



Ministerie van Veiligheid en Justitie

Audit Wpg politie Drenthe

Rapport

Datum
Status

6 januari 2012
Definitief

Colofon

Afzendgegevens

Departementale Auditdienst

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

Contactpersonen

drs.
drs.

T 070 370 65 60
M wpg@minvenj.nl

Projectnaam

Audit Wet Politiegegevens

Ons kenmerk

DDS/5719708/11

Auteurs

drs. ing.

Inhoud

Colofon 3

1 Assurance Verklaring 7

2 Samenvatting 9

3 Inleiding 17

- 3.1 Algemeen 17
- 3.2 Aanleiding 17
- 3.3 Doelstelling, aard en scope van de opdracht 17
- 3.4 Afbakening 18
- 3.5 Normenkader 18
- 3.6 Beperkingen voor de privacy audit 19
- 3.7 Onderzoeksmethoden en werkwijze 19
- 3.8 Doelgroep van het rapport 19

4 Bevindingen 20

- 4.1 Inleiding 20
- 4.2 Verantwoordelijke (artikel 1.f) 21
- 4.3 Kwaliteitsaspecten van politiegegevens (artikel 3 en 4) 21
- 4.4 Gevoelige gegevens (artikel 5) 24
- 4.5 Autorisatie (artikel 6) 24
- 4.6 Geautomatiseerd Vergelijken (GV)/In Combinatie Met Elkaar Verwerken (ICMEV)(artikel 11) 26
- 4.7 Bewaartermijnen (artikel 14) 28
- 4.8 Ter beschikking stellen (artikel 15) 29
- 4.9 Verstrekken (artikel 16/24) 31
- 4.10 Rechten van betrokkenen (artikel 25/28) 33
- 4.11 Protocolplicht (artikel 32) 34
- 4.12 Audits (artikel 33) 36
- 4.13 Privacyfunctionaris (artikel 34) 36
- 4.14 Functionaris Gegevensbescherming (artikel 36) 36

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 augustus en september 2011 is een privacy audit uitgevoerd bij het korps Drenthe.

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 Drenthe.

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 Drenthe, 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 Drenthe te nemen maatregelen. Ook is gebleken dat het korps Drenthe voor het volledig kunnen voldoen aan de Wpg eisen mede afhankelijk is van besluiten die buiten het korps Drenthe 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 Drenthe, 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 Drenthe. 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

2 Samenvatting

Vanaf augustus 2011 werken de drie noordelijke korpsen samen aan een doorstart van de implementatie van de Wpg. Daartoe hebben zij een gemeenschappelijke werkgroep opgericht met doorzettingsmacht. De werkgroep werkt samen met partners voor het realiseren van de vereiste veranderingen. De in deze rapportage van de Departementale Audit dienst aangegeven manco's en kanttekeningen worden door de werkgroep meegenomen bij het opstellen van een actieplan om de drie korpsen in opzet, bestaan en werking te laten voldoen aan de Wpg.

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 zoals genoemd in 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
Artikel 1.f, Verantwoordelijke			
1.f	Mandaatbesluit		Er is een vigerend mandaatbesluit van 27 december 2010, welke het mandaat regelt, het ondermaat, de volmacht, de subvolmacht en de machtigingen. Hiermee wordt voldaan aan de Wpg.
Artikel 3 en 4, Kwaliteitsaspecten van politiegegevens			
8.1 en 9.1	Onderscheid onderzoek Dagelijkse Politietaken (8) versus Bepaald geval (9)		Op Intranet is uitleg en voorlichting te vinden over de verschillen van artikel 8 en 9 van de WPG. Met casuïstiek worden voorbeelden gegeven. In opsporingsonderzoeken wordt buiten de omvang van de gegevensverzameling de duur van het onderzoek (MRO) en het gebruik van BOB-middelen gehanteerd als criteria. In de toekomst zal worden aangesloten bij de landelijke richtlijnen die hiervoor worden ontwikkeld. Hiermee wordt voldaan aan de Wpg.
3.1 t/m 3.3 (8) 4.1 (8)	Noodzakelijkheid (8) Doelbinding Rechtmatigheid Juistheid Volledigheid		Het korps Drenthe gebruikt TrueBlue voor bewaking van de kwaliteit van een aantal velden in BVH. Binnen het korps zijn Wpg cursussen gegeven. Daarna is het Wpg bewustzijn weggeëbd bij gebrek aan continuïteit in de communicatie. Het korps Friesland heeft de uitrol naar Blauw nog niet afgerond. Binnen het korps wordt een gebrek aan

Norm	Aspect		Bevinding en oordeel
			doorzettingsmacht ervaren en er vindt geen monitoring plaats op de uitvoering van de Wpg. 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		Het onderzoeksproces bevat waarborgen voor deze aspecten. De PDCA-cyclus sluit via het OM en de rechter. Tevens is bij de recherche nu meer aandacht voor de vastlegging van bronnen en hoe informatie uit andere onderzoeken wordt verkregen. Er is een registratiefunctie om toe te zien op de kwaliteit. Hiermee wordt voldaan aan de Wpg.
3.4 (10 en 12) 4.1 (10 en 12)	Noodzakelijkheid (10 en 12) Doelbinding Rechtmatigheid Herkomst en wijze van verkrijging Juistheid Nauwkeurig Volledigheid		De CIE heeft een proceshandboek. De CIE OvJ houdt toezicht. Bij de RID liggen de kwaliteitscriteria al in het doel van de taak vast. Hiermee wordt voldaan aan de Wpg.
4.3	Beveiliging (isolatie)		Het korps heeft nog geen beleid voor de mappenstructuur. De landelijke en regionale informatiesystemen zijn nog niet Wpg-proof. Hiermee wordt niet voldaan aan de Wpg.
Artikel 5, gevoelige gegevens			
	• Gevoelige gegevens		Er zijn geen niet-toegestane gegevensverzamelingen gebaseerd op gevoelige gegevens aangetroffen. Het korps heeft regels voor de omgang met gevoelige gegevens op intranet staan. Hiermee wordt voldaan aan de Wpg.
Artikel 6, Autorisatie			
	• Korpsautorisatiematrix		Er is een autorisatiematrix van SSCN. Hiermee wordt voldaan aan de Wpg.
	• Aanvraagproces		Het aanvraagproces van autorisaties verloopt via SSCN en vtsPN, en is gedocumenteerd. Hiermee wordt voldaan aan de Wpg.
	• Wijziging en verwijdering		Het verwijderproces van autorisaties verloopt via SSCN en vtsPN, en is gedocumenteerd. De rechten op de mappenstructuur van de kantoorautomatiseringsomgeving zijn echter minder goed geregeld. Er is nog geen ICT systeem beschikbaar dat reconciliatie en schoning adequaat ondersteunt. Er is sprake van een, niet geautomatiseerde, handmatige administratie. Dit belemmert een snel overzicht van alle verleende autorisaties. Hiermee wordt niet 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. De CIE OvJ heeft het autorisatiebeleid goedgekeurd.

