



Ministerie van Veiligheid en Justitie

Audit Wpg politie Limburg-Zuid

Rapport

Datum
Status

6 januari 2012
Definitief

Colofon

Afzendgegevens

Contactpersonen

Projectnaam

Ons kenmerk

Auteurs

Departementale Auditdienst

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

drs. **1** RE CISA
drs. ing. **1** RO CIA

T 070 370 65 60
M wpg@minvenj.nl

Audit Wet Politiegegevens

DDS/5719716/11

1 BEc CISA

Inhoud

Colofon 3

1 Assurance Verklaring 7

2 Samenvatting 9

3 Inleiding 18

3.1 Algemeen 18

3.2 Aanleiding 18

3.3 Doelstelling, aard en scope van de opdracht 18

3.4 Afbakening 19

3.5 Normenkader 19

3.6 Beperkingen voor de privacy audit 20

3.7 Onderzoeksmethoden en werkwijze 20

3.8 Doelgroep van het rapport 20

4 Bevindingen 21

4.1 Inleiding 21

4.2 Verantwoordelijke (artikel 1.f) 22

4.3 Kwaliteitsaspecten van politiegegevens (artikel 3 en 4) 22

4.4 Gevoelige gegevens (artikel 5) 25

4.5 Autorisatie (artikel 6) 26

4.6 Geautomatiseerd Vergelijken/In Combinatie Met Elkaar Verwerken (artikel 11) 28

4.7 Bewaartermijnen (artikel 14) 29

4.8 Ter beschikking stellen (artikel 15) 31

4.9 Verstrekken (artikel 16/24) 32

4.10 Rechten van betrokkenen (artikel 25/28) 34

4.11 Protocolplicht (artikel 32) 35

4.12 Audits (artikel 33) 36

4.13 Privacy functionaris (artikel 34) 37

4.14 Functionaris Gegevensbescherming (artikel 36) 37

1

Assurance Verklaring

In het jaar 2011 heeft de Departementale Auditdienst (DAD) van het ministerie van Veiligheid en Justitie (VenJ) in opdracht van de landelijke stuurgroep implementatie Wpg, waarin de Directeur-Generaal Politie en het Korpsbeheerders Beraad (KBB) zijn vertegenwoordigd, privacy audits op grond van de Wet politiegegevens (Wpg) uitgevoerd naar de verwerkingen die in de Wpg zijn beschreven bij de politiekorpsen. In de maanden november en december 2011 is een privacy audit uitgevoerd bij het korps Limburg-Zuid.

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-Zuid.

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-Zuid, naar de stand van ultimo november 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-Zuid te nemen maatregelen. Ook is gebleken dat het korps Limburg-Zuid voor het volledig kunnen voldoen aan de Wpg eisen mede afhankelijk is van besluiten die buiten het korps Limburg-Zuid 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-Zuid, is, op grond van artikel 4 lid 1 van de Regeling Periodieke Audit Politiegegevens, verplicht binnen drie maanden een verbeterrapport op te stellen waarin de maatregelen worden beschreven die getroffen zijn ter verbetering van de in de privacy audit geconstateerde tekortkomingen. Op grond van artikel 4 lid 3 dient hercontrole plaats te vinden. Wij adviseren deze hercontrole te laten uitvoeren door de interne auditfunctie van het korps Limburg-Zuid. 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 large, stylized handwritten signature in blue ink, consisting of several loops and a long horizontal stroke at the bottom.

J.C. van Praat RE RA

2 Samenvatting

Het korps Limburg-Zuid heeft een aantal zaken in opzet goed opgepakt, zoals de melding van de doelen van onderzoeken, het gebruik van een autorisatiematrix gekoppeld aan het personeelssysteem, de brede aanpak van opleidingen binnen het korps en de gedegen aanpak van verstrekkingen binnen het RIK. De korpsleiding toont hiermee en met andere initiërende activiteiten haar aandacht voor de Wpg.

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

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

Criteria:

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

Norm	Aspect		Bevinding en oordeel
Art. 1.f, Verantwoordelijke			
1.f	Mandaatbesluit		Er is een Mandaatbesluit Wet politiegegevens politieregio Limburg-Zuid d.d. 12 februari 2010, waarin wordt aangetoond dat het bevoegd gezag (plaatsvervangend korpsbeheerder), met terugwerkende kracht tot en met 1 januari 2008, zijn mandaat verleent aan de korpschef van het regionaal politiekorps Limburg-Zuid. Hiermee wordt voldaan aan de Wpg.
Art. 3 en 4, Kwaliteitsaspecten van politiegegevens			
8.1 en 9.1	Onderscheid onderzoek Dagelijkse Politietask (8) versus Bepaald geval (9)		Er zijn criteria opgesteld voor het onderscheid tussen art. 8 en art. 9 onderzoeken. Deze zijn echter niet bij alle betrokkenen bekend. Hiermee wordt deels voldaan aan de Wpg.
3.1 t/m 3.3 (8) 4.1 (8)	Noodzakelijkheid (8) Doelbinding Rechtmatigheid Juistheid Volledigheid		Het korps heeft in diverse procesbeschrijvingen en ander documentatie aangegeven hoe het korps zorg draagt voor de kwaliteitsaspecten van politiegegevens. Er zijn instructies gegeven aan de blauwe medewerkers. De Wpg E-learning module was niet verplicht. Het gebruik van deze module is gemeten. Het korps zal op basis hiervan vervolgvactiteiten opnemen in het te realiseren verbeterplan. 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		Het rechteproces bevat waarborgen voor deze aspecten. De teamleider ziet toe op kwaliteitsaspecten binnen zijn onderzoek. De PDCA-cyclus sluit via het OM en de rechter. Er zijn geen procesbeschrijvingen opgesteld. Hiermee wordt deels voldaan aan de Wpg.

Norm	Aspect		Bevinding en oordeel
	Volledigheid		
3.4 (10 en 12)	Noodzakelijkheid (10 en 12)		Voor de CIE is er een strakke regeling omtrent het omgaan met binnenkomende informatie en het verwerken daarvan in de systemen. De werkwijze staat beschreven in het landelijk CIE proceshandboek. Toezicht op de naleving van de regelgeving door de CIE vindt plaats door de CIE OvJ. Daarnaast voert de teamcoach ook controles uit. Hiermee wordt voldaan aan de Wpg.
4.1 (10 en 12)	Doelbinding Rechtmatigheid Herkomst en wijze van verkrijging Juistheid Nauwkeurig Volledigheid		
4.3	Beveiliging		
Hiermee wordt deels voldaan aan de Wpg.			
Art. 5, Gevoelige Gegevens			
• Gevoelige gegevens			Recent heeft de Hoge Raad een uitspraak gedaan over het gebruik van gevoelige gegevens. Volgens deze uitspraak zou bij gebruik van gevoelige gegevens een rechter commissaris moeten worden betrokken in plaats van een OvJ. Het Landelijk OM heeft de korpsen verzocht de werkwijze nog niet aan te passen tot dat zij de implicaties hiervan heeft afgewogen. Om deze reden zijn er nog geen beschrijvingen of instructies die aangeven hoe men binnen het korps met gevoelige gegevens om dient te gaan. Hiermee wordt niet voldaan aan de Wpg.
Art. 6, Autorisatie			
• Korpsautorisatiematrix			Korps Limburg-Zuid maakt gebruik van een korpsautorisatiematrix. Deze wordt beheerd door de Informatiebeveiligingsfunctionaris. Hiermee wordt voldaan aan de Wpg.
• Aanvraagproces			Personeelszaken maakt een autorisatieaanvraagformulier aan m.b.v. de autorisatiematrix. Dit gaat via de Servicedesk naar functioneel beheer die de autorisaties instelt. Overige autorisaties worden door de leidinggevende gevraagd. Het autorisatieproces staat beschreven in het handboek autorisaties. Hiermee wordt voldaan aan de Wpg.
• Wijziging en verwijdering			Indien een medewerker doorstroomt geeft de leidinggevende dit door via de PMA. Die legt dit neer bij Personeelszaken. De afdeling Personeelszaken maakt een doorstroomformulier op wat naar de informatiebeveiligingsfunctionaris wordt gestuurd. Hij toetst de aanvraag en stuurt deze, indien akkoord, naar functioneel beheer die de autorisaties wijzigt. In geval van uitdiensttreding maakt Personeelszaken

Norm	Aspect		Bevinding en oordeel
			een formulier aan wat via de Servicedesk wordt doorzet naar functioneel beheer die de autorisaties intrekt. In het autorisatie handboek niet beschreven hoe controles worden uitgevoerd. De informatiebeveiligingsfunctionaris voert steekproefsgewijs controles uit op autorisaties. Volgens het ontvangen overzicht zijn op 7 van de 32 systemen controles uitgevoerd. Hiermee wordt deels voldaan aan de Wpg.
	• Autorisatiebeheer CIE en RID.		Autorisaties voor medewerkers van de CIE en RID worden toegekend door het hoofd van de CIE respectievelijk RID. Door de overzichtelijke afdelingen zijn de hoofden goed in staat de autorisaties te beheren. Hiermee wordt voldaan aan de Wpg.
32.1.c	Protocollering autorisaties		Een totaaloverzicht van alle huidige autorisaties wordt gegenereerd door per systeem een overzicht van de autorisaties binnen dat systeem uit te draaien. Hiermee wordt voldaan aan de Wpg.
32.3 voor 32.1.c	Bewaren protocolgegevens autorisaties		De logginggegevens (van mutaties) van autorisaties voor alle systemen blijven bewaard. Ook de historische mutaties, zodat na is te gaan wie wanneer waarvoor geautoriseerd is geweest. Daarnaast zijn per functioneel beheerder de aanvragen en wijzigingsverzoeken uit de mailbox te herleiden. Hiermee wordt voldaan aan de Wpg.
Art. 11, Geautomatiseerd vergelijken en in combinatie zoeken			
	• Hanteerbare interpretatie		Binnen het korps Limburg Zuid is geen uitleg over de begrippen in combinatie met elkaar verwerken en geautomatiseerd vergelijken gepubliceerd. Hiermee wordt niet voldaan aan de Wpg.
	• Aangewezen functionarissen		Het geautomatiseerd vergelijken en in combinatie gebeurt onder verantwoordelijkheid van de onderzoeksleider/bevoegd functionaris door informatierechercheurs. Hiermee wordt voldaan aan de Wpg.
11.4	Bevoegd gezag		In september 2011 heeft het korps afspraken gemaakt met het OM over de afhandeling van verzoeken voor het in combinatie verwerken. De bevoegd functionarissen zijn door het hoofd tactiek geïnstrueerd dat alleen in combinatie mag worden verwerkt nadat zij hiervan schriftelijke toestemming van de bevoegd functionaris hebben ontvangen. Deze afspraken zijn nog niet schriftelijk vastgelegd in de een procesbeschrijving of vuistregels voor bevoegd functionarissen. Hiermee wordt deels aan de Wpg
32.1.d en 32.1.h	Protocollering 11.1, 11.2, 11.4 en 11.5		Het bevoegd gezag geeft schriftelijk toestemming om in combinatie te verwerken. Dit wordt vastgelegd binnen het onderzoek. De

Norm	Aspect	Bevinding en oordeel
		privacyfunctionaris wordt nog niet geïnformeerd over deze verwerkingen. Hierdoor kan de privacyfunctionaris niet identificeren voor welke onderzoeken in combinatie wordt verwerkt en kan hiermee nog onvoldoende effectief toezicht te houden. 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	De artikel 11 verwerkingen zijn nog niet inzichtelijk voor de privacyfunctionaris. Hiermee wordt niet voldaan aan de Wpg.
Art. 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 Zuid-6-verband geadviseerd de nieuwe functionaliteiten in BVH niet te activeren. De korpsbeheerder en korpsleiding hebben zich aan het landelijke standpunt geconformeerd. Hiermee wordt niet voldaan aan de Wpg.
8.6	(8) verwijderen na 5 jaar	Doordat gegevens uit Xpol in BVH zijn overgezet, bevat BVH gegevens die ouder zijn dan 5 jaar. 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	Doordat gegevens uit Xpol in BVH zijn overgezet, bevat BVH gegevens die ouder zijn dan 5 jaar. 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 krijgt afloopberichten van het lokale OM. Alle ontvangen afloopberichten worden conform de Wpg verwerkt. De betreffende artikel 9 onderzoeken worden hiermee verwijderd. Voor zaken die in hoger beroep worden behandeld komt van uit het OM geen afloopbericht binnen. De verwijderingsperiode is hierdoor voor deze onderzoeken niet eenduidig vast te stellen. Hiermee wordt deels voldaan de Wpg.
14.1 (9)	(9) vernietigen na 5 jaar verwijderd	Er is nog veel onduidelijkheid rondom het opschonen van artikel 9 onderzoeken. Hierbij is de ketensamenwerking en specifiek de overdracht van Informatie over afgesloten zaken van OM naar de politie een aandachtspunt. Hiermee wordt niet voldaan aan de Wpg.
10.6	(10) verwijderen na 5 jaar geen subjectwaardige registratie	Bij de RID wordt niet voldaan aan de eisen op het gebied van bewaartermijnen. Hoewel de BVO de CIE niet ondersteund bij het verwijderen, wordt dit handmatig verzorgd. Hiermee voldoet de CIE wel. Hiermee wordt deels voldaan de Wpg.
14.1 (10)	(10) vernietigen na 5 jaar verwijderd	Bij de RID wordt niet voldaan aan de eisen op het gebied van bewaartermijnen. Hoewel de BVO de CIE niet ondersteund bij het verwijderen, wordt dit

Norm	Aspect		Bevinding en oordeel
			handmatig verzorgt. Hiermee voldoet de CIE wel. Hiermee wordt deels voldaan de Wpg.
14.3	Hernieuwde verwerking		In september 2011 heeft het korps afspraken gemaakt met het OM over de afhandeling van verzoeken voor hernieuwde verwerkingen. De bevoegd functionarissen en functioneel beheerders zijn geïnstrueerd dat gegevens alleen hernieuwd mogen worden verwerkt na schriftelijk goedkeuring van het OM. De afspraken met de functioneel beheerders zijn nog niet schriftelijk vastgelegd in een procesbeschrijving of werkafpraak. Hiermee wordt deels voldaan aan de Wpg.
32.1.e	Protocollering 14.3		De schriftelijke toestemming wordt vastgelegd binnen het betreffende onderzoek. De privacyfunctionaris wordt nog niet geïnformeerd over alle hernieuwde verwerkingen. Hierdoor kan de privacyfunctionaris niet identificeren voor welke onderzoeken hernieuwd wordt verwerkt en kan hiermee nog onvoldoende effectief toezicht te houden. Hiermee wordt niet voldaan aan de Wpg.
32.3 voor 32.1.e	Bewaren protocolgegevens 14.3		De schriftelijke toestemming wordt vastgelegd binnen het betreffende onderzoek. De privacyfunctionaris wordt nog niet geïnformeerd over alle hernieuwde verwerkingen. Hiermee wordt niet voldaan aan de Wpg.
12.2	(12) verwijderen na 4 maanden		Het omzetten van bruto naar netto informatie gebeurt binnen 4 maanden, maar meestal al binnen 2 weken. Hierop wordt toegezien bij het ter beschikking stelling van informatie. Hiermee wordt voldaan aan de Wpg.
12.6	(12) controleren en vernietigen		Binnen de CIE wordt regelmatig gecontroleerd en geschoond. Bij de RID worden de nalevingstermijnen niet goed nageleefd. Hiermee wordt deels voldaan de Wpg.
Art. 15, Ter beschikking stellen			
• Infodesk voor bevraging			De infodesk deelt alleen artikel 8 en artikel 13 informatie. Informatie over artikel 9 en 10 wordt via de bevoegd functionaris ter beschikking gesteld. Hiermee wordt voldaan aan de Wpg.
• Codering			Codering wordt alleen gebruikt binnen de CIE. Voor Art. 9 onderzoeken wordt geen gebruik gemaakt van codering, maar deze informatie wordt altijd via de bevoegd functionaris ter beschikking gesteld. Hiermee wordt voldaan aan de Wpg.
• Aanwijzing Bevoegd Functionaris			Er is een aanwijzingbesluit bevoegd functionarissen waarmee de bevoegd functionarissen op basis van functie zijn aangewezen. Hiermee wordt voldaan aan de Wpg.
• Opleiding Bevoegd Functionaris			De bevoegd functionarissen hebben de opleiding bevoegd functionaris gevolgd bij de Politieacademie en bij een extern bureau.

Norm	Aspect		Bevinding en oordeel
			Hiermee wordt voldaan aan de Wpg.
15.2	Weigeringgronden		In de opleiding bevoegd functionaris is aandacht gegeven aan de wettelijke weigeringsgronden in relatie tot de verplichting tot het delen van informatie. Hiermee wordt voldaan aan de Wpg
Art. 16 t/m 24, Verstrekking			
	• Verstrekkingenwijzer (landelijk)		De landelijke verstrekkingenwijzer is bekend en wordt breed gehanteerd. Er is een lokaal handboek verstrekkingen opgesteld met gedetailleerde afspraken. Hiermee wordt voldaan aan de Wpg.
	• Proces voor convenanten		Er is een beschreven proces voor het opstellen en goedkeuren van convenanten. Het korps maakt hierbij gebruik van een speciaal ontwikkelde template. De convenanten zijn te vinden op het intranet. Het proces van uitgifte van convenanten wordt uitgevoerd door de privacyfunctionaris. Op 13 juli 2011 heeft de korpschef een notitie uitgebracht over de verstrekking van politiegegevens aan het RIEC. Deze notitie heeft geleid tot onduidelijkheid binnen onder andere de infodesk. Op basis van de notitie zou de impressie kunnen ontstaan dat gegevens verstrekt moeten worden zonder dat de verstrekking afdeling een controle uitvoert op doelbinding. Dit laatste is binnen de Wpg niet mogelijk. Hiermee wordt deels voldaan aan de Wpg.
	• Proces voor Art. 20 Besluiten		Artikel 20 besluiten zijn opgenomen in het convenantenproces. Hiermee wordt voldaan aan de Wpg.
	• Verstrekkingenschema (regio)		Eind 2010 is men binnen Limburg-Zuid begonnen met het inventarisatie van de afdelingen die Informatieverzoeken afhandelen. Deze inventarisatie is nog niet vertaald in een lijst met afspraken wie welke informatie verzoeken binnen het korps afhandelt. Verschillende afdelingen binnen het korps houden zich bezig met verstrekkingen, zonder van elkaars activiteiten op de hoogte te zijn. Hierdoor zouden op den duur conflicterende werkwijzen kunnen ontstaan en is er geen centraal overzicht van gedane externe verstrekkingen. Het korps heeft dit punt onderkent en is voornemens dit in 2012 inzichtelijk te maken. Hiermee wordt niet voldaan aan de Wpg.
	• Proces voor geautomatiseerde verstrekking		Er zijn geautomatiseerde verstrekkingen geïdentificeerd. Zo heeft het korps onder andere vanuit het Ministerie van Veiligheid en Justitie de verplichting gekregen om gegevens geautomatiseerd te verstrekken voor bijvoorbeeld JCO-J. Het korps heeft geen proces of registratie

Norm	Aspect		Bevinding en oordeel
			voor geautomatiseerde verstrekkingen. Hierdoor is het binnen het korps niet inzichtelijk welke gegevens geautomatiseerd worden verstrekt en is periodieke controle niet mogelijk. Hiermee wordt niet voldaan aan de Wpg
7.2	Geheimhouding		Zowel bij het opstellen van convenanten als bij elke verstrekking vanuit de infodesk wordt de ontvanger gewezen op de geheimhoudingsplicht. Hiermee wordt voldaan aan de Wpg
32.1.f	Protocollering verstrekking		De verstrekkingen die worden gedaan door de infodesk worden conform de afspraken vastgelegd in de infodeskmodule. Het handboek verstrekkingen beschrijft de protocolleringsprocedure voor de medewerker "blauw". Hiermee voldoet het korps in opzet aan de Wpg. Op de werkvloer is men zich hier niet altijd van bewust of worden hiervoor andere systemen of methoden gebruikt dan beschreven. Door de ontbrekende vastlegging of de vastlegging in verkeerde systemen is geen centraal overzicht van alle gedane verstrekkingen beschikbaar voor de privacyfunctionaris. Hiermee wordt deels voldaan aan de Wpg
32.3 voor 32.1.f	Bewaren protocolgegevens verstrekking		Indien protocolgegevens in de hiervoor bedoelde systemen worden bewaard (BVO, BVH), worden de gegevens bewaard conform de bewaartermijnen. Hiermee wordt voldaan aan de Wpg.
• Toezicht door leidinggevenden op verstrekkingen en protocollering			Op de afdelingen die verantwoordelijk zijn voor het merendeel van de verstrekkingen wordt toegezien op de correcte vastlegging van verstrekkingen. In het veld wordt niet altijd toegezien op goede vastlegging van de verstrekkingen. Hiermee wordt deels voldaan aan de Wpg.
Art. 25 t/m 31, Rechten van de betrokkene			
25.1	Verzoek om kennisgeving		Er is een procesnota 'rechten van betrokkene' waarin is beschreven hoe wordt omgegaan met de rechten van betrokkene. De nota wordt door de privacyfunctionaris gebruikt. Hiermee wordt voldaan aan de Wpg.
28.1 t/m 28.3	Correctie		procesnota 'rechten van betrokkene' beschrijft hoe het korps verzoeken tot correctie afhandelt. In de procesnota is artikel 30 echter buiten beschouwing gelaten. Hierdoor is niet inzichtelijk hoe externe partners op de hoogte worden gebracht van gewijzigde of onjuiste gegevens. De eerder genoemde knelpunten bij verstrekkingen vormen tevens knelpunten voor de uitvoering van artikel 30. Hiermee wordt deels voldaan aan de Wpg.
Art. 32, Protocolplicht (32.1.c, d, e, f en h behandeld bij thema's)			
9.2 en 32.1.a	Protocollering doel onderzoek		Het korps heeft duidelijke afspraken over de melding van art 9 onderzoeken. Deze afspraken worden in de praktijk controleerbaar uitgevoerd.

Norm	Aspect		Bevinding en oordeel
			Hiermee wordt voldaan aan de Wpg.
32.3 voor 32.1.a	Bewaren protocolgegevens doel onderzoek		De protocolgegevens worden in ieder geval bewaard tot na de externe audit. Hiermee wordt voldaan aan de Wpg.
13.4 en 32.1.b	Protocollering Art. 13 gegevensverzameling en		Het korps heeft op 27 oktober 2011 tien protocollen voor landelijke artikel 13 systemen ontvangen van expertgroep politiegegevens en privacy. Deze zullen korps specifiek worden gemaakt en binnen het korps geïmplementeerd. Daarnaast heeft het korps een lijst van mogelijke artikel 13 gegevensverzamelingen van de infodesk ontvangen. Deze lijst is nog gevalideerd. De privacyfunctionaris heeft hiermee nog geen complete lijst met de artikel 13 gegevensverzamelingen binnen Limburg-Zuid. Hiermee wordt niet voldaan aan de Wpg.
32.3 voor 32.1.b	Bewaren protocolgegevens Art. 13 gegevensverzameling en		Het korps heeft geen overzicht van de aanwezige artikel 13 gegevensverzamelingen. Hiermee wordt niet voldaan aan de Wpg.
32.1.g	Protocollering onrechtmatige handeling		Bureau Interne Zaken meldt onrechtmatige verwerkingen aan de privacyfunctionaris. De privacyfunctionaris komt zelf geen onrechtmatige verwerkingen tegen. Hiermee wordt voldaan aan de Wpg.
32.3 voor 32.1.g	Bewaren protocolgegevens onrechtmatige handeling		Bureau Interne Zaken meldt onrechtmatige verwerkingen aan de privacyfunctionaris. De privacyfunctionaris komt zelf geen onrechtmatige verwerkingen tegen. Hiermee wordt voldaan aan de Wpg.
32.2	Gemeenschappelijke verwerking		Wij hebben geen gemeenschappelijke verwerkingen aangetroffen.
Art. 33, Audits			
RPAP 3.1	Interne audit-functie		Het korps heeft een interne Wpg auditor aangesteld en opgeleid. Hiermee wordt voldaan aan de Wpg.
RPAP 3.4	Interne audit-plan		Er is een intern auditplan opgesteld en de benodigde capaciteit was ingepland voor een audit. Hiermee wordt voldaan aan de Wpg.
RPAP 3.6	Interne audit-rapport		Gelet op de op landelijk niveau gehouden discussies ten aanzien van de impact Wpg op de Nederlandse Politie binnen de Raad van Korpschefs alsmede met het CBP en het Ministerie Van Veiligheid en Justitie is er een advies uitgebracht geen interne audit uit te voeren. Het korps heeft dit advies opgevolgd en de interne audit is uiteindelijk niet uitgevoerd, waardoor er geen intern audit rapport beschikbaar is. Hiermee wordt niet voldaan aan de Wpg.
Art. 34, Privacyfunctionaris			
34.1 en 34.4	Benoemd en gemeld		Het korps heeft een privacyfunctionaris benoemd en aangemeld bij het CBP. Hiermee wordt voldaan aan de Wpg.

Norm	Aspect		Bevinding en oordeel
34.2	Overzicht over protocollering		De privacyfunctionaris heeft inzicht in de verschillende geprotocolleerde gegevens en gebruikt deze bij zijn toezichthoudende taak. Hiermee wordt voldaan aan de Wpg.
34.3	Jaarverslag		Het korps heeft over 2010 geen jaarverslag opgesteld. De huidige privacyfunctionaris bekleedt deze functie sinds eind 2010. De privacyfunctionaris heeft beperkt tijd voor zijn controle taken vanwege nevenverplichtingen. Hiermee wordt niet voldaan aan de Wpg.
Optioneel Art. 36, Functionaris Gegevensbescherming			
36.1 en 36.2	Benoemd		Niet van toepassing. Er is geen functionaris gegevensbescherming benoemd zoals beschreven in de WBP.
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-Zuid 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-Zuid in de maanden oktober en november 2011.

3.2 Aanleiding

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

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

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

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

3.3 Doelstelling, aard en scope van de opdracht

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

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 november 2011, van maatregelen en procedures, waarmee het

politiekorps Limburg-Zuid beoogt te voldoen aan de beheersdoelstellingen die bij of krachtens de Wpg gelden.

Binnen deze audit richten wij ons (conform de artikelen van de Wpg) op de volgende thema's:

- Noodzakelijkheid, rechtmatigheid en doelbinding (artikel 3)
- Juistheid, volledigheid en beveiliging politiegegevens (artikel 4)
- Gevoelige gegevens (artikel 5)
- Autorisaties (artikel 6)
- Geautomatiseerd vergelijken en in combinatie verwerken (artikel 11)
- Bewaartermijnen (artikel 14)
- Ter beschikking stellen van politiegegevens (artikel 15)
- Verstrekkingen (artikel 16 t/m 24)
- Rechten van betrokkenen (artikel 25 t/m 31)
- Protocolplicht (artikel 32)
- Audits (artikel 33)
- Privacyfunctionaris (artikel 34)
- Functionaris gegevensbescherming (artikel 36)

Deze audit richt zich op de opzet, het bestaan en waar mogelijk, de werking van de implementatie van de Wpg per politiekorps. Pas wanneer wij, tijdens het uitvoeren van de audit bij een politiekorps, hebben geconstateerd dat de opzet en het bestaan aan de daaraan te stellen eisen voldoen voeren wij aanvullende werkzaamheden uit om de werking vast te stellen.

3.4 Afbakening

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

3.5 Normenkader

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

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

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

3.6 Beperkingen voor de privacy audit

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

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

3.7 Onderzoeksmethoden en werkwijze

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

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

Wij hebben onze werkzaamheden uitgevoerd in de periode van 7 november 2011 tot en met 29 december 2011.

Het conceptrapport met bevindingen is op 5 januari besproken met de korpschef van het korps Limburg-Zuid en wordt aan de korpsbeheerder aangeboden. 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. ¹

mr. ¹ neemt namens DG Politie deel aan de stuurgroep.

drs. ¹ neemt namens het KBB deel aan de stuurgroep.

De specifieke doelgroep waarvoor het rapport is bestemd bestaat uit:

- Onze opdrachtgever zoals bovengenoemd.
- De korpsbeheerder dhr. O. Hoes korpsbeheerder Politie Limburg-Zuid.
- De korpschef drs. G.J. Veldhuis, korpschef Politie Limburg-Zuid.
- De Hoofd Officier van Justitie mr. J. Penn - te Strake Hoofdofficier van Justitie, Arrondissement Maastricht.
- De privacyfunctionaris dhr.L.Wassercordt, Politie Limburg-Zuid.
- De voorzitter van het College Bescherming Persoonsgegevens

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

Voor de implementatie van de Wpg heeft het korps Limburg-Zuid geparticipeerd binnen samenwerkingsverband "Zuid Zes". Dit samenwerkingsverband heeft gezamenlijk een productenmatrix opgesteld, waarin de te implementeren Wpg producten waren geïnventariseerd. Op basis van dit document is een impactanalyse gemaakt voor Limburg-Zuid. De impactanalyse bevat 14 onderdelen die binnen de het korps moesten worden ingevoerd. Om deze onderdelen daadwerkelijk binnen het korps op te zetten is het implementatie kernteam opgericht, waarin ca. 10 medewerkers deelnamen. In dit team zaten onder andere de privacyfunctionaris, de functionaris gegevensbeveiliging, applicatiebeheerders en een juridisch adviseur. Het implementatie kernteam kwam gemiddeld een keer per maand bij elkaar. Dit was mede afhankelijk van de ontwikkelingen.

Om de activiteiten van het implementatie team te leiden is een PID opgesteld. In het PID staat beschreven waar men zich in eerste instantie op ging richten. Om daar sturing aan te geven kwam de projectgroep wekelijks bij elkaar en gaf daarover terugkoppeling aan de proceseigenaar informatie. Vanuit de regio werd gekeken wat de regionale consequenties waren. Als daar niet een lijn in was, dan werd dat opgeschaald naar zuid zes niveau of naar het landelijke projectleideroverleg. Besluitvorming vond vervolgens in het korps plaats.

Algemene aandachtspunten die bij de audit binnen Politie Limburg-Zuid naar voren zijn gekomen zijn:

- Hoewel in opzet veel aspecten door het implementatieteam zijn ontwikkeld ontbreekt het in bepaalde gevallen aan de uitrol richting de werkvloer. De medewerkers zijn door middel van de trainingen en communicatie op de hoogte van de Wpg maar hebben minder kennis van afspraken die specifiek binnen het korps zijn gemaakt. Denk hierbij aan afspraken over het protocolleren van vertrekkingen of het onderscheid tussen artikel 8 en artikel 9.

4.1.2 *Bekendheid met de Wpg binnen de organisatie*

Voor opleidingen is Limburg-Zuid aangesloten bij Brabant Midden en West. Het train de trainer concept is binnen het korps gehanteerd. Hierbij hebben de trainers de taak met presentaties hun kennis te verspreiden. De opleiding (door de regionale trainers) van nieuwe medewerkers is geborgd via de afdeling personeelszaken. Als iemand van functie wijzigt, dan zorgt de afdeling personeelszaken dat hiervoor een Wpg training wordt verzorgd. In de aspiranten opleiding vanuit de Politieacademie is de Wpg nog niet meegenomen. Om de Wpg landelijk effectief te implementeren zou dit wel moeten.

Vanuit de projectgroep zijn de eenheden bezocht en is voorlichting gegeven, ook aan de hand van documentatiemateriaal uit het land. De praktijkvoorbeelden spreken daarbij meer tot de verbeelding dan de theorie. Ook heeft men een e-learning traject laten uitvoeren door alle medewerkers, met daaraan gekoppeld een cursus waar iedereen voor was uitgenodigd. Als daar behoefte aan is dan wordt het kernteam nog steeds door teamchefs verzocht om voorlichting te geven, bijvoorbeeld voor nieuwe agenten. Wpg zit nog niet in het aanbod van de politieacademie. Omdat kennis op den duur zou kunnen wegzakken wordt verwezen naar de infodesk omdat daar de professionals zitten die er dagelijks mee bezig zijn. Daar kunnen medewerkers met hun vragen terecht.

4.1.3 *Wpg en de praktijk*

In de praktijk heeft men veel last van de applicaties die onvoldoende ondersteunen bij het uitvoeren van de Wpg. Het kost veel moeite om een aantal zaken handmatig op te pakken.

Ook het achterblijven van de afloopberichten vanuit het OM maakt een goede uitvoering van de Wpg zeer lastig. Zolang dit probleem niet wordt aangepakt is het correct afhandelen van artikel 9 onderzoeken praktisch niet mogelijk. De afhankelijkheid van andere instanties maakt dat Limburg-Zuid in een aantal gevallen een minder positief oordeel heeft gekregen dan het korps op basis van de eigen initiatieven had gewenst.

4.2 Verantwoordelijke (artikel 1.f)

Mandaatbesluit

4.2.1 *Norm*

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

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

4.2.2 *Bevindingen*

Er is een Mandaatbesluit Wet politiegegevens politieregio Limburg-Zuid d.d. 12 februari 2010, waarin wordt aangetoond dat het bevoegd gezag (plaatsvervangend korpsbeheerder), met terugwerkende kracht tot en met 1 januari 2008, zijn mandaat verleent aan de korpschef van het regionaal politiekorps Limburg-Zuid. Daarnaast is er ook een Ondermandaatbesluit Wet politiegegevens politieregio Limburg-Zuid d.d. 9 februari 2010, waarin de korpschef van Limburg-Zuid ondermandaat verleent aan o.a. de chefs van de Districten, de privacyfunctionaris, Divisies en Stafafdeling Bedrijfsvoering. Het korps is voornemens bij de vorming van Nationale Politie de mandatering aan te passen.

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**

Als medewerkers op een juiste manier willen verwerken is het van belang dat zij het onderscheid kunnen maken tussen artikel 8 en 9 gegevensverzamelingen. Korps Limburg-Zuid heeft criteria opgesteld om het onderscheid tussen artikel 8 en artikel 9 onderzoeken duidelijk te maken. Deze informatie is voor de medewerkers te vinden op intranet (PILZ). Medewerkers zijn ervan op de hoogte dat er een onderscheid is. Zij hebben echter moeite met het benoemen van de criteria van onderscheid. Hiermee wordt in opzet voldaan.

Opleiding

In samenspraak met de Wpg projectleider heeft de privacyfunctionaris een verdeling gemaakt van de eenheden voor het geven van een Wpg instructie. Alle medewerkers hebben een dagdeel opleiding gehad in het eerste half jaar van 2011. Hierbij is echter de afdeling Casescreeening en Werkvoorbereiding overgeslagen. De privacyfunctionaris is nu op eigen initiatief bezig met een opfriscursus. De privacyfunctionaris probeert nieuwe medewerkers ook te instrueren door als er voldoende nieuwe medewerkers zijn een Wpg-bijeenkomst te organiseren. De privacyfunctionaris verzorgt ook zelf de interne opleiding voor het RIK en LIK. De bevoegd functionarissen hebben allen een opleiding bevoegd functionaris gevolgd bij de Politieacademie en een certificaat ontvangen. Een aantal medewerkers heeft de e-learning opleiding Wpg gevolgd, deze was echter niet verplicht. Het gebruik van deze module is gemeten. Mede op basis van deze informatie zal het korps vervolgvactiteiten opnemen in het te realiseren verbeterplan.

Borging van de kwaliteitsaspecten art. 8 en 9

Het korps heeft in diverse procesbeschrijvingen en ander documentatie aangegeven hoe het korps zorg draagt voor de kwaliteitsaspecten van politiegegevens bij het gebruik tijdens de dagelijkse politietaak. De uiteindelijke verantwoordelijkheid voor de correctheid van de gegevens ligt bij de invoerder en vervolgens bij de lijn. Korps Limburg-Zuid maakt gebruik van Trueblue om de kwaliteit van vastleggingen te bevorderen. Via Trueblue krijgen medewerkers geautomatiseerd een melding als een ingevoerde registratie onjuist is vastgelegd.

Ondanks dit controlemechanisme staan er nog veel dubbele registraties in BVH. Momenteel wordt er geen actie ondernomen om deze dubbele registraties weg te werken. Dit wordt gezien als onbegonnen werk zolang de invoer aan de voorkant niet beter geregeld wordt. Hier zou strakker toezicht op moeten komen van de leidinggevend. De leidinggevend geven aan dat ze de kwaliteit van de vastleggingen controleren. Ze lezen regelmatig processen verbaal en na de sturingsbijeenkomsten, waarbij de dagrapporten worden doorgenomen, vindt terugkoppeling plaats naar de medewerkers indien de vastlegging niet op orde is. Leidinggevend kunnen zelf lijsten uit BVH uitdraaien om toezicht te houden op de kwaliteit van vastleggingen. Een ander controlemiddel is dat de leidinggevende een akkoord moet geven voordat de registratie van een medewerker afgesloten wordt.

Binnen Blauw sturen leidinggevend op de informatie die medewerkers in de systemen vastleggen. De kwaliteit moet goed zijn en het woordgebruik professioneel. Dit doen zij niet zozeer onder de vlag van de Wpg, maar onder die van integriteit. Integriteit is een terugkomend item zowel in het afdelingsoverleg als in de ontwikkelgesprekken.

Er zijn geen specifieke vuistregels opgesteld voor opsporing betreffende de rechtmatigheid, doelbinding, noodzakelijkheid, volledigheid en juistheid van gegevens naar aanleiding van de invoering van de Wpg. Van nature besteedt een rechercheur echter veel aandacht aan de herkomst, rechtmatigheid en

nauwkeurigheid van politiegegevens alvorens deze te gebruiken voor opsporingsactiviteiten. Voor Opsporing is het belangrijk dat een zaak later niet stukloopt op procedurefouten. De dwingende kracht hierbij komt onder andere van de advocaten die op zoek zijn naar procedurefouten. De eisen uit artikel 3, 4 en 5 worden daarom streng in de gaten gehouden door de leider van het onderzoek. De afdeling "Casescreening & Werkvoorbereiding" heeft hierbij een controlerende rol en beoordeelt de dossiers. De bevoegd functionarissen hebben allen een opleiding bevoegd functionaris gevolgd bij de Politieacademie en een certificaat ontvangen.

Binnen de werkprocessen is in feite een gesloten PDCA-cyclus. Het onderzoek leidt tot een procesdossier, dat wordt overhandigd aan het OM. Tijdens de zitting wordt het procesdossier getoetst door de rechter. Indien deze constateert dat de kwaliteitsaspecten niet strikt zijn geborgd, zal deze de zaak afwijzen. OM koppelt dit terug naar Opsporing, waarop de interne werkprocessen worden verbeterd.

Borging van de kwaliteitsaspecten art. 10

Voor de CIE is er een strakke regeling omtrent het omgaan met binnenkomende informatie en het verwerken daarvan in de systemen. De werkwijze staat beschreven in het landelijk CIE proceshandboek Het brutoverslag wordt in een afgeschermd deel van BVO verwerkt. Een deel van BVO bruto wordt overgezet naar de BVO netto bak. Bij de RID wordt op soortgelijke manier met bruto en netto informatie gewerkt. In de BVO bruto en netto bak wordt met een informantcode gewerkt. De vertalingtabel ligt in een kluis. Toezicht op de naleving van de regelgeving door de CIE vindt plaats door de CIE OvJ. Deze voert controles uit op de dossiers van de informanten en subjecten. Daarnaast voert de teamcoach ook controles uit. Binnen de RID worden deze controles niet uitgevoerd.

De infodesk toetst de identiteit van de aanvrager door het e-mailadres of telefoonnummer te controleren. Indien dit niet kan en de aanvrager onbekend is wordt het DE-nummer (personeelsnummer) gecontroleerd of wordt er contact opgenomen met de lijnchef. Infodeskmedewerkers zijn geïnstrueerd om bij informatieverzoeken te vragen naar het doel waarvoor de gegevens zullen worden gebruikt. Indien uit een informatieaanvraag niet te herleiden is waarvoor de gegevens gebruikt gaan worden, wordt contact opgenomen met de aanvrager. Het RIK deelt of verstrekt geen informatie uit artikel 9 of 10 verzamelingen. Het RIK is wel in staat op basis van hit/ no hit te zien of deze gegevens aanwezig zijn. Het is niet mogelijk om alle informatie te controleren die door de infodesk wordt gebruikt, maar in bepaalde gevallen (zoals bij dubbele registraties of namen) wordt dit teruggekoppeld aan de functionaris die verantwoordelijk is voor de kwaliteit van het specifieke district.

Beveiliging

De mappenstructuur is Wpg-compliant ingericht. Er is specifieke autorisatie nodig om toegang tot mappen te krijgen. Hierdoor kunnen medewerkers over het algemeen alleen bij de mappen van hun eigen afdeling of unit. Eventuele artikel 9 of 10 gegevens zijn hierdoor niet breed toegankelijk. Landelijke applicaties, zoals BVH, zijn nog niet Wpg-proof. Een aantal systemen voorzien nog niet in de afscherming van artikel 9 gegevens en ondersteunen nog niet bij het verwijderen en vernietigen. Een aantal van deze systemen zoals Integrale Bevraging (zoeksysteem), waarschuwen wel al als gegevens hadden moeten worden vernietigd. In IB worden gegevens ouder dan 5 jaar in het rood weergegeven.

De infodesk verstuurt informatie via de beveiligde verbindingen van VTSPN. Als de informatie naar externen wordt verstuurd, moet er naast de firewall aan de VTSPN kant, ook een firewall aan de kant van de externe zijn, anders worden gegevens niet

over de lijn verstuurd. De meldkamer heeft een eigen netwerk. Hier zit een zware beveiliging op. Het systeem wordt beheerd door een samenwerkingsverband uit rood, wit en blauw. De veiligheidsdirectie heeft hierover de leiding. De RID en CIE hebben ook een eigen systemen/netwerken om informatie op te slaan. Er zijn geen lijnen naar buiten. Het netwerk wordt beheerd door henzelf, alleen de hardware wordt aangesloten door functioneel beheer.

De RID en CIE zitten in fysiek afgesloten ruimte. Alleen de RID- en CIE-medewerkers beschikken over een toegangspas en sleutel. Bezoekers worden niet alleen gelaten en worden alleen binnengelaten als er geen informatie meer in het zicht ligt.

Het korps is verantwoordelijk voor beveiliging van al haar gegevens. Ook als de systemen waarin deze gegevens zijn opgeslagen niet door het korps zelf worden beheerd. De systemen in de meldkamer worden beheerd door de veiligheidsdirectie. Het is van belang dat er afspraken worden gemaakt met de veiligheidsdirectie over de omgang met de politiegegevens. Hierbij kan men denken aan afspraken over screening van de medewerkers en toegang tot de gegevens. Het korps is momenteel bezig met het ontwikkelen van een bewerkers overeenkomst.

4.3.3

Verbeterpunten

Als verbeterpunten zijn te noemen:

- Er zijn criteria voor het onderscheid tussen artikel 8 en artikel 9 onderzoek. Deze zijn echter niet breed bekend binnen het korps. Zorg dat deze criteria binnen het korps worden gecommuniceerd.
- Voor de opleidingen is het korps afhankelijk van inzet en alertheid van de Privacyfunctionaris. Zorg voor een gestructureerde aanpak van opleiding van nieuwe medewerkers die niet afhankelijk is van de inspanning van één persoon.
- Zorg ervoor dat de kennis die per medewerkergroep nodig is geïnventariseerd wordt en zorg voor structurele aandacht voor de kennis van de Wpg binnen het afdelingen. Hiervoor kan onder andere gebruik worden gemaakt van praktijk casussen.
- Motiveer VtsPN op landelijk niveau om alle landelijke applicaties aan de Wpg te laten voldoen.

4.4 Gevoelige gegevens (artikel 5)

4.4.1

Norm

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

4.4.2

Bevindingen

Uit de interviews blijkt dat gevoelige gegevens alleen worden genoteerd als dit onvermijdelijk is voor het doel. Met name de RID en CIE hebben hiermee te maken. Er zijn geen niet-toegestane gegevensverzamelingen gebaseerd op gevoelige gegevens aangetroffen. Recent heeft de Hoge Raad een uitspraak gedaan over het gebruik van gevoelige gegevens. Bij de toepassing zou een rechter commissaris moeten worden betrokken in plaats van een OvJ. Het Landelijk OM heeft het korps verzocht de werkwijze nog niet aan te passen tot dat de zij de implicaties hiervan heeft afgewogen. Om deze reden zijn er nog geen beschrijvingen of instructies die aangeven hoe men met gevoelige gegevens om dient te gaan.

4.4.3 *Verbeterpunt*

Als verbeterpunt is te noemen:

- Stel na afstemming met het Landelijk OM procesbeschrijvingen op hoe men binnen het korps dient om te gaan met gevoelige gegevens.

4.5 Autorisatie (artikel 6)

4.5.1 *Norm*

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

4.5.2 *Bevindingen*

Autorisatiematrix

Het korps Limburg-Zuid beschikt over een korpsautorisatiematrix die ongeveer twee jaar geleden is opgesteld naar aanleiding van de implementatie van de Wpg. Deze autorisatiematrix wordt beheerd door de informatiebeveiligingsfunctionaris. Hij en de privacyfunctionaris zijn verantwoordelijk voor het onderhoud van de matrix. De autorisatiematrix heeft een koppeling met het personeelsregistratie systeem Beaufort.

Autorisatieproces

Uit de interviews blijkt dat medewerkers bekend zijn met de stappen die ondernomen moeten worden om tot een autorisatie te komen. Indien er nieuwe medewerkers in dienst komen, maakt Personeelszaken een autorisatieaanvraagformulier aan. Zij maken hierbij gebruik van de autorisatiematrix door te kijken welke autorisaties voor de functie nodig zijn. Personeelszaken stuurt dit formulier naar de Servicedesk van vtsPN die de autorisaties registreren. De Servicedesk stuurt het vervolgens door naar functioneel beheerder voor de betreffende applicatie. Dit gebeurt dus niet automatisch vanuit het Beaufort personeelssysteem. Voor BVH en BVO geldt dat autorisaties alleen worden toegekend door functioneel beheer als de medewerker is opgeleid voor het betreffende systeem. Voor BVH geldt dat de verschillende functies met bijhorende autorisatie zijn voorgeprogrammeerd. De functioneel beheerder hoeft alleen nog de juiste functie te selecteren en dan worden de juiste autorisaties toegewezen. Overige autorisaties worden door de direct leidinggevenden aangevraagd door middel van een digitaal aanvraagformulier, welke ze kunnen downloaden. Hierbij gaat het met name om toegang tot afdelings-/teammappen en uitgebreide autorisaties. Functioneel beheer voert een check uit of iemand een autorisatie echt nodig heeft. Bij twijfel wordt contact opgenomen met de informatiebeveiligingsfunctionaris. Autorisatieaanvragen worden opgeslagen in de autorisatiemailbox en in het systeem van de Servicedesk. Het autorisatie proces staat beschreven in het document "Autorisatieprocedure Regiopolitie Limburg-Zuid" d.d. 10-05-2010.

Autorisatieverzoeken voor externe politiemedewerkers lopen via de informatiebeveiligingsfunctionaris, die nagaat of de autorisatie verstrekt mag worden. In de meeste gevallen krijgen externe politiemedewerkers een autorisatie voor 1 jaar.

Tijdelijke autorisaties, voor bijvoorbeeld TGO's, worden alleen verstrekt voor die modules die op dat moment nodig zijn. Dit gebeurt niet zo heel vaak, maximaal 10 keer per jaar. Er is een beperkt aantal aanvragen voor tijdelijke autorisaties omdat

over het algemeen een beroep gedaan op medewerkers die al over de gewenste autorisaties beschikken.

Wijzigen en Verwijderen

Indien een medewerker doorstroomt geeft de leidinggevende via de PMA door dat de medewerker binnen zijn afdeling gaat werken. PMA legt dit neer bij Personeelszaken en zij maken een doorstroomformulier op. Dit formulier wordt naar de informatiebeveiligingsfunctionaris gestuurd. Hij gebruikt de autorisatiematrix om de aanvraag te toetsen. Indien akkoord wordt het doorgestuurd naar functioneel beheer.

In geval van uitdiensttreding maakt Personeelszaken een formulier aan. Zij sturen dit door naar de Servicedesk die het weer doorzet naar functioneel beheer. Dit is voor hen het signaal dat de autorisaties ingetrokken moeten worden. Dit geldt voor alle autorisaties, zowel voor de Windows omgeving, als voor de verschillende systemen (zoals BVH).

De informatiebeveiligingsfunctionaris voert steekproefsgewijs controles uit op autorisaties. Voor de systemen BVH en BVO gebeurt dit twee keer per jaar. Voor de andere systemen één keer per jaar. De informatiebeveiligingsfunctionaris genereert dan vanuit Beaufort een overzichtslijst met de actuele functies van medewerkers. Vervolgens kijkt hij, met behulp van de korpsautorisatiematrix, of de verstrekte autorisaties overeenkomen met deze functies. Op basis hiervan zijn bestaande autorisaties in de lijn ingetrokken. Uit het Excel bestand "controle autorisaties.xls" blijkt dat in 2011 op 7 van de 32 applicaties controles zijn uitgevoerd.

Functioneel beheer BVO draait periodiek een uitdraai uit met daarin gegevens hoe lang iemand niet in een applicatie heeft gewerkt. Als dat meer dan een half jaar is, wordt de betreffende autorisatie ingetrokken. Als het meer dan een jaar is, dan wordt de toegang tot het systeem ingetrokken.

De processen voor het aanvragen controleren en verwijderen lijken goed te verlopen. De processen voor het aanvragen en verwijderen staan beschreven in de eerder genoemde procesbeschrijving. De procesbeschrijving geeft echter niet aan hoe en hoe vaak de controles op juistheid van de autorisaties worden uitgevoerd.

Autorisaties RID en CIE

Het hoofd CIE verzorgt de autorisaties voor de medewerkers op zijn afdeling. Er zijn verschillende niveaus waarop hij kan autoriseren. Zo kan het hoofd CIE en zijn plaatsvervangers van uit zijn toezichtrol alles zien (niveau 8). Runners krijgen autorisaties tot niveau 6. Als functionarissen geautoriseerd willen worden voor het RID-gedeelte van BVO gaat dat via het hoofd RID. De Officier van Justitie toetst de autorisaties van de RID. Door de overzichtelijke afdelingen zijn de hoofden goed in staat de autorisaties te beheren.

Protocollering autorisaties

Het is niet mogelijk om het systeem een totaaloverzicht van alle huidige autorisaties te laten genereren. In plaats daarvan moet per systeem een overzicht van de autorisaties binnen dat systeem worden gehaald. De logginggegevens (van mutaties) van autorisaties voor alle systemen blijven wel bewaard. Ook de historische mutaties, zodat na is te gaan wie wanneer waarvoor geautoriseerd is geweest. Daarnaast zijn per functioneel beheerder de aanvragen en wijzigingsverzoeken uit de mailbox te herleiden. Deze worden bewaard zolang dat nodig is.

4.5.3 *Verbeterpunt*

Als verbeterpunt is te noemen:

- Het realiseren van zicht op autorisaties in de KA omgeving.
- Leg de wijze van controle op de autorisaties vast in de procesbeschrijving autorisaties.
- Hoewel alle autorisatiegegevens bewaard blijven, zijn ze niet direct en gemakkelijk toegankelijk. Zorg dat alle aanvragen en wijzigingsverzoeken op een centrale locatie worden bewaard.

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

4.6.1 *Norm*

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

4.6.2 *Bevindingen*

De inhoud van de activiteiten geautomatiseerd vergelijken en in combinatie met elkaar verwerken is niet bij veel medewerkers binnen het korps bekend. Waar bekendheid met deze begrippen uit de Wpg wel aanwezig is, komt direct de vraag aan de orde waar de grenzen van deze activiteiten liggen en op welke wijze daarmee in de praktijk moet worden omgegaan. Het korps heeft geen definitie voor de begrippen vastgesteld en uitgedragen.

Het geautomatiseerd vergelijken en in combinatie zoeken gebeurt onder verantwoordelijkheid van de onderzoeksleider/bevoegd functionaris door informatierechercheurs. Voor het in combinatie verwerken van artikel 9 gegevens is vooraf toestemming van het bevoegd gezag nodig.

In september 2011 heeft het korps afspraken gemaakt met het OM over de afhandeling van verzoeken voor in combinatie verwerken. De Officier van Justitie is het vaste aanspreekpunt als het gaat om Justitiële zaken. Als het gaat om rechercheonderzoeken dan geeft de zaaksofficier opdracht. De bevoegd functionarissen zijn door het hoofd tactiek geïnstrueerd dat alleen in combinatie mag worden verwerkt nadat zij hiervoor schriftelijke toestemming van het bevoegd gezag hebben ontvangen. Hierbij is het van belang dat er wel doelbinding is, en dat er sprake is van een zwaarwegend algemeen belang. De afspraken met de bevoegd functionarissen zijn mondeling gemaakt en per e-mail naar de bevoegd functionarissen gestuurd. Ze zijn echter niet schriftelijk vastgelegd in de een procesbeschrijving of vuistregels voor bevoegd functionarissen. Hierdoor is nog niet geborgd dat nieuwe bevoegd functionarissen op deze afspraak worden gewezen.

Hoewel het bevoegd gezag schriftelijk toestemming om geeft om in bepaalde gevallen in combinatie te verwerken wordt dit alleen vastgelegd binnen het betreffende onderzoek. De privacyfunctionaris wordt nog niet op de hoogte gesteld van dit soort artikel 11 verwerkingen en heeft hiermee nog geen volledig zicht.

4.6.3

Verbeterpunten

Als verbeterpunten zijn te noemen:

- Op landelijk niveau: Stel een definitie op van geautomatiseerd vergelijken en in combinatie met elkaar verwerken. Geef daarbij de grenzen aan van geautomatiseerd vergelijken en in combinatie met elkaar verwerken en ontwikkel casuïstiek aan de hand waarvan geautomatiseerd vergelijken en in combinatie met elkaar verwerken kan worden besproken.
- Op korps niveau: Draag deze definitie uit en bespreek de casuïstiek met medewerkers die te maken hebben met geautomatiseerd vergelijken en in combinatie met elkaar verwerken.
- Stel schriftelijke afspraken op over hoe bevoegd functionarissen alleen in combinatie mogen verwerken nadat hier schriftelijke toestemming voor is gegeven door het bevoegd gezag. Denk hierbij aan de melding aan de privacyfunctionaris in relatie tot de protocolplicht.

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 worden gedurende een periode van maximaal een half jaar verwerkt teneinde te bezien of zij aanleiding geven tot een nieuw onderzoek als bedoeld in artikel 9 of een nieuwe verwerking als bedoeld in artikel 10, en na verloop van deze termijn worden verwijderd.

4.7.2

Bevindingen

Proces handhaving

Voor de invoering van BVH maakte het korps gebruik van de applicatie Xpol. Gegevens uit Xpol zijn overgezet naar BVH, waardoor BVH gegevens bevat die al 13 jaar oud kunnen zijn. Deze gegevens zijn voor alle geautoriseerde medewerkers in BVH zichtbaar. Binnen het korps is ertoe besloten deze gegevens niet handmatig te schonen, omdat het om veel registraties gaat en schoning hoge kosten met zich mee zou brengen. Op 17 mei 2010 heeft een speciaal hiervoor opgerichte projectgroep een implementatieplan voor de schoning van BVH geschreven. Hierin beschrijven de leden van de werkgroep hoe zij in samenwerking met vtsPN de BVH gegevensverzamelingen willen schonen. VtsPN heeft in 2011 een BVH versie uitgebracht die de geautomatiseerde schoning mogelijk maakt. Op 1 september 2011 is de Wpg stuurgroep voor Zuid-6 bij elkaar gekomen en heeft men een zevental issues in de nieuwe versie van BVH geïdentificeerd. De portefeuillehouder politiegegevens hiervan op 2 september schriftelijk op de hoogte gebracht. Het korps is door de Zuid-6 stuurgroep geadviseerd de nieuwe functionaliteiten in BVH niet te activeren tot dat er duidelijkheid is over de issues. De korpsbeheerder en korpsleiding hebben zich aan dit standpunt geconformeerd.

Andere applicaties binnen het korps bevatten al enige waarborgen. Bij gebruik van het geïntegreerd bevragingssysteem (waarmee BVH en BVO bevestigd kunnen worden) krijgen medewerkers wel een melding als politiegegevens ouder dan 5 jaar zijn. De gegevens zelf zijn in dat geval wel zichtbaar, maar medewerkers worden erop gewezen dat gebruik van deze gegevens mogelijk niet rechtmatig is.

Proces opsporing

Voor het verwijderen en vernietigen van opsporingsinformatie is het noodzakelijk dat het duidelijk is op welk moment gegevens kunnen worden verwijderd. Hierbij is de ketensamenwerking en specifiek de overdracht van informatie over afgesloten zaken van OM naar de politie een aandachtspunt. Het OM heeft inzicht in de wijze van afdoening van zaken en moet dit delen met de politie om aan te geven wanneer WPG verwijderingstermijnen gaan lopen. Het korps krijgt sinds kort afloopberichten van het lokale OM. Op basis daarvan, en de erin opgenomen afdoeningsgrond, worden politiegegevens conform de Wpg geschoond. Het lokale OM is echter maar een onderdeel van de keten. Tot op het moment dat van uit het gehele OM structureel afloopberichten worden verstuurd is het niet mogelijk efficiënt politiegegevens te verwijderen. Bij het korps Limburg-Zuid sluit men aan op de landelijke ontwikkelingen, en schoont men de gegevens niet handmatig.

Voor de schoning van lokale mappen worden de schoningstermijnen van art. 9. informatie gehanteerd. Na het ontvangen van een afloopbericht, worden de gegevens uit de mappen verwijderd. De chef recherche houdt hier toezicht op. Voor het mappenbeheer zijn de bevoegd functionarissen en leidinggevend verantwoordelijk. De functionaris gegevensbescherming heeft hier ook een rol in.

Uit de interviews blijkt dat het idee leeft dat de bewaar- en vernietigingstermijnen niet overeenstemmen met de termijnen in het Wetboek voor Strafvordering. In het geval van cold cases ontstaan problemen wanneer na 10 jaar gegevens vernietigd worden. In deze gevallen zouden gegevens niet vernietigd moeten worden, maar moeten worden voorzien van een signaal waaruit blijkt dat het om oude gegevens gaat. Zo blijven de gegevens beschikbaar voor hernieuwde verwerking.

CIE en RID

Binnen de CIE en RID gelden strakke eisen voor de bewaartermijnen van politiegegevens. Na vier maanden is informatie van informanten niet meer te gebruiken om ter beschikking te stellen aan een operationele afdeling omdat deze informatie te oud is. Het omzetten van bruto naar netto informatie gebeurt dan ook altijd binnen 4 maanden, maar meestal al binnen 2 weken. Hierop wordt toegezien bij het ter beschikking stellen van informatie.

Aan ZWACRI informatie moet een code worden gehangen waardoor het duidelijk is dat het om subjectwaardige informatie gaat. Het systeem kan echter nog geen onderscheid maken tussen subjectwaardige en niet-subjectwaardige informatie. Hierdoor werkt het geautomatiseerd schonen ook niet goed.

Een probleem is ook het schonen van subjecten. Als een subject geschoond wordt, dan zijn ook de contacten weg, die mogelijk gekoppeld zijn aan een ander subject. Door deze issue's is het schonen een handmatig proces. Hiervoor wordt binnen de CIE tijd en mankracht vrijgemaakt. Er is in overleg met OvJ besloten om de gegevens na de periode van 5 jaar na de laatste subjectwaardige registratie direct te vernietigen. Binnen de CIE wordt de naleving van bewaartermijnen scherper gecontroleerd dan bij de RID.

Kantoorautomatiseringsomgeving

Politiegegevens worden niet alleen bewaard in de daarvoor beschikbare systemen zoals BVH en BVO, maar ook in de kantoorautomatiseringsomgeving (de mappenstructuur en afdelings- en persoonlijke mailboxen).

De afdelings- en persoonlijke mailboxen worden regelmatig geschoond. Dat is niet ingegeven door de eisen die de Wpg stelt aan bewaartermijnen. De beperkte opslagcapaciteit maakt het nodig om regelmatig te schonen, omdat de mailboxen anders vol zitten.

Voor het beheer van de mappenstructuur zijn de bevoegd functionarissen en leidinggevend verantwoordelijk. De functionaris gegevensbescherming heeft hier ook een rol in.

Hernieuwde verwerkingen

Als politiegegevens zijn verwijderd mogen ze in principe niet meer worden gebruikt voor operationele doeleinden. De wetgever heeft echter de mogelijkheid gegeven om in bijzondere gevallen deze gegevens toch te gebruiken na goedkeuring van het bevoegd gezag. Tijdens het overleg tussen het korps en het OM in september 2011 is het OM ook gewezen op haar verantwoordelijkheden met betrekking tot het beoordelen van verzoeken tot hernieuwde verwerkingen. Voor hernieuwde verwerkingen wordt schriftelijk toestemming gegeven door het OM. Voor BVO zijn tot op heden nog geen verzoeken geweest om verwijderde gegevens opnieuw te kunnen verwerken. Hernieuwde verwerkingen worden technisch mogelijk gemaakt door een individuele autorisatie te geven waardoor in de bak (het onderzoek) weer kan worden gewerkt.

Hoewel het bevoegd gezag schriftelijk toestemming kan geven om, in bepaalde gevallen, verwijderde gegevens opnieuw te verwerken is momenteel de afspraak dat dit alleen vastgelegd wordt binnen het betreffende onderzoek. De privacyfunctionaris wordt nog niet op de hoogte gesteld van hernieuwde verwerkingen en kan hiermee nog niet zijn toezichthoudende taak uitvoeren.

4.7.3

Verbeterpunten

- Voer controle uit op de gegevens in de kantoorautomatisering.
- Stel schriftelijke afspraken op voor de functioneelbeheerders onder welke voorwaarden zij verwijderde gegevens opnieuw beschikbaar mogen maken voor hernieuwde verwerkingen. Denk hierbij aan de melding aan de privacyfunctionaris in relatie tot de protocolplicht.
- Hou beheersmaatregelen voor verwijdering en vernietiging in de systemen BVH en BVO landelijk op de agenda.

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

Algemeen kan worden gesteld dat binnen het korps informatie tussen collega's mondeling en/of telefonisch ter beschikking wordt gesteld. Deze informatie staat in de meeste gevallen in BVO en het ter beschikking stellen wordt op dit systeem vastgelegd. Het heeft moeite gekost om het ter beschikking stellen onder de aandacht te brengen. De komst van de Wpg heeft geleid tot bewustwording. Dit is een geleidelijk proces wat dat op kan worden versneld door aandacht aan te blijven besteden aan het belang van het delen van informatie.

De infodesk speelt een belangrijke rol in het ter beschikking stellen van informatie. De infodesk deelt alleen artikel 8 en 13 informatie. Artikel 9 en 10 informatie wordt gedeeld via de bevoegd functionarissen. De infodeken hebben tijdens de audit laten zien dat men op gedegen wijze met de informatieverzoeken om gaat.

Het korps heeft de bevoegd functionarissen op basis van hun functie aangesteld. Hiertoe is een aanwijzingsbesluit voor bevoegd functionarissen (d.d. 28 juni 2010, getekend door G. Veldhuis) opgesteld.

De bevoegd functionarissen hebben allen een opleiding bevoegd functionaris gevolgd bij de Politieacademie en bij een extern bureau en hiervoor een certificaat ontvangen. In deze opleiding is ook aandacht voor de wettelijke weigeringsgronden. Er zijn een aantal waarborgen om het ter beschikking stellen van informatie goed te laten verlopen:

- Om CIE informatie ter beschikking te stellen binnen het korps, stelt de CIE een verstrekkingrapport op. Dit rapport wordt door de runner opgemaakt en door het hoofd CIE gecontroleerd voordat het naar buiten gaat.
- Er worden codes gehanteerd: 00 wordt niet verstrekt, hoogstens aan de korpschef; 01: kan in uitzonderlijke gevallen verstrekt worden, maar moet in overleg; 11: mag worden verstrekt.
- De infodesk deelt geen informatie zonder goedkeuring van de bevoegd functionaris.
- Wanneer een medewerker van de infodesk ziet dat er op een vraag van een rechercheur een hit is op een onderzoek van de CIE, dan wordt de CIE hierover geïnformeerd. De CIE kan vervolgens bepalen of ze de bevoegd functionaris op de hoogte willen brengen van hun onderzoek.

4.8.3 *Verbeterpunten*

- Wijs de bevoegd functionarissen periodiek op het belang van het delen van informatie.

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*

Binnen Limburg-Zuid is veel aandacht besteed aan de rechtmatige verstrekking van politiegegevens. Er is binnen het korps een groot aantal documenten en procesbeschrijvingen opgesteld en uitgedeeld om het verstrekkingproces te ondersteunen, zoals het regionale verstrekkingenhandboek de landelijke verstrekkingenwijzer, een procesbeschrijving I90 etc. De privacyfunctionaris fungeert als centraal aanspreekpunt bij lastige gevallen en is te vinden voor de medewerkers binnen het korps. Lastige informatieverzoeken worden door de privacyfunctionaris zelf afgehandeld. Afdelingen die structureel informatie aan partners verstrekken, zoals het Regionaal Informatie Knooppunt, zijn goed geïnstrueerd hoe met informatieverzoeken dient te worden omgegaan en controleren onder andere op aspecten zoals doelbinding. Daarnaast worden alle ontvangers gewezen op de verplichting tot geheimhouding conform Artikel 7 van de Wpg. De hoofden van zowel afdeling casescreening als het Regionaal Informatie Knooppunt houden toezicht dat de externe verstrekkingen conform de gemaakte werkafspraken. Alle verstrekking die worden gedaan vanuit de Infodesk worden vastgelegd in de infodeskmodule van BVO. Deze gegevens worden ten minste tot na de externe audit bewaard. De privacyfunctionaris en de functioneel beheerder hebben toegang tot overzichten van alle verstrekkingen uit de infodesken.

Hoewel op verschillende plaatsen binnen het korps het proces van verstrekkingen strak is geregeld, lijkt het te ontbreken aan een breed uitgedragen beleid. Verschillende afdelingen binnen het korps houden zich bezig met verstrekkingen, zonder van elkaars activiteiten op de hoogte te zijn. De afdeling casescreening en werkvoorbereiding heeft bijvoorbeeld geen zicht op de verstrekkingen van de infodesk. Hierdoor zouden op den duur conflicterende werkwijzen kunnen ontstaan en is er geen centraal overzicht van gedane verstrekkingen. Hoewel het regionale verstrekkingenhandboek voorschrijft dat het verstrekken van politiegegevens dient te worden vastgelegd in I90, is dit niet breed bekend. De medewerkers zijn zich ervan bewust dat de verstrekking vastgelegd dient te worden, maar gebruiken hiervoor andere systemen of methoden. Ook wordt niet door alle wijkchefs toegezien op vastlegging van de verstrekkingen. Dit maakt de controletaak en het zenden van wijzigingsverzoeken naar externen, op basis van Art. 30, lastig. Indien de verstrekking wel conform het verstrekkingenhandboek als I90 worden vastgelegd is het wel mogelijk de verstrekking terug te vinden. De I90 binnen BVH worden niet geschoond.

Binnen het korps bestaat het beeld dat er geen politiegegevens automatisch, zonder tussenkomst van een medewerker, worden verstrekt aan organisaties buiten het politiedomein. Bij de gesprekken bleek dat er toch een beperkt aantal van dit soort koppelingen zijn. Denk hierbij aan verstrekkingen ten behoeve van CHV (collectieve hulpverlening) en abonnementen binnen het veiligheidshuis. Het gebruik van dit soort automatische gegevensverstrekkingen kunnen het politieproces efficiënt ondersteunen, hierbij is het van belang dat deze verstrekkingen inzichtelijk zijn en binnen het toezicht van onder andere de privacyfunctionaris vallen.

Convenanten

Het korps heeft diverse convenanten opgesteld voor samenwerkingsverbanden met structurele verstrekkingen. De convenanten worden binnen Limburg Zuid opgesteld en beheerd door de privacyfunctionaris en een medewerker van juridische zaken. Recent zijn alle convenanten geïnventariseerd, wat heeft geresulteerd in een overzicht van alle convenanten en van convenanten die zijn verlopen. De convenanten op basis waarvan politiegegevens kunnen worden gedeeld, zijn te vinden op het intranet van het korps, PILZ.

De convenanten worden opgesteld aan de hand van een stappenplan en een model privacy paragraaf. Het gebruik van deze middelen bevordert de eenduidigheid en zorgt ervoor dat alle Wpg relevante aspecten in de convenanten worden opgenomen. Tijdens het opstellen van convenanten worden de partners gewezen op de geheimhoudingsplicht die rust op politiegegevens. De documenten zorgen ervoor dat vooraf aandacht gegeven wordt aan de keuze welke gegevens beschikbaar worden gesteld. Hiermee heeft het korps er voor gekozen om de beslissing van de verantwoordelijke om gegevens te delen, expliciet is opgenomen in het convenant. Er is dus geen sprake van een los Art. 20 besluit, maar dit is opgenomen in het convenantenproces. De medewerker juridische zaken of de privacyfunctionaris toetst het concept besluit voordat het voor ondertekening wordt aangeboden.

Hoewel de convenanten op het intranet te vinden zijn, is dit niet bekend bij alle geïnterviewde personen. Hierdoor is het niet direct duidelijk of het toegestaan is om gegevens te verstrekken. Zo is het bij het veiligheidshuis niet duidelijk of het verouderde convenant dat zij hebben Wpg-proof is.

Bij ons gesprek bij het Regionaal Informatieknooppunt had men geen directe toegang tot de inhoud van de convenanten. Echter, ze worden wel op de hoogte

gesteld indien nieuwe convenanten worden uitgegeven en doen navraag bij de privacyfunctionaris als er zaken onduidelijk zijn.

De medewerkers van het Regionale informatieknooppunt zijn opgeleid om, conform de werkafspraken, verstrekkingen op zaken als doelbinding en noodzaak te controleren. Uit onze gespreken is gebleken dat er echter binnen het korps onduidelijkheid bestaat over de verstrekkingen aan het RIEC. Op 13 juli 2011 is er een document genaamd "notitie met betrekking tot het verstrekken van politiegegevens aan het RIEC" door de korpschef is uitgebracht om deze onduidelijkheid weg te nemen. In de notitie wordt gesteld dat het vooraf niet duidelijk is welke informatie het RIEC kan gebruiken bij de uitvoering van de taken. Daarnaast wordt gesteld dat de doelbinding voor de verzoeken vast is omschreven in het convenant. Hierdoor lijkt dat alle artikel 8 gegevens voor het RIEC beschikbaar mogen worden gesteld zonder dat men voor individuele verstrekkingen aan het RIEC de doelbinding dient te testen. Het breed verstrekken zonder de doelbinding te controleren zou maken dat de verantwoordelijke geen controle heeft over de eigen politiegegevens.

Het korps loopt met de samenwerking met het RIEC vooruit op de landelijke ontwikkelingen die mogelijk leiden tot een wijziging in het besluit politiegegevens (BPG). Gezien het feit dat de verstrekkingen aan het RIEC nog niet onder artikel 18 vallen is er een convenant opgesteld.

4.9.3

Verbeterpunten

- Onderzoek en inventariseer welke geautomatiseerde gegevensverstrekkingen er plaatsvinden vanuit het korps.
- Maak afspraken wie verantwoordelijk is voor het verstrekken aan bepaalde partners en maak deze afspraken bekend binnen het korps. Wellicht kan hiervoor een regionale verstrekkingenwijzer worden gemaakt.
- Zorg dat het voor alle afdelingen bekend is op welke wijze zij verstrekkingen dienen te protocolleren.
- Stem de werkwijze met betrekking tot de verstrekkingen aan het RIEC intern af en schep duidelijkheid omtrent de controle op doelbinding.

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

Het korps Limburg Zuid heeft een procedure voor rechten van betrokkenen. Alle verzoeken met betrekking tot rechten van betrokken, zoals inzagerecht van burgers, dienen via de privacyfunctionaris te verlopen. Het is bij de meeste medewerkers bekend dat deze verzoeken naar de privacyfunctionaris dienen te worden doorgestuurd. Het komt echter voor dat verzoeken soms buiten de privacyfunctionaris om worden afgehandeld.

Uit interviews blijkt dat bij wijzigingen van politiegegevens, externe partijen worden geïnformeerd conform Art 30. Dit blijkt echter niet uit de procesbeschrijving. Daarnaast kunnen de eerder beschreven gaten in de vastlegging van verstrekkingen een obstakel zijn bij de volledigheid van partners die worden geïnformeerd.

4.10.3

Verbeterpunten

- Het verdient aanbeveling de rol van de privacyfunctionaris bij aanvragen van rechten van betrokkene breed onder de aandacht te brengen.
- Pas de procesbeschrijving aan zodat hieruit blijkt hoe partners worden geïnformeerd over wijzigingen in verstrekte politiegegevens.

4.11 Protocolplicht (artikel 32)

4.11.1

Norm

De verantwoordelijke draagt zorg voor de schriftelijke vastlegging van:

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

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

4.11.2

Bevindingen

De protocolplicht houdt in dat het korps middels schriftelijke vastlegging verantwoording aflegt over de wijze waarop zij omgaat met privacy gevoelige gegevens.

Doelen van artikel 9 onderzoeken

Om de vastlegging en melding van de doelen van artikel 9 onderzoeken te faciliteren heeft Limburg Zuid onder andere een formulier voor de melding hiervan ontwikkeld. Dit formulier wordt zowel geprint als digitaal aan de recherche medewerkers ter beschikking gesteld. Op de bezochte recherche afdeling hangen deze formulieren naast een aftekenlijst. Op deze lijst worden de BVO nummers van onderzoeken ingevuld. De lijst wordt daarnaast gebruikt als overzicht om te zien of het doel al is aangemeld. De formulieren worden per post, dan wel per e-mail, aan de functioneel beheerder BVO gestuurd. Deze heeft mappen staan waarin alle aanvragen zijn opgeslagen. Daarnaast wordt een digitaal overzicht aangehouden in BVO. Hierdoor is de functioneel beheerder in staat om aan te geven voor welke onderzoeken nog geen doel is aangemeld. Deze informatie wordt gedeeld met de recherche coördinator en de privacyfunctionaris die toezicht houden op het stelsel. De mappen met de doelen van artikel 9 onderzoeken zijn beschikbaar vanaf het moment dat de gestart is met de vastlegging ongeveer 1 jaar geleden. De protocolgegevens worden conform de Wpg in ieder geval bewaard tot na de externe audit.

Gegevensverzamelingen op grond van Art. 13

Artikel 13 van de Wpg geeft het korps de mogelijkheid om gegevensverzamelingen aan te houden voor bepaalde doeleinden, zoals identificatie van personen of zaken. Veel van deze systemen zoals HKS hebben een landelijk karakter. Landelijk zijn regels en richtlijnen opgesteld voor het gebruik van dit soort systemen. Limburg

Zuid houdt zich strikt aan deze regels. Het korps heeft op 27 oktober 2011, tien protocollen voor landelijke artikel 13 systemen ontvangen van de expertgroep politiegegevens en privacy. Deze protocollen geven per applicatie onder andere bewaartermijnen en doelomschrijving aan. De protocollen kunnen korps specifiek gemaakt worden door de korpsnaam in te vullen en te controleren of de omschreven termijnen overeenkomen met het eigen gebruik. Het korps is voornemens deze protocollen zo spoedig mogelijk over te nemen en te implementeren. Naast de lijst met de tien landelijke artikel 13 systemen, hebben wij een lijst ontvangen met daarop 19 van mogelijke artikel 13 gegevensverzamelingen binnen de infodesk. Of dit daadwerkelijke artikel 13 gegevensverzamelingen en of er nog meer artikel 13 gegevensverzamelingen zijn is nog niet vastgesteld. De privacyfunctionaris heeft hiermee nog geen complete lijst met de artikel 13 gegevensverzamelingen binnen Limburg-Zuid.

Onrechtmatige verwerkingen

De privacyfunctionaris houdt toezicht op onrechtmatige verwerkingen binnen het korps. Hiervoor heeft de privacyfunctionaris onder andere steekproeven gedaan op de bronvermelding in BVO. De meeste kans om onrechtmatige verwerkingen te achterhalen heeft Bureau Interne Zaken. Er wordt alleen op een aanleiding geacteerd. Bureau Interne Zaken meldt onrechtmatige verwerkingen aan de privacyfunctionaris. De privacyfunctionaris komt zelf geen onrechtmatige verwerkingen tegen.

Gemeenschappelijke verwerkingen

Gemeenschappelijke verwerkingen zijn gegevensverzamelingen die onder het beheer van meerdere beheerders zouden kunnen vallen. Tijdens onze audit hebben wij geen gemeenschappelijke verwerkingen in het Korps Limburg Zuid aangetroffen.

4.11.3 Verbeterpunt

- Inventariseer alle Art. 13 gegevensverzamelingen binnen het korps en stel de bijbehorende protocollen op.

4.12 Audits (artikel 33)

4.12.1 Norm

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

4.12.2 Bevindingen

Binnen het korps Limburg Zuid is een interne Wpg auditor aangesteld en deze is in 2009 opgeleid. Hij heeft in 2011 een intern audit plan opgesteld welke alle verplichte elementen bevat. Er was voor de interne audit capaciteit binnen het korps vrijgemaakt. Gelet op de op landelijk niveau gehouden discussies ten aanzien van de impact Wpg op de Nederlandse Politie binnen de Raad van Korpschefs alsmede met het CBP en het Ministerie Van Veiligheid en Justitie is er een advies uitgebracht geen interne audit uit te voeren. Het korps heeft dit advies opgevolgd en de interne audit is uiteindelijk niet uitgevoerd, waardoor er geen intern audit rapport beschikbaar is.

4.12.3 Verbeterpunt

- Richt een vaktechnisch verantwoorde en meerjarig gerichte auditplanning in.

4.13 Privacy functionaris (artikel 34)

4.13.1 Norm

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

4.13.2 Bevindingen

Binnen Limburg Zuid is de privacyfunctionaris, middels Mandaatbesluit Wet politiegegevens Privacy, aangewezen. Hij bekleedt deze functie sinds eind 2010. De privacyfunctionaris is formeel benoemd en aangemeld bij het CBP. Voor de uitvoering van zijn functie heeft de privacyfunctionaris een opleiding tot gecertificeerd privacyfunctionaris gevolgd bij de Politieacademie.

Elders in dit audit rapport is beschreven hoe het korps Limburg-Zuid de protocollering conform Art. 32.1 heeft ingericht. Alle plaatsen waar protocolgegevens worden vastgelegd, zijn bekend en direct of indirect toegankelijk voor de privacyfunctionaris. In 2011 heeft de privacyfunctionaris verschillende steekproeven genomen ter beoordeling van de werking van het stelsel van maatregelen.

De privacyfunctionaris heeft diverse controles uitgevoerd. Waaronder controles bij de CIE, RID, Bureau interne zaken, EPICC en het bureau ondersteuning systemen (BOS). Daarnaast overlegt de privacyfunctionaris tweewekelijks met de informatie beveiligingsfunctionaris over de autorisaties. Hiermee houdt de privacyfunctionaris toezicht op het stelsel van autoriseren.

Het korps heeft over 2010 geen jaarverslag opgesteld. De huidige privacyfunctionaris bekleedt deze functie sinds eind 2010. Deze heeft een jaarplan gemaakt voor het jaarverslag over 2011.

De privacyfunctionaris is fulltime aangesteld, maar heeft naast zijn toezicht- en adviestaken nog enige neventaken. Zo is de privacyfunctionaris circa 2 dagen per maand als hulpofficier van justitie werkzaam, in voorkomende gevallen CHIN bij SGB0 (circa 2 dagen per jaar gemiddeld). Het afhandelen van WOB en inzage verzoeken kost de privacyfunctionaris gemiddeld anderhalve dag per week. De privacyfunctionaris heeft ook een belangrijke rol bij het opstellen en onderhouden van de convenanten voor samenwerkingverbanden en het geven van Wpg trainingen. Bovendien heeft de afdeling waar de privacyfunctionaris werkzaam is een tijdelijk personeelstekort waardoor de privacyfunctionaris een deel van de klachtafhandeling moet doen. Wij maken ons zorgen dat door de neventaken die de privacyfunctionaris uitvoert er onvoldoende tijd is voor controle en advies.

4.13.3 Aanbevelingen

- Borg de toezichthoudende taak van de privacyfunctionaris, zoals in de Wpg benoemd.
- Maak onderscheid tussen uitvoerende taken in het kader van de Wpg, zoals het opstellen van convenanten en het geven van opleidingen, en de toezichthoudende en adviserende taak.

4.14 Functionaris Gegevensbescherming (artikel 36)

De Functionaris Gegevensbescherming bestaat niet als functie bij het korps Limburg-Zuid.