de privacyfunctionaris. Hiermee wordt niet voldaan aan de Wpg.
32.3 voor 32.1.d en 32.1.h	Bewaren protocolgegevens 11.1, 11.2, 11.4 en 11.5		Artikel 11 Wpg zoekacties worden bij het korps Limburg-Noord niet of nauwelijks geprotocolleerd. In een enkel geval blijkt de toestemming van het bevoegde gezag te zijn geregistreerd in het zaaksjournaal. De zoekacties op grond van artikel 11.5 Wpg worden tevens niet vastgelegd, blijkende uit het jaarverslag van de privacyfunctionaris. Hiermee wordt niet voldaan aan de Wpg.
Artikel 14, Bewaartermijnen			
8.2 en 8.3	(8) van 1 tot 5 jaar		Er is in de nieuwe release van BVH een schoningsmodule gebouwd. Het korps is in verzorgingsgebied Zuid-6-verband geadviseerd de nieuwe functionaliteiten in BVH niet te activeren. De korpsbeheerder en korpsleiding hebben zich aan het

Norm	Aspect		Bevinding en oordeel
			landelijke standpunt geconformeerd. Hiermee wordt niet voldaan aan de Wpg mede op basis van het landelijk advies..
8.6	(8) verwijderen na 5 jaar		In de nieuwe release van BVH (versie 1.2.2) is een schoningsmodule aanwezig, maar deze is op landelijk verzoek van de voorzitter van de stuurgroep nog niet geactiveerd. Binnen Zuid-6-verband is besloten deze gegevens niet te schonen. Hiermee wordt niet voldaan aan de Wpg.
14.1 (8)	(8) vernietigen na 5 jaar verwijderd		Er vindt nog geen vernietiging van informatie uit BVH plaats. Binnen Zuid-6-verband is besloten deze gegevens niet te schonen. Hiermee wordt niet voldaan aan de Wpg.
9.4	(9) verwijderen na OH plus ½ jaar		Het korps Limburg-Noord wordt niet structureel op de hoogte gehouden door het OM wanneer binnen een zaak het laatste rechtsmiddel is afgedaan. Hierdoor loopt men het risico dat het OH-moment niet (tijdig) kan worden bepaald. Het korps heeft geen procedurele maatregelen genomen om dit te ondervangen. Hiermee wordt niet voldaan aan de Wpg.
14.1 (9)	(9) vernietigen na 5 jaar verwijderd		Ook deze termijn is afhankelijk van het OH-moment. Zoals geconstateerd loopt het korps het risico dat het OH-moment niet kan worden bepaald. Hierdoor kan men niet garant staan dat artikel 9 gegevens vijf jaar na verwijdering worden vernietigd. Hiermee wordt niet voldaan aan de Wpg.
10.6	(10) verwijderen na 5 jaar geen subjectwaardige registratie		Voor het verwijderen en vernietigen van artikel 10 Wpg-informatie volgt de CIE de procedure uit het landelijke CIE-proceshandboek. Deze procedure voldoet aan de gestelde vereisten uit de Wpg. Hiermee wordt voldaan aan de Wpg.
14.1 (10)	(10) vernietigen na 5 jaar verwijderd		Voor het verwijderen en vernietigen van artikel 10 Wpg-informatie volgt de CIE de procedure uit het landelijke CIE-proceshandboek. Deze procedure voldoet aan de gestelde vereisten uit de Wpg. Hiermee wordt voldaan aan de Wpg.
14.3	Hernieuwde verwerking		Een procedure is opgesteld met betrekking tot artikel 14.3 Wpg-verwerkingen. Toestemming dient te worden gevraagd aan het bevoegde gezag. Wanneer het BRI (de Infodesk) een aanvraag krijgt en constateert dat informatie uit de zoekresultaten reeds is verwijderd conform de Wpg, dan dient BRI de bevoegde functionaris te raadplegen. Bij

Norm	Aspect		Bevinding en oordeel
			geschoonde informatie wordt tevens toestemming aan de betreffende Officier van Justitie gevraagd. Tevens moet conform het CIE-handboek het bevoegde gezag opdracht geven voor de hernieuwde verwerking. Hiermee wordt voldaan aan de Wpg.
32.1.e	Protocollering 14.3		Hernieuwde verwerking wordt geregistreerd in de BVO-infodeskmodule. De privacyfunctionaris verricht één keer per half jaar een steekproef om vast te stellen of er sprake is van rechtmatige hernieuwde verwerkingen. Hiermee wordt voldaan aan de Wpg.
32.3 voor 32.1.e	Bewaren protocolgegevens 14.3		Hernieuwde verwerking wordt geregistreerd in de BVO-infodeskmodule. De privacyfunctionaris verricht één keer per half jaar een steekproef om vast te stellen of er sprake is van rechtmatige hernieuwde verwerkingen. De protocollering kan men terugvinden in de BVO-infodeskmodule en wordt daarmee vastgelegd. Hiermee wordt voldaan aan de Wpg.
12.2	(12) verwerken tot 4 maanden		Artikel 12 Wpg Informatie wordt wekelijks overgeheveld naar andere verwerkingen (artikel 8, 9 of 10 Wpg) door de informatiebeheerders. Hiermee wordt voldaan aan de Wpg.
12.6	(12) controleren en vernietigen		De CIE-Officier van Justitie voert elk half jaar samen met een parketsecretaris een controle uit op de informanten, de Zwacri-subjecten en vertaling van bruto- naar netto-informatie. Indien nodig wordt geschoond. Het OM heeft daartoe toegang tot zowel de inhoud van BVO-bruto als BVO-netto. Het korps heeft echter niet geborgd dat gegevens daadwerkelijk na maximaal 10 jaar worden vernietigd. Hiermee wordt deels voldaan aan de Wpg.
Artikel 15, Ter beschikking stellen			
	• Infodesk voor bevraging		Er is een Infodesk aangewezen als centraal punt waar informatieverzoeken kunnen worden ingediend. Voor de Infodesk is een werkinstructie opgesteld hoe te handelen bij de behandeling van Informatieverzoeken, en op welke kwaliteitsaspecten deze verzoeken getoetst behoren te worden.

Norm	Aspect	Bevinding en oordeel
		In de praktijk blijkt dat er geen structurele controle plaatsvindt op de functie van de vraagsteller. Men controleert alleen of de vraagsteller binnen de regio werkzaam is. Daarmee bestaat het risico dat de aanvrager informatie verkrijgt waarover die uit hoofde van de uitvoering van zijn of haar taak niet mag beschikken. Hiermee wordt niet geheel voldaan aan de Wpg.
	• Codering	De bruto-informatie (gecodeerd als 00-informatie) wordt gescheiden opgeslagen van netto informatie (gecodeerd als 01-informatie). Hiermee wordt voldaan aan de Wpg.
	• Aanwijzing Bevoegd Functionaris	In het aanwijzingsbesluit zijn functies aangewezen die als bevoegde functionaris binnen het korps gaan fungeren. Wanneer men een dergelijke functie gaat vervullen vervult men automatisch de rol van bevoegde functionaris. Hiermee wordt voldaan aan de Wpg.
	• Opleiding Bevoegd Functionaris	Er zijn verschillende trainingen gegeven aan de leidinggevendenden van de opsporingseenheden in het kader van de Wpg. Eén van de trainingen betreft de tweedaagse opleiding tot bevoegde functionaris. Hiermee wordt voldaan aan de Wpg.
15.2	Weigeringgronden	De bevoegde functionarissen zijn op de hoogte van de wettelijke weigeringgronden in relatie tot de verplichting van het ter beschikking stellen. Dit is opgenomen in de opleiding voor bevoegde functionarissen. Hiermee wordt voldaan aan de Wpg.
Artikel 16 t/m 24, Verstrekking		
	• Verstrekkingenwijzer (landelijk)	Limburg-Noord maakt gebruik van de landelijke verstrekkingwijzer en heeft deze beschikbaar gesteld aan de medewerkers. Limburg-Noord heeft tevens deze verstrekkingenwijzer geactualiseerd aan de hand van de nu van toepassing zijnde regelgeving. Hiermee wordt voldaan aan de Wpg.
	• Proces voor convenanten	Er is een implementatieproject opgezet om de convenanten Wpg-geschied te maken. De privacyfunctionaris houdt een overzicht van 'nog af te sluiten' convenanten bij. Op Intranet is voor alle medewerkers een overzicht beschikbaar van alle convenanten die binnen regio Limburg-Noord zijn vastgesteld. In totaal zijn er achttien artikel 20 Wpg samenwerkingsverbanden

Norm	Aspect	Bevinding en oordeel
		geïdentificeerd. De convenanten dienen getekend te zijn door de Korpsbeheerder, de Hoofdofficier van Justitie en de betreffende Burgemeester. De partners in het netwerkoeverleg zijn gehouden aan een geheimhouding en zijn daar ook over geïnformeerd. Alvorens de besluiten definitief worden gemaakt, worden deze eerst bij de juridische afdeling ter goedkeuring gelegd. Een overzicht van alle convenanten is bij de privacyfunctionaris beschikbaar. Hiermee wordt voldaan aan de Wpg.
• Proces voor Artikel 20 Besluiten		Er is een implementatieproject opgezet om de convenanten Wpg-geschikt te maken. De privacyfunctionaris houdt een overzicht van 'nog af te sluiten' convenanten bij. Op intranet is voor alle medewerkers een overzicht beschikbaar van alle convenanten die binnen regio Limburg-Noord zijn vastgesteld. In totaal zijn er achttien artikel 20 Wpg samenwerkingsverbanden geïdentificeerd. De convenanten dienen getekend te zijn door de Korpsbeheerder, de Hoofdofficier van Justitie en de betreffende Burgemeester. De partners in het netwerkoeverleg zijn gehouden aan een geheimhouding en zijn daar ook over geïnformeerd. Alvorens de besluiten definitief worden gemaakt, worden deze eerst bij de juridische afdeling ter goedkeuring gelegd. Een overzicht van alle convenanten is bij de privacyfunctionaris beschikbaar. Hiermee wordt voldaan aan de Wpg.
• Verstrekkingenschema (regio)		De vaste partners in het veiligheidshuis zijn de Politie, het Openbaar Ministerie, procesmanagers, bureau jeugdzorg, reclassering en verslavingszorg (justitiële partners). Elke morgen vindt een briefing plaats met de vaste partners en worden de incidenten per regio per dag besproken. De briefings worden vastgelegd op een aparte schijf bij de politie. In de briefing wordt ook bepaald wie wordt gevolgd. Hiermee wordt voldaan aan de Wpg.
• Proces voor geautomatiseerde verstrekking		Er vinden geen geautomatiseerde verstrekkingen plaats.

Norm	Aspect		Bevinding en oordeel
7.2	Geheimhouding		Bij verstrekkingen wordt er gewezen op de daarbij behorende geheimhoudingsplicht. De artikel 20-besluiten bevatten een verwijzing naar artikel 7.2 Wpg waarmee op de geheimhoudingsplicht wordt gewezen. Hiermee wordt voldaan aan de Wpg.
32.1.f	Protocollering verstrekking		Er is een procesbeschrijving beschikbaar met betrekking tot het protocolleren van verstrekkingen in een I90-formulier, daarbij is toestemming van het bevoegde gezag vereist. Bij de CIE worden verstrekkingen vastgelegd in een procesverbaal. Echter, binnen de andere afdelingen van Limburg-Noord is geen sprake van een structurele vastlegging van verstrekkingen. In de praktijk blijkt namelijk dat het I90-formulier niet door iedereen structureel wordt gebruikt. Vaak maakt men hiervan een losse vermelding in een BVO-mutatie. Hierbij kan het totaal van verstrekkingen niet inzichtelijk worden gemaakt en is daarmee niet controleerbaar. Hiermee wordt niet voldaan aan de Wpg.
32.3 voor 32.1.f	Bewaren protocolgegevens verstrekking		In opzet is de protocollering van de verstrekking door middel van I90-formulieren goed geregeld. Een procesuitleg is beschikbaar. Echter, in de praktijk blijkt dat het I90-formulier niet door iedereen structureel wordt gebruikt. Vaak maakt men hiervan een losse vermelding in een BVO-mutatie. Doordat niet altijd gebruik wordt gemaakt van een I90-formulier kan het overzicht niet als compleet worden beschouwd. Daarmee kan de privacyfunctionaris zijn controlerende taak niet geheel effectief uitvoeren. Hiermee wordt deels voldaan aan de Wpg.
• Toezicht door leidinggevenden op verstrekkingen en protocollering			De privacyfunctionaris voert kwalitatieve steekproeven uit op de geregistreerde verstrekkingen. Tevens monitort de privacyfunctionaris de kwantiteit van de ingevulde verstrekkingen. Hiermee wordt voldaan aan de Wpg.

Norm	Aspect		Bevinding en oordeel
Artikel 25 t/m 31, Rechten van de betrokkene			
25.1	Verzoek om kennisneming		De verzoeken worden centraal geadministreerd en ter afwerking uitgezet naar de territoriale afdelingen. Bij twijfel kan de privacyfunctionaris of de jurist worden geraadpleegd. Hiermee wordt voldaan aan de Wpg.
28.1 t/m 28.3	Correctie		Er zijn twee klachten ingediend, deze zijn door de privacyfunctionaris afgehandeld. Hiermee wordt voldaan aan de Wpg.
Artikel 32, Protocolplicht (32.1.c, d, e, f en h behandeld bij thema's)			
9.2 en 32.1.a	Protocollering doel onderzoek		Het doel van onderzoeken worden vastgelegd middels MRO. De privacyfunctionaris houdt een overzicht bij van de BVO-registraties, inclusief het doel van het onderzoek en de naam van de teamleider van dit onderzoek. De privacyfunctionaris voert hierop een halfjaarlijkse steekproef uit. Uit het onderzoek van de privacyfunctionaris blijkt dat MRO's van het doel van het onderzoek niet structureel plaatsvindt. Hiermee wordt niet voldaan aan de Wpg.
32.3 voor 32.1.a	Bewaren protocolgegevens doel onderzoek		Wanneer de MRO's wel zijn ingediend worden de doelen van de onderzoeken vastgelegd. Deze worden gesorteerd op jaartal bij de privacyfunctionaris en bij de functioneel beheerder van BVO opgeslagen. Hiermee wordt voldaan aan de Wpg.
13.4 en 32.1.b	Protocollering Artikel 13 gegevensverzameling en		De artikel 13-gegevensverzamelingen zijn geïdentificeerd. Korps Limburg-Noord geeft aan geen gebruik te maken van regionale artikel 13-gegevensverzamelingen buiten de landelijke systemen. Protocollering van landelijke artikel 13 gegevensverzamelingen wordt middels landelijk beschikbaar gestelde standaardformulieren verricht. Hiermee wordt voldaan aan de Wpg.
32.3 voor 32.1.b	Bewaren protocolgegevens Artikel 13 gegevensverzameling en		De artikel 13-gegevensverzamelingen zijn geïdentificeerd. Korps Limburg-Noord geeft aan geen gebruik te maken van regionale artikel 13-gegevensverzamelingen buiten de landelijke systemen. Protocollering van landelijke artikel 13 gegevensverzamelingen wordt middels landelijk beschikbaar gestelde standaardformulieren verricht.

Norm	Aspect		Bevinding en oordeel
			en als zodanig bewaard. Hiermee wordt voldaan aan de Wpg.
32.1.g	Protocollering onrechtmatige handeling		Incidenten worden gemeld door de taakaccenthouders privacy en informatiebeveiliging. De privacyfunctionaris doet zelf ook onderzoek door middel van steekproeven. De onrechtmatige handelingen worden in een overzicht bewaard door de privacyfunctionaris. Hiermee wordt voldaan aan de Wpg.
32.3 voor 32.1.g	Bewaren protocolgegevens onrechtmatige handeling		De onrechtmatige handelingen worden in een overzicht bewaard door de privacyfunctionaris. Hiermee wordt voldaan aan de Wpg.
32.2	Gemeenschappelijke verwerking		Niet van toepassing. Er zijn geen gemeenschappelijke verwerkingen waarin het korps participeert.
Artikel 33, Audits			
RPAP 3.1	Interne audit-functie		Er zijn twee Interne auditors aangewezen om de jaarlijkse interne audit naar de Wpg te doen. De interne audit-functie is weliswaar belegd, maar er heeft in 2011 geen volledige interne audit plaatsgevonden. Hiermee wordt niet voldaan aan de Wpg.
RPAP 3.4	Interne audit-plan		Het korps wacht de resultaten van de externe-audit af voor de vorming van het auditplan 2012. Er is geen audit gehouden in 2011 omdat dit deels samenliep met de externe audit. Hiermee wordt niet voldaan aan de Wpg.
RPAP 3.6	Interne audit-rapport		Het korps wacht de resultaten van de externe-audit af voor de vorming van het auditplan 2012. Er is geen audit gehouden in 2011 omdat dit deels samenliep met de externe audit. Hiermee wordt niet voldaan aan de Wpg.
Artikel 34, Privacyfunctionaris			
34.1 en 34.4	Benoemd en gemeld		Er is een privacyfunctionaris aangesteld sinds 1 maart 2010 en is tevens aangemeld bij het CBP. Hiermee wordt voldaan aan de Wpg.
34.2	Overzicht over protocollering		Periodiek voert de privacyfunctionaris controles uit, bijvoorbeeld middels Cognos om overzicht te verschaffen over de protocollering. Vanaf begin af aan wordt er controle uitgeoefend op BVH I90-verstrekking en I42-adviezen. Sinds 2011 tevens controle op E62-bestuurlijke rapportages en E67-rechtshulpverzoeken.

Norm	Aspect		Bevinding en oordeel
			Hiermee wordt voldaan aan de Wpg.
34.3	Jaarverslag		De privacyfunctionaris heeft over 2010 een jaarverslag opgesteld. Het verslag over 2011 is nog in ontwikkeling. Hiermee wordt voldaan aan de Wpg.
Optioneel Artikel 36, Functionaris Gegevensbescherming			
36.1 en 36.2	Benoemd		Niet van toepassing. Er is geen functionaris gegevensbescherming benoemd.
Wbp 63.3	Gemeld		Niet van toepassing.
Wbp 64.1 t/m 64.4	Toezichthoudende rol		Niet van toepassing.

3 Inleiding

3.1 Algemeen

In opdracht van de landelijke stuurgroep Wpg, waarin de Directeur-Generaal Politie en het KBB zijn vertegenwoordigd, heeft de DAD van het ministerie van VenJ een privacy audit uitgevoerd bij het korps Limburg-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 Limburg-Noord in de maanden mei en november tot en met december 2011.

3.2 Aanleiding

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

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

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

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

3.3 Doelstelling, aard en scope van de opdracht

Doelstelling

Deze privacy audit heeft tot doel op systematische wijze te toetsen of aan de bepalingen van de Wpg op adequate wijze uitvoering is gegeven ten aanzien van de in de wet genoemde verwerkingen bij het korps Limburg-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 mei 2011, van maatregelen en procedures, waarmee het korps

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

3.4 Afbakening

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

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

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

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

Wij hebben onze werkzaamheden uitgevoerd in de periode mei 2011 en november tot en met december 2011.

Het eindrapport is met inachtneming van het ontvangen commentaar vastgesteld.

3.8 Doelgroep van het rapport

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

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

De stuurgroep wordt voorgezeten door drs. 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 Drs H.M.F. Bruls.
- De korpschef B. Rookhuijzen.
- De Hoofd Officier van Justitie mr. P.J.D.J Muijen.
- De privacyfunctionaris P.L.M. Streutjens.
- De voorzitter van het College Bescherming Persoonsgegevens.

Het rapport mag uitsluitend met toestemming van de korpsbeheerder dan wel de korpschef van korps Limburg-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*

Uit de praktijk blijkt dat binnen de diverse onderdelen van het korps Limburg-Noord men goed is doordrongen van de kwaliteitscriteria zoals noodzakelijkheid, rechtmatigheid etc.

Algemene aandachtspunten die bij de audit binnen politie Limburg-Noord naar voren zijn gekomen zijn:

- De privacyfunctionaris vormt een vast aanspreekpunt voor de Wpg binnen het korps. De privacyfunctionaris geeft ten aanzien van de Wpg periodiek terugkoppeling aan de korpsleiding. Hiervoor voert de privacyfunctionaris periodiek controles uit binnen diverse onderdelen van het korps.
- Voor de sturing op strategisch niveau heeft de privacyfunctionaris ieder kwartaal overleg met de korpsleiding.
- De sturing op districtsniveau (tactisch niveau) is nog niet optimaal. De Wpg wordt door het 'Blauw' nog beschouwd als een administratieve last en stuit op weerstand. Het wegnemen van beelden over het bureaucratische denken vanuit de leiding heeft veel energie en tijd gekost.
- Men wil wel voldoen aan de wet, maar onder andere de techniek blokkeert soms een efficiënte en effectieve invulling van de Wpg.
- Men geeft aan dat de opleiding van agenten ook tekort schiet in het overbrengen van Wpg-kennis. In de basistraining wordt er een halve dag aan besteed.

De uitrol en borging van de Wpg steunt op mensen zoals de privacyfunctionaris. Deze groep personen is van vitaal belang voor de ondersteuning van de Wpg-uitrol. Bij het wegvallen van deze mensen bestaat het risico dat daarmee tevens de steun voor de Wpg vervalst.

Korps Limburg-Noord heeft door middel van een communicatieplan is veel aandacht aan de implementatie van de Wpg besteed, echter vanwege bezuinigingen binnen het korps is de uitvoering van dit plan deels stil te komen liggen 2010.

4.1.2 *Bekendheid met de Wpg binnen de organisatie*

De Wpg is nog niet expliciet onder de aandacht bij alle onderdelen van politie Limburg-Noord. In de praktijk wordt het delen van informatie binnen het korps goed vormgegeven.

- Ten aanzien van de kennis en toetsing op doelbinding is nog winst te behalen. Men richt zich nu vooral op de privacyaspecten.

- Met name voor de artikel 8 en artikel 9 informatie geldt dat onvoldoende kennis van de gebruiks- en bewaartermijnen van politiegegevens is.
- Door controle (privacy functionaris) op aanvang onderzoek, MRO en restinformatie neemt kennis en van het toepassen van de Wpg toe.
- Bij de nieuwe instroom leidinggevenden wordt geen cursus Wpg aangeboden, waardoor de aandacht voor de sturing op de Wpg niet in continuïteit is geborgd.

4.1.3 *Wpg en de praktijk*

Op het uitvoerend niveau, dus het 'Blauw' op straat, wordt de Wpg als knelpunt ervaren. Met name de administratieve last van de vastleggingen van de verstrekkingen wordt als negatief ervaren en de naleving van de Wpg ondervindt veel weerstand. Dit heeft als gevolg dat men vanuit 'pragmatisch' oogpunt niet structureel conform de Wpg werkt.

De wijze waarop nu moet worden gewerkt met convenanten en vastleggingen wordt als te bureaucratisch ervaren. Het is niet altijd helder wanneer een convenant moeten worden opgesteld, en wanneer informatie mag worden verstrekt aan partners.

Kennis

Een ander aspect is kennis. Kennis over de Wpg kan opgedaan worden via de Intranetsite Noord Limburg. Op deze intranetsite staat bijvoorbeeld informatie over convenanten, tekstvoorbeelden voor het maken van een convenant, inhoudelijke informatie, tips, artikelen over de WPG en zelfs een e-learning training. Alle medewerkers in het korps hebben toegang tot deze intranetsite. Daarnaast zijn er voor wijkagenten en de medewerker Politie Jeugdtaak themadagen georganiseerd. Voorts zijn teamleiders in het opsporingsproces tijdens hun werkoverleg bezocht om in het kader van de Wpg informatie te verstrekken. Om de bewustwording te bevorderen is veelal aan medewerkers de VPRO reportage 'Wat nou privacy' gepresenteerd.

4.2 Verantwoordelijke (artikel 1.f)

Mandaatbesluit

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.

De korpschef heeft vervolgens middels ondermandatering een aantal bevoegdheden binnen het korps Limburg-Noord belegd. De mandatering en ondermandatering zijn ondertekend.

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

Onderscheid artikel 8 en 9 gegevens

De bevoegde functionarissen hebben een apart seminar gevolgd met betrekking tot de Wet politiegegevens. Tevens zijn er presentaties gegeven aan de leidinggevendenden binnen het korps.

Aan nieuw aangewezen bevoegde functionarissen wordt geen extra aandacht meer gegeven met betrekking tot de Wpg, dit omdat de Wpg volgens het korps voldoende wordt behandeld tijdens de opleiding aan de politieacademie.

Middels het *teach-the-teacher*-principe heeft men de kennis omtrent de wet korps breed uitgedragen. Daarnaast heeft 'Blauw' door middel van een e-learning training ook kennis kunnen vergaren. De e-learning is benaderbaar via het intranet.

Andere maatregelen die genomen zijn om bekendheid en bewustzijn met de Wpg te genereren zijn:

- Op intranet is er een aparte Wpg-pagina beschikbaar met daarop relevante informatie zoals nieuws, handreikingen, protocollen en documentatie.
 - Verstrekkingwijzer
 - E-learning
 - Formulier "Aanmelding WPG-verwerking"
 - Wetgeving
 - Vragen voor wijkagenten en baliemedewerkers
- Bij de privacyfunctionaris kan men terecht voor vragen.
- Men kan ook bij de medewerkers privacy op de districten terecht voor meer informatie.

Aan de hand van een organisatiematrix is per functie bepaald welke cursus werd aangeboden. De tien (elf) gouden vuistregels die tijdens de presentatie aan medewerkers van Limburg-Noord zijn verspreid:

- 1 Waarom leg ik deze informatie vast (doelbinding)?
- 2 Is deze informatie betrouwbaar (bron)?
- 3 Deel (stel ik wel beschikbaar) ik mijn informatie wel (zakboekjes)?
- 4 Stel ik beschikbaar (politie KMar) of ben ik aan het verstrekken (derden)?
- 5 Mag ik aan deze persoon/instantie politie-informatie verstrekken?
- 6 Heb ik de verstrekte politie-informatie wel vastgelegd (geprotocolleerd)?
- 7 Is er met deze instantie een convenant afgesloten?
- 8 Heb ik mijn onderzoek wel aangemeld bij de privacyfunctionaris?
- 9 Van ik wist het naar wij weten het!
- 10 Van 'nice to know' naar 'need to know' (autorisaties)!
- 11 Ken ik de houdbaarheidsdatum van deze informatie?

Bekendheid met de Wpg

Uit de gespreksverslagen komt naar voren dat trainingen zijn gegeven in het kader van de Wet politiegegevens, echter niet elke medewerker heeft deze gevolgd. De medewerkers die geen training hebben gevolgd worden middels een zelfstudiemodule (e-learning) en een presentatie op de hoogte van de relevante bepalingen van de Wpg gebracht. De tekst van de Wet politiegegevens heeft het korps ter raadpleging op intranet geplaatst.

De leidinggevendenden van de opsporingseenheden hebben een specifieke Wpg-training gehad, echter werd het overdragen van de Wpg-kennis als moeilijk ervaren. De aangestelde interne auditor heeft één dag speciale Wpg-training gehad.

Basisopleiding

Men geeft aan dat de opleiding van agenten ook tekort schiet in het overbrengen van Wpg-kennis. In de basistraining wordt een halve dag aan de Wpg besteed.

Kwaliteitscriteria 8

Er vinden middels diverse deelcontroles toetsingen plaats op de juistheid van de gegevens. De inhoudelijke kwaliteitscontrole wordt door gegevensbeheer verricht. Het korps maakt gebruik van TrueBlue voor de gedeeltelijke controle op juistheid in BVH. De geconstateerde onjuistheden worden naar de invoerder en diens chef gestuurd zodat het (mogelijk) kan worden aangepast.

Op elke eenheid is een dagcoördinator aangewezen. Deze persoon controleert de invoeringen in de systemen waaronder BVH. Bij BRI verrichten de medewerkers van gegevensinvoer correctiewerkzaamheden.

Tevens is op intranet een formulier "Aanmelding BVO registratie en WPG VERWERKING" beschikbaar gesteld voor verwerkingen van artikel 8 tot en met 13 Wpg, inclusief een summiere toelichting wat wordt verstaan onder deze artikelen.

- Het formulier dwingt de aanvrager een keuze te maken voor koppeling aan een bepaald artikel.
- Tevens moet het doel van de verwerking worden aangegeven in het geval van een artikel 9-verwerking. Ook de bevoegde functionaris moet worden vermeld.
- Na invulling wordt het formulier automatisch opgestuurd naar de functioneel beheerder voor registratie in BVO. Een kopie wordt verstuurd aan de privacyfunctionaris.

Noodzakelijkheid

Er is te weinig aandacht voor gegevensbeheer en kwaliteit van gegevens vanwege onvoldoende (gekwificeerde) capaciteit. Bovendien is driekwart van de afdeling gegevensbeheer opgeheven (wegbezuinigd) ten gunste van het 'Blauw' op straat.

Er vindt geen toetsing en validatie van gegevens plaats. In de validatie van de gegevens zijn nog een aantal verbeterlagen te maken om het kwaliteitsniveau omhoog te krijgen.

Kwaliteitscriteria 9

Doelbinding

Men is bewust van de doelbinding, het verschil tussen artikel 8 en 9 Wpg informatie. De informatie uit het ene onderzoek mag niet zonder meer in het andere worden gebruikt. Bijna alle onderzoeken vallen vanaf het begin onder artikel 9 Wpg. De onderzoeken worden gemeld aan de privacyfunctionaris, daarvoor wordt een MRO ingediend.

Juistheid en noodzakelijkheid

Binnen het onderzoek is één persoon die alle informatie globaal controleert. Tevens vindt inhoudelijke kwaliteitscontrole plaats op de *juistheid* via collegiale reviews op mutaties van anderen. Als hij in mutaties van anderen constateert dat iets niet juist is spreekt hij die persoon erop aan en/of vraagt gegevensbeheerder de gegevens te corrigeren.

De tapverslagen worden gescreend door de tapcoördinator. Vanuit de onderzoeksleiding is dit de enige controle op diverse aspecten van door rechercheurs verzamelde informatie. Dit is geen sluitend systeem dat controleert op

de noodzakelijkheid daartoe. Er wordt gecorrigeerd op de invoer van persoonsgegevens, koppelingen etc.

Kwaliteitscriteria artikel 10 en 12

Noodzakelijkheid (geen overbodige informatie)

Alleen noodzakelijke gegevens worden opgenomen en overbodige ballast wordt niet opgenomen in de dossiers.

Rechtmatigheid

Informatie die wordt gebruikt moet altijd langs formele weg worden vastgelegd. Onderzoeksleider en/of de Officier van Justitie moeten goedkeuring geven tot ter beschikking stellen.

Doelbinding

Relevantie is het belangrijkste criterium voor de vraag of informatie vastgelegd wordt of niet. Het is niet wenselijk dat de relevantie wordt getoetst door de runners. In het vak van de runners is heel veel informatie relevant. De Officier van Justitie moet een goed beeld krijgen van een potentiële informant om te kunnen bepalen of daar verder mee mag worden gesproken. Daardoor is heel veel informatie relevant en noodzakelijk voor de oordeelsvorming. Men is zich bewust van het feit dat informatie een doel moet dienen.

De runners zetten informatie in de 'bruto-bak'. Voor de 'bruto bak' zijn alleen de runners, chef CIE, de coach, de CIE-analist en de informatiebeheerder CIE geautoriseerd. De informatiebeheerder CIE controleert of de informatie, die bij het exporteren van de bruto naar de netto (productie-)omgeving in het Zwacri-register terecht is gekomen, daar ook daadwerkelijk thuishoort en voldoet aan de gestelde Zwacri-criteria.

Voor het Zwacri-register zijn tevens Chef-RID en andere CIE-medewerkers van verzorgingsgebied Zuid 6 geautoriseerd. Indien het niet voldoet aan de criteria, dan wordt het opgeslagen in Zwacri-beheerregister. Hiertoe is de toegang beperkt tot uitsluitend CIE. Daarmee is gecontroleerd op doelbinding. Indien blijkt dat de informatie niet juist is, dan geeft de informatiebeheerder CIE dat door aan de runner.

Juistheid en volledigheid

De runner controleert zelf de door de informant verstrekte informatie. Informatie wordt 'uitgerechercheerd' voor analyse van de gegeven informatie. Grotendeels verricht de runner zelf deze handelingen, deels zet hij het uit bij de functioneel beheerders. In enkele gevallen worden de CIE's van andere regio's of buitenlandse instanties hierbij betrokken.

Als informatie is ingevoerd en gemuteerd in BVO, dan kan de functioneel beheerder BVO deze gegevens verwijderen als achteraf blijkt dat er bijvoorbeeld dubbelingen in het systeem zijn opgenomen. Bij de recherche wordt streng gecontroleerd op relevantie van de geregistreerde gegevens.

De notities van gesprekken met informanten worden binnen 3x24 uur vastgelegd in de bruto-verslagen. De notatieblokken en dergelijke worden daarna meteen vernietigd.

Kwaliteitscriteria RID

De juistheid en volledigheid van informatie, ook in de verslaglegging, staat centraal. Sinds 1 januari 2011 wordt er gewerkt met BVO voor de verwerking van openbare orde gegevens. Hierdoor is de openbare orde informatie opvraagbaar door alle RID-medewerkers in Verzorgingsgebied Zuid-6. Zuid 6 is de beheerregio van vtsPN waar Limburg-Noord toe behoort.

Echter, een deel van de informatie, onder meer ten behoeve van analyse, kan niet worden opgeslagen, zodat daarvoor de RID-server moet worden gebruikt. In BVO kan bijvoorbeeld geen fotomateriaal worden opgeslagen. Door de beperkingen van BVO bestaat het risico dat de kwaliteit van het werk minder wordt. Hetzelfde geldt voor de analyses. Korps Limburg-Noord heeft aangegeven dit op de actielijst te plaatsen.

De kwaliteit van de aangeleverde informatie toetst de RID door middel van het lezen van documenten en verslagen. In de toekomst zal de analist hier een bijdrage gaan leveren door zijn analyses. Deze kan dan aangeven waar nog extra informatie benodigd is, 'invulling van de witte vlekken', om het beeld aan te vullen. Daarbij kan straks die informatieanalist analyses opstellen (regionale beelden en informatie ten behoeve van keuzes in de bedrijfsvoering/ inzet politiecapaciteit) die input zijn voor de lange termijn.

Ten aanzien van de kwaliteit van AIVD-informatie ligt de toets op kwaliteit centraal bij de AIVD.

Isolatie Divisie Regionale Recherche

Voor het onderling uitwisselen van gegevens in de KA-omgeving heeft de Divisie Regionale Recherche van Limburg-Noord (DRR) autorisatie om alle mappen van de andere rechercheonderdelen van Limburg-Noord te raadplegen.

Andersom is de autorisatie voor Limburg-Noord beperkt in verband met verwerking van Zwacri-gegevens (art. 10-gegevens) door DRR. Limburg-Noord krijgt bij DRR alleen de map met het relevante onderzoek te zien.

In BVH en BVO is er geen onderscheid in systeem tussen zoeken op identiteit en gecombineerd zoeken. Dit is niet te doen in de vastleggingen. IN BVH wordt veel artikel 9 Wpg informatie opgeslagen omdat BVO slecht toegankelijk is (artikel 8 en 9 informatie loopt door elkaar). Bovendien is niet in het systeem ingebouwd dat na één jaar informatie achter een virtueel schot verdwijnt waardoor elke agent vijf jaar bij de informatie kan.

Isolatie van gegevensverwerkingen buiten BVH en BVO

De afdeling BRI in de divisie regionale recherche bestaat uit de afdelingen:

- Infodesk.
- CIE.
- RID.
- Analyse. De afdeling Analyse is weer op te splitsen in:
 - tactische analyse: Scenario's, voorkomen van tunnelvisie bij onderzoeken, beleidsonderzoek, algemene rapportages.
 - veiligheidsanalyse: In de aard identiek aan tactische analyse, maar algemener en meer wetenschappelijk, maatschappelijke vraagstukken.
 - operationele analyse: Analyse ten behoeve van zaken, tijdlijnen, routeschema's bij onderzoeken.

De artikel 8 en 9 Wpg-informatie wordt niet onderscheiden door de software van de systemen BVH en BVO. Dit wordt ervaren als een grote tekortkoming van de software. BVH bevat zowel artikel 8- als artikel 9-informatie. Gezien de problematiek van BVH en BVO wordt hiervoor de kantoorautomatisering-omgeving gebruikt.

De tactisch analist heeft de rol van 'de luis in de pels' zijn in een onderzoek met als doel het voorkomen van blindstaren en het voorkomen van een tunnelvisie binnen het onderzoeksteam. Om deze rol zo goed mogelijk te kunnen vervullen heeft de misdaadanalist (en zijn collega's) de beschikking over alle mogelijke informatie (ook CIE-informatie) uit de beschikbare politiesystemen.

Gebruik kantoorautomatisering

In de regel dient alle informatie met betrekking tot de werkzaamheden van de misdaadanalist te worden opgeslagen in de daarvoor aangemaakte mappen en niet te worden opgeslagen in de persoonlijke werkomgeving. De mogelijkheid voor opslag in de eigen werkomgeving bestaat wel en het kan ook wel eens voorkomen dat informatie daarin wordt opgeslagen.

Bij aanvang van een TGO maakt de misdaadanalist een map in de KA-omgeving aan met onderzoeksgegevens in het TGO. De map kan door alle deelnemers in het TGO worden gebruikt. De misdaadanalist geeft aan dat niet duidelijk is hoe het zit met de bewaartermijnen en schoning. Het is voor de misdaadanalist niet inzichtelijk wie welke politiegegevens van een zaak binnen de KA-omgeving bewaart.

De mappenstructuur binnen de KA-omgeving is artikelsgewijs ingedeeld. Per artikel is een map aangewezen en vervolgens heeft men gekozen voor een indeling van de mappen op jaartal, zodat men aan de hand hiervan de schoningstermijnen in de gaten kan houden.

De misdaadanalist is bekend met de diverse bewaartermijnen die door de Wpg worden gesteld. De methode voor bewaking van de bewaartermijnen in de mappen vormt een zorgpunt.

Het kan zijn dat gegevens op de O:\schijf\groep analisten, de persoonlijke werkomgeving op de N:\schijf of zijn standalone pc staan, waarbij de bewaartermijn is verstreken en dus moeten worden verwijderd of vernietigd.

Alle analisten bij afdeling Analyse kunnen bij deze gegevens, alle collega-analisten zijn voor de standalone PC van de misdaadanalist geautoriseerd. Een deel van de mappen is echter beveiligd, waarvoor door de misdaadanalist dergelijke autorisatie wordt verleend.

Toegang tot de onderzoeksmappen

Om toegang te kunnen verschaffen tot de onderzoeksmappen dient de onderzoeksleider, door middel van een autorisatieformulier, toegang voor de teamleden aan te vragen. In deze aanvraag dient ook te worden aangegeven welke rechten de te autoriseren personen horen te verkrijgen. Men kan hierbij kiezen uit leesrechten, schrijfrechten en/of verwijderrechten.

In geval van het intrekken van de autorisaties dient dezelfde onderzoeksleider dit aan de hand van hetzelfde formulier aan te geven.

Uit de audit is niet gebleken dat het korps Limburg-Noord beleid heeft opgesteld ten aanzien van de kantoorautomatisering, betreffende:

- de relaties naar onderzoeken;
- gebruiks- en bewaartermijnen en de daaruit voortvloeiende schoningsprocedures.

Door het ontbreken van beleid en adequate controle hierop is:

- de mappenstructuur divers en niet controleerbaar;
- er voor TGO en Zwacri-onderzoeken onzekerheid ten aanzien van de afscherming, omdat per district de rechercheurs in elkaars map mogen kijken.

Gezien voorgaande vormt de schoning van politiegegevens ook een uitdaging. Het proces voor het beheren van de autorisaties op de mappen is in opzet beschreven. Er is een indeling op jaartal gemaakt. Echter er is geen standaardproces ingericht voor tijdige schoning van informatie in de mappen. Er is geen procedure voor schoning van de politiegegevens.

Informatiebeheerder BRI

Voor een groot deel van de systemen geldt dat de systemen geen autorisatiebeperkingen kennen, alleen BVO heeft beveiligingsniveaus. De informatiebeheerder BRI is geautoriseerd tot en met niveau 4 in BVO voor de onderzoeken waaraan zij gekoppeld is. Voor informatie boven dat niveau moet de betreffende onderzoeksleider worden gevraagd. De vragen en antwoorden die de informatiebeheerder behandelt in de onderzoeken worden opgeslagen in de Infodeskmodule van BVO en zijn daarmee ook voor de andere beheerders toegankelijk.

Sommige informatie kan niet goed in BVO worden opgeslagen. Wanneer dat het geval is, dan wordt de plek vermeld waar deze wel is opgeslagen op de O-schijf. Bij uitzondering zijn enkele onderzoeken van een collega informatiebeheerder niet voor de anderen toegankelijk. In ieder geval is dat bij interne onderzoeken van toepassing.

Isolatie CIE

Binnen de afgeschermd (standalone) KA-omgeving van Limburg-Noord waar alleen Hoofd CIE autorisatie heeft, registreert men de informanten. De afscherming van informanten is cruciaal in het informatieproces. De te registreren informanten krijgen een uniek nummer dat samen met papieren bescheiden wordt opgeborgen in een kluis. Tot die kluis hebben vier mensen toegang: Hoofd CIE, diens plaatsvervanger en twee administratieve krachten. Hierdoor is geborgd dat alleen Hoofd CIE de NAW-gegevens van de informanten kent en de runner enkel de NAW-gegevens kent van de eigen informanten. Het al dan niet inschrijven als informant wordt bepaald door Hoofd CIE in samenwerking met de CIE-officier. Daartoe heeft hoofd CIE wekelijks overleg met de CIE-officier.

Binnen BVO en KA gelden alleen de toegekende autorisaties van de teamleden.

Fysieke beveiliging CIE

De clean-desk policy wordt strikt gehanteerd. Aan het eind van de dag, of bij langere afwezigheid gedurende de dag worden alle papieren achter slot en grendel bewaard. De kamer is alleen toegankelijk voor CIE. Derden, inclusief de schoonmakers worden nooit alleen op de kamer toegelaten. Overigens wordt de CIE-informatie naar collega CIE-medewerkers van andere regio's per aangetekende post verstuurd. Dit wordt gezien als een veiligheidsrisico.

De fysieke toegang tot ruimtes is via pasjes geregeld. Chef BURO autoriseert deze toegangspasjes. De deur bij de CIE is alleen te openen met deze toegangspas. In de dossierkasten bij de CIE staat geen inhoudelijke informatie opgeslagen, dit bewaartde CIE in kluizen. Bovendien heeft een beperkt aantal mensen toegang tot de kast. Jaloezieën gaan dicht vanwege inkijk overburen. Elke twee á drie jaar worden kamers 'gesweept'. Daarbij wordt ook kritisch gekeken naar zichtbare aanwezigheid informatie.

Isolatie RID

De taak van de RID met name op het punt Openbare Orde is het heimelijk inwinnen van openbare orde informatie over groepen van personen die door hun activiteiten een ernstige bedreiging van de openbare orde kunnen vormen. De RID ondersteunt 'blauw' met specifieke inlichtingenexpertise en biedt handelingsperspectief, zowel voor, tijdens als na eventuele verstoringen de openbare orde.

De RID verwerkt de openbare orde gegevens tot 1 januari 2011 op een RID-server die zich fysiek bevindt in de RID-kantoorruimte. Op deze server worden strikt gescheiden ook de AIVD-gegevens opgeslagen. Vanaf 1 januari 2011 worden openbare orde gegevens opgeslagen binnen BVO in de bak 23RIDOO. Daarmee zijn gegevens door andere daartoe geautoriseerden opvraagbaar.

Deze RID-server is op basis van autorisaties alleen toegankelijk voor RID-medewerkers. De informatie op deze RID-server wordt opgeslagen op de logische partitie voor Openbare Orde informatie (tot 1 januari 2011), of op de partitie met alleen AIVD-informatie. Openbare orde- en AIVD-informatie zijn strikt gescheiden opgeslagen.

In de toekomst wil men het opslaan van onder andere de analysebeelden informatie laten plaatsvinden binnen de zogenaamde 'rode' KA-omgeving. De 'rode KA-omgeving' is tevens fysiek beveiligd. Op het moment maakt de RID voor de openbare orde taak gebruik van deze 'oude' RID-server.

4.3.3

Verbeterpunten

Als verbeterpunten zijn te noemen:

- Opstellen van procedures, richtlijnen voor het inrichten van een mappenstructuur die voldoet aan de vereisten vanuit de Wpg.
- Controle op de bewaartermijnen van de aangehouden informatie binnen de KA-omgeving.
- Opstellen van procedures en richtlijnen voor toetsing van de kwaliteitsaspecten op de informatie aangehouden in de KA-omgeving.
- Analyse van het proces en belegging van verantwoordelijkheden voor inhoudelijke controle van gegevens door gegevensbeheer, chefs etc.
- Ter borging van de kwaliteit is het wenselijk dat permanent een gegevensbeheerder participeert in de onderzoeken en vastlegging daarvan. De onderzoeksleider zou daarvoor, gelet op de competenties, de aangewezen functionaris zijn.

4.4 Gevoelige gegevens (artikel 5)

4.4.1

Norm

Artikel 5. De verwerking van politiegegevens betreffende iemands godsdienst of levensovertuiging, ras, politieke gezindheid, gezondheid, seksuele leven, alsmede persoonsgegevens betreffende het lidmaatschap van een vakvereniging vindt slechts plaats in aanvulling op de verwerking van andere politiegegevens en voor zover dit voor het doel van de verwerking onvermijdelijk is.

De bevindingen zullen hieronder worden gecategoriseerd in rechtmatigheid, volledigheid, juistheid en beveiliging.

4.4.2 Bevindingen

Zwacri

Het team belast met Zwacri-onderzoeken legt gevoelige gegevens vast indien dat noodzakelijk is (i.e. direct met de zaak te maken heeft). Deze informatie is tevens beperkt toegankelijk.

Runners

Net als alle andere informatie van de informanten worden ook deze gegevens alleen opgenomen als daar een noodzaak toe bestaat. Men is voldoende bewust van de gevoeligheid en noodzaak tot terughoudend vastleggen.

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

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

Aanvraagproces en Korpsautorisatiematrix

De lijnscheefs zijn bevoegd voor het indienen van autorisatieverzoeken. Bij de afwezigheid van een lijnchef, kan een districtschef of divisiechef een verzoek indienen. De mandaten voor autorisatieverzoeken zijn dus toegekend aan functies, niet aan personen. Een ondertekend formulier wordt door de verantwoordelijke middels de autorisatiemailbox naar de vtsPN gestuurd. De vtsPN handelt verder de autorisatiemutaties af.

- Dergelijke procedures zijn ook opgesteld voor andere verzoeken zoals tijdelijke studentautorisaties.
- Bovendien zijn procedures opgesteld voor schorsingen, en wijzigingen.

De procesbeschrijving is tevens vastgelegd in process flows.

Voor autorisatie op onderzoeksmappen wordt door de onderzoeksleider middels een formulier autorisatie op schijven aangevraagd. Op dit formulier moet tevens worden vermeld welke rechten (bijv. lees- en schrijfrechten) men wenst aan te vragen. De aanvraag wordt verstuurd naar de Servicedesk Zuid.

Bovenregionale autorisatieprocedure

Voor dergelijke autorisaties geldt dat deze binnenkomen bij de ISC Helpdesk. De autorisatieverzoeken worden ingediend door de privacyfunctionaris van het desbetreffende korps.

- De controle van de validiteit van de verzoeken ligt bij die privacyfunctionaris van het desbetreffende korps. De functioneel beheerder voert de autorisatiemutaties uit.
- Een kopie van de mail wordt naar de privacyfunctionaris gezonden. De privacyfunctionaris houdt een overzicht bij van de bovenregionale autorisaties.

Autorisatiematrix en verwijdering en schoning

De korpsautorisatiematrix is door de privacyfunctionaris opgevraagd. De autorisatiematrix is gedurende de audit niet beschikbaar gesteld. Het korps kan derhalve niet controleren of de gegeven autorisaties nog noodzakelijk zijn (need-to-have). Bovendien kan het korps niet toetsen of de geregistreerde mutaties (administratie in de autorisatiematrix) overeenkomen met de daadwerkelijk toegekende rechten in de applicaties.

De autorisatiematrix is niet inzichtelijk voor het korps. De verantwoordelijken kunnen de zorgvuldigheid en evenredigheid niet toetsen. Hiermee wordt niet voldaan aan de Wpg.

Autorisatie CIE

De chef CIE is degene die bepaalt wie geautoriseerd wordt. Hij is bij besluit aangewezen als bevoegde functionaris en daarmee gemachtigd medewerkers (uit hele regio en uit andere regio's) te autoriseren. De functioneel beheerder BVO voert de mutaties uit gebruikmakende van het landelijk autorisatiemodel. In het landelijk autorisatiemodel is vastgelegd welke functie op welk niveau mag werken.

Voor de KA moeten autorisatieverzoeken worden afgehandeld via VtsPN (via de reguliere of versnelde procedure). Binnen BVO is een aantal pijlers, bijvoorbeeld per onderzoek. Iedere pijler heeft 9 niveaus. Niveau 1 is voor iedereen toegankelijk die is geautoriseerd voor BVO. Niveau 1 maakt inzichtelijk of er een onderzoek tegen iemand is. De onderliggende informatie is afgeschermd door hogere niveaus. Alleen de Chef CIE en diens plaatsvervanger zijn geautoriseerd voor niveau 8, de overige autorisatie gaan niet verder dan niveau 4.

De rechercheurs werken op niveau 5, de onderzoeksleider heeft het autorisatieniveau van 7. De rechercheur ziet dus niet alle informatie binnen het onderzoek. De gegevens van de onderzoeken worden verwerkt in BVO, BVH en in de KA.

De onderzoeksleider is geautoriseerd voor alle mappen. Dit is met name van belang voor het opstarten van een onderzoek. Voor de opstart zijn een aantal lege mappen beschikbaar. De bruto-verslagen worden opgeslagen binnen BVO, maar met een streng autorisatieregime. Naast de reguliere inlogstappen die van toepassing zijn, is er tevens een extra beveiliging ingebouwd. De bruto-verslagen zijn alleen toegankelijk voor de zes runners, de coach, chef en CIE-analist. Het Zwacri-register is toegankelijk voor CIE, RID en de CIE-analisten. BRI-intake kan tot niveau 4 zien dat iemand in Zwacri-register is opgenomen, maar moet de CIE vragen om de achterliggende informatie.

Protocollering autorisatie

Een kopie van het autorisatieformulier wordt verstuurd naar de privacyfunctionaris (PF), deze wordt echter niet bewaard. In plaats daarvan ontvangt de PF per zes maanden een overzicht met de autorisaties en verzoeken. Bovendien ontvangt de PF de lijst 'uitdiensttreding'. De privacyfunctionaris heeft wel een overzicht van de externe autorisatieformulieren, en toetst deze zelf.

Halfjaarlijks vindt er door de privacyfunctionaris een steekproefsgewijze controle plaats op de autorisaties. In geval van functiewisselingen vindt dezelfde controle plaats.

Een overzicht van alle autorisaties is beschikbaar bij de Organisatieontwikkeling & Informatiemanagement (O&I). De protocolleringen van de autorisatieverzoeken vindt plaats door middel van de functionele mailbox van vtsPN.

De uitgegeven autorisaties worden vastgelegd aan de hand van de ingestuurde autorisatieformulieren. Twee keer per jaar ontvangt de privacyfunctionaris een overzicht van de instantie die deze formulieren ontvangt en controleert deze steekproefsgewijs op mogelijke onregelmatigheden. Op verzoek heeft de privacyfunctionaris toegang tot het overzicht van de autorisaties.

De privacyfunctionaris heeft tevens toegang tot de vastlegging van de mutaties van autorisaties bij CIE, RID, OT en AT. Bij de CIE en de RID heeft hij echter geen inhoudelijke inzage.

Bewaren Protocolgegevens autorisaties

Mutaties komen via functionele mailbox terecht bij VtsPN. Daar worden ze door de Servicedesk Zuid ingevoerd in Expertdesk en zo worden alle (vervolg) acties geregistreerd. Deze gegevens worden bewaard. Er is geen bewaartermijn vastgesteld, echter er wordt niets vernietigd.

De protocolgegevens worden bewaard bij O&I en zijn op te vragen door de privacyfunctionaris.

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

4.6.1

Norm

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

4.6.2

Bevindingen

Interpretatie artikel 11 Wpg

Het geautomatiseerd vergelijken of het in combinatie zoeken van enkel politiegegevens betreft het werkproces analyse binnen de afdeling Bureau Regionale Informatie. BRI zoekt breed naar informatie en koppelt deze aan elkaar wanneer daar aanleiding voor is. Een analyse wordt verricht op verzoek van de bevoegde functionaris binnen deze afdeling of de Officier van Justitie van het betreffende onderzoek. Het geautomatiseerd vergelijken of het in combinatie zoeken van enkel politiegegevens mag slechts plaatsvinden na verkregen toestemming.

Het korps Limburg-Noord maakt voor geautomatiseerd vergelijken gebruik van de applicatie BlueView. Door middel van deze applicatie is het mogelijk om informatie te verzamelen uit onder meer BVH en BVO. De misdaadanalist kan zelf een keuze maken (op basis van bestaande coderingen) of gegevens in een zaak worden gebruikt. Daarnaast wordt gebruik gemaakt van de analysetool Analyst NoteBook.

Primair kunnen de informatiecoördinatoren gebruik maken van deze tools, hiervoor zijn een beperkt aantal autorisaties beschikbaar. Alle zoekacties en de resultaten daarvan dienen te worden vastgelegd in het zaaksjournaal welke open blijft staan gedurende de tijd dat het onderzoek loopt. Het zaaksjournaal wordt continu aangevuld met de nieuwe zoekacties en resultaten.

Binnen het systeem BVI-IB worden alle opvragingen gelogd, zoals bovenmatige opvragingen. In de BVI-IB moet je de reden van je bevraging invoeren en de doelbinding moet worden vermeld. Een gedragscode voor het werken met dit systeem is beschikbaar.

RID en CIE

De regionale inlichtingendienst (RID) volgt in de openbare orde taak de speerpunten die op de *Intelligence agenda* worden besproken. Deze onderwerpen worden meegenomen en tevens besproken in het regionaal overleg waarmee voor de RID legitimatie wordt verkregen om op deze onderwerpen te gaan verzamelen. Het hoofd RID kiest vervolgens zelf (o.b.v. van subsidiariteit en proportionaliteit) welke operationele keuzes worden gemaakt.

In specifieke gevallen worden scenario's opgesteld, vervolgens een beslissing genomen en een verstrekkingenrapport opgemaakt conform een landelijk sjabloon RID-verstrekking. In specifieke situaties wordt een proces-verbaal vervaardigd of wordt een informant overgedragen aan dan wel overgenomen van de CIE. Dit is afhankelijk van de situatie. Voor controle op gebruik van de doorgegeven informatie is een verstrekkingenlijst en een proces-verbaallijst aanwezig.

Blauw

Voor al het 'Blauw' is de integrale bevraging beschikbaar, men dient zich hierbij te houden aan de gedragscode die hiervoor in het leven is geroepen.

Gecombineerd zoeken

In BVH en BVO is er geen onderscheid in systeem tussen zoeken op identiteit en gecombineerd zoeken. In BVH wordt veel artikel 9 informatie opgeslagen, omdat BVO slecht toegankelijk is (artikel 8 en 9 Wpg informatie loopt door elkaar).

Aangewezen functionarissen

Primair kunnen de informatiecoördinatoren / misdaadanalist gebruik maken van de artikel 11 zoekmogelijkheden, hiervoor zijn een beperkt aantal autorisaties beschikbaar.

Bevoegd gezag

De Regionale Inlichtingen Dienst

Toezicht en controle op de werkzaamheden van de RID is minder strak georganiseerd als wat betreft de werkzaamheden van de CIE.

De CIE-officier van het OM heeft hierin een aansturende rol bij werkzaamheden van de CIE. Bij het RID is deze rol belegd bij meerdere burgemeesters, waardoor het gezag meer op afstand is komen te staan en daarmee het toezicht en de controle minder stringent is. Ten behoeve van toezicht, controle en transparantie zou dit voor de RID beter uitgewerkt kunnen worden. Dit is landelijk een aandachtspunt.

Criminele Inlichtingen Eenheid

Bij de CIE vindt te allen tijde aansturing plaats door de CIE-Officier van Justitie van het Openbaar Ministerie. Er vindt wekelijks overleg plaats met de CIE waarbij in elk geval onderstaande aspecten aan bod komen:

- Opgemaakte processen-verbaal: van bepaalde categorieën PV's is vastgesteld dat die voor het ter beschikking stellen besproken moeten worden. De rest wordt na ter beschikking stelling van de PV's besproken.
- Inschrijvingen en uitschrijvingen informanten.
- Benoeming van subjecten.
- De Kwestie 'Schoning registers'.
- Tipgeld aanvraag.
- Ontwikkeling start onderzoeken en lopende onderzoeken.
- Bijzonderheden (zoals verwikkelingen met informanten, potentiële deal- of bedreigde getuigen).

Protocollering 11.1, 11.2, 11.4 en 11.5

Een artikel 11 Wpg zoekactie dient bij het BRI te worden geregistreerd in de BVO-Infodeskmodule. Daarmee maken ze de informatie voor de Infodesk-collega's breed toegankelijk en kan daardoor ter beschikking worden gesteld naar aanleiding van andere vragen.

Echter, uit het onderzoek van de privacyfunctionaris van Limburg-Noord naar het vastleggen van artikel 11 Wpg verwerkingen bleek dat in 2010 gedurende de periode maart – december 2010 van 8 TGO's en 4 CBO's een analyse is geproduceerd. Voorts waren nog in 60 andere onderzoeken analyses gemaakt. In een enkel geval blijkt de toestemming van het bevoegde gezag te zijn geregistreerd in het zaaksjournaal. Zoekacties op grond van artikel 11.5 Wpg worden tevens niet vastgelegd, zo blijkt uit het jaarverslag van de privacyfunctionaris.

Voor bovenstaande zaken is door de privacyfunctionaris een toestemmingsformulier ontwikkeld en gaat de PF met de chef BRI en portefeuillehouder opsporing om de tafel over hoe de registraties in de toekomst geborgd gaan worden.

4.7 Bewaartermijnen (artikel 14)

4.7.1

Norm

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

4.7.2

Bevindingen

Artikel 8 bewaartermijnen

Korps Limburg-Noord geeft aan geen *regionale* applicaties te gebruiken om politiegegevens te verwerken. In de nieuwe release van BVH (versie 1.2.2) is een schoningsmodule aanwezig, maar deze staat op landelijk verzoek van de voorzitter van de stuurgroep nog niet aan. De gevolgen van het activeren kan nog in onvoldoende mate worden ingeschat.

Binnen BVH zijn de bewaartermijn nog niet ingeregeld zoals dit op grond van de Wpg is vereist. VtsPN is destijds via het Zuid6-overleg verzocht hierover mee te denken, doch blijft een oplossing vanuit vtsPN achterwege. Binnen het Zuid6-verband zijn hiervoor oplossingen bedacht en ter hand gesteld van vtsPN.

Bij misdaadanalyse komt er in de regel meer informatie binnen dan uiteindelijk, na bewerking / veredeling, nodig is voor een zaak. Informatie wordt door meerdere personen verzameld en ontvangen. Al deze personen hebben de beschikking tot deze informatie en hebben tevens de mogelijkheid om (een deel van) deze informatie in hun persoonlijke werkomgeving op te slaan.

Men geeft aan dat het hierdoor lastig te bepalen is wie welke informatie heeft opgeslagen, waardoor het moeilijk is om een schoningstermijn in acht te worden nemen.

In dergelijke gevallen kan men deze verantwoordelijkheid beleggen bij de informatiehouders zelf. De medewerkers dienen dan zelf rekening te houden met de bewaartermijnen en de gegevens tijdig te verwijderen. Ook zou intern vastgelegd kunnen worden wie met welke zaken bezig is, aan de hand van die lijsten zou geschoond kunnen worden.

Hernieuwde verwerking artikel 8

Voor een hernieuwde verwerking (artikel 14, derde lid Wpg) mogen slechts de analisten bij deze informatie.

BPS

In het oude registratiesysteem BPS is informatie van langer dan vijf jaar terug afgeschermd conform de wettelijke termijn.

KA-omgeving

Binnen de KA-omgeving zijn de politiegegevens opgeslagen in onderzoeksmappen. De mappenstructuur is ingedeeld per artikel (8 en 9 Wpg) en vervolgens is er per artikel een verdeling gemaakt op jaartallen. Aan de hand van deze indeling dient de controle plaats te vinden, maar dit is nog niet voorgekomen omdat dit jaar voor het eerst de vijfjaarstermijn is aangebroken. Voor de controle hierop moeten bij Limburg-Noord nog personen worden aangewezen.

De lijnchef dient erop toe te zien of de politiegegevens op de KA-omgeving tijdig worden verwijderd.

Bewaartermijn archief

Het *hard copy* archief wordt centraal opgeslagen in het archief bij Dienst Informatie Voorziening (DIV) in Venlo. Op de wijkbureaus wordt geen papieren archief aangehouden, uiteindelijk komen alle papieren dossiers in het DIV-archief terecht. Wel komt het voor dat de documenten voor een korte periode op het wijkbureau wordt aangehouden alvorens deze richting het archief gaat. Deze blijven ongeveer 12 maanden op het wijkbureau.

Schoning van het DIV-archief vindt plaats aan de hand van schoningslijsten. Aangegeven wordt dat er soms te scherp aan de termijnen wordt gehouden waarop het voor kan komen dat cold cases-gegevens tevens worden vernietigd.

Korps Limburg-Noord geeft aan dat men het als een belemmering ziet dat niet alle wetgeving gelijk is als het aankomt op de bewaartermijnen. Voor het archief is wat betreft Limburg-Noord de archiefwet leidend.

Artikel 9 verwijderen na OH plus ½ jaar

Terugkoppeling van het Openbaar Ministerie vindt plaats aan de hand van afloopberichten die hard copy op een centraal punt binnenkomen. Deze worden op het centrale punt verwerkt in de systemen; een kopie gaat in de map en een andere kopie gaat naar de recherche-eenheid om aan te geven wat de status van de zaak is.

In de praktijk blijkt dat vaak een melding van het Openbaar Ministerie uitblijft wanneer een zaak door de rechtbank is afgedaan ofwel het laatste rechtsmiddel is gebruikt. Hierdoor is het niet altijd mogelijk de bewaartermijn voor artikel 9 Wpg gegevens in acht te nemen, immers niet in alle gevallen kan het OH-moment worden bepaald.

Sinds twee maanden wordt er tevens gebruik gemaakt van de applicatie BOSZ. Limburg-Noord geeft echter aan dat deze niet Wpg-proof is. Bovendien maakt het OM nog geen gebruik van BOSZ waardoor de terugkoppeling nog niet is geborgd.

Er kan niet worden geborgd dat artikel 9 gegevens een half jaar na het OH-moment worden verwijderd. Hiermee wordt niet voldaan aan de Wpg.

Beheer BVO

Een medewerker van BRI doet het functioneel beheer van BVO. Deze medewerker is werkzaam bij de CIE. Hij en de chef CIE schonen de gegevens.

Artikel 9 verwijderen na 5 jaar verwijderd

Korps Limburg-Noord geeft aan dat gegevens in BVO niet kunnen worden verwijderd (na 5 jaar), maar wel vernietigd (na 10 jaar).

- Vijf jaar na datum laatste invoer (in de praktijk vijf jaar na einde onderzoek) wordt het autorisatieniveau van alle mutaties in de registratie opgehoogd naar niveau 9 ('verwijderen').
- Vijf jaar na verwijdering (zie vorig punt) wordt de betreffende registratie vernietigd. De schoning van gegevens in BVO in het kader van de Wpg gebeurt bij Bureau Regionale Inlichtingendienst (BRI) van Limburg-Noord.

Aangegeven wordt dat er in de praktijk geen bericht wordt ontvangen wanneer een zaak in kracht van gewijsde is gegaan. Daarom heeft men gekozen voor de termijn van vijf jaar om onrechtmatige verstrekking te voorkomen. Wanneer delen en/of verstrekken van de informatie in een voorkomend geval toch noodzakelijk is, kan men door het verlagen van het registratieniveau toch aan deze behoefte voldoen.

Gebruik informatiesystemen CIE

Het systeem om de informatie op te slaan van BVO is niet in overeenstemming met de systematiek van de wetgeving, wat als een probleem wordt ervaren.

Het ontbreken van een schoningstool vormt een belemmering in de nakoming van de verplichtingen uit de Wpg. Dit probleem is regelmatig besproken in het Landelijk Platform CIE-officieren. Tot voor kort gold de afspraak in verzorgingsgebied Zuid 6-verband dat vanwege het ontbreken van de tool, niet zou worden geschoond.

Nu het ter beschikking komen van de functionaliteit al lang op zich laat wachten, gaat het niet-schonen steeds meer knellen en wordt gezocht naar een andere oplossing.

Verwijderen en vernietigen na 5 jaar geen subjectwaardige registratie

De CIE van korps Limburg-Noord werkt volgens het landelijke CIE-proceshandboek waarin ook de aanpak met betrekking tot de bewaartermijnen procedureel zijn geregeld.

De beknopte werkwijze zoals omschreven in het proceshandboek is als volgt. De gegevens die niet langer noodzakelijk zijn voor het doel van verwerking en die waarvan de datum van laatste verwerking 5 jaar of langer is geleden moet worden verwijderd. De datum laatste verwerking wordt bepaald aan de hand van de laatste Zwacri-waardige informatie die bij het subject is geregistreerd. Op basis van een peildatum wordt een voorstel tot verwijderen gemaakt. Na controle en op basis van onderstaande criteria wordt dit voorstel uitgevoerd. De daadwerkelijke verwijdering van gegevens wordt op basis van onderstaande criteria uitgevoerd:

- Meest recente Zwacri-waardige informatie is 5 jaar of langer geleden waar het subject aan gekoppeld is.
- Als de informatie als artikel 10 Wpg gemarkeerd is.
- Binnen een onder het geselecteerde regime vallende registratie valt die binnen de gevraagde regio geregistreerd is en die de meest recente invoerdatum is van alle artikel 10 waardige gegevens waar het subject aan gekoppeld is.

Van het verwijderen wordt een verwijdersverslag in het werkjournaal opgesteld. Dit verslag bevat geen persoonsgegevens dan wel naar personen herleidbare gegevens.

Het hoofd CIE dient ervoor zorg te dragen dat het gegevensbestand regelmatig wordt gecontroleerd ten einde te beoordelen of de noodzaak voor de verwerking van gegevens nog steeds aanwezig is. Deze controle vindt elk half jaar plaats.

Voor het verwijderen en vernietigen van artikel 10 Wpg-informatie volgt de CIE de procedure uit het landelijke CIE-proceshandboek.

Hernieuwde verwerking

Wanneer het BRI (de Infodesk) een aanvraag krijgt en constateert dat informatie uit de zoekresultaten reeds is verwijderd conform de Wpg, dan dient BRI de bevoegde functionaris te raadplegen. Bij geschoonde informatie wordt tevens toestemming aan de betreffende Officier van Justitie gevraagd.

In de applicaties wordt tevens aangegeven dat als de bewaartermijn is overschreden men toestemming dient aan te vragen om gebruik te mogen maken van deze data.

CIE

De CIE heeft – aan de hand van het landelijke CIE proceshandboek – voorwaarden vastgesteld om verwijderde en bewaarde gegevens voor hernieuwd gebruik beschikbaar te stellen:

- Er is een opdracht van het bevoegd gezag. Dit bevoegd gezag is de Officier van Justitie indien het gaat om strafrechtelijke handhaving.
- Alleen bevoegde ambtenaren moeten deze mogelijkheid krijgen.
- Het doel van het raadplegen moet bekend zijn.
- Ongericht zoeken is niet toegestaan.
- Het in combinatie met nieuwe gegevens verwerken is niet toegestaan.
- Beschikbaar stellen voor hernieuwd gebruik mag alleen ten behoeve van een artikel 9 of 10 doel.

Een procedure is opgesteld met betrekking tot artikel 14.3 verwerkingen. Toestemming dient te worden gevraagd aan het bevoegde gezag.

Protocollering 14.3

Hernieuwde verwerking wordt geregistreerd in de BVO-infodeskmodule. De privacyfunctionaris gaat hierbij zelf op onderzoek uit of er sprake is van rechtmatige hernieuwde verwerkingen. Deze steekproef vindt een keer per half jaar plaats.

De protocollering kan men terugvinden in de BVO-infodeskmodule en wordt daarmee vastgelegd.

Artikel 12 informantenregister

Artikel 12 Wpg informatie wordt wekelijks overgeheveld naar andere verwerkingen (Artikel 8, 9 of 10 Wpg) door de informatiebeheerders. Een medewerker van BRI doet het functioneel beheer van BVO. Deze medewerker is werkzaam bij de CIE. Deze medewerker schoont samen met de chef CIE de gegevens.

Artikel 12 controleren

De CIE-Officier van Justitie voert elk half jaar samen met een parketsecretaris een controle uit op de informanten, de Zwacri-subjecten en vertaling van bruto- naar netto-informatie. Indien nodig wordt geschoond. Het Openbaar Ministerie heeft daartoe toegang tot zowel de inhoud van BVO-bruto als BVO-netto.

De CIE-Officier van Justitie geeft echter aan geen zicht te hebben of de gegevens in het informantenregister na maximaal 10 jaar zijn vernietigd. Er vindt dan ook geen effectieve controle plaats door de CIE OvJ op het tijdig vernietigen van artikel 12 gegevens.

Een halfjaarlijkse controle op het Informantenregister vindt plaats door de CIE-Officier van Justitie van Limburg-Noord.

Artikel 12 vernietigen

Het korps heeft niet geborgd dat gegevens daadwerkelijk na maximaal 10 jaar worden vernietigd. De CIE hanteert een breed netwerk van informanten om een goed veiligheidsbeeld te geven en om in te kunnen spelen op geprioriteerde thema's. Op enig moment kan de behoefte bestaan om een (ex-) informant die al lange tijd niet meer benaderd is wederom te benaderen voor een specifieke gebeurtenis of thema.

Informatie die door informanten wordt verstrekt gaat met name over subjecten. Deze informatie wordt vanuit de bruto-omgeving overgezet naar de netto-omgeving. Als deze informatie wordt verstrekt aan een tactisch team wordt teruggevallen op de uitgebreide beschrijving in de bruto-omgeving om te komen tot een betrouwbaarheidsoordeel. Dit wordt lastig als de informatie uit de bruto-omgeving inmiddels verwijderd c.q. vernietigd zou zijn.

Gezien bovenstaande worden deze gegevens momenteel niet geschoond. Er wordt in samenspraak met het OM landelijk bekeken hoe binnen CIE Nederland de schoning op uniforme wijze kan plaats vinden.

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

Informatiebeheerder BRI

De vragen en antwoorden in de onderzoeken die worden behandeld worden opgeslagen in de Infodeskmodule van BVO en zijn daarmee ook voor de andere beheerders toegankelijk. Sommige informatie kan echter niet goed in BVO worden opgeslagen, in dat geval wordt de plek vermeldt waar deze wel is opgeslagen (bijv. op de O-schijf). Bij uitzondering zijn enkele onderzoeken van een collega informatiebeheerder niet voor de anderen toegankelijk. In ieder geval is dat het geval bij interne onderzoeken.

Infodesk

Het ter beschikking stellen van informatie gebeurt via de Infodesk van de afdeling Bureau Regionale Informatie (BRI). Het BRI behandelt alle informatievragen en bepaalt tevens waar de vragen uitgezet gaan worden in bijvoorbeeld BlueView.

De rechercheonderzoeken worden via de Districtelijke Opsporings Onderzoek (DOO) overlegd aan de stuurgroep voor de prioritering en capaciteitsplanning. Deze DOO's worden opgesteld door de projectvoorbereider of de mensen in de informatieknooppunten.

De chef van het BRI heeft voor de afdeling een aantal doelen gesteld:

- Beter en sneller verbanden leggen tussen incidenten, en (groepen) verdachten, inclusief analyse.
- Beslissers beter in staat te stellen goede besluiten te nemen door gevalideerde informatie die wordt aangeleverd.
- Beter informatie uitwisselen met partners.

Nationaal Intelligence Model (NIM) als basis voor BRI

Het Nationaal Intelligence Model (NIM) is één richtinggevende concern-brede visie op welke wijze informatie de politie stuurt en de wijze waarop de politie op de informatieprocessen stuurt. Hierin is de Wpg ook opgenomen. Het NIM dient als basis voor het functioneren van de afdeling (architectuur). Jaarlijks wordt de chef BRI ge-audit of hij voldoet aan de waterlijn, de criteria van het intelligence model. Middels een format wordt in een ronde tafel gesprek ongeveer 100 vragen beantwoord over richten, inrichten en verrichten. Het landelijk bureau doet vervolgens de waardering.

Een analist van de Criminele Inlichtingen Eenheid (CIE) bij het korps Limburg-Noord zit tevens bij BRI en valt onder het hoofd CIE. Eén analist is aangewezen als CIE analist en heeft toegang tot alle CIE informatie (en de brute informatie).

Procedure Infodesk

Voor de Infodesk is een werkinstructie opgesteld hoe te handelen bij de behandeling van informatieverzoeken, en op welke kwaliteitsaspecten deze verzoeken getoetst behoren te worden. Deze werkinstructie bevat de processtappen voor controle op:

- Ontvankelijkheid artikel 15 Wpg.
- Registratie in BVO Infodeskmodule, artikel 11 en 32 Wpg.

- Doorzetting naar het relevante onderdeel voor verdere afhandeling afhankelijk van het verzoek.
- Ten behoeve van het informatieverzoek wordt informatie verzameld. In het geval van artikel 9, 10, of 12 Wpg informatie wordt de betreffende Bevoegd Functionaris geraadpleegd. Tevens vindt controle plaats op de vastgestelde bewaartermijn van de informatie.
- Bepaling van de informatie die mag worden gedeeld, dan wel verstrekt (conform de verstrekkingenwijzer). De landelijke verstrekkingenwijzer is door het korps Limburg Noord geactualiseerd.
- Eventuele veredeling van informatie in de vorm van een e-mail of verstrekkingenrapport.
- Bij een verstrekking wordt deze vastgelegd in de BVO-Infodeskmodule.

Er is een Infodesk aangewezen als centraal punt waar informatieverzoeken kunnen worden ingediend. In opzet dient de Infodesk aan de in de Wpg gestelde criteria te toetsen. In de praktijk blijkt deze toetsing echter minder stringent te zijn dan in de werkinstructie is voorgeschreven.

Ter beschikking stellen

Voor het ter beschikking stellen van persoonsdossiers is er een model ontwikkeld. Wanneer men binnen een onderzoek een dergelijk dossier nodig heeft wordt deze alleen ter beschikking gesteld aan de informatie coördinator van het betreffende onderzoek, en niet aan alle rechercheurs. In het geval van een klein onderzoek waarbij er geen informatie coördinator aanwezig is wordt er echter wel direct aan de rechercheurs ter beschikking gesteld.

In opzet geldt: Er wordt kritisch naar de functie van de aanvrager gekeken alvorens er informatie ter beschikking wordt gesteld. Niet iedere Limburg-Noord medewerker kan dus om informatie vragen. Wanneer de vraag veel informatie oplevert, of de vraagstelling nog onduidelijk is, dan wordt de aanvrager gevraagd het doel voor het informatieverzoek te motiveren. In overleg wordt bepaald of de informatie ter beschikking wordt gesteld. Daarbij wordt tevens gekeken naar de functie van de aanvrager. Het is niet toegestaan om alle informatie op te vragen.

In de praktijk blijkt dat er geen structurele controle plaatsvindt op de functie van de vraagsteller. Men controleert alleen of de vraagsteller binnen de regio werkzaam is. Daarmee bestaat het risico dat de aanvrager informatie verkrijgt waarover die uit hoofde van de uitvoering van zijn of haar taak niet mag beschikken.

CIE

Alleen de chef van de CIE is bevoegd om CIE-informatie ter beschikking te stellen, dit gebeurt in overleg met de CIE-Officier van Justitie. Informatie die aan andere CIE-medewerkers ter beschikking dient te worden gesteld gaat via de zogeheten 'Zwacri-omgeving', waarvoor een strak autorisatieregime geldt. De informatiebeheerder stelt gegevens ter beschikking aan andere CIE-leden en legt dat vast in een rapport.

Delen niet Zwacri-informatie

Van de 'restinformatie' die bestaat uit persoonsgegevens, adresgegevens en 'telefoonnummers bekend' wordt een lijst opgesteld, waaruit de regionale recherche zijn keuze kan bepalen. Deze lijst wordt ter beschikking gesteld aan de Regionale Recherche en aan de recherche op de districten.

CIE ter beschikking stellingen

Informatie wordt structureel gescreend door chef CIE en CIE-Officier van Justitie, mede met het oog op de strikte bewaartermijnen die binnen CIE gelden. Informatie

van informanten wordt in bruto-verslag opgenomen. Van daaruit worden de relevante gedeelten daarvan opgenomen in het Zwacri-register. Ter beschikking stelling vindt alleen plaats middels een proces-verbaal van de chef CIE. Daarmee is feitelijk sprake van een extra kwaliteitsslag wat betreft de rechtmatigheid.

Codering CIE

Wanneer een runner een potentiële informant spreekt, wordt dit bij de CIE-chef gemeld. Alleen in bijzondere gevallen wordt de CIE Officier van Justitie vooraf ingelicht, bijvoorbeeld als het gaat om minderjarige potentiële informanten of een geheimhouder.

Met de CIE-chef en CIE OvJ wordt besproken of de informant wordt opgenomen in het informantenregister. Bij opname van de informant in het informantenregister, wordt het gespreksverslag opgenomen in BVO. De 'bruto' informatie (artikel 12 Wpg informatie) wordt gescheiden opgeslagen van netto informatie (codering 00/200/300). Alleen de functionarissen met de daartoe bevoegde autorisaties kunnen deze informatie inzien. Bij bijzonderheden worden de gespreksverslagen door de CIE OvJ geraadpleegd. De runner verzorgt de codering zelf.

Het werken met BVO wordt gezien als te omslachtig. Het omzetten van 'bruto-' naar 'netto'-informatie gebeurt via selecteren en benoemen van bruto-informatie (naar 00, 01 of hoger).

Alleen de runners maken de verslagen op van de gesprekken met informanten. In deze verslagen markeren ze informatie die de informatiebeheerder exporteert naar de netto-productieomgeving. Na het exporteren van de netto-informatie wordt de bruto-informatie voorzien van een hoger autorisatieniveau en is daarmee alleen nog bereikbaar voor de eigen beheerder CIE. De informatie over de informanten zelf verlaat nooit de 'bruto-bak'.

Het informantenregister met daarin de NAW-gegevens van de informanten betreft een aparte lijst (kluisapplicatie). Alleen de chef CIE en diens plaatsvervanger heeft toegang tot deze kluis.

Verslagen van de gesprekken die gevoerd worden met de informanten worden vastgelegd in BVO-bruto. De informatie, die niet herleidbaar is naar de bron en bruikbaar is voor onderzoeken, wordt vastgelegd in BVO-netto. Voor het delen van (00/200/300-)gegevens met andere CIE's geldt dat de bruto gegevens niet gedeeld worden. BVO-netto is zichtbaar voor de zes zuidelijke regio's (Zuid-6) voor zover de afhandelingscode dit toelaat. Ook herleidbare Zwacri-informatie wordt als 00-informatie vastgelegd in BVO-netto.

Het delen van informatie met andere CIE's vindt op dit moment alleen nog op papier plaats (aangetekend verzenden, met alle risico's van dien). Een project om dit proces te automatiseren is momenteel nog in ontwikkeling.

Ter beschikking stellen

De rechercheur Zwacri vraagt en zoekt informatie op in alle systemen waartoe hij is geautoriseerd. Voor overige informatie raadpleegt hij BRI-intake, de CIE of de informatiebeheerder die verbonden is aan het onderzoeksteam.

Informatie uit andere artikel 9-onderzoeken wordt verkregen via informele gegevensuitwisseling met zijn collega's die aan ander onderzoek werken om zo te achterhalen of ze elkaar kunnen helpen met informatie uit de respectievelijke

onderzoeken. Indien blijkt dat de informatie bruikbaar is wordt vervolgens de formele weg gevolgd.

Op de District Recherche Opsporing (DRO) lijsten wordt in het kort aangegeven welke informatie per zaak beschikbaar is. Deze lijsten worden voorgelegd aan de stuurgroep van de districten. Het district beslist wanneer behoefte is aan informatie. Indien behoefte is aan informatie, dan wordt een proces-verbaal opgemaakt in BVO. Op dit moment wordt niet vastgelegd welke informatie aan wie en op welke datum wordt verstrekt, buiten de voornoemde lijsten.

Het Hoofd CIE maakt uiteindelijk het proces-verbaal op. De CIE-Officier van Justitie geeft akkoord op het Proces-verbaal. Bij de recherche (en/of bij de zaakofficier) wordt het lopende onderzoek afgestemd en vastgesteld welke informatiebehoefte er is bij het onderzoeksteam. De CIE maakt de afweging of in deze behoefte kan worden voorzien, en op welke wijze de informatie ter beschikking wordt gesteld.

Controle

Twee keer per jaar vindt er een controle plaats door de CIE-Officier van Justitie op drie informantendossiers en vijf subjectendossiers. Een behoefte tot subjectbenoeming kan voortkomen uit een strafrechtelijk onderzoek, door scanning.

Vaker komt een subject voort uit informatie van informanten in relatie tot al geregistreerde subjecten, uit een onderzoek dat al bij de politie bekend is of er wordt op geattendeerd door een andere CIE (andere regio), bijvoorbeeld na verhuizing.

Per subjectbenoeming wordt de daaraan ten grondslag liggende mutatie(s) voorgelegd aan de CIE OvJ. Wanneer dit subject als zodanig aangemerkt wordt, wordt dit vastgelegd in BVO (subject). De CIE ziet regelmatig de MRO van de recherche.

Vastlegging van informatieverzoeken

Vastlegging van de informatieverzoeken gebeurt bij het BRI in de BVO-Infodeskmodule. In deze module worden in het kader van de Wpg alle verzoeken vastgelegd. Al deze verzoeken dienen per e-mail te worden gesteld, ook in het geval dat het informatieverzoek per telefoon is gestart.

Informatieverzoeken die niet door de klantmedewerkers van het BRI binnen een uur kunnen worden behandeld worden doorgestuurd naar Infobeheer. Infobeheer behandelt deze aanvragen vervolgens en stelt de informatie ter beschikking door middel van een verstekkingsrapport.

Het gericht ter beschikking stellen van artikel 10 Wpg informatie aan een opsporingsteam door de CIE geschiedt door middel van het opmaken van een Proces-verbaal (Pv) dat wordt vergezeld van een evaluatieformulier. De CIE-officier wordt wekelijks geïnformeerd over deze verstrekte processen-verbaal. In twijfelgevallen wordt het verzoek vooraf aan de CIE-officier voorgelegd.

Opdrachten

Daar waar sprake is van opdrachten worden deze niet op speciaal daarvoor landelijk ontwikkeld formulier vastgelegd (het I-90 formulier in BVH). Wel bevestigt men de gevraagde werkzaamheden met een e-mail aan de opdrachtgever, bijvoorbeeld de informatieregisseur. De opdracht voor werkzaamheden wordt bevestigd via een e-mail. Het resultaat wordt verstrekt aan de informatieregisseur.

Logging zoekvragen

In bepaalde systemen worden de zoekvragen die worden ingevoerd automatisch gelogd. Echter, bij Limburg-Noord is niet bekend welk systeem dit wel en welk systeem dit niet doet.

Beschikbare informatiebronnen

De klantmedewerkers hebben – inclusief de systemen die door BVI worden ontsloten – de beschikking over ongeveer 25 systemen. De politiegegevens, die bijvoorbeeld door de applicatie BlueView ontsluitbaar zijn, zijn tot vijf jaar terug beschikbaar.

De e-mails met informatieverzoeken worden maximaal drie weken bewaard. Het verzoek wordt met antwoord verwerkt in de Infodeskmodule die pas sinds anderhalf jaar in gebruik is.

Meldkamer

Vanuit de meldkamer komen weinig vragen bij de Infodesk van BRI, omdat de meldkamer voldoende geautoriseerd is om vragen van blauw vanuit de auto direct te kunnen beantwoorden. De meldkamer beschikt niet over een link naar de Infodesk van BRI in verband met capaciteitsproblemen bij BRI.

Bevoegde functionarissen

In het aanwijzingsbesluit zijn functies aangewezen die als bevoegde functionaris binnen het korps gaan fungeren. Wanneer men een dergelijke functie gaat vervullen vervult men automatisch de rol van bevoegde functionaris.

Er zijn verschillende trainingen gegeven aan de leidinggevenden van de opsporingseenheden in het kader van de Wpg. Een van de trainingen betreft de tweedaagse opleiding tot bevoegde functionaris. Een functionaris heeft laatstgenoemde opleiding gevolgd en deze kennis vervolgens overgebracht aan de andere twee bevoegde functionarissen.

Aan nieuw aangewezen bevoegde functionarissen wordt geen extra aandacht meer gegeven met betrekking tot de Wpg, omdat de Wpg volgens het korps voldoende wordt behandeld tijdens de opleiding aan de politieacademie.

Weigeringsgronden

De bevoegde functionarissen zijn op de hoogte van de wettelijke weigeringsgronden in relatie tot de verplichting van het ter beschikking stellen. Dit is opgenomen in de opleiding voor bevoegde functionarissen.

4.9 Verstrekken (artikel 16/24)

4.9.1

Norm

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

4.9.2 *Bevindingen*

De landelijke verstrekkingswijzer

Korps Limburg-Noord heeft de landelijke verstrekkingswijzer beschikbaar gesteld voor medewerkers op intranet. Uit de gehouden interviews blijkt dat medewerkers bekend zijn met deze verstrekkingswijzer. Deze wijzer wordt gebruikt, echter niet door alle medewerkers die betrokken zijn bij de verstrekkingen.

De landelijke verstrekkingswijzer is tevens actueel gehouden door korps Limburg-Noord en voldoet daarmee aan de meest actuele wettelijke bepalingen.

Ondersteuning door landelijk project Wpg

Vanuit het landelijke project zijn er "verstrekkingswijzers" verstrekt die in gebruik zijn bij Limburg-Noord. Vanuit dit landelijke project zijn 2 en 5-daagse trainingen aangeboden, waarbij de interne auditors met de leden van hun projectteam een 2-daagse Wpg-training hebben gehad. Het 'Blauw' heeft een eendaagse training gevolgd, waarin o.a. aandacht wordt besteed aan convenanten en verstrekkingen.

Artikel 16 en artikel 23 verstrekking aan Openbaar Ministerie

Vier medewerkers van het Openbaar Ministerie hebben (op basis van artikel 16 en 23 Wpg) rechtstreeks toegang gekregen tot BVH. De verantwoordelijke – de korpsbeheerder – heeft hiervoor zijn goedkeuring gegeven. Tevens zijn de geautoriseerde mensen onderworpen aan een betrouwbaarheidsonderzoek.

Kijkende naar artikel 16 van de Wpg is verstrekking alleen toegestaan voor zover het OM deze gegevens behoeven voor de in het artikel gestelde doeleinden (noodzaak en doelbinding). Door middel van het verlenen van onbegrensde toegang tot BVH is geenszins geborgd dat de gegevens die het OM verwerkt uit BVH gerechtvaardigd is.

Door toekenning van deze structurele toegang is de koppeling van een bevraging met de noodzaak en doelbinding vooraf niet toetsbaar. Een controle op bevragingen vooraf ontbreekt.

Ook artikel 23 (rechtstreekse verstrekking aan leden van het OM) stelt aanvullende waarborgen met betrekking tot het verstrekken van gegevens aan het Openbaar Ministerie. De verantwoordelijke dient passende technische en organisatorische maatregelen te treffen teneinde te waarborgen dat rechtstreekse verstrekking uitsluitend plaatsvindt voor zover noodzakelijk is op grond van het bepaalde in de eerste twee leden van dit artikel. Door rechtstreekse toegang aan BVH te verschaffen aan leden van het OM ontbreekt ook de controle op bovenstaande punten.

Aangaande deze rechtstreekse verstrekking van politiegegevens heeft men een convenant opgesteld met de bedoeling bovenstaande punten af te dekken.

- Echter, door rechtstreekse toegang tot het systeem ontbreekt – ondanks door het contractueel af te dichten – de controle *vooraf*. Alleen controle *achteraf* is hierdoor nog mogelijk.
- Bovendien is er geconstateerd door de privacyfunctionaris dat logging – een van de maatregelen in het opgestelde document – als instrument nauwelijks is ontwikkeld zodat controle op de correcte toepassing van toegekende autorisaties niet goed mogelijk is.

Artikel 17 Rechtshulpverzoek (RHV)

Het korps Limburg-Noord heeft een procedure opgesteld hoe om te gaan met rechtshulpverzoeken op grond van artikel 17 Wpg. Hiervoor is de werkinstructie 'Wpg werkinstructie restinformatie rechtshulpverzoeken' samengesteld.

Tevens komt aan bod hoe om te gaan met restinformatie die is gegenereerd door (het uitvoeren) van rechtshulpverzoeken. Uitsluitend de Officier van Justitie is bevoegd om hierover uitsluitel te geven. Als men restinformatie uit een RHV wil gebruiken moet men toestemming van de Officier hebben.

Artikel 19 incidentele verstrekking

Incidentele verstrekkingen aan derden op basis van artikel 19 Wet politiegegevens kan plaatsvinden op voorwaarde dat het bevoegd gezag (burgemeester van de gemeente waarin het politieteam opereert en de Officier van Justitie) moet instemmen met een dergelijke verstrekking.

Alvorens de gegevens worden uitgewisseld, wordt zowel de Burgemeester als de Officier van Justitie geïnformeerd. Na informering en toestemming, wordt pas gestart met gegevensuitwisseling door het betreffende politieteam.

Er mogen in principe alleen noodzakelijke politiegegevens uit een artikel 8 of artikel 13 Wpg verwerking worden verstrekt. Gegevens uit een artikel 9 of 10 onderzoek, eerste lid onder a of c (CIE en RID) Wpg-verwerking mogen alleen worden verstrekt bij dringende noodzakelijkheid voor de uitvoering van de politietaak na overleg met de bevoegde functionaris (leider onderzoek of chef CIE/RID).

Korps Limburg-Noord gebruikt hiervoor het formulier 'Informatieoverzicht in het kader van gegevensuitwisseling van politie met derden'. Dit formulier bevat de volgende informatie:

- Onderwerp gegevensuitwisseling.
- Ontvanger.
- Welke gegevens.
- Datum verstrekking.
- Doel van de verstrekking.
- Noodzakelijkheid van de verstrekking.
- Geheimhoudingsclausule.

Dit formulier wordt ondertekend door zowel de Burgemeester, de Officier van Justitie en de districtchef.

Artikel 20 besluiten

Bij verstrekkingen buiten de landelijke verstrekkingenwijzer is het beleid bij korps Limburg-Noord om voor deze verstrekkingen een convenant op te stellen. In samenwerking met de senior juridisch medewerker van Limburg-Noord heeft men convenanten conform artikel 19 en 20 Wpg opgesteld.

Op intranet is voor alle medewerkers een overzicht beschikbaar van alle convenanten die binnen regio Limburg-Noord zijn vastgesteld. In totaal zijn er achttien artikel 20 Wpg samenwerkingsverbanden geïdentificeerd.

De convenanten dienen getekend te zijn door de Korpsbeheerder, de Hoofdofficier van Justitie en de betreffende Burgemeester. De partners in het netwerkoverleg zijn gehouden aan een geheimhouding en zijn daar ook over geïnformeerd.

De convenanten bevatten ten minste de volgende afspraken:

- De beslissing van de informatieverstrekking.
- Doel van de gegevensverstrekking.
- De wijze van verstrekking.
- De te verstrekken gegevens.
- Bijzondere verplichtingen, zoals de geheimhouding conform artikel 7 Wpg.
- Looptijd van de beslissing.

Alvorens de besluiten definitief worden gemaakt, wordt deze eerst bij de juridische afdeling ter goedkeuring gelegd. Een overzicht van alle convenanten is tevens bij de privacyfunctionaris beschikbaar.

Het korps heeft bij de implementatie van de Wpg de convenanten en artikel 20-besluiten geïnventariseerd. Daarbij zijn Wpg-relevante artikel 20-besluiten Wpg-geschikt gemaakt en beschikbaar gesteld op het intranet. Deze zijn voor iedereen inzichtelijk. De artikel 20-besluiten bevatten een verwijzing naar artikel 7.2 Wpg waarmee er op de geheimhoudingsplicht wordt gewezen. Tevens is er een overzicht van convenanten aanwezig waarin de status van de individuele convenanten in is opgenomen.

Verstrekkingenschema regionaal

De vaste partners in het veiligheidshuis zijn de Politie, het Openbaar Ministerie, procesmanagers, bureau jeugdzorg, reclassering en verslavingszorg (justitiële partners). Elke morgen vindt een briefing plaats met de vaste partners en worden de incidenten per regio per dag besproken. De briefings worden vastgelegd op een aparte schijf bij de politie. In de briefing wordt ook bepaald wie wordt gevolgd.

Media en nutsbedrijven

Er vinden niet veel verstrekkingen aan derden plaats. Verstrekkingen aan media verlopen via bureau communicatie. Dit gebeurt dan naar aanleiding van persvragen of uit eigen beweging ten behoeve van de opsporing. Tevens komt het voor dat er aan nutsbedrijven informatie wordt verstrekt. Er ligt een convenant ten grondslag aan de verstrekkingen aan nutsbedrijven.

Verstrekkingen aan de media wordt vastgelegd in een afsprakenjournaal. Bij overdracht van de mediavoorlichting van de politieregio Limburg-Noord naar het Openbaar Ministerie is de afspraak dat de voorlichter wel contact blijft houden met de onderzoeksleider.

Dergelijke verstrekkingen gebeuren in de meeste gevallen niet rechtstreeks aan de aanvrager. Veel diensten hebben hun eigen Infodesk en dan vindt verstrekking via hen plaats. Verstrekking aan bijvoorbeeld gemeentes vindt plaats via de gebiedsmentor.

CIE

De CIE-informatie wordt gedeeld met andere CIE-diensten in Nederland via of rechtstreeks aan andere regio's. De NCIE heeft zicht op welke onderzoeken waar draaien en kan zo beter bepalen voor welke andere regio informatie relevant is. De ontvangende regio krijgt geen persoonsgegevens over de informant maar ziet wel uit welke regio het komt, zodat die voor nadere informatie daar terecht kan. De informant krijgt altijd een landelijk informantenummer toegewezen door de NCIE, maar krijgt hier ook een regionaal nummer. De werkelijke identiteit van de informant is alleen bekend bij de oorspronkelijke regio (in de kluis) en de NCIE.

De CIE Officier van Justitie wordt in elk geval achteraf ingelicht over verstrekkingen van de CIE. In bepaalde afgesproken gevallen, waaronder verstrekkingen aan het buitenland wordt er vooraf ingelicht. Het hoofd CIE accordeert elke verstrekking en tekent hiervoor. Het hoofd wordt hierbij geassisteerd door de CIE-coach.

Er is geen sprake van een structurele evaluatie van verstrekkingen tussen de CIE en CIE-Officier van Justitie. Wel wordt regelmatig besproken of alle beleidsspeerpunten voldoende aandacht krijgen en voldoende zijn belegd.

RID

Wanneer er bij de Regionale Inlichtingendienst (RID) informatie wordt verstrekt aan andere RID's gebeurt dit door middel van schriftelijke verstrekkingen en/of via BVO, gebruikmakende van labelling.

Proces voor geautomatiseerde verstrekking

Binnen Limburg-Noord is geen sprake van geautomatiseerde verstrekkingen.

Geheimhouding

Bij het verstrekken wordt er gewezen op de daarbij behorende geheimhoudingsplicht. Zowel in de afgesloten convenanten als op de verstekkingsformulieren wordt er gewezen op de geheimhouding conform artikel 7 Wpg.

Protocollering van verstrekkingen

Een werkinstructie is aanwezig met betrekking tot het protocolleren van verstrekkingen. Uitgelegd wordt welke gegevens geprotocolleerd dienen te worden in het I90-formulier.

Er is een procedure voor verstrekkingen in het algemeen opgesteld. De procedure geeft de criteria aan voor artikel 16, 17 en 18 verstrekkingen en voorbeelden van partners die onder deze artikelen worden geschaard.

Tevens wordt aangegeven dat bij artikel 19-verstrekkingen het bevoegde gezag goedkeuring moet geven. Daarnaast wordt een verwijzing gemaakt naar structurele samenwerkingsverbanden als in artikel 20 Wpg.

De procedure bevat een omschrijving van de minimale vereisten die de verstrekker in de protocollering moet vastleggen.

Protocollering in de praktijk

De protocollering van verstrekkingen vindt gedeeltelijk plaats door middel van het invullen van een I90-formulier. Het protocolleren wordt binnen de verschillende lagen van het korps als een te zware last ervaren en leidt tot ergernissen. Hierdoor worden lang niet alle verstrekkingen schriftelijk vastgelegd. Uit verschillende interviews is bovendien geconstateerd dat verstrekkingen niet structureel worden geprotocolleerd middels het gebruik van I90-formulieren.

In het geval van een netwerkoverleg wordt er een algemene mutatie aangemaakt met daarin het gespreksverslag. Vervolgens komt deze mutatie in een I90-formulier te hangen zodat er een algemene verantwoording plaatsvindt.

CIE

Elke verstrekking wordt vastgelegd in een proces-verbaal. Ter beschikking stellen verloopt alleen via een proces-verbaal van de chef. Vooraf peilt deze chef de

behoefte daartoe om te voorkomen dat 'processen-verbaal worden opgemaakt zonder dat tot het opstarten van een (vervolg-) onderzoek wordt overgegaan.

Verstrekkings Veiligheidshuis

De gegevensverstrekking binnen de veiligheidshuizen vindt plaats op grond van de vigerende convenanten. In de applicatie GCOS (geïntegreerde casusoverleg ondersteunende systeem) worden alle verstrekkingen bijgehouden. De betreffende Casemanager kan alleen maar meldingen van zijn casussen zien. GCOS biedt één geautomatiseerde ondersteuning voor casusoverleggen dat ook zal moeten gaan ondersteunen met een ingebouwde zorgvuldigheid. Daarbij zal ook een afwegingproces moeten zijn welke gegevens een professional wel of niet kan delen. GCOS bevindt zich nog in een pilotfase, de logging moet bijvoorbeeld nog worden ingebouwd. Tevens is het nog niet uitgekristalliseerd op welke wijze bewaartermijnen in GCOS geïmplementeerd moeten worden.

Toezicht op verstrekkingen en protocollering

De privacyfunctionaris geeft aan dat het niet uitmaakt op wat voor manier deze vastleggingen dienen te gebeuren, als de vereiste gegevens maar worden ingevuld. Als maar het wat, wanneer en over wie is vastgelegd, dan maakt het de privacyfunctionaris niet uit waarin dit is vastgelegd. De protocollering van de verstrekkingen moet echter wél inzichtelijk zijn.

De privacyfunctionaris voert kwalitatieve steekproeven uit op de geregistreerde verstrekkingen. Tevens monitort de privacyfunctionaris de kwantiteit van de ingevulde verstrekkingen.

4.9.3 Verbeterpunten

Een aantal onderdelen van het korps Limburg-Noord vertoont een structureel gebruik van I90-formulieren. Enkele onderdelen maken nauwelijks gebruik van deze formulieren. Een aandachtspunt voor het korps is om het structureel gebruik van de I90-formulieren in alle korpsonderdelen verder te stimuleren.

4.10 Rechten van betrokkenen (artikel 25/28)

4.10.1

Norm

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

4.10.2

Bevindingen

Inzagerecht

Binnen regio Limburg-Noord laat men de afhandeling van verzoeken tot kennisneming, verbetering, aanvulling, verwijdering of afscherming van politiegegevens over aan medewerkers op de districten die hiermee belast zijn. Deze medewerkers kunnen bij twijfel de privacyfunctionaris of de jurist raadplegen over specifieke verzoeken.

De verzoeken worden door de afdeling post en archief centraal geadministreerd en ter afwerking uitgezet naar de territoriale afdelingen. In 2010 werden op de peildatum 31 januari 2010 totaal 268 verzoeken ontvangen.

Dit proces is vastgelegd en bevat waarborgen dat de aanvragen binnen zes weken en conform de Wpg worden afgehandeld. De privacyfunctionaris houdt een overzicht bij van het aantal verzoeken dat is gedaan. Over 2010 gaat het om de volgende aantallen:

Onderdeel	Aantal
Venlo	93 afgehandeld (12 in behandeling)
Venray	38 afgehandeld (0 in behandeling)
Midden-Limburg	114 afgehandeld (11 in behandeling)

Er zijn in totaal twee klachten ingediend aan de hand van de inzageverzoeken.

Recht op correctie

Uit interviews is gebleken dat de privacyfunctionaris op de hoogte is van de wettelijke vereisten voor afhandeling van de correctieverzoeken van betrokkene.

De medewerkers kunnen bij twijfel de privacyfunctionaris of de jurist raadplegen over correctieverzoeken.

4.10.3 *Verbeterpunten*

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; en
- 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*

Protocollering doel onderzoek

Aan de hand van de afgenomen interviews komt het beeld naar voren dat men bekend is met het feit dat bij korps Limburg-Noord het doel van het onderzoek vastgelegd dient te worden in het formulier 'Melding Recherche Onderzoek' (MRO). De privacyfunctionaris houdt bovendien een overzicht bij van de BVO-registraties. Dit overzicht bevat ook het doel van een onderzoek en de naam van de teamleider van het desbetreffend onderzoek. Het overzicht bevat tevens een controle op de startmutatie. De privacyfunctionaris verricht halfjaarlijkse steekproeven op de protocollering.

Uit het overzicht uit 2011 van de privacyfunctionaris blijkt dat MRO's niet structureel worden ingevuld voor de registratie van een onderzoek. Via e-mail en tijdens werkoverleggen zijn de betreffende onderzoeksleiders hierop gewezen.

Wanneer de MRO's wel zijn ingediend worden de doelen van de onderzoeken vastgelegd. Deze worden gesorteerd op jaartal en zowel bij de privacyfunctionaris als bij de functioneel beheerder van BVO opgeslagen.

Protocollering artikel 13 gegevensverzameling

De gegevensverzamelingen op grond van artikel 13 zijn binnen Limburg-Noord geïdentificeerd. Het korps Limburg-Noord geeft aan geen gebruik te maken van regionale systemen en gegevensverzamelingen buiten de landelijke systemen. De protocollering van de landelijke artikel 13 systemen (zoals HKS) vindt op een landelijk niveau plaats middels standaard protocolformulieren. De protocollering van deze systemen wordt in de systemen aangehouden. Deze (standaard) schriftelijke vastlegging, waaronder 'Schriftelijke vastlegging HKS politie regio Limburg-Noord' bevat de volgende gegevens:

- Begripsbepalingen.
- Doelen van de verwerkingen.
- Toelichting op de verwerkingen.
- De categorieën van personen die verder worden verwerkt.
- De soorten gegevens die verder worden verwerkt.
- Opsomming van de gegevens die landelijk ter beschikking worden gesteld.

Tevens wordt aangegeven of gevoelige gegevens worden verwerkt en wanneer de gegevensverwerking dient te worden beëindigd. Het protocol is ondertekend door de korpsbeheerder.

Bewaren protocolgegevens onrechtmatige handeling

Door de privacyfunctionaris (PF) is onderzoek gedaan naar onrechtmatige of onbevoegde verwerkingen. Hierbij heeft de PF zich gericht op incidenten op het gebied van de privacywetgeving. Incidenten worden gemeld door de taakaccenthouders privacy en informatiebeveiliging of door overige medewerkers. Sommige incidenten zijn door de privacyfunctionaris zelf vastgesteld.

In totaal zijn er 15 incidenten met relevante privacyaspecten gemeld. Veel incidenten zijn te herleiden naar het onbewust onzorgvuldig omgaan met (politie-) informatie. Functioneel beheer is scherp op de controle of bepaalde handelingen wel stroken met de functie van de persoon.

De protocolgegevens van onrechtmatige handelingen worden bewaard door de privacyfunctionaris.

Gemeenschappelijke verwerking

Er zijn geen gemeenschappelijke verwerkingen waarin korps Limburg-Noord participeert.

4.12 Audits (artikel 33)

4.12.1

Norm

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

4.12.2 *Bevindingen*

Interne audit functie

Mr. W.M. Verhoeven-Beckers (senior medewerker juridische zaken / stafafdeling Kabinet) en Dhr. L.J.H. Vrenken (projectcoördinator BOEC) zijn de aangewezen personen om de vereiste jaarlijkse interne audit naar de Wpg te doen.

Er heeft geen interne audit plaatsgevonden bij korps Limburg-Noord. Een plan daartoe is wel opgesteld (conform de gestelde vereisten in artikel 3 lid 4 RPAP), maar de uitvoering heeft echter niet plaatsgevonden. Als reden wordt aangegeven dat op het moment dat men van plan was te starten met de uitvoering van de audit, de externe audit eveneens ging plaatsvinden. Het korps achtte het niet wenselijk om twee audits parallel te laten plaatsvinden. Het korps wacht de resultaten van de externe audit af.

4.13 Privacyfunctionaris (artikel 34)

4.13.1 *Norm*

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

4.13.2 *Bevindingen*

Benoeming en melding

Dhr. Streutjens vervult op verzoek van de Korpsleiding sinds 1 maart 2010 de functie van privacyfunctionaris. Naast zijn werk als privacyfunctionaris is hij ook Hulpofficier van Justitie, Teamleider Explosieven Opruiming, Officier van Dienst en volgt hij een studie (TLL) aan de Politieacademie. De privacyfunctionaris is aangemeld bij het CBP.

Aan de privacyfunctionaris is door de korpsleiding toegang verleend tot alle politiegegevens die er binnen het korps worden verwerkt.

De rol van de privacyfunctionaris

De privacyfunctionaris heeft als taak: Advies, Toezicht en Controle ten aanzien van de Wet politiegegevens. Voor de uitvoering hiervan verricht de functionaris de volgende taken:

- Toezichtstaak. De privacyfunctionaris ziet namens de verantwoordelijke toe op de verwerking van politiegegevens in overeenstemming met het bij of krachtens de Wpg bepaalde.
- Adviestaak. De privacyfunctionaris dient de verantwoordelijke van advies ten aanzien van deze verwerkingen.
- Overzichtstaak. De privacyfunctionaris houdt een overzicht bij van de schriftelijke vastlegging van bepaalde verwerkingsoorten, autorisaties, verstrekkingen en gegevensvergelijkingen.

Overzicht over de protocollering

Periodiek voert de privacyfunctionaris controles uit, bijvoorbeeld middels Cognos om overzicht te verschaffen over de protocollering. Vanaf begin af aan wordt er controle uitgeoefend op BVH I90-verstrekking en I42-adviezen. Sinds 2011 vindt tevens controle plaats op E62-bestuurlijke reportages en E67-rechtshulpverzoeken.

Jaarverslag

De privacyfunctionaris heeft een jaarverslag opgesteld over het jaar 2009-2010 met daarin de bevindingen. Dit jaarverslag is tevens voorgelegd aan de korpsleiding.

Een samenvatting van de bevindingen van de privacyfunctionaris over 2010 volgt hieronder.

Toeziichts- of controletaak

- Er is geen interne audit verricht in 2010 ondanks de verplichting die vanaf 1 januari 2009 van kracht is.
- De nieuwe basisvoorzieningen zijn nog niet geheel toegespitst op de wettelijke eisen waardoor medewerkers bijvoorbeeld de gelegenheid hebben vijf jaar breed te kunnen raadplegen.
- Bovendien is er geconstateerd door de privacyfunctionaris dat logging – een van de maatregelen in het opgestelde document – als instrument nauwelijks is ontwikkeld zodat controle op de correcte toepassing van toegekende autorisaties niet goed mogelijk is.

Adviestaak

- Er zijn diverse adviezen uitgebracht, waaronder de autorisaties voor de nieuwe basisvoorzieningen zoals BVO en BVH. Dit heeft geleid tot intrekking van niet toegestane autorisaties.
- Er is veel aandacht besteed aan voorlichting aan de decentrale taakaccenthouders en andere groepen medewerkers.
- Er is tevens aandacht geschonken aan de inrichting van een intranetsite met informatie op het gebied van de Wet politiegegevens.

Overzichtstaak

- In totaal werden er 57 onderzoeken aangemeld. In 50 gevallen gebeurde dat niet geheel conform de wettelijke voorschriften. Van 43 onderzoeken was er een startmutatie, van 27 onderzoeken een melding recherche onderzoeken (MRO). Slechts 7 onderzoeken doorliepen op correcte wijze het gehele proces.
- Voor de ondersteunende verwerkingen is aangesloten bij het landelijk beleid. De privacyfunctionaris heeft voorlopig gekozen voor handhaving van de bestaande reglementen.
- Er is een regionaal overzicht van autorisaties. De privacyfunctionaris voert daarop één keer in het half jaar een steekproef uit.
- Verstrekkingen aan derden worden gemuteerd in de bronsystemen. Er bestaat geen goed overzicht van de verstrekkingen die gedaan zijn binnen de samenwerkingsverbanden.
- De incidentenregistratie bevat privacy-technische incidenten. In totaal zijn 15 incidenten met privacyaspecten gemeld. Veel van de incidenten zijn terug te leiden naar onbewust onzorgvuldig omgaan met (politie)informatie.

4.14 Functionaris Gegevensbescherming (artikel 36)

De FGB bestaat niet als functie bij het korps Limburg-Noord.