Norm	Aspect		Bevinding en oordeel
			Hiermee wordt voldaan aan de Wpg.
32.1.c	Protocollering autorisaties		Binnen SSCN wordt iedere aanvraag voor een mutatie op een autorisatie geregistreerd. Hiermee wordt voldaan aan de Wpg.
32.3 voor 32.1.c	Bewaren protocolgegevens autorisaties		Binnen SSCN wordt iedere aanvraag voor een mutatie op een autorisatie bewaard. Hiermee wordt voldaan aan de Wpg.
Artikel 11, Geautomatiseerd vergelijken en in combinatie met elkaar verwerken			
	• Hanteerbare interpretatie		De begrippen geautomatiseerd vergelijken en in combinatie met elkaar verwerken zijn nog onvoldoende bekend binnen het korps. Hiermee wordt niet voldaan aan de Wpg.
	• Aangewezen functionarissen		De Infodesk wordt niet altijd benut voor het in combinatie met elkaar verwerken en geautomatiseerd vergelijken. Ondanks dat er een concept werkinstructie is, zijn de rollen in het kader van de Wpg nog niet daadwerkelijk expliciet belegd. Hiermee wordt deels voldaan aan de Wpg.
11.4	Bevoegd gezag		Doordat in combinatie met elkaar verwerken niet eenduidig is vastgesteld, is het onbekend wanneer het bevoegd gezag moet worden geraadpleegd. Hiermee wordt niet voldaan aan de Wpg.
32.1.d en h	Protocollering 11.1, 11.2, 11.4 en 11.5		Aanvragen die via de Infodesk binnenkomen worden geprotocolleerd. Hiermee wordt voldaan aan de Wpg.
32.3 voor 32.1.d en h	Bewaren protocolgegevens 11.1, 11.2, 11.4 en 11.5		Aanvragen die via de Infodesk binnenkomen worden bewaard. Hiermee wordt voldaan aan de Wpg.
Artikel 14, Bewaartermijnen			
8.2 en 8.3	(8) van 1 tot 5 jaar		Gegevens ouder dan één jaar na eerste vastlegging in BVH worden niet achter schot gezet. Medewerkers gaan ervan uit dat de gegevens die ze te zien krijgen ook mogen worden gebruikt voor verdere verwerking. Met name medewerkers op operationeel niveau zijn zich hiervan niet voldoende bewust. Hiermee wordt niet voldaan aan de Wpg.
8.6	(8) verwijderen na 5 jaar		De regels voor de verwijdering van oude artikel 8 gegevens zijn moeilijk uitvoerbaar omdat het handmatig moet gebeuren. Daardoor krijgt het verwijderen en schonen nog onvoldoende prioriteit. Er is met betrekking tot artikel 8 en 9 Wpg geen procedure aangetroffen voor de omgang met bewaartermijnen en vernietiging van politiegegevens. Hiermee wordt niet voldaan aan de Wpg.
14.1 (8)	(8) vernietigen na 5 jaar verwijderd		Artikel 8 gegevens worden nog niet op het voorgeschreven moment vernietigd. Hiermee wordt niet voldaan aan de Wpg.]
9.4	(9) verwijderen na OH plus ½ jaar		Het opschonen van artikel 9 onderzoeken gebeurt nog onvoldoende. Hierbij is de ketensamenwerking

Norm	Aspect		Bevinding en oordeel
			en specifiek de overdracht van informatie over afgesloten zaken van OM naar de politie een aandachtspunt. Hiermee wordt niet voldaan aan de Wpg.
14.1 (9)	(9) vernietigen na 5 jaar verwijderd		Doordat het juiste moment van verwijdering niet bekend is, kan niet 5 jaar na verwijdering worden vernietigd. Hiermee wordt niet voldaan aan de Wpg.
10.6	(10) verwijderen na 5 jaar geen subjectwaardige registratie		De CIE OvJ voert periodiek controles uit waarbij ook naar de bewaartermijnen wordt gekeken. Hiermee wordt voldaan aan de Wpg.
14.1 (10)	(10) vernietigen na 5 jaar verwijderd		De CIE OvJ voert periodiek controles uit waarbij ook naar de bewaartermijnen wordt gekeken. Hiermee wordt voldaan aan de Wpg.
14.3	Hernieuwde verwerking		Gegevens worden niet verwijderd. Er is geen proces ingericht voor hernieuwde verwerking in opdracht van het bevoegd gezag. Hiermee wordt niet voldaan aan de Wpg.
32.1.e	Protocollering 14.3		Er is geen proces voor hernieuwde verwerking. Hiermee wordt niet voldaan aan de Wpg.
32.3 voor 32.1.e	Bewaren protocolgegevens 14.3		Er is geen proces voor hernieuwde verwerking. Hiermee wordt niet voldaan aan de Wpg.
12.2	(12) gebruiken tot 4 maanden		De CIE OvJ voert periodiek controles uit waarbij ook naar de bewaartermijnen wordt gekeken. Informatie van informanten 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. Bij de RID gebeurt dit elke 5 jaar. Bij de CIE toetst de CIE-OvJ jaarlijks het informantenregister. Hiermee wordt voldaan aan de Wpg.
Artikel 15, Ter beschikking stellen			
• Infodesk voor bevraging			In de praktijk verloopt niet alles via de Infodesk. Ter beschikking stelling van politiegegevens wordt niet meer in de BVO Infodesk module geregistreerd. Aan de protocolplicht wordt niet altijd voldaan. Informatie wordt niet altijd over de regio's heen ter beschikking gesteld wordt vanwege het feit dat sommige informatie in de mappenstructuur moet worden opgeslagen. Hiermee wordt niet voldaan aan de Wpg.
• Codering			Er is een overzicht van de coderingen die kunnen worden gebruikt door de CIE en tevens in het kader van een MRO. Deze coderingen staan vermeld in het Proceshandboek van de CIE. Hiermee wordt voldaan aan de Wpg.

Norm	Aspect		Bevinding en oordeel
• Aanwijzing Bevoegd Functionaris			De bevoegd functionarissen zijn aangewezen en initieel opgeleid. Hiermee wordt voldaan aan de Wpg.
• Opleiding Bevoegd Functionaris			De bevoegd functionarissen zijn onder andere de recherchechefs. Zij hebben een hoge positie binnen de organisatie, maar houden zich inhoudelijk weinig bezig met de WPG. De bevoegd functionarissen zijn vooral in 2009 opgeleid. Hun kennis van de Wpg is echter deels weggezaakt. Het korps biedt in 2012 een opfriscursus aan. Hiermee wordt deels voldaan aan de Wpg.
15.2	Weigeringgronden		De weigeringgronden zijn onderwezen aan de bevoegd functionaris. Hiermee wordt voldaan aan de Wpg.
Artikel 16 t/m 24, Verstrekking			
• Verstrekkingenwijzer (landelijk)			De korpsen Groningen, Friesland en Drenthe hebben een gezamenlijk Intranet, waarop de landelijke verstrekkingenwijzer is geplaatst. De verstrekkingenwijzer wordt gehanteerd, maar is niet bij iedereen bekend. Hiermee wordt deels voldaan aan de Wpg.
• Proces voor convenanten			Er is centraal geen procedure vastgesteld voor verstrekkingen aan ketenpartners en er is geen sturing op de noodzaak en de inhoud van convenanten. De opgestelde convenanten voldoen niet in alle gevallen aan de gestelde criteria. Indien ketenpartners buiten de convenanten om informatie proberen te verkrijgen, bepalen medewerkers zelfstandig hoe zij hiermee omgaan. Hierop wordt niet gestuurd. Samen met de regio's Friesland en Groningen wordt thans een inhaalslag gemaakt om de bestaande samenwerkingsverbanden WPG-proof te maken. Nieuwe besluiten worden door de gemandateerde leidinggevers gemaakt en voor een juridische toetsing aangeboden aan de Juridische afdeling. Indien akkoord bevonden wordt het besluit getekend door de partners en gearhiveerd bij de Juridische Dienst. Het besluit en het eventuele convenant worden intern gepubliceerd op Intranet en zijn aldus zichtbaar en beschikbaar voor de medewerkers. Hiermee wordt deels voldaan aan de Wpg.
• Proces voor Artikel 20 Besluiten			Er zijn weinig convenanten waar een besluit aan ten grondslag ligt. Bij een aantal convenanten ontbreekt het artikel 20 besluit. Eind 2011 zijn de korpsen Groningen, Friesland en Drenthe bezig met een inhaalslag. Hiermee wordt deels voldaan aan de Wpg.
• Verstrekkingenschema (regio)			Het korps heeft op het intranet een gegevensbeheerlijst staan met de organisaties

Norm	Aspect	Bevinding en oordeel
		waaraan informatie mag worden verstrekt. Het is echter niet duidelijk wie verantwoordelijk is voor het proces in totaliteit. Hiermee wordt deels voldaan aan de Wpg.
• Proces voor geautomatiseerde verstrekking		Het korps geeft aan dat er momenteel geen geautomatiseerde verstrekkingen plaatsvinden, anders dan de in het Besluit politiegegevens toegestane verstrekkingen, zoals aan RDW bij het invorderen van een rijbewijs of kentekenbewijs. Vanuit Amazone vinden geen externe verstrekkingen plaats. Hiermee wordt voldaan aan de Wpg.
7.2	Geheimhouding	Bij het Veiligheidshuis hebben de ketenpartners getekend voor geheimhouding. Ook in andere convenanten is de geheimhoudingsplicht vermeld. Geheimhoudingsplicht ten aanzien van politiegegevens is vastgelegd in de artikel 20 besluiten. Voor de CIE geldt dat informatie uitsluitend op grond van PV wordt verstrekt, met ondertekening van hoofd CIE en met steekproefsgewijze goedkeuring van de CIE OvJ. CIE benadrukt dat de door hen verstrekte gegevens niet verder mogen worden doorverstrekt. Hiermee wordt voldaan aan de Wpg.
32.1.f	Protocollering verstrekking	Het grootste gedeelte van de verstrekkingen gebeurt via de Infodesk en de CIE. Bij de Infodesk en de CIE is de vastlegging van verstrekkingen goed geregeld. Voor andere afdelingen en onderdelen geldt dat vastlegging van verstrekkingen met een I90 formulier gebruikelijk is, maar nauwelijks plaatsvindt. Hiermee wordt deels voldaan aan de Wpg.
32.3 voor 32.1.f	Bewaren protocolgegevens verstrekking	De wel vastgelegde gegevens over verstrekkingen worden bewaard. Hiermee wordt voldaan aan de Wpg.
• Toezicht door leidinggevenden op verstrekkingen en protocollering		Bij de Infodesk wordt toezicht gehouden door het Hoofd Infodesk. Bij het management van de overige onderdelen van het korps bestaat geen automatisme om verstrekkingen te toetsen. De begrippen subsidiariteit en proportionaliteit worden onvoldoende toegepast. Het zicht op verstrekkingen door medewerkers van andere afdelingen ontbreekt grotendeels. Er is korpsbreed geen sturing op de noodzaak en de inhoud van convenanten. Hiermee wordt niet voldaan aan de Wpg.
Artikel 25 t/m 31, Rechten van de betrokkene		
25.1	Verzoek om kennisneming	Er is een procesbeschrijving over verstrekken van gegevens aan burgers in verband met het inzagerecht. In korps Drenthe is deze taak vrijwel

Norm	Aspect		Bevinding en oordeel
			volledig bij de privacyfunctionaris belegd, die formeel is geplaatst bij de Juridische dienst van het SSCN. De privacyfunctionaris handelt verzoeken af in het kader van de rechten van betrokkenen. Dit is een ongewenste vermenging van functies, aangezien de privacyfunctionaris toezicht dient te houden op dit proces. Dit is bij het onderwerp "Privacyfunctionaris" verder uitgewerkt. Hiermee wordt voldaan aan de Wpg.
28.1 t/m 28.3	Correctie		Het proces voor rechten van betrokkenen wordt goed doorlopen. Hiermee wordt voldaan aan de Wpg.
Artikel 32, Protocolplicht (32.1.c, d, e, f en h behandeld bij thema's)			
9.2 en 32.1.a	Protocollering doel onderzoek		Doelbinding conform artikel 9.2 wordt niet altijd op de juiste wijze vastgelegd. De drie noordelijke korpsen hebben plannen BOSZ te implementeren, waarin onder andere het doel van een onderzoek wordt vastgelegd. Hiermee wordt deels voldaan aan de Wpg.
32.3 voor 32.1.a	Bewaren protocolgegevens doel onderzoek		De MRO wordt bewaard in VROS. Hiermee wordt voldaan aan de Wpg.
13.4 en 32.1.b	Protocollering Artikel 13 gegevensverzameling en		Het korps Drenthe beschikt deels over een Artikel 13 Register. Hiermee wordt deels voldaan aan de Wpg.
32.3 voor 32.1.b	Bewaren protocolgegevens Artikel 13 gegevensverzameling en		Het korps Drenthe beschikt deels over een Artikel 13 Register. Hiermee wordt deels voldaan aan de Wpg.
32.1.g	Protocollering onrechtmatige handeling		Een overzicht van onrechtmatige verwerkingen ontbreekt. Hiermee wordt niet voldaan aan de Wpg.
32.3 voor 32.1.g	Bewaren protocolgegevens onrechtmatige handeling		Een overzicht van onrechtmatige verwerkingen ontbreekt. Hiermee wordt niet voldaan aan de Wpg.
32.2	Gemeenschappelijke verwerking		Het Shared Service Center Noord (SSCN) is een gemeenschappelijk onderdeel van drie korpsen, waarbij iedere medewerker onder een van de drie korpschefs valt. Door het ontbreken van een landelijke richtlijn voor het positioneren een gemeenschappelijk onderdeel in relatie tot de Wpg, kunnen wij ons vooralsnog geen onderbouwd oordeel vormen over het wel of niet voldoen aan de Wpg. Wij adviseren een nader onderzoek.

Norm	Aspect		Bevinding en oordeel
Artikel 33, Audits			
RPAP 3.1	Interne audit-functie		De interne Wpg audit-functie is niet structureel belegd. Hiermee wordt niet voldaan aan de Wpg.
RPAP 3.4	Interne audit-plan		Er is geen vaktechnisch verantwoord en meerjarig intern Wpg audit-plan. Hiermee wordt niet voldaan aan de Wpg.
RPAP 3.6	Interne audit-rapport		Er is geen intern Wpg audit-rapport. Hiermee wordt niet voldaan aan de Wpg.
Artikel 34, Privacyfunctionaris			
34.1 en 34.4	Benoemd en gemeld		De privacyfunctionaris voor het korps Drenthe is ondergebracht bij de juridische dienst van het SSCN en is aangemeld bij het CBP. Hiermee wordt voldaan aan de Wpg.
34.2	Overzicht over protocollering		Er is geen overzicht bijgehouden van de schriftelijke vastlegging van onder meer geautomatiseerde vergelijkingen, onrechtmatige verwerkingen en verstrekkingen. Hiermee wordt niet voldaan aan de Wpg.
34.3	Jaarverslag		Alhoewel de privacyfunctionaris zijn adviestaak uitvoert, is er beperkt invulling gegeven aan de toezichthoudende taak. De privacyfunctionarissen bij het SSCN voeren andere taken uit dan de toezichthoudende. Er is geen jaarverslag over het jaar 2008. Het was de intentie over 2010 één rapport op te stellen voor Groningen, Friesland en Drenthe. Door een veranderende prioriteitstelling in het korps is dit verslag echter niet opgesteld. Hiermee wordt niet voldaan aan de Wpg.
Optioneel Artikel 36, Functionaris Gegevensbescherming			
36.1 en 36.2	Benoemd		Niet van toepassing. Er is geen functionaris gegevensbescherming benoemd.
Wbp 63.3	Gemeld		Niet van toepassing.
Wbp 64.1 t/m 64.4	Toezichthoudende rol		Niet van toepassing.

3 Inleiding

3.1 Algemeen

In opdracht van de landelijke stuurgroep Wpg, waarin de Directeur-Generaal Politie en het KBB zijn vertegenwoordigd, heeft de DAD van het ministerie van VenJ een privacy audit uitgevoerd bij het korps Drenthe 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 Drenthe in de maanden augustus en september 2011.

3.2 Aanleiding

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

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

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

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

3.3 Doelstelling, aard en scope van de opdracht

Doelstelling

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

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 Drenthe beoogt te voldoen aan de beheersdoelstellingen die bij of krachtens de Wpg gelden.

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

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

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

3.4 Afbakening

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

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

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 Drenthe en het Openbaar Ministerie, deelwaarnemingen in de procesbeschrijvingen en andersoortige documentatie en deelwaarnemingen in informatiesystemen.

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

Het eindrapport is met inachtneming van het ontvangen commentaar vastgesteld.

3.8 Doelgroep van het rapport

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

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

De stuurgroep wordt voorgezeten door drs.

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

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

De specifieke doelgroep waarvoor het rapport is bestemd bestaat uit:

- onze opdrachtgever zoals bovengenoemd;
- de korpsbeheerder;
- de korpschef;
- de Hoofd Officier van Justitie mr. ;
- de privacyfunctionaris ;
- de voorzitter van het College Bescherming Persoonsgegevens.

Het rapport mag uitsluitend met toestemming van de korpsbeheerder dan wel de korpschef van korps Drenthe 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 *Interregionale opstart en Wpg project*

Bij de politiekorpsen Groningen, Friesland en Drenthe is in september 2009 de implementatie in noordelijk verband opgezet op basis van de formule van een interregionaal gecoördineerd en afgestemd, maar per korps zelfstandig en onder eigen regie te doorlopen proces. De gezamenlijke projectgroep heeft begin 2010 een veelheid aan procesbeschrijvingen opgeleverd. Deze zijn ter goedkeuring voorgelegd aan de respectievelijke korpsleidingen. De besluitvorming op deze producten heeft in het Regionaal Management Team plaatsgevonden, maar de implementatie is gestagneerd mede onder invloed van de vorming van het Shared Service Center Noord (SSCN).

Gesignaleerd wordt dat vanuit de inherente attitude van veel ambtenaren van politie en de persoonlijke invulling van een aantal sleutelfunctionarissen in het kader van de Wpg veel goede dingen worden gedaan op het gebied van privacy bescherming enerzijds en het voorzichtig omgaan met informatie anderzijds. Verder is er over het algemeen sprake van een hoog Wpg bewustzijn bij de specifieke informatie-verwerkende afdelingen zoals CIE, RID en Infodesk/RIK. Waar het volgens geïnterviewden en de geraadpleegde documenten aan ontbreekt, is dat er binnen het korps onvoldoende urgentie en prioriteit voor de implementatie van de Wpg is geweest. Daardoor wordt door medewerkers op dit dossier een gebrek aan doorzettingsmacht ervaren.

De huidige procesbeschrijvingen en processchema's spreken de meeste uitvoerende collega's in het algemeen niet aan. De procesbeschrijvingen zijn niet actueel en vaak door de NIM-bril, de TGO-bril of Abrio-bril opgesteld. De bestaande beschrijvingen zijn niet vanuit de Wpg opgesteld. Er zijn een aantal stappen binnen de werkprocessen beschreven, maar niet vanuit het oogpunt en de boodschap van de Wpg. De organisatie en inrichting van de processen zijn voor de Wpg nog niet evenwichtig.

Het korps heeft op intranet een site met daarop alle beschikbare procesbeschrijvingen. Uit de interviews komt echter naar voren dat er op de werkvloer behoefte is aan werkinstructies, stroomschema's etc. waarin de regelgeving van de Wpg gebruikersvriendelijk en functiegericht wordt beschreven. Dit biedt de functionaris handvatten bij het uitvoeren van de dagelijkse werkzaamheden conform de Wpg. In lijn hiermee is er in opzet ook specifiek te weinig vastgelegd over het hanteren van een aantal artikelen uit de Wpg, waaronder bijvoorbeeld het ter beschikking stellen en het verstrekken van politiegegevens. Hierdoor bestaat er nog veel onduidelijkheid over het vastleggen van verstrekkingen en wordt de reikwijdte van deze artikelen niet optimaal benut.

Er is geen overzicht per korpsonderdeel van alle specifieke verwerkingen/regimes en de daartoe behorende proceseigenaren aangetroffen. De borging en naleving van de Wpg is nog niet ingebed in de managementcontrolcyclus. Uit onze interviews komt naar voren dat men zich hiervan bewust is binnen het korps.

4.1.2 *Regie en doorzettingsmacht voor de Wpg implementatie*

Waar het volgens geïnterviewden en de geraadpleegde documenten aan schort, is dat het onderwerp Wpg niet hoog genoeg op de strategische agenda van de korpsleiding staat, waardoor urgentie en prioriteit ontbreekt. Op dit dossier wordt een gebrek aan doorzettingsmacht ervaren, doordat gerichte sturing door de korpsleiding ontbreekt en er geen monitoring plaatsvindt op de uitvoering van de Wpg.

4.2 **Verantwoordelijke (artikel 1.f)**

4.2.1 *Norm*

Mandaatbesluit

4.2.2 *Norm*

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

4.2.3 *Bevindingen*

Er is een vigerend mandaatbesluit van 27 december 2010, welke het mandaat regelt, het ondermaat, de volmacht, de subvolmacht en de machtigingen. Hiermee wordt voldaan aan Art. 1.f van de Wpg.

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*

Met de kwaliteitsaspecten rechtmatigheid, doelbinding en noodzakelijkheid dient al bij de eerste vastlegging van persoonsgegevens rekening gehouden te worden. Daarna zijn vrijwel alle geledingen van de politie erbij betrokken.

Het korps heeft de volgende criteria voor het verschil tussen artikel 8 en artikel 9 onderzoeken op intranet geplaatst, aangevuld met casuïstiek:

- Artikel 8 gaat over de verwerking van persoonsgegevens met het oog op de uitvoering van de dagelijkse politietaak, ofwel het 'basispolitiewerk'. Een paar voorbeelden hiervan kunnen zijn:
 - Surveillance.
 - Afhandeling van de verkeersproblematiek.
 - Het verlenen van hulp.
 - Het handhaven van wetten en regels.
 - Eenvoudige recherche werkzaamheden zoals het onderzoeken van diefstallen en inbraken ('6-uurszaken'), het veilig stellen van sporen en het opnemen van een aangifte van een inbraak.

- Een artikel 9 verwerking houdt in dat de Politie overgaat tot een gerichte en omvangrijke verzameling van gegevens over personen, met als doel de rechtsorde te herstellen of schendingen daarvan te voorkomen. Waar het in deze gevallen om gaat is dat de politie, naar aanleiding van een naar tijd beperkte gebeurtenis of situatie dan wel een serie van gebeurtenissen, over gaat tot gerichte en omvangrijke gegevensverzameling over personen. Een paar voorbeelden hiervan kunnen zijn:
 - Een opsporingsonderzoek (er is bijvoorbeeld een moord gepleegd).
 - Een verkennend onderzoek (er is veel drugsmisdaad in een bepaald gebied gesignaleerd, of de aanpak van de overlast bij een school of coffeeshop).
 - Landelijke coördinatieonderzoeken (bijvoorbeeld landelijke verkiezingen).
 - Het bewaken en beveiligen van personen.
 - Het ten aanzien van een veelpleger een dossier opmaken ten behoeve van de verdere aanpak.
- Binnen regio-Noord is afgesproken dat ten minste deze zaken een artikel 9 verwerking zijn:
 - Binnen tactische opsporing, TGO / SGB0 is er altijd sprake van een artikel 9 onderzoek.
 - Als er BOB aanvraag is gedaan, met uitzondering van het alleen opvragen van informatie / beelden (artikel 126 n t/m ni Wetboek van Strafvordering).
 - Als de onderzoeksduur de termijn van 5 dagen overschrijdt, of als de verwachting is dat de termijn van 5 dagen wordt overschreden.

De kennis over de eisen die de Wpg stelt aan persoonsgegevens is niet bij alle onderdelen van de politie even groot. Medewerkers in de dagelijkse politietaak zijn zich over het algemeen minder bewust van de eisen die de WPG stelt aan het verwerken van persoonsgegevens dan rechercheurs en medewerkers van de afdelingen RID en CIE.

Bij de afdeling RID is de Wpg afdelingsbreed behandeld. Het proces van de RID is echter niet beschreven, maar zit in hoofden van medewerkers. Het toezicht op werken conform de Wpg is hier nog niet voldoende ingeregeld.

De CIE en de CIE OvJ hebben een rol in de borging van de kwaliteit van de informatie. Met name de CIE OvJ heeft een controlerende taak op het werk van de CIE.

In de praktijk wordt soms afgeweken van het proceshandboek CIE. Dan wordt CIE informatie bijvoorbeeld verstrekt aan het district Assen. Het district gaat ermee naar de driehoek en op die manier komt informatie alsnog bij de gemeente terecht. Dit is niet conform de voorschriften van de WPG.

Ook de privacyfunctionaris heeft een toezichthoudende taak op de naleving van de Wpg door de medewerkers. Aan deze toezichtstaak komt de privacyfunctionaris echter niet toe.

Beveiliging van gegevens is door het korps heen op verschillende manieren ingericht. Daar waar extra gevoelige gegevens worden bewaard (zoals bij de RID en de CIE) zijn extra fysieke beveiligingsmaatregelen getroffen.

BVH en BVO voorzien in logging van de verwerking van gegevens. Bekend is dat logging volledig maar low level en afhankelijk van de systemen plaatsvindt in verband met de beperkte opslagcapaciteit van loggegevens.

In het kader van de beveiliging van gegevens is de gebruikersvriendelijkheid van BVH en BVO een aandachtspunt. Medewerkers zoeken naar andere mogelijkheden

(opslag op gemeenschappelijke of persoonlijke schijf) om politiegegevens te bewaren. De beveiligingsmaatregelen, zoals logging en autorisatiebeheer, zijn op deze gegevens slechts in beperkte mate van toepassing.

De volgende beheersmaatregelen zijn geïmplementeerd:

- Registratiesystemen zoals BVH en BVO dwingen via workflow bepaalde vastleggingen af; daardoor wordt bijvoorbeeld volledigheid nagestreefd, denk aan het MRO bij BVO.
- Een Informatie Centrum op lokaal niveau zal in de toekomst meer waarborgen geven voor de kwaliteit van de informatie. Er wordt dan bijvoorbeeld gekeken of het niet om aannames gaat. De informatie moet dan worden veredeld en passen binnen wettelijke kaders.
- Bij de CIE wordt de kwaliteit in het bijzonder geborgd door de toezichhoudende rol van CIE OvJ. In het proceshandboek CIE wordt één landelijke uniforme gegevensverwerking beschreven voor de Regionale Criminele Inlichtingen Eenheden.
- Wanneer gegevens uit afgesloten onderzoeken voor een ander doel worden gebruikt dan waarvoor ze zijn verkregen, moet toestemming van de BF worden verkregen.

Kwaliteitsbewaking met TrueBlue in BVH

Het korps Drenthe gebruikt het scanhulpmiddel TrueBlue voor de bewaking van de kwaliteit van een aantal velden in BVH. Landelijk is er een lijst met kennisregels opgemaakt, die elk korps naar behoefte in BVH kan activeren. Door het korps Drenthe worden geen eigen kennisregels gemaakt. De beschikbare kennisregels zijn gedocumenteerd. Daarnaast heeft het korps een 'Beleidsnota invoer kwaliteitscontrole' (2007) als een aangepaste versie van 'Invoer kwaliteitscontrole en TrueBlue' (2009), het document 'Invoer en vaststelling kwaliteitscontrole', de procedure 'Borging en aanpassen autorisatie' en de Handleiding 'Onderhoudsmenu TrueBlue'.

Informatievoorziening

Er bestaat nog geen vigerend beleid voor het beheer en de inrichting van de mappenstructuur. Er is een poging gedaan om uniformiteit te bereiken bij het gebruik en beheer van de mappenstructuur bij 8Noord, maar hierbij is nog niet het gewenste doel bereikt. Via het project 'Sturen op opslag' zijn initiële beleidsafspraken geformuleerd.

De landelijke systemen, zoals onder andere BVH en BVO, en de regionale systemen zijn niet voorzien van beheersmaatregelen op het gebied van termijnen voor verwijderen en vernietigen van politiegegevens. De regels voor de verwijdering van oude gegevens zijn moeilijk uitvoerbaar omdat het voorsnóg handmatig moet gebeuren.

4.3.3

Oordeel over artikel 3 en 4

Het korps heeft de criteria voor het verschil tussen Art. 8 versus Art. 9 onderzoeken op intranet geplaatst, inclusief casuïstiek. Er zijn Wpg cursussen gegeven. Daarna is het Wpg bewustzijn weggeëbd bij gebrek aan continuïteit in de communicatie. Het korps Drenthe gebruikt TrueBlue voor de bewaking van de kwaliteit van een aantal velden in BVH.

Het korps Drenthe heeft de uitrol naar Blauw nog niet afgerond.

Er wordt een gebrek aan doorzettingsmacht ervaren en er vindt geen monitoring plaats op de uitvoering van de Wpg.

Hiermee wordt niet voldaan aan de Wpg.

Het rechteproces bevat waarborgen voor deze aspecten. De PDCA-cyclus sluit via het OM en de rechter. Tevens is bij de rechteproces nu meer aandacht voor de vastlegging van bronnen en hoe informatie uit andere onderzoeken wordt verkregen.

Hiermee wordt voldaan aan de Wpg.

De CIE heeft een proceshandboek. De CIE OvJ houdt toezicht.

Hiermee wordt voldaan aan de Wpg.

De landelijke en regionale informatiesystemen zijn nog niet Wpg-proof.

Hiermee wordt niet voldaan aan de Wpg.

4.4 Gevoelige gegevens (artikel 5)

4.4.1 *Norm*

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

4.4.2 *Bevindingen*

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

Het korps heeft procedurele regels voor de omgang met gevoelige gegevens op intranet staan. Hierin is vastgelegd dat medewerkers van Politie Drenthe gevoelige gegevens alleen mogen vastleggen als dat onvermijdelijk is voor het uitvoeren van de politietaken. Hiermee wordt voldaan aan artikel 5 van de Wpg.

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 autorisatie proces wordt uitgevoerd door het politiekorps, het Shared Service Centrum Noord (SSCN) en de vtsPN. Het beheer vindt plaats op basis van een procesbeschrijving Autorisatiebeheer, dat door het SSCN-Noord is opgesteld en voldoet aan de aanwijzingen van de Wpg. Medewerkers worden geautoriseerd voor de vervulling van hun taken. De leidinggevende geeft aan wie geautoriseerd moet worden en tot welk niveau. Het SSCN-Noord voert deze autorisatie uit. Over het algemeen moeten medewerkers een opleiding volgen voor het systeem dat ze gaan gebruiken voordat ze geautoriseerd worden.

In het korps Drenthe zijn volgens een intern onderzoek naar de WPG in 2009/2010 alle autorisaties in beeld gebracht. Uit de interviews blijkt echter dat samenvattende overzichten van toegekende autorisaties niet gemakkelijk zijn te verkrijgen. Controle daarop vindt ook niet plaats. Door interne verplaatsingen is sprake van vervuiling van toegekende autorisaties. Het komt daardoor voor dat medewerkers

op basis van hun oude functie kunnen muteren in systemen waartoe ze op basis van hun nieuwe functie niet geautoriseerd zouden moeten zijn.

De CIE OvJ heeft een rol in het toetsen van de autorisaties van de CIE. De korpschef zou conform art. 6 van de WPG aan de CIE OvJ autorisatielijsten moeten sturen, waarbij zij zou moeten controleren of de juiste categorieën medewerkers geautoriseerd zijn. Dat werkt nu nog niet zo. De CIE OvJ heeft deze lijsten zelf opgevraagd en gecontroleerd. Daarbij zijn categorieën die niet op de lijst horen (zoals recherche assistenten) aangegeven. Deze zijn vervolgens verwijderd.

In de leeswijzer is uitgeschreven welke functie welke autorisatie moet hebben. Als een categorie medewerkers aan de autorisatielijst wordt toegevoegd, dan ziet de CIE OvJ dat via de CIE chef, en kan zo'n toevoeging dan goedkeuren of afkeuren.

Een toets of medewerkers niet buiten hun autorisaties werken vindt niet plaats, volgens de CIE OvJ. Een medewerker kan bijvoorbeeld van een ander account gebruik maken waar een hoger autorisatieniveau geldt.

De privacyfunctionaris heeft een toezichthoudende rol, maar komt daar door tijdgebrek niet aan toe.

Er zijn twee onderzoeken uitgevoerd vanuit Informatiebeveiliging bij de Afdeling Integriteit en bedrijfsveiligheid van Politie Groningen, gericht op het gemeenschappelijk proces voor autorisatiebeheer. Deze hebben plaatsgevonden in mei 2009 en februari 2010. In beide rapporten is de conclusie dat het gemeenschappelijke systeem van autorisaties niet voldoet aan de daaraan te stellen normen zoals beschreven in het Basisbeveiligingsniveau Nederlandse Politie (BBNP) en de Wpg.

Het eerste rapport is "Interne audit van de autorisaties", Afdeling Integriteit en bedrijfsveiligheid, Informatiebeveiliging, mei 2009. Hierin wordt een telling beschreven van de autorisaties in 5 applicaties, namelijk BPS-PCS, HKS, BVO, GRN en BVH. Deze autorisaties zijn vergeleken met de medewerkers die in 2009 dienst zijn. Het rapport trekt een tweetal conclusies:

- vtsPN-NO is niet in staat de door de Politie Groningen opgevraagde lijsten met gebruikers voor alle systemen volledig en betrouwbaar op te leveren. Daardoor moest het onderzoek worden beperkt tot de vijf voornoemde applicaties en kon geen onderzoek worden gedaan naar autorisaties in de kantooromgeving (mappen), BlueView en Corsa.
- Van de in totaal 5.249 autorisaties zijn er 2.920 (56%) rechtmatig en 2.394 (44%) onrechtmatig, namelijk van personen die niet in 2009 voor de Politie Groningen werkzaam zijn.

Het onderzoek naar autorisaties is opnieuw uitgevoerd in februari 2010. Het rapport is "Interne audit van het systeem van autorisaties 2010", Afdeling Integriteit en bedrijfsveiligheid, Informatiebeveiliging. Hierbij zijn de autorisaties beschouwd in BPS-PCS, Ping, BVO, HKS, Kantoorautomatisering, BlueView, BVH, Corsa, BVCM, Beaufort en SmartStream. Het rapport trekt een tweetal conclusies:

- De onderzoeker stelt vast dat Politie Groningen niet kan aantonen wie er toegang heeft gehad tot de politiegegevens, dus ook niet of er sprake is van onrechtmatige toegang tot die politiegegevens.
- Van de in totaal 14.176 autorisaties zijn er 10.764 (76%) rechtmatig en 3.415 (24%) onrechtmatig, namelijk van personen die niet in 2010 voor Politie Groningen werkzaam zijn.

Geïmplementeerde beheersmaatregelen zijn:

- Er is een SSCN brede autorisatieprocedure, waarin ook de registratie wordt geadresseerd.
- De chef is verantwoordelijk voor het aanvragen van autorisaties. Indien deze het gevoel heeft dat wordt overvraagd, wordt getoetst bij de privacyfunctionaris.
- Voor wat betreft BVO krijgt de functioneel beheerder een lijst met ontslagen medewerkers vanuit het personeelssysteem.
- Hoofd CIE en Hoofd RID houden zelf toezicht op autorisaties en zien ook toe op het verwijderen van autorisaties bij uitdiensttreding.
- Voordat medewerkers voor BVH, BVO en BlueView worden geautoriseerd, moeten zij eerst een opleiding succesvol afronden voor het betreffende systeem.

4.5.3

Oordeel over het autorisatieproces

De korpsautorisatiematrix is ingericht zoals redelijkerwijs kan worden verwacht en geeft tevens weer op welke wijze rollen binnen de drie korpsen samenwerken bij toegang tot de applicaties.

Hiermee wordt voldaan aan de Wpg.

Het aanvraagproces van autorisaties verloopt via SSCN en vtsPN, en is gedocumenteerd.

Er zijn echter twee onderzoeken uitgevoerd vanuit Informatiebeveiliging bij de Afdeling Integriteit en bedrijfsveiligheid van Politie Groningen, gericht op de autorisaties. Deze hebben plaatsgevonden in mei 2009 en februari 2010. In beide rapporten is de conclusie dat het gemeenschappelijke systeem van autorisaties niet voldoet aan de daaraan te stellen normen zoals beschreven in het Basisbeveiligingsniveau Nederlandse Politie (BBNP) en de Wpg.

Het verwijderproces van autorisaties verloopt via SSCN en vtsPN, en is gedocumenteerd. De rechten op de mappenstructuur van de kantoorautomatisering zijn echter minder goed geregeld.

Hiermee wordt niet voldaan aan de Wpg.

Autorisaties voor medewerkers van de CIE en RID worden toegekend door het hoofd van de CIE respectievelijk RID. De CIE OvJ heeft het autorisatiebeleid goedgekeurd. Hiermee wordt voldaan aan de Wpg.

Binnen SSCN wordt iedere aanvraag voor een mutatie op een autorisatie geregistreerd en bewaard.

Hiermee wordt voldaan aan de Wpg.

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*

Geautomatiseerd vergelijken en in combinatie met elkaar verwerken zijn begrippen die niet bij alle geïnterviewden bekend zijn. Het wordt dan ook met name uitgevoerd door analisten bij de CIE, RID en Infodesk.

Waar bekendheid met deze begrippen uit de Wpg aanwezig is, is direct de vraag aan de orde waar de grenzen van GV en ICMEV liggen en op welke wijze daarmee dan in de praktijk moet worden omgegaan.

Bij de implementatie van een toekomstige release van BVH (namelijk 1.2.2) kunnen ambtenaren van politie die belast zijn met de dagelijkse politietaak gegevens ouder dan een jaar (die achter het schot' zijn geplaatst) niet zelf vergelijken met soortgelijke politiegegevens. Daarvoor wenden zij zich dan tot de Infodesk.

Uitvoering vindt plaats door geautoriseerde medewerkers, die gebruik maken van een veelheid van systemen. Voor de uitvoering van hun taak zijn zij specifiek opgeleid. De leidinggevers van deze medewerkers zien erop toe dat het proces geordend en volgens de Wpg regels verloopt.

Er zijn nog geen nadrukkelijk toegekende taken en verantwoordelijkheden in de context van de Wpg. Het inbedden van Wpg binnen de werkprocessen is nog niet voltooid.

Er zijn geen instructies voor het vergelijken van politiegegevens met openbare bronnen.

Geïmplementeerde beheersmaatregelen zijn:

- In een cursus voor Infodeskmedewerkers is de "Landelijke BVO Infodesk casuïstiek" behandeld.
- Voor alle infodeskmedewerkers is de handleiding "Module 4 Infodesk" beschikbaar, waarin de wijze van vastlegging van verstrekkingen (VST) is behandeld en dat door hen als naslagwerk kan worden gebruikt.
- Binnen het de infodesk is een werkinstructie "Verkorte handleiding BVO" waarin de wijze van vastlegging van verstrekkingen door het Infohuis is vastgelegd.
- De CIE legt de bronnen vast bij opdracht tot analyse.
- De RID volgt in deze eveneens een stringente vastlegging van bronnen.

4.6.3 *Oordeel over artikel 11*

De begrippen geautomatiseerd vergelijken en in combinatie met elkaar verwerken zijn nog in onvoldoende mate bekend binnen het korps. Hiermee wordt niet voldaan aan de Wpg.

De Infodesk is onder andere belast met het in combinatie met elkaar verwerken en geautomatiseerd vergelijken. De taken in het kader van artikel 11 zijn echter nog niet expliciet belegd binnen de werkprocessen en nog niet expliciet toegekend aan met name genoemde onderdelen van het korps Drenthe. Hiermee wordt niet voldaan aan de Wpg.

Doordat in combinatie met elkaar verwerken niet eenduidig is vastgesteld, is het onbekend wanneer het bevoegd gezag moet worden geraadpleegd. Doordat het vergelijken van politiegegevens met andere dan politiegegevens volgens artikel 11.5 niet eenduidig is omschreven, is het onbekend welke handelingen onder dit artikellid vallen.

Aanvragen die via de Infodesk binnenkomen worden geprotocolleerd en de vastleggingen worden bewaard.

4.7 Bewaartermijnen (artikel 14)

4.7.1 Norm

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

4.7.2 Bevindingen

De landelijke systemen zoals BPS, BVH en BVO zijn niet voorzien van beheersmaatregelen op het gebied van termijnen voor verwijderen en vernietigen van politiegegevens. Het is in BVH en BPS niet mogelijk informatie na bijvoorbeeld 1 jaar achter een schot te plaatsen zodat deze informatie niet meer kan worden geraadpleegd. Ook vinden er geen handmatige verwijderingen plaats. In het nieuwe release 1.2.2 van BVH zou dit wel tot de mogelijkheden behoren. De hierin opgenomen schoningsscripts zijn nog niet geactiveerd in het korps Drenthe.

In BVO worden registraties gesloten wanneer een zaak is afgesloten en dan worden de autorisaties voor het betreffende onderzoek op nul gezet zodat men niet meer bij de informatie kan.

Een halfjaarlijkse controle op de noodzakelijkheid van informatie vindt, behalve bij de CIE, niet plaats.

Er is met betrekking tot artikel 8 en 9 Wpg geen procedure aangetroffen voor de omgang met bewaartermijnen en vernietiging van politiegegevens.

Gegevens die in de kantoorautomatisering zijn opgeslagen vallen helemaal buiten beeld. Controle op de bewaartermijnen en vernietiging vindt hierop niet plaats. Er is geen totaaloverzicht van wat er in die omgeving is opgeslagen.

De outlook-mailboxen vereisen hier bijzondere aandacht, zoals bijvoorbeeld verzonden mails met verstrekkingen.

Uit de gesprekken is naar voren gekomen dat de kennis van de bewaartermijnen en vernietiging niet altijd aanwezig is.

De rapportage Wet politiegegevens d.d. 4-8-2011 geeft aan dat verbinding met het OM moet worden gezocht om ervoor te zorgen dat een dossier met een onherroepelijke veroordeling uit de systemen wordt verwijderd.

Binnenkort gaat een project 'sturen op opslag' van start. Dit is een door de vtsPN geïnitieerd project met het doel grip te krijgen op de niet gestructureerde opslag van gegevens (gegevens buiten de concernsystemen).

Het korps Drenthe heeft nog geen proces ingericht om te voldoen aan artikel 14.3 van de Wpg, namelijk hernieuwde verwerking met in opdracht van het bevoegd

gezag. Doordat niet conform de eisen van de Wpg wordt verwijderd, is het nog niet mogelijk een proces voor hernieuwde verwerking in te richten.

4.7.3 *Oordeel over bewaartermijnen voor artikel 8*

Gegevens ouder dan één jaar na eerste vastlegging in BVH worden niet achter schot gezet. Medewerkers gaan er van uit dat de gegevens die ze te zien krijgen ook mogen worden gebruikt voor verdere verwerking. Met name medewerkers op operationeel niveau zijn zich hiervan niet voldoende bewust. De regels voor de verwijdering van oude artikel 8 gegevens zijn moeilijk uitvoerbaar omdat het handmatig moet gebeuren. Daardoor krijgt het verwijderen en schonen nog onvoldoende prioriteit. Artikel 8 gegevens worden nog niet op het voorgeschreven moment vernietigd. Hiermee wordt niet voldaan aan de Wpg.

4.7.4 *Oordeel over bewaartermijnen voor artikel 9*

Het opschonen van artikel 9 onderzoeken kan nog verder worden geoptimaliseerd. Hierbij is de ketensamenwerking en specifiek de overdracht van informatie over afgesloten zaken van OM naar de politie een aandachtspunt. Doordat het juiste moment van verwijdering niet bekend is, kan niet 5 jaar na verwijdering worden vernietigd. Hiermee wordt niet voldaan aan de Wpg.

4.7.5 *Oordeel over de bewaartermijnen voor artikel 10 en 12*

Bij de CIE voert de OvJ periodiek controles uit waarbij ook naar de bewaartermijnen wordt gekeken. Informatie van informanten 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. Informatie wordt binnen de CIE en RID regelmatig gecontroleerd en geschoond. Bij de RID gebeurt dit elke 5 jaar. Bij de CIE toetst de CIE-OvJ jaarlijks het informantenregister. Hiermee wordt voldaan aan de Wpg.

4.8 **Ter beschikking stellen (artikel 15)**

4.8.1 *Norm*

De verantwoordelijke stelt politiegegevens ter beschikking aan personen die door hemzelf dan wel door een andere verantwoordelijke zijn geautoriseerd voor de verwerking van politiegegevens, voor zover zij deze behoeven voor de uitvoering van hun taak.

4.8.2 *Bevindingen*

In het bijzonder de Infodesk speelt een centrale rol bij het ter beschikking stellen van gegevens binnen het politiedomein. Ter beschikking stelling van politiegegevens wordt niet meer in de BVO infodesk module geregistreerd.

Bij het ter beschikking stellen van politiegegevens dient de ontvanger de herkomst en wijze van verkrijgen van de gegevens vast te leggen (protocolplicht). Aan deze protocolplicht wordt niet altijd voldaan. Daardoor is het spoor naar de herkomst (bron) en de wijze van verkrijging van de informatie niet te achterhalen.

Zogenaamde restinformatie (informatie die niet nodig is voor een onderzoek, maar mogelijk kan worden ingebracht in een andere zaak) wordt nauwelijks opgenomen in het zwacri register. Ook worden op basis van restinformatie nauwelijks nieuwe

registraties aangemaakt. Voor hernieuwd gebruik van informatie is geen structuur aanwezig.

Binnen de CIE stelt het proceshandboek CIE regels aan het ter beschikking stellen van politiegegevens. De CIE en de RID zijn beide strikt in het vastleggen van het ter beschikking stellen van gegevens. Bij de CIE is een extra waarborg dat de CIE-OvJ toezicht houdt.

In de praktijk wordt soms afgeweken van het proceshandboek CIE. Dan wordt CIE informatie bijvoorbeeld verstrekt aan het district Assen. Het district gaat ermee naar de driehoek en op die manier komt informatie alsnog bij de gemeente terecht. Dit is niet conform de voorschriften van de WPG.

De CIE maakt gebruik van de onderstaande coderingen met betrekking tot de betrouwbaarheid van een informant:

- A. Betrouwbaar.
- B. Meestal betrouwbaar.
- X Niet te beoordelen.

Met betrekking tot de wijze waarop de informant aan zijn informatie is gekomen:

- 1. Waargenomen door de bron zelf.
- 2. Gehoord van iemand die erbij is geweest.
- 3. Indirect gehoord, via via.

Dus bijv. A 1 = betrouwbaar en door de bron zelf waargenomen.

De CIE maakt volgens het 'Proceshandboek van de CIE' gebruik van de volgende afhandelingscodes in BVO en de MRO:

- 11. De informatie is operationeel bruikbaar (wordt nimmer gebruik gemaakt van deze code, maar altijd minstens van code 01).
- 01. De informatie is operationeel bruikbaar.
- 00. De informatie kan niet operationeel worden gebruikt.
- 200. De informatie kan niet operationeel worden gebruikt en kent een verhoogd afbreukrisico.
- 300. De informatie kan niet operationeel worden gebruikt en kent extra bron beschermingsbelangen.

Er is aangegeven dat in de praktijk nog niet alles via de Infodesk verloopt en dat er nog aanvragen terecht komen bij de privacyfunctionaris. Door de opslag van politiegegevens in de kantoorautomatisering kan het voorkomen dat de informatie die ter beschikking wordt gesteld uit landelijke systemen niet volledig is.

In de bijlage "Functies die aansluiten bij de werkprocessen/Opleiding en instructie" bij het implementatierapport van de "Interregionale projectgroep implementatie wet politiegegevens Drenthe, Fryