

AUDITRAPPORTAGE
Politie Midden en West Brabant



Ministerie van Veiligheid en Justitie

Audit Wpg politie Midden en West Brabant

Rapport

Datum
Status

16 december 2011
Definitief

Colofon

Afzendgegevens

Departementale Auditdienst

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

Contactpersonen

drs. [REDACTED]
drs. [REDACTED]
Senior auditors

T 070 370 65 60
M wpg@minvenj.nl

Projectnaam

Audit Wet Politiegegevens

Ons kenmerk

DDS/5719706/11

Auteurs

[REDACTED]

11-11-11

11-11-11

Inhoud

Colofon 3

1 Assurance Verklaring 7

2 Samenvatting 9

3 Inleiding 16

3.1 Algemeen 16

3.2 Aanleiding 16

3.3 Doelstelling, aard en scope van de opdracht 16

3.4 Afbakening 17

3.5 Normenkader 17

3.6 Beperkingen voor de privacy audit 18

3.7 Onderzoeksmethoden en werkwijze 18

3.8 Doelgroep van het rapport 18

4 Bevindingen 19

4.1 Inleiding 19

4.2 Verantwoordelijke (artikel 1.f) 22

4.3 Kwaliteitsaspecten van politiegegevens (artikel 3 en 4) 22

4.4 Gevoelige gegevens (artikel 5) 25

4.5 Autorisatie (artikel 6) 25

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

4.7 Bewaartermijnen (artikel 14) 28

4.8 Ter beschikking stellen (artikel 15) 29

4.9 Verstrekken (artikel 16/24) 30

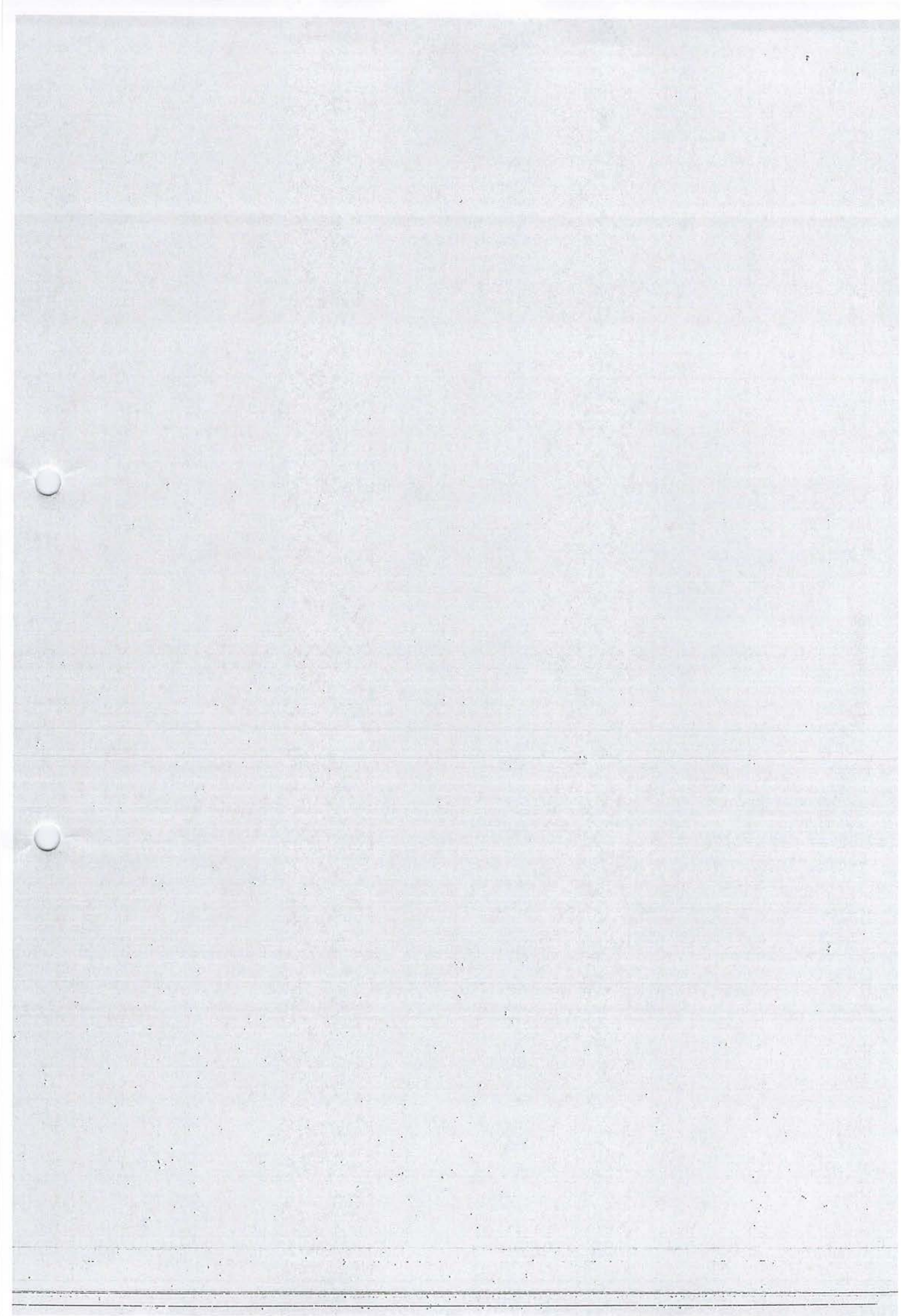
4.10 Rechten van betrokkenen (artikel 25/28) 31

4.11 Protocolplicht (artikel 32) 32

4.12 Audits (artikel 33) 33

4.13 Privacyfunctionaris (artikel 34) 33

4.14 Functionaris Gegevensbescherming (artikel 36) 34



1

Assurance Verklaring

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

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 Midden en West Brabant.

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

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

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

Den Haag, 16 december 2011

De Directeur van de Departementale Auditdienst



J.C. Van Praat RE RA

2 Samenvatting

Het korps Midden en West Brabant heeft een aantal zaken in opzet opgepakt, zoals een autorisatiematrix en het Wpg-proof maken van de convenanten voor verstrekkingen. Ook is er een Borgings Implementatie Commissie ingesteld. De korpsleiding toont hiermee en met andere initiërende activiteiten haar aandacht aan voor de Wpg.

Niettemin voldoet het door ons beschouwde stelsel van maatregelen nog niet in opzet, bestaan en werking aan de vereisten 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.
- Geel = 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 (vastgesteld op 12 oktober 2009) en een ondermandaatbesluit (vastgesteld op 15 oktober 2009) 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 procesbeschrijvingen waarin onderscheid wordt gemaakt tussen artikel 8 en artikel 9 politiegegevens. Voor de processen voor het forensisch en technisch onderzoek ontbreken dergelijke procesbeschrijvingen. Hiermee wordt deels voldaan aan de Wpg.
3.1 t/m 3.3 (8) 4.1 (8)	Noodzakelijkheid (8) Doelbinding Rechtmatigheid Juistheid Volledigheid	Er zijn procesbeschrijvingen om te borgen dat aan de eisen van art. 3 en 4 wordt voldaan. Er wordt in de praktijk echter nauwelijks gecontroleerd op noodzakelijkheid, doelbinding, juistheid of volledigheid. Hiermee wordt niet voldaan aan de Wpg.
3.1 t/m 3.4 (9) 4.1 (9)	Noodzakelijkheid (9) Doelbinding Rechtmatigheid Herkomst en wijze van verkrijging Juistheid Nauwkeurig Volledigheid	Er zijn procesbeschrijvingen om te borgen dat aan de eisen van art. 3 en 4 wordt voldaan. Deze voldoen nog niet allemaal. De systemen borgen hier voor een deel de noodzakelijkheid, doelbinding, rechtmatigheid en herkomst en wijze van verkrijgen. Hiermee wordt deels voldaan aan de Wpg.
3.4 (10 en 12) 4.1 (10 en 12)	Noodzakelijkheid (10 en 12) Doelbinding Rechtmatigheid Herkomst en wijze	Bij de CIE en RID zijn de kwaliteitscriteria in verband met de aard van het werk goed ingeregeld. Zeker bij de CIE is hier controle op door de CIE-OvJ. Hiermee wordt voldaan aan de WPG.

Norm	Aspect	Bevinding en oordeel
	van verkrijging Juistheid Nauwkeurig Volledigheid	
4.3	Beveiliging	Het korps hanteert verschillende fysieke beveiligingsmaatregelen (zoals pasjessystemen) en digitale beveiligingsmaatregelen (zoals log-in procedures met autorisatieniveaus) om informatie te beschermen. Er zijn bij verschillende dienstonderdelen beveiligingsfunctionarissen aangesteld. Landelijke Wpg-proof applicaties worden volgens planning gezamenlijk door de zuidelijke 6 regio's geïnstalleerd. Tot op heden zijn nog geen volledig Wpg-proof applicaties opgeleverd. De regionale informatiesystemen zijn geëvalueerd op Wpg-aspecten. Besloten is geen aanpassingen te doen en deze systemen uit te faseren. Gebruikers (enkelen) zijn Wpg opgeleid. Hiermee wordt deels voldaan aan de Wpg.
Art. 5, Gevoelige gegevens		
	• Gevoelige gegevens	Gevoelige gegevens worden niet als kenmerk aan een persoon toegekend, maar als omschrijving bij het Incident. Er zijn hier echter geen richtlijnen voor. Er wordt wel volgens de Wpg gehandeld, maar de werkwijze is niet vastgelegd en daardoor misschien niet bij iedereen bekend. Hiermee wordt deels voldaan aan de Wpg.
Art. 6, Autorisatie		
	• Korpsautorisatiematrix	Er is een korpsautorisatiematrix die is afgestemd op de elsen van de Wpg. Hiermee wordt voldaan aan de Wpg.
	• Aanvraagproces	Er zijn autorisatieprocedures. De unit Informatiemanagement wordt conform afspraken benaderd voor het aanvragen van nieuwe autorisaties. Hiermee wordt voldaan aan de Wpg.
	• Wijziging en verwijdering	De autorisaties van de belangrijkste applicaties zijn geschoond. Bij de door- en uitstroom van medewerkers worden, door het ontbreken van meldingen van functiewijzigingen, onterecht autorisatieprofielen behouden. Er is een procedure ontwikkeld waardoor dit grotendeels ondervangen wordt. Maandelijks vindt schoning plaats in een accestool die gevuld wordt met personeelsgegevens en autorisatiegegevens van de belangrijkste applicaties waarvoor geautoriseerd wordt. Hiermee wordt deels voldaan aan de Wpg.
	• Autorisatiebeheer CIE en RID	Autorisaties voor medewerkers van de CIE en de

Norm	Aspect	Bevinding en oordeel
		RID worden toegekend door het hoofd van de CIE respectievelijk de RID. De CIE OvJ heeft het autorisatiebeleid goedgekeurd. Hiermee wordt voldaan aan de Wpg.
32.1.c	Protocollering autorisaties	De aanvraag voor autorisaties komt in Expertdesk vtsPN. Uitzonderingen worden ook vastgelegd. De privacyfunctionaris heeft toegang tot de vastlegging van alle mutaties in autorisaties, inclusief die bij CIE, RID en OT. De privacyfunctionaris heeft volledig inzicht bij welke functioneel beheerders of medewerkers een overzicht verkrijgbaar is van de actuele autorisaties. Hiermee wordt voldaan aan de Wpg.
32.3 voor 32.1.c	Bewaren protocolgegevens autorisaties	De protocolgegevens worden elektronisch bewaard. De Privacyfunctionaris voert enkele malen per jaar een steekproef uit op de vastgelegde mutaties op autorisaties. Hiermee wordt voldaan aan de Wpg.
Art. 11, Geautomatiseerd vergelijken en in combinatie zoeken		
	• Hanteerbare interpretatie	Binnen het korps zijn procesbeschrijvingen opgesteld voor het geautomatiseerd vergelijken en in combinatie zoeken. Hiermee wordt voldaan aan de Wpg.
	• Aangewezen functionarissen	De medewerkers RIO zijn de aangewezen functionarissen voor het geautomatiseerd vergelijken en in combinatie zoeken. Hiermee wordt voldaan aan de Wpg.
11.4	Bevoegd gezag	Volgens de procesbeschrijving moet het bevoegd gezag toestemming geven. Hiermee wordt voldaan aan de Wpg.
32.1.d en 32.1.h	Protocollering 11.1, 11.2, 11.4 en 11.5	Geautomatiseerde vergelijkingen en in combinatie zoeken worden beperkt vastgelegd. 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	Protocolgegevens worden overeenkomstig de termijnen voor artikel 8, 9 en 10 bewaard. De privacyfunctionaris heeft toegang tot deze vastleggingen. Hiermee wordt voldaan aan de Wpg.
Art. 14, Bewaartermijnen		
8.2 en 8.3	(8) van 1 tot 5 jaar	Er is in de nieuwe release een schoningsmodule in BVH, maar deze staat op besluit van de korpsbeheerder door de korpschef nog niet aan. Hiermee wordt niet voldaan aan de Wpg.
8.6	(8) verwijderen na 5 jaar	BVH wordt nu nog niet geschoond omdat de gegevens die erin zitten nog geen vijf jaar oud zijn. Landelijk is opgelegd dat BPS in zijn geheel wordt verwijderd per december 2011. BPS wordt op de O-schijf bewaard. 6 personen zijn geautoriseerd om deze gegevens te bevragen. Deze informatie omvat verschillende termijnen omdat er sprake kan zijn van art 8,9,13 informatie. Hiermee wordt niet voldaan aan de Wpg.

Norm	Aspect	Bevinding en oordeel
14.1 (8)	(8) vernietigen na 5 jaar verwijderd	Er vindt nog geen vernietiging van gegevens uit BVH plaats, omdat dit nog niet nodig is. Gegevens in de BPS historie die voor vernietiging in aanmerking komen, worden niet vernietigd. Er zijn ook nog geen waarborgen voor het tijdig schonen van art. 8 informatie in de mappenstructuur. Hiermee wordt niet voldaan aan de Wpg.
9.4	(9) verwijderen na OH plus ½ jaar	Het OM levert geen afloopberichten op basis waarvan gegevens kunnen worden verwijderd na onherroepelijk worden. Hiermee wordt niet voldaan aan de Wpg.
14.1 (9)	(9) vernietigen na 5 jaar verwijderd	Er vindt nog geen verwijdering van informatie uit BVO plaats, want er staat nog geen informatie langer dan 5 jaar in. De informatie die wel ouder dan 5 jaar is, zit nog in lopende zaken. Hiermee wordt deels voldaan aan de Wpg.
10.6	(10) verwijderen na 5 jaar geen subjectwaardige registratie	Dit wordt door de CIE en RID nageleefd. Hiermee wordt voldaan aan de Wpg.
14.1 (10)	(10) vernietigen na 5 jaar verwijderd	Dit wordt door de CIE en RID nageleefd. Hiermee wordt voldaan aan de Wpg.
14.3	Hernieuwde verwerking	De richtlijnen voor hernieuwde verwerking worden niet altijd gevolgd. Hiermee wordt deels voldaan aan de Wpg.
32.1.e	Protocollering 14.3	Hernieuwde verwerking van politiegegevens wordt niet altijd vastgelegd. Hiermee wordt deels voldaan aan de Wpg.
32.3 voor 32.1.e	Bewaren protocolgegevens 14.3	De privacyfunctionaris houdt een overzicht bij van protocolgegevens. Hiermee wordt voldaan aan de Wpg.
12.2	(12) verwijderen na 4 maanden	Informatie wordt binnen een termijn van maximaal 4 maanden verwerkt en netto in een andere omgeving gezet. Dit zit vast in de werkwijze van de CIE. Hiermee wordt voldaan aan de Wpg.
12.6	(12) controleren en vernietigen	Informatie wordt binnen de CIE en RID regelmatig gecontroleerd en geschoond. Hiermee wordt voldaan aan de Wpg.
Art. 15, Ter beschikking stellen		
• Infodesk voor bevraging		De Infodesk benadert de bevoegd functionaris altijd met de vraag of informatie mag worden gebruikt en gedeeld. Hiermee wordt voldaan aan de Wpg.
• Codering		De bevoegd functionaris kan bepaalde gegevens vooraf coderen die onder zijn verantwoordelijkheid verder mogen worden verwerkt voor een ander doel. Dit is onderdeel van de opleiding voor de bevoegd functionaris. Hiermee wordt voldaan aan de Wpg.
• Aanwijzing Bevoegd Functionaris		De bevoegde functionarissen zijn bij besluit door de

Norm	Aspect	Bevinding en oordeel
		korpschef aangewezen. Hiermee wordt voldaan aan de Wpg.
	• Opleiding Bevoegd Functionaris	De bevoegd functionarissen zijn opgeleid in de Wpg. Dit is opgenomen in de opleidingscyclus van de regio. Hiermee wordt voldaan aan de Wpg.
15.2	Welgeringgronden	De bevoegd functionarissen zijn opgeleid in de Wpg. Indien ter beschikking stelling van gegevens om gegronde reden wordt geweigerd, wordt deze weigering vastgelegd in BVO. Hiermee wordt voldaan aan de Wpg.
Art. 16 t/m 24, Verstrekking		
	• Verstrekkingenwijzer (landelijk)	De verstrekkingenwijzer is beschikbaar op Intranet en in een grote oplage fysiek aanwezig voor betrokkenen en geactualiseerd. Hiermee wordt voldaan aan de Wpg.
	• Proces voor convenanten	Binnen het korps is geïnventariseerd welke convenanten zijn afgesloten en is gestart met het Wpg-proof maken van de convenanten. Hiermee wordt deels voldaan aan de Wpg.
	• Proces voor Art. 20 Besluiten	Verstrekkingen onder art. 20 vinden alleen plaats als sprake is van een zwaarwegend algemeen belang, en na toestemming door de CIE OVJ. Hiermee wordt voldaan aan de Wpg.
	• Verstrekkingenschema (regio)	De uitgangspunten en het beleid zijn vastgelegd in een handboek verstrekken. Dit is beschikbaar via Intranet. De functionarissen zijn opgeleid. Verstrekken was daarbij een belangrijk onderdeel. Zij kunnen gebruik maken van de Instructies op Intranet. Er is een werkinstructie voor Incidentele verstrekkingen aan derden conform Art. 19. Hiermee wordt aan de Wpg voldaan.
	• Proces voor geautomatiseerde verstrekking	Er is geen sprake van geautomatiseerde verstrekkingen.
7.2	Geheimhouding	Bij verstrekkingen wordt gewezen op de geheimhoudingsverplichting. Hiermee wordt voldaan aan de Wpg.
32.1.f	Protocollering verstrekking	Niet alle verstrekkingen worden vastgelegd. Met name verstrekkingen door 'blauw' worden nauwelijks vastgelegd. Hiermee wordt niet voldaan aan de Wpg.
32.3 voor 32.1.f	Bewaren protocolgegevens verstrekking	De bewaartermijn van de protocolgegevens is gekoppeld aan de bewaartermijn van het Incident. Hiermee wordt voldaan aan de Wpg.
	• Toezicht door leidinggevendenden op verstrekkingen en protocollering	Een enkele leidinggevende stuurt op het vastleggen van verstrekkingen. Hiermee wordt deels voldaan aan de Wpg.
Art. 25 t/m 31, Rechten van de betrokkene		
25.1	Verzoek om kennisneming	Het korps heeft een werkinstructie voor de afhandeling van inzage verzoeken van een

Norm	Aspect	Bevinding en oordeel
		betrokkene. De Instructie is via Intranet beschikbaar en bekend bij de behandelaars. De afhandeling van verzoeken om kennisgeving gebeurt niet altijd binnen de wettelijke termijnen. Het probleem is onderkend door de korpsleiding. Er wordt naar oplossingen gezocht. Er zijn maatregelen genomen om de procedure te versnellen. Hiermee wordt deels voldaan aan de Wpg.
28.1 t/m 28.3	Correctie	Er is een werkinstructie voor verbetering, aanvulling, verwijdering of afscherming van politiegegevens Ingeval van feitelijk onjuiste gegevens. Deze is beschikbaar via Intranet. Als gegevens worden gecorrigeerd, dan wordt daarvan mededeling gedaan aan wie in het jaar voorafgaand aan het verzoek en in de sinds dat verzoek verstreken periode de betreffende politiegegevens zijn verstrekt. Hiermee wordt voldaan aan de Wpg.
Art. 32, Protocolplicht (32.1.c, d, e, f en h behandeld bij thema's)		
9.2 en 32.1.a	Protocollering doel onderzoek	Er is in 2011 gewerkt aan een systeem om het overzicht van doelen van artikel 9 onderzoeken compleet te maken. Bij alle artikel 9 aanmeldingen zijn de doelen bekend. Hiermee wordt voldaan aan de Wpg.
32.3 voor 32.1.a	Bewaren protocolgegevens doel onderzoek	De bewaartermijn van de protocolgegevens lopen mee met de bewaartermijn van het betreffende onderzoek. Hiermee wordt voldaan aan de Wpg.
13.4 en 32.1.b	Protocollering Art. 13 gegevensverzameling en	Een overzicht van artikel 13 verwerkingen wordt bijgehouden. De Privacyfunctionaris kan hier op terugvallen. Hiermee wordt voldaan aan de Wpg.
32.3 voor 32.1.b	Bewaren protocolgegevens Art. 13 gegevensverzameling en	De protocolgegevens worden elektronisch bewaard. In verband met de landelijke afstemming wordt aangesloten bij de door de portefeuillehouder aan te leveren art 13 registraties. Hiermee wordt voldaan aan de Wpg.
32.1.g	Protocollering onrechtmatige handeling	De afdeling belast met integriteitszaken houdt een overzicht bij van verwerkingen waarvan aanwijzingen bestaan dat zij door onbevoegden of anderszins onrechtmatig zijn verricht. Medewerkers die belast zijn met het beheer van applicaties, melden verwerkingen waarvan aanwijzingen bestaan dat zij door onbevoegden of anderszins onrechtmatig zijn verricht. De privacyfunctionaris krijgt zijn informatie via de IBF, of door eigen waarneming. Hiermee wordt voldaan aan de Wpg.
32.3 voor 32.1.g	Bewaren protocolgegevens onrechtmatige	De protocolgegevens worden elektronisch bewaard, in ieder geval gedurende de termijn van de betreffende verwerking.

Norm	Aspect	Bevinding en oordeel
	handeling	Hiermee wordt voldaan aan de Wpg.
32.2	Gemeenschappelijke verwerking	N.v.t. Het korps kent geen gemeenschappelijke verwerkingen.
Art. 33, Audits		
RPAP 3.1	Interne audit-functie	De interne auditfunctie is niet structureel belegd. In samenwerking met de regio Zeeland zal deze functie in de nieuw te vormen regio Zuid West Nederland worden ingevuld. Hiermee wordt niet voldaan aan de Wpg.
RPAP 3.4	Interne audit-plan	Er is geen intern auditplan opgesteld. Hiermee wordt niet voldaan aan de Wpg.
RPAP 3.6	Interne audit-rapport	Er is geen interne audit uitgevoerd. Hiermee wordt niet voldaan aan de Wpg.
Art. 34, Privacyfunctionaris		
34.1 en 34.4	Benoemd en gemeld	De privacyfunctionaris is benoemd en aangemeld bij het CBP. Hiermee wordt voldaan aan de Wpg.
34.2	Overzicht over protocollering	De privacyfunctionaris beschikt niet over alle protocolgegevens die de Wet vereist. Daarmee wordt deels voldaan aan de Wpg.
34.3	Jaarverslag	Over 2010 is een jaarverslag uitgebracht. Hiermee wordt voldaan aan de Wpg.
Optioneel Art. 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	Toezichhoudende 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 Midden en West Brabant 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 Midden en West Brabant in de maand september 2011.

3.2 Aanleiding

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

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

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

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

3.3 Doelstelling, aard en scope van de opdracht

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

De privacy audit leidt tot een assurance verklaring met een oordeel over de genoemde doelstelling en over de in dit rapport aangegeven thema's. Daarnaast brengen wij de knelpunten in beeld en voorzien wij elk korps schriftelijk van advies (en overkoepelend de opdrachtgever).

De privacy audit richt zich op de opzet, het bestaan en indien van toepassing de werking, per ultimo september 2011, van maatregelen en procedures, waarmee het

korps Midden en West Brabant 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 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 Midden en West Brabant. Dit betekent dat wij geen onderzoek hebben verricht naar door de vtsPN aan het korps Midden en West Brabant geleverde faciliteiten, voor zover de verantwoordelijkheid daarvoor is belegd bij de vtsPN of bij anderen dan het korps Midden en West Brabant.

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 Midden en West Brabant en het Openbaar Ministerie, deelwaarnemingen in de procesbeschrijvingen en andersoortige documentatie en deelwaarnemingen in informatiesystemen.

Wij hebben onze werkzaamheden uitgevoerd in de periode van 6 september 2011 tot en met 28 september 2011.

Het conceptrapport met bevindingen is op 27 oktober 2011 besproken met de korpschef van het korps Midden en West Brabant en op 2 november 2011 in de regionale driehoek.

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 dhr. mr. P.G.A. Noordanus;
- de wnd. korpschef dhr. D.Schouten;
- de Hoofd Officier van Justitie dhr. mr. H.M.P. Hillenaar;
- de privacyfunctionaris dhr. Mr. W. Andelbeek;
- de voorzitter van het College Bescherming Persoonsgegevens.

Het rapport mag uitsluitend met toestemming van de korpsbeheerder dan wel de korpschef van korps Midden en West Brabant 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

Organisatieplan

Het korps Midden en West Brabant beschikt over een Korpsbeschrijving 2011¹. Hierin staat het korps beschreven in de context van de omgeving, samenwerkingspartners en -verbanden, historie, omvang, toekomstplannen en strategie. Het stuk bevat ook een summier organogram. Dit organogram is op het intranet van het korps nader uitgewerkt met per onderdeel een hyperlink voor verdere informatie. De Korpsbeschrijving 2011 staat niet op zichzelf, maar borduurt voort op het visiedocument "Zien naar 2010"². Dit is een visie document met kernwaarden en strategische keuzes.

Met het oog op de toekomst is Midden en West Brabant eind 2009 begonnen met de ontwikkeling van het project Regionale Informatie Organisatie (RIO). In het Inrichtingsplan RIO d.d. 06 juli 2010³ wordt een beschrijving gegeven van de inrichting van de Regionale Informatie Organisatie in oprichting. In het RIO wordt de organisatorische inrichting van de informatie organisatie met de onderdelen Criminele Inlichtingen Eenheid (CIE), Regionale Inlichtingen Dienst (RID), Unit infodesk, Unit analyse en Unit kwaliteit & veiligheidsinformatieproducten besproken. Beschreven worden de taken en verantwoordelijkheden, producten en diensten, klanten, functies en formatie, toegevoegde waarde en werking.

Organisatorische maatregelen inzake beheersdoelstellingen Wpg

Het korps Midden en West Brabant heeft in maart 2008 een 'Impactanalyse Invoering Wet politiegegevens'⁴ gemaakt. Deze geeft weer wat de gevolgen zijn van de implementatie van de Wpg voor 'de bouwstenen van de organisatie'. Deze bouwstenen zijn: strategie, structuur, cultuur, mensen, middelen en resultaten. Het stuk geeft door het opstellen van de "Ist-situatie" en de "Soll-situatie" inzicht in de impact van de Wpg.

Midden en West Brabant heeft aansluitend in oktober 2008 een Project Initiatie Document (PID)⁵ opgesteld om de invoering van de Wpg in het korps daadwerkelijk

¹ Politie Midden en West Brabant (2010), 'Korpsbeschrijving 2011'.

² Politie Midden en West Brabant (2005), 'Zien naar 2010. De burger centraal. De visie van het politiekorps van Midden en West Brabant'.

³ Politie Midden en West Brabant (2010), 'Inrichtingsplan d.d. 06 juli 2010'.

⁴ Politie Midden en West Brabant (2008), 'Impactanalyse Invoering Wet politie gegevens'.

⁵ Politie Midden en West Brabant (2008), 'Project Initiatie Document, Implementatie Wet politiegegevens (WPG) Korps Midden en West Brabant'.

vorm te geven. Dit document is door het KLO goedgekeurd⁶ waarna een projectleider Wpg aan de slag is gegaan met de uitvoering. Het project Wpg is in juni 2010 opgeleverd waarna het projectteam op 26 oktober 2010 van de korpsleiding decharge heeft gekregen. Dit staat beschreven in een overdrachtsdocument⁷. Dit document gaat in op de stand van zaken op het moment van schrijven en geeft aanbevelingen voor verdere implementatie van de Wpg. Uit de documenten blijkt dat de centrale thema's van de Wpg telkens onder andere termen worden gepresenteerd. De Impactanalyse uit 2008 spreekt over bouwstenen⁸ die in latere documenten niet meer worden aangehaald. Deze bouwstenen zijn geclusterde thema's⁹ geworden in het PID die op hun beurt niet één op één terug te lezen zijn in het Overdrachtsdocument¹⁰.

Vervolgens heeft het korps in november 2010 uit haar geledingen een Borging Implementatie Commissie (BIC) Wpg¹¹ opgericht. Het BIC is belast met het borgen van een verdere implementatie van de Wpg. Het BIC komt wekelijks bijeen en de voortgang van het BIC wordt gerapporteerd aan het KLO en/of KMT.

Specifieke verwerkingen/regimes/informatiesystemen/applicaties

Korps Midden en West Brabant heeft in maart 2009 een plan van aanpak 'PVA Wpg thema ICT'¹² opgesteld. Dit moet een overzicht geven van de applicaties die in gebruik zijn in Midden en West Brabant. Het doel van het plan van aanpak is het bepalen van de impact van de Wpg op de gebruikte applicaties en het benoemen van maatregelen die nodig zijn om Wpg-proof te werken (de applicaties Wpg-proof te maken of de werkwijze (omgang met applicaties) te veranderen). In juli 2009 heeft het korps een document¹³ opgesteld, waarin de resultaten van de uitvoering van het plan van aanpak worden weergegeven. Er is een lijst opgesteld van die applicaties die Wpg gerelateerde informatie bevatten. Deze is gesplitst in applicaties die landelijk (bij vtsPN) worden beheerd en regionale applicaties. Op de landelijke applicaties heeft het korps geen directe invloed. Van de lijst regionale applicaties is geconstateerd dat deze uitgefaseerd worden. Er bestaat daardoor geen wens of noodzaak deze applicaties aan te passen. Besloten is dat het korps zich bij deze applicaties voornamelijk gaat richten op de bewustwording van de gebruikers op de Wpg thema's.

Migratieplan Wpolr naar Wpg, projectplannen, implementatieplannen, voortgangsrapportages

Midden en West Brabant heeft sinds de invoering van de Wpg verschillende plannen opgesteld om de implementatie van de Wpg in goede banen te leiden. Een punt van aandacht hierbij betreft het versiebeheer. Niet alle documenten zijn opgemaakt als definitief exemplaar (zijn niet getekend, dragen een titel "concept", etc., terwijl in voortgangsrapportages is aangegeven dat ze besproken zijn en door de korpsleiding

⁶ Tijdens het KLO van 18 november 2008 is het KLO akkoord gegaan met de aanpak en implementatie van het PID.

⁷ Politie Midden en West Brabant (2010), 'Implementatie van de Wet politiegegevens (Wpg) – Van Project tot Dagelijks Werk'.

⁸ Bouwstenen: strategie, structuur, processen, cultuur, mensen en middelen.

⁹ Geclusterde thema's: projectlogistiek, functionele eisen en techniek, organisatie en processen, autorisaties en protocollering, wet en regelgeving, auditing, bewustwording en eenmalige activiteiten.

¹⁰ In het Overdrachtsdocument worden maar liefst 17 verschillende thema's die op regionaal gebied gelden: Project Strategie, Project Structuur, Project Systeem, Project Proces, 'In Control', Privacyfunctionaris, Bevoegd Functionaris, Samenwerkingsconvenanten, Mandaat, Verstrekkingen, Inzake verzoeken en verzoeken tot wijziging Wpg, Protocolleren, Gegevensbeheer, ICT, Opleidingen Wpg, Audit en Samenwerking Openbaar Ministerie.

¹¹ W. Andelbeek en G. [naam] (2010), 'Borging Implementatie Commissie Wpg'.

¹² [naam] (2009), 'PVA Wpg thema ICT – Wpg-proof omgaan met applicaties'.

¹³ [naam] (2009) 'Rapport – Advies aanpak applicaties MWB a.g.v. WPG'.

zijn geaccordeerd). Zie verder onder het kopje "organisatorische maatregelen inzake beheersdoelstellingen Wpg".

Documenten borging managementcyclus

Korps Midden en West Brabant heeft de afgelopen jaren documenten opgesteld om de managementcyclus rond de implementatie van de Wpg te borgen. Tijdens de uitvoering van het PID is een groot aantal voortgangsrapportages opgeleverd bij verschillende overlegorganen. De rapportages variëren in onderwerpen (thema's, aandachtsgebieden) waarover wordt gerapporteerd. De variatie brengt als risico met zich mee dat oorspronkelijke producten en doelstellingen van het PID gedurende de uitvoering uit het oog zijn verloren.

Binnen het korps zijn instrumenten ontwikkeld (in te vullen overzichten) om op decentraal niveau aandacht voor Wpg-aspecten te kunnen monitoren. Deze worden (op districtsniveau) in toenemende mate in managementcycli gebruikt.

Aanwijzing bevoegde functionarissen

In het Korps Midden en West Brabant worden de bevoegde functionarissen benoemd door de korpschef. Hiertoe is binnen het korps een aanwijzingsbesluit bevoegde functionarissen opgesteld. Dit aanwijzingsbesluit beschrijft uitgebreid de functies die als bevoegde functionaris worden aangewezen.

Binnen het korps is de opleiding bevoegde functionaris opgenomen in het opleidingsplan en zijn aangewezen bevoegde functionarissen ook daadwerkelijk opgeleid.

4.1.2

Verbeterpunten

- Het bij alle processen en dienstonderdelen zorgen voor een actuele beschrijving van deze processen met op de praktijk gerichte procedures die Wpg proof zijn.
- Het verankeren van de aandacht voor de implementatie van de Wpg in alle managementcycli van het korps (ook in de decentrale cycli) door systematisch te rapporteren over een vaste set thema's. Flexibiliteit kan in deze vaste set worden ingebouwd door het bijhouden van een mutatieregister (een dergelijk register bevat een overzicht van wijzigingen in de set thema's) en deze parallel te presenteren.
- Het invoeren van een steviger regime wat betreft documentbeheer: het nauwlettender bijhouden van een overzicht van geactualiseerde en definitieve versies van besluitvormingsdocumenten en voortgangsoverzichten vereenvoudigt het beheer, toezicht, verantwoorden en sturen van Wpg-processen.

4.1.3

Bekendheid met de Wpg binnen de organisatie

Het korps zet kennisbevordering in als instrument om Wpg-bewustzijn te bevorderen. Er is een communicatieplan rond de implementatie van de Wpg opgesteld en in uitvoering genomen en binnen het opleidingsplan zijn cursussen opgenomen die zich (deels) richten op de Wpg. Binnen het korps Midden en West Brabant hebben op basis hiervan verschillende Wpg-specifieke voorlichtingsactiviteiten plaatsgevonden om groepen medewerkers te informeren over de eisen van de wet. Het korps is echter nog niet klaar met het bevorderen van het "informatiebewustzijn". Conform de plannen staan voor 2011 verschillende voorlichtings- en scholingsactiviteiten gepland.

4.1.4

Wpg en de praktijk

Vanwege de geringe ondersteuning vanuit de informatiesystemen, wordt de Wpg door veel medewerkers binnen het korps ervaren als een toename van de administratieve last. Ook het feit dat schonings- en bewaringstermijnen niet stroken met de termijnen in de Strafvordering worden als beperking van de Wpg gezien.

4.2 Verantwoordelijke (artikel 1.f)

Mandaatbesluit

Net als onder de oude Wet Politiregisters (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.

De mandaten van de korpsbeheerder en de korpschef zijn naar aanleiding van de invoering van de Wpg, conform artikel 1f Wpg, aangepast om aan de voorwaarden van de Wpg te kunnen voldoen.

We hebben verder documentatie aangetroffen waarin geen proceselgenaren voor verwerkingen worden benoemd. Binnen het korps geldt dat het proceseigenaarschap verloopt via de organisatorische indeling.

4.3 Kwaliteitsaspecten van politiegegevens (artikel 3 en 4)

4.3.1 Norm

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

4.3.2 Bevindingen

Het voldoen aan de bepalingen van deze artikelen is een aangelegenheid waarin bijna alle geledingen van de politie zijn betrokken. De politie Midden en West Brabant heeft in 2010 een onderzoek¹⁴ uitgevoerd naar de kwaliteit en kwantiteit van haar informatie. Dit resulteerde in de conclusie dat de kwaliteit en de kwantiteit van gegevens binnen het korps voor verbetering vatbaar was. Men constateerde:

- onvolledige invoer (niet alles wordt vastgelegd);
- foutieve invoer (foute keuzes in bijv. codering);
- gegevens worden op een verkeerde plek geplaatst (alles in de toelichting);
- niet-integere invoer;
- dubbele registratie van gebeurtenissen.

Naar aanleiding van het onderzoek is een plan¹⁵ opgesteld om de kwaliteit en de kwantiteit van gegevens te verbeteren. Hierin staan verschillende (met elkaar samenhangende) maatregelen, die in 2010 en 2011 binnen de organisatie zijn uitgerold. Ze richten zich op bewustwording van gebruikers om de kwaliteit en kwantiteit te optimaliseren en op het genereren van een instrumentarium voor het management om hierop te sturen.

Parallel aan het plan heeft het korps verschillende maatregelen getroffen om te borgen dat aan de eisen in artikel 3 en 4 wordt voldaan. Een eerste waarborg is het opstellen van procesbeschrijvingen. Deze kunnen per processtap verwijzen naar geldende Wpg-bepalingen en te volgen procedures en overige instrumentatie aanreiken om aan de bepalingen te voldoen.

Voor de meeste dienstonderdelen en werkprocessen binnen Midden en West Brabant zijn procesbeschrijvingen aangetroffen. Een dergelijke beschrijving ontbreekt voor het forensisch en technisch onderzoek.

¹⁴ [REDACTED] (2010), Kwaliteit en kwantiteit van gegevens

¹⁵ Politie Midden en West Brabant (2010), Trappenplan Kwaliteit en Kwantiteit van gegevens (Q&Q)

Een aantal van de aangetroffen procesbeschrijvingen geven per werkstap duidelijk te volgen procedures en/of overige instrumentatie. Dit geldt echter niet voor alle procesbeschrijvingen.

Het korps zet ook kennisbevordering in als instrument om te bevorderen dat aan artikel 3 en 4 wordt voldaan. Er is een communicatieplan rond de implementatie van de Wpg opgesteld en in uitvoering genomen en zijn binnen het opleidingsplan cursussen opgenomen die zich (deels) richten op de Wpg. Binnen het korps Midden en West Brabant hebben op basis hiervan verschillende Wpg-specifieke voorlichtingsactiviteiten plaatsgevonden om groepen medewerkers te informeren over de eisen van de wet. Ook zijn deze aspecten van de Wpg soms onderwerp van studie binnen cursussen. Het korps is echter nog niet klaar met het bevorderen van het "informatiebewustzijn". Conform de plannen staan voor 2011 en 2012 verschillende voorlichtings- en scholingsactiviteiten gepland.

Meer in het algemeen ter borging van de Wpg functioneert binnen het korps een privacyfunctionaris. Deze wordt door verschillende dienstonderdelen benaderd voor vragen omtrent de Wpg, waaronder ook vragen over het borgen van artikel 3 en 4.

Korpsbeheerders zijn eindverantwoordelijk voor de informatiebeveiliging en hebben deze verantwoordelijkheid gedelegeerd aan de korpschefs. De basis voor informatiebeveiliging in politiekorps Midden en West Brabant is neergelegd in de nota "Informatiebeveiliging¹⁶". Deze nota gaat eerst in op doelstellingen, strategische uitgangspunten en randvoorwaarden bij informatiebeveiliging. Vervolgens behandelt de nota zaken als de organisatie en verantwoordelijkheidsverdeling van de beveiligingsfunctie, concrete maatregelen en financiering toetsing en evaluatie.

Conform de nota is binnen het KMT de proceseigenaar Bedrijfsvoering portefeuillehouder voor de beveiliging van de informatievoorzieningen en de proceseigenaar Informatie voor de beveiliging van de informatie zelf. De portefeuillehouder informatiebeveiliging is namens de korpsleiding verantwoordelijk voor het richten, inrichten en monitoren van de informatiebeveiliging in het korps. De primaire verantwoordelijkheid voor het uitvoeren van informatiebeveiliging ligt bij het lijnmanagement en is belegd bij de desbetreffende districtschef/hoofd divisie. Het technisch beheer van de informatievoorzieningen en de beveiliging ervan is belegd bij de vtsPN.

Het korps hanteert verschillende fysieke beveiligingsmaatregelen (zoals pasjessystemen) en digitale beveiligingsmaatregelen (zoals log-in procedures met autorisatieniveaus) om informatie te beschermen. Om informatiebeveiliging vorm te geven of nader uit te werken binnen het korps zijn bij verschillende dienstonderdelen beveiligingsfunctionarissen aangesteld. Er wordt momenteel een monitor ontwikkeld ter periodieke toetsing van een aantal indicatoren. MWB is ook capacitair aangesloten bij een landelijk verbetertraject in dezen onder aansturing van de KC Noord Holland Noord. In 2012 vindt een audit plaats door het I.O.O.V. Informatiebeveiliging wordt meer en meer een onderdeel van de kwaliteitszorg binnen de regio.

Landelijke Wpg-proof applicaties worden volgens planning gezamenlijk door de zuidelijke 6 regio's geïnstalleerd. Tot op heden zijn nog geen volledig Wpg-proof applicaties opgeleverd.

¹⁶ [REDACTED] (2009), Informatiebeveiliging

De regionale informatiesystemen zijn geëvalueerd op Wpg-aspecten. Besloten is geen aanpassingen te doen en deze systemen uit te faseren. Gebruikers (enkel) zijn Wpg opgeleid.

De zogenaamde mappenstructuur wordt gezamenlijk door de zuidelijke 6 regio's ingericht en toegepast.

Met betrekking tot verschillende soorten politiegegevens (artikel 8, 9, 10 en 12) gelden specifieke bevindingen ten aanzien van het borgen van artikel 3 en 4.

Met betrekking tot artikel 8 informatie *'verwerken van politiegegevens ten behoeve van de dagelijkse politiepraktijk'* moet worden geconstateerd dat artikel 3 en 4 van de Wpg een beperkte rol spelen. Er wordt niet tot beperkt gecontroleerd op noodzakelijkheid, doelbinding, juistheid of volledigheid. Hoge werkdruk in combinatie met prioriteitstelling is een oorzaak van het achterwege laten van een dergelijke controle. Onbekendheid met de Wpg is ook een oorzaak.

De verantwoordelijkheid te voldoen aan artikel 3 en 4 wordt door functionarissen die artikel 8 informatie verwerken vaak belegd bij anderen binnen het korps. Men wijst dan naar de afdelingen die proceseigenaar zijn (als men ondersteunend werkt), functionarissen die een gegeven in een systeem invoeren, de informatieafdeling, leidinggevend, enzovoort. Ze achten zich daarmee niet verantwoordelijk voor het ondernemen van activiteiten om de artikelen na te leven. Dit geldt naast noodzakelijkheid, doelbinding, juistheid of volledigheid ook expliciet de rechtmatigheid van gegevens.

Een positieve impuls op het naleven van artikel 3 en 4 inzake artikel 8 informatie wordt soms gegeven door operationeel leidinggevend. Zij die nut en noodzaak van de wet zien, sturen binnen hun teams op naleving.

In artikel 9 Wpg wordt gesproken over het *'gericht verwerken van politiegegevens ten behoeve van een onderzoek met het oog op de handhaving van de rechtsorde in een bepaald geval'*. Net als bij artikel 8 informatie verwijzen ondersteunende medewerkers voor de verantwoordelijkheid voor de naleving van de artikel 3 en 4 naar proceseigenaren of naar de informatieafdeling.

Systemen en procedures borgen hier echter beter de rechtmatigheid, doelbinding en noodzakelijkheid, volledigheid en juistheid. Een melding van een onderzoek in de BVO is namelijk tevens te beschouwen als Wpg-melding. Meldingen Recherche Onderzoek (MRO) worden vervolgens automatisch aangemaakt voor correcte bovenregionale gegevensverspreiding. Het formulier hiervoor legt ook het doel van de rechercheonderzoeken vast.

Medewerkers van rechercheafdelingen hebben van origine veel oog voor de rechtmatigheid van verkregen informatie. Bij hen dreigt immers de mogelijkheid dat ze geconfronteerd worden met het schaden van vervolgingsmogelijkheden of het stranden van zaken vanwege het gebruik van onrechtmatig verkregen bewijs. Door hen verricht werk is dan nutteloos. Binnen Midden en West Brabant vindt vanuit dit perspectief ook achteraf (bij dossiervorming) een toets op rechtmatigheid plaats.

Informatie inzake artikel 10 *'verwerken van politiegegevens met het oog op het verkrijgen van inzicht in de betrokkenheid van personen bij bepaalde ernstige bedreigingen van de rechtsorde'* en artikel 12 informatie *'verwerken van politiegegevens met het oog op controle op en het beheer van een informant alsmede de beoordeling en verantwoording van het gebruik van informantgegevens'* wordt vooral verwerkt bij de CIE en de RID. Deze organisatieonderdelen besteden van oudsher al specifieke aandacht aan de kwaliteitsaspecten die nu ook door de Wpg in artikel 3 en 4 worden benadrukt.

Zo is er een handboek CIE waarin de belangrijkste werkprocessen staan beschreven. Daarnaast hebben de CIE medewerkers, inclusief de CIE chiefs

opleidingen gevolgd en zijn ze allemaal gecertificeerd. Binnen de CIE afdeling vindt strakke sturing en controle plaats op protocollen, regelgeving en werkregels. Daarbij hebben het Hoofd CIE, de Operationeel Chefs en de CIE OvJ ieder hun eigen rol en verantwoordelijkheid. Ze hebben veelvuldig gezamenlijk overleg. De CIE-OvJ vervult een specifieke kwaliteitsborgende rol door het houden van controle en toetsing.

Binnen de RID geldt een soortgelijk kwaliteitsregime.

De RID geeft wel aan dat er verbeteringen wenselijk zijn op het gebied van het gegevensbeheer. Niet alle gegevens worden gecontroleerd (GBA, vuurwapengevaarlijk etc.) door medewerkers die invoeren.

4.3.3

Verbeterpunten

Als verbeterpunten zijn te noemen:

- Het structureel organiseren van de monitoring van de kwaliteit van informatie met specifieke aandacht voor artikel 3 en 4 van de Wpg.
- Het bewaken van de uitvoering van de verschillende, in gang te zetten en gezette maatregelen om de kwaliteit van informatie te bevorderen en de resultaten van de inzet van maatregelen.
- Het bewaken van de samenhang van de in gang te zetten en gezette maatregelen.
- Het continueren van de activiteiten om de aandacht voor kwaliteit van informatie binnen alle geledingen van het korps te bevorderen. Naast activiteiten als scholing en voorlichting is daarbij structurele sturing vanuit de lijn op het besteden van aandacht gewenst als ook het organiseren van toezicht hierop. Een inhaalslag moet in dit kader worden gemaakt inzake artikel 8 informatie.
- Het ervoor zorgen dat het onderwerp Wpg hoog op de agenda van de korpsleiding staat (stuur hier in de praktijk ook op en vraag verantwoordingsinformatie), zodat naar de organisatie het signaal van urgentie en prioriteit uitgaat.

4.4 Gevoelige gegevens (artikel 5)

4.4.1

Norm

Art. 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

Uit het onderzoek is gebleken dat niet iedere politieambtenaar zich bewust is van deze bepaling. Een waarborg is niettemin dat veel medewerkers niet genelgd zijn deze gegevens op te nemen, tenzij dit strikt noodzakelijk is.

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

Het korps Midden en West Brabant heeft in 2010 het autorisatiebeheer aangepakt. Er is regiobreed een autorisatiematrix opgesteld, de autorisatieprocedures zijn herzien en de autorisaties van belangrijke applicaties zijn opgeschoond. De autorisatiematrix wordt sinds maart 2011 gebruikt en er is een tussentijdse evaluatie gepland naar de werking van de matrix. De bedoeling is dat het autorisatiebeheer in 2011 structureel volgens de ontwikkelde werkwijze wordt uitgevoerd.

Binnen de nieuwe werkwijze is de unit informatiemanagement is verantwoordelijk voor het op verzoek van leidinggevend en wijzigen of intrekken van autorisaties. Om dit te faciliteren zijn aanvraagformulieren ontworpen voor het aanvragen, wijzigen en intrekken van autorisaties.

Binnen het korps wordt voor opslag van politiegegevens ook gebruik gemaakt van kantoorautomatisering. Er zijn daartoe verschillende schijven en mappen. Korpsbreed is afgesproken dat één schijf mag worden gebruikt voor het opslaan van bestanden met operationele politiegegevens. Lijnchefs zijn verantwoordelijk voor het autorisatiebeheer en de bewaartermijnen van binnen de schijf voor hen gecreëerde mappen.

In de praktijk blijkt dat ook andere schijven worden gebruikt voor de opslag van operationele informatie (deze informatie kan ook politiegegevens bevatten). Het is daardoor mogelijk dat niet-geautoriseerden deze gegevens inzien of gebruiken. Op het moment van de audit is het korps bezig een kwaliteitsslag te maken op het eenduidig inrichten, gebruik en beheer (inclusief eenduidig autorisatiebeheer) van de schijven.

Autorisatieproces

In de praktijk blijkt binnen het korps dat de unit informatiemanagement conform afspraak benaderd wordt voor het aanvragen van autorisaties. Er komen bij de unit echter relatief weinig verzoeken binnen voor het wijzigen of intrekken van autorisaties. Daardoor worden bij de door- en uitstroom van medewerkers onterecht autorisatieprofielen behouden.

Door de beheerders van de unit informatiemanagement is een procedure ontwikkeld om bovenstaand probleem te ondervangen. Zij kunnen de toegekende autorisaties matchen met het personeelssysteem om te controleren of autorisaties goed toegekend zijn en beheerd worden. Als blijkt dat er verschil zit tussen het personeelssysteem i.v.m. de autorisatiematrix en de daadwerkelijke autorisaties, dan wordt dit gemeld bij leidinggevend. Vervolgens zetten deze een proces in gang om deze autorisaties op de functies aan te laten sluiten. Maandelijks worden de data van de medewerkers uit dienst gecontroleerd en per kwartaal de wijzigingen.

Protocolering

De aanvraag voor autorisaties komt in Expertdesk vtsPN,. Uitzonderingen worden ook vastgelegd.

De privacyfunctionaris heeft toegang tot de vastlegging van alle mutaties in autorisaties, inclusief die bij CIE, RID en OT.

De privacyfunctionaris heeft volledig inzicht bij welke functioneel beheerders of medewerkers een overzicht verkrijgbaar is van de actuele autorisaties.

Hiermee wordt voldaan aan de Wpg.

4.5.3

Verbeterpunten

Als verbeterpunten zijn te noemen:

- Voer de geplande tussentijdse evaluatie uit naar de werking van de autorisatiematrix. Verifieer bij de start van deze evaluatie dat de matrix Wpg-proof is (aan alle eisen van de Wpg voldoet).

- Zorg ervoor dat binnen het korps de procedure wordt toegepast die P-mutaties adequaat verwerkt tot autorisatiewijzigingen en zorg ervoor dat hier controle en toezicht op wordt gehouden.
- Ga door met het uitvoeren van de kwaliteitslag op de schijven binnen de kantoorautomatisering die voorkomt dat niet-geautoriseerden politiegegevens verwerken. Stuur op structurele borging van de kwaliteitsslag en houdt hierop toezicht.

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

Binnen het korps zijn procesbeschrijvingen opgesteld waarin is aangegeven hoe bij geautomatiseerd vergelijken en in combinatie met elkaar verwerken moet worden gehandeld. Daarbij zijn de grenzen aangegeven van geautomatiseerd vergelijken en in combinatie met elkaar verwerken alsook aan de protocolplicht. De beschrijvingen zijn via het intranet beschikbaar gesteld waarbij ook ontwikkelde casuïstiek is opgenomen.

In de praktijk zijn niet alle medewerkers in het korps bekend met de inhoud van de begrippen geautomatiseerd vergelijken en in combinatie met elkaar verwerken. Het is binnen het korps ook niet duidelijk wat de voorwaarden zijn voor het geautomatiseerd vergelijken en in combinatie met elkaar verwerken in concrete gevallen. Hierbij speelt specifiek voor informatiespecialisten de vraag of ze allerlei nieuwe technieken en applicaties mogen gebruiken die het mogelijk maken (ook oudere) informatie te ontsluiten.

Momenteel regelt elke unit/afdeling zelf hoe zij omgaan met geautomatiseerd vergelijken en in combinatie met elkaar verwerken. Vaak verwijzen medewerkers in het kader van deze verwerkingen naar de belangrijke rol die de ondersteunende dienstonderdelen als de Infodesk, de analisten, TIK's, DIK's en RIK's spelen. Hier besteedt men informatie vragen uit.

Het komt daarbij ook voor dat politieambtenaren gegevens ouder dan een jaar (die achter een 'schot' zijn geplaatst) middels geautomatiseerd vergelijken bij een dergelijk dienstonderdeel opvragen en krijgen. Bij het in combinatie met elkaar verwerken wordt ook gekeken in gegevens die ouder zijn dan 1 jaar.

De ondersteunende afdelingen geven aan een controle op rechtmatigheid niet uit te voeren. Zij verwijzen naar de verantwoordelijkheid van de proceseigenaren. Verzoeken tot in combinatie met elkaar verwerken aan de Infodesk gebeuren in principe schriftelijk. Verwerkingen blijken schriftelijk doorgaans niet als zodanig terug te vinden. Daaraan zal ook debet zijn dat er landelijk nog geen eenduidigheid bestaat over de uitleg van de twee begrippen.

Medewerkers binnen het korps gebruiken ook openbare bronnen bij het geautomatiseerd vergelijken. Uit veiligheidsoverwegingen gebeurt dat op stand-

alone PC's. Het korps biedt twee cursussen aan voor het gebruik van openbare bronnen voor politiewerk: de cursus internet rechercheren (IRN) en de cursus internet surveilleren (lager niveau).

4.6.3

Verbeterpunten

Als verbeterpunten zijn te noemen:

- Hanteer de procesbeschrijvingen die aangeven hoe bij geautomatiseerd vergelijken en in combinatie met elkaar verwerken moet worden gehandeld en houdt hierop toezicht.

4.7 Bewaartermijnen (artikel 14)

4.7.1

Norm

Politiegegevens worden vernietigd zodra zij niet langer noodzakelijk zijn voor de uitvoering van de dagelijkse politietaken (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 ten einde 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

In 2010 heeft het korps onderzoek verricht naar het archiefbeheer (papieren en digitale archieven en archiefbestanden in software). Geconcludeerd werd dat er binnen het korps geen sprake was van deugdelijk archiefbeheer. Het korps sluit voor verbeteracties aan bij samenwerkingspartner Zeeland. Daarnaast zijn de volgende ontwikkelingen relevant:

- er komt een nieuwe BVH versie. In de nieuwe release zijn echter problemen geconstateerd. De release houdt namelijk rekening met een verkeerde startdatum voor de bewaartermijnen.
- voor de netto werkbak van BVO is een geautomatiseerde schoningsmodule gerealiseerd, waarbij schonen van gegevens automatisch plaatsvindt. Deze module wordt nog geïmplementeerd.

Het niet kunnen voldoen aan de genoemde bewaartermijnen heeft verschillende oorzaken:

- landelijke ICT-systemen zijn niet voorzien van beheersmaatregelen op het gebied van termijnen voor verwijderen en vernietigen van politiegegevens.
- de landelijke ICT-systemen (BPS, BVH en BVO) zijn niet in staat om gegevens die automatisch ontoegankelijk te maken voor niet-geautoriseerden.
- het OM moet in afloopberichten toestemming geven voor de vernietiging van bepaalde gegevens, maar dit gebeurt in de praktijk niet of nauwelijks. Met het OM wordt bekeken hoe dit knelpunt opgelost kan worden (bijvoorbeeld met het draaien en aanleveren van bepaalde queries).
- het gebruik van kantoorautomatisering waar niet automatisch wordt geschoond. Het schonen en vernietigen van informatie in de kantoorautomatisering heeft een incidenteel karakter. Daarbij wordt niet zozeer gekeken naar bewaartermijnen, maar eerder naar de ruimte die de informatie inneemt.
- Onduidelijkheden in verantwoordelijkheid voor schoning.

Slechts in bijzondere gevallen en voor bepaalde doelen mogen politiegegevens in opdracht van het bevoegd gezag ter beschikking worden gesteld voor hernieuwd gebruik. Hier bestaat de verplichting tot vastlegging. Bij de privacyfunctionaris is

bekend dat zich binnen het korps casussen hebben voorgedaan waarbij gebruik is gemaakt van de mogelijkheid om gegevens hernieuwd te gebruiken, maar geen daarvan is geregistreerd. Er is in deze gevallen formeel sprake van onrechtmatige verwerkingen. Doorgaans zijn medewerkers zich hier niet van bewust en kent men de voorwaarden niet die vastzitten aan het hernieuwd gebruik van politiegegevens.

Binnen de CIE vindt elk half jaar controle op noodzaak van het bewaren van informatie plaats. Dit gebeurt door een document dat de runners opstellen en het document bevat de hoeveelheid gesprekken, de verstrekkingen en een algemeen beeld van de informant. Op basis van dit document licht de CIE OvJ en het CIE unithoofd de informant door. Recent heeft er een schoning plaatsgevonden en na de 10 jaar termijn wordt de informatie vernietigd.

Voor de netto werkbak voor BVO is de automatiseringsschoningsmodule gerealiseerd. Dit is een automatische schoningstool.

Ook bij de RID wordt toegezien op tijdige vernietiging van informatie.

4.7.3

Verbeterpunten

Als verbeterpunten zijn te noemen:

- Landelijk op de agenda houden van beheersmaatregelen voor verwijdering en vernietiging in de systemen BVH en BVO.
- Implementeer structureel de verbeteracties in het archiefbeheer (papieren en digitale archieven en archiefbestanden in software). Ontwikkel daarbij met regiokorps Zeeland een procedure voor bewaartermijnen en vernietiging.
- Zet in op bewustwording van regels voor bewaartermijnen, stuur hierop vanuit de lijn en organiseer meer toezicht.

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

Het ter beschikking stellen van politiegegevens geschiedt binnen het korps Midden en West Brabant via de binnen het korps gebruikte applicaties en shares. Ze komen ter beschikking voor de medewerkers die voor deze systemen en shares zijn geautoriseerd.

Bij het gebruik van shares geldt dat politiegegevens niet altijd voor iedereen direct beschikbaar zijn. Politieambtenaren die niet rechtstreeks betrokken zijn bij een onderzoek of deel uitmaken van een afdeling kunnen in de regel niet bij een share die hiervoor is ingericht, terwijl ze gezien de aard van de informatie soms wel recht hebben op toegang tot deze informatie.

Bij het ter beschikking stellen van politiegegevens aan andere politiemedewerkers binnen en buiten de regio spelen binnen Midden en West Brabant de ondersteunende dienstonderdelen als de Infodesk, TIK's, DIK's en RIK's een belangrijke rol. Verschillende andere politieonderdelen besteden informatievragen uit aan deze ondersteunende dienstonderdelen.

Bij het ter beschikking stellen van informatie door de Infodesk worden alle vragen en verzoeken met een module in BVO vastgelegd. Medewerkers van de Infodesk kunnen een beperkt deel van artikel 10 informatie raadplegen en zien, maar doorgaans wordt deze informatie niet ter beschikking gesteld. Als er een dergelijk

verzoek van een andere regio komt, speelt de Infodesk dit verzoek door naar de verantwoordelijke van het regiokorps, die het vervolgens verder afhandelt.

Binnen de districtsrecherche, de CIE en de RID wordt informatie vooral binnen de eigen afdeling gedeeld. Dit gebeurt altijd met de vermelding dat het alleen voor intern gebruik is. Ter beschikking stellen aan anderen (aan een ander researchteam) gebeurt alleen met toestemming van de officier van justitie. Als een onderzoek in gevaar komt door terbeschikkingstelling van gegevens, kan dit ook geweigerd worden. Dit wordt beargumenteerd vastgelegd in BVO.

4.8.3

Verbeterpunten

Als verbeterpunt is te noemen:

- Organiseer een uniforme toegang tot de in de kantoorautomatiseringsomgeving vastgelegde gegevens voor medewerkers die deze niet rechtstreeks kunnen benaderen maar (gezien de aard van de informatie) wel recht hebben op toegang tot deze 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. Art. 20 regelt de omstandigheden en voorwaarden voor de verstrekkingen aan derden structureel voor samenwerkingsverbanden.

4.9.2

Bevindingen

Het korps Midden en West Brabant heeft in 2010 geen substantiële groei signaleerd van het vastgelegde verstrekkingen. Tegelijkertijd moet worden vastgesteld dat niet alle verstrekkingen die het korps doet schriftelijk worden vastgelegd. Soms speelt hier het probleem dat medewerkers zich niet bewust zijn van de verplichting hiertoe; soms het probleem dat het wordt gezien als administratieve handeling met weinig meerwaarde.

Overigens geldt hierbij dat de registratie van verstrekkingen divers is, niet alleen binnen het korps maar ook binnen dienstonderdelen zelf. Zo heeft de Meldkamer een eigen standaardregistratiesysteem Topdesk maar hanteert ook separate lijsten voor de registratie van verstrekkingen. Wijkteams gebruiken bijvoorbeeld een registratiemodule van BVH, een eigen registratie en een procedure waarbij van verstrekkingen melding wordt gedaan bij leidinggevend.

Het ontbreken van een totaaloverzicht van verstrekkingen belemmert mogelijke sturing hierop. Doordat politiegegevens in meerdere verschillende systemen worden verwerkt is eenduidige herkenbare protocollering onmogelijk.

Om verstrekkingen correct te laten verlopen worden binnen het korps verschillende instrumenten ingezet:

- er is een verstrekkingwijzer opgesteld met voorschriften bij het doen van verstrekkingen. Deze is raadpleegbaar voor iedereen die geconfronteerd wordt met verstrekkingen.
- leidinggevend wordt gevraagd te sturen op het doen van juiste verstrekking van politiegegevens.
- om de leidinggevend te ondersteunen bij sturen op verstrekkingen zijn via de BIC handvatten aangereikt in de vorm van overzichten.

- verschillende dienstonderdelen binnen de organisatie hanteren processchema's waarin de Wpg aan werkprocessen wordt gerelateerd. Hier kan ook een onderdeel "verstrekkingen" zijn uitgewerkt met te volgen stappen.
- ondersteunende afdelingen verzorgen soms een kwaliteitscontrole bij het doen van verstrekkingen. Commentaar dat hieruit volgt leggen ze terug bij de lijnorganisatie (die de verstrekking afwerkt).
- voor verstrekking van artikel 9 en 10 is instemming van bevoegd gezag (OvJ dan wel burgemeester) vereist.
- er zijn convenanten opgesteld die het verstrekken van informatie aan ketenpartners reguleren. Binnen het korps is geïnventariseerd welke convenanten zijn afgesloten en is gestart met het Wpg-proof maken van de convenanten.

4.9.3 *Verbeterpunten*

Als verbeterpunten zijn te noemen:

- Breng de verstrekkingwijzer opnieuw onder de aandacht van de medewerkers. Dit kan bijvoorbeeld door de leidinggevendenden de verstrekkingwijzer bij een teamoverleg onderwerp van gesprek te laten maken.
- Ga verder met het Wpg-proof maken van de convenanten en het onder de aandacht van de medewerkers, leidinggevendenden en ondersteuners brengen van deze convenanten.
- Creëer een cultuur waarin leidinggevendenden medewerkers aanspreken op het niet vastleggen van verstrekkingen.
- Zorg voor maandelijkse overzichten van verstrekkingen, zodat hierop sturing kan plaatsvinden.
- Spreek leidinggevende aan op hun sturende taken inzake verstrekkingen.
- Evalueer het aanwezige stelsel aan maatregelen op functioneren en beoordeel of aanvullende beheersmaatregelen nodig zijn die gericht zijn op een volledige registratie van verstrekkingen.

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 aantal kennisneming- en verstrekkingverzoeken bij het korps Midden en West Brabant is sinds 2002 sterk gestegen. Daarnaast wordt de afhandeling gecompliceerd doordat de verzoeken vaak tegen verschillende wetgeving moeten worden afgewogen. De beschikbare formatiesterkte binnen het korps is niet meegestegen met de toename van het aantal verzoeken (gesproken wordt over gelijkblijvende dan wel krimpende capaciteit voor de uitvoering van de taak door de jaren heen). Door het te grote werkaanbod worden wettelijk voorgeschreven verwerkingstermijnen veelvuldig en ruimschoots overtreden. De korpsleiding is hiermee bekend en laat actief onderzoeken welke mogelijkheden er zijn om dit probleem te ondervangen. In september zijn reeds twee deeltijdmedewerkers aangesteld voor deze werkzaamheden. Voorst is er een pilot waarin een deel van de werkzaamheden decentraal is belegd.

Voor het afhandelen van verzoeken zijn binnen het korps een procesbeschrijving en sjabloonbrieven vastgesteld. Het jaarplan 2011 van de privacyfunctionaris meldt overigens dat de procedure verder gestroomlijnd wordt.

4.10.3 *Verbeterpunten*

- Zoek naar mogelijkheden om de verwerkingstermijnen voor verzoeken van betrokkenen terug te brengen.

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, tenminste tot de datum waarop de laatste controle (audit) is verricht.

4.11.2 Bevindingen

In het kader van zijn toezichthoudende taak houdt de privacyfunctionaris van een aantal protocolverplichtingen overzicht bij. Daarbij maken wij de volgende opmerkingen:

- De doelen van artikel 9 onderzoeken:
Dit overzicht was over 2010 niet compleet aangezien niet alle onderzoeken werden gemeld. In 2011 is gewerkt aan een systeem en verbetering van de procedure om een digitaal overzicht van alle onderzoeken te krijgen (inclusief duidelijke omschreven doelen). De privacyfunctionaris en de functioneel gegevensbeheerder hebben toegang tot dit bestand.
- Gegevens die op grond van ondersteunende taken worden vastgelegd (artikel 13):
Het korps gaat ervan uit dat voor het vastleggen van de gegevens nog steeds oude (onder de wet Politieregisters vastgestelde) reglementen gelden met bijbehorende registers, totdat deze vervangen zijn. Met betrekking tot Vreemdelingen, HKS en rapporten en Processen-verbaal, is een artikel 13 register opgemaakt. Vanwege het belang van landelijke eenduidigheid wordt voor verdere vernieuwing aangesloten bij landelijke initiatieven.
- De toekenning van autorisaties:
Er is een autorisatiematrix binnen het korps, er zijn autorisatieprocedures en de autorisaties van de belangrijkste systemen zijn geschoond. De privacyfunctionaris geeft aan dat hijzelf afwijkende autorisaties accordeert. Het korps is echter nog niet klaar: de procedures worden nog niet honderd procent gevolgd en nog niet alle applicaties zijn geschoond. Een tweede probleem betreft het gebruik van kantoorautomatisering die niet Wpg-proof is ingericht.
- De geautomatiseerde vergelijking van gegevens met openbare bronnen:
Geautomatiseerde vergelijking en verwerking in combinatie worden binnen het korps beperkt vastgelegd. Hierbij speelt ook de landelijke verwarring over hetgeen verstaan moet worden onder de termen.
- De hernieuwde verwerking van politiegegevens op grond van artikel 9 of 10, ex artikel 14:
Wat geldt voor geautomatiseerde vergelijking, geldt volgens het privacyjaarverslag ook voor de hernieuwde verwerking van artikel 9 en 10 politiegegevens. Gegevens over hernieuwde verwerking worden niet of beperkt vastgelegd, terwijl het wel voorkomt dat politiegegevens opnieuw worden verwerkt.

- De verstrekking van politiegegevens:
Bij het creëren van dit overzicht doen zich verschillende problemen voor. Ondanks deze problematiek heeft de privacyfunctionaris met de functioneel beheerders afgesproken dat hij periodiek een lijst krijgt van bepaalde, geregistreerde verstrekkingen. Deze toetst hij op bijzonderheden.
- Signalen van onbevoegde of onrechtmatige verwerkingen;
Deze worden binnen het korps niet structureel aangeleverd door leidinggevend. De privacyfunctionaris houdt wel een overzicht bij van de incidentele meldingen die hij ontvangt (al dan niet van de informatie-beveiligingsfunctionarissen of bureau interne onderzoeken) of zelf signaleert. Dat verwerkt hij in zijn jaarverslag.

4.11.3 *Verbeterpunten*

- Zet activiteiten in gang om volledig te voldoen aan de protocolplicht. Beleg externe problematiek (problematiek waarbij het korps geen zeggenschap over de oplossing heeft) daarbij expliciet bij de extern verantwoordelijken.

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 Midden- en West-Brabant is geen interne audit uitgevoerd. Wel zijn verschillende activiteiten uitgevoerd die corresponderen met activiteiten die binnen een interne audit verwacht kunnen worden. Twee initiatieven moeten in dit kader expliciet worden benoemd. Een uitgevoerde quickscan en het oprichten van een Borging Implementatie Commissie (BIC).

De quickscan richtte zich op de implementatie van de Wpg. Het rapport van deze quickscan is op 1 september 2011 opgeleverd. De rapportage presenteert een ordening van de activiteiten die het korps heeft verricht in het kader van de Wpg en een stand van zaken per september 2011.

De BIC (Borging Implementatie Commissie) is samengesteld uit functionarissen van verschillende geledingen binnen het korps. De BIC heeft een lijst met activiteiten op tien aandachtsgebieden opgesteld, waarmee de verdere implementatie (na decharge van het Wpg-project) en borging van de Wpg beoogd wordt.

Desondanks is de auditfunctie met betrekking tot de Wpg niet structureel belegd binnen het korps. Er is ook geen vaktechnisch verantwoorde en meerjarige audit ingericht.

4.12.3 *Verbeterpunt*

- Beleg structureel de auditfunctie met betrekking tot de Wpg en richt een vaktechnisch verantwoorde en meerjarig gerichte audit in.

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*

Binnen het korps is door de korpschef een privacyfunctionaris formeel aangesteld. Deze is aangemeld bij het CBP. De leidinggevende van de privacyfunctionaris is het hoofd van het Kabinet van de Korpsleiding. In verband met de aanwezigheid van een cluster privacy binnen de Unit Veiligheid en Integriteit (UVI), een stafafdeling van de Korpsleiding, heeft de privacyfunctionaris daar zijn werkplek.

De privacyfunctionaris is belast met Wpg-werkzaamheden op het gebied van advies en toezicht. Hij stelt hiertoe een jaarplan op en legt verantwoording af in een jaarverslag. Als adviseur is de privacyfunctionaris sterk betrokken bij:

- de implementatie van de Wpg geweest (dit project is eind 2010 opgeleverd).
- de borging implementatie commissie (BIC) bij de Wpg: de privacyfunctionaris is hiervan lid.
- het beoordelen van verstrekking- en kennisnemingverzoeken.
- het toetsen van convenanten. De privacyfunctionaris participeert in een commissie die belast is het toetsen of convenanten (nieuw en reeds bestaand) voldoen aan Wpg-regelgeving.
- de samenwerking met het RIEC en de gemeente Tilburg (afdeling veiligheid).
- het participeren in gepland en ongepland overleg binnen het korps. Zo weet de privacyfunctionaris uit verschillende geledingen van de organisatie wat er op Wpg-gebied speelt en hoe de wet leeft. Vanuit die kennis kan de privacyfunctionaris leidinggevend adviseren.

Het zwaartepunt van de werkzaamheden van de privacyfunctionaris heeft tot voor kort op de adviesfunctie gelegen. In het kader van zijn toezichtsfunctie houdt de privacyfunctionaris overzichten bij. Hij voldoet daarmee ten dele aan de protocolplicht uit de Wpg (artikel 32). In de paragraaf 'protocolplicht' maken wij opmerkingen bij de overzichten die de privacyfunctionaris bijhoudt of ontvangt.

Naast de privacyfunctionaris is binnen het korps een tweede privacyfunctionaris actief die met name belast is met het afhandelen van met WOB-verzoeken en overige verzoeken tot kennisgeving en verstrekking. Deze tweede privacyfunctionaris wordt ondersteund door twee medewerkers (in deeltijd) en kan terugvallen op de groepschef van het cluster privacy. Tussen bovengenoemde medewerkers is frequent contact voor informatie-uitwisseling en het afstemmen van werkzaamheden.

4.13.3 *Verbeterpunt*

- Inventariseer vanuit het takenpakket van de privacyfunctionaris het tijdsbeslag dat gepaard gaat met de uitvoering van de taken waar de privacyfunctionaris thans aan toekomt en maak een inschatting van tijdsbeslag dat gepaard gaat met (toezichthoudende) taken die nu blijven liggen. Leg de resultaten van deze inventarisatie voor bij de korpsleiding.

4.14 Functionaris Gegevensbescherming (artikel 36)

Het korps Midden en West Brabant heeft geen functionaris gegevensbescherming. Dit is ook geen formele eis vanuit de Wpg.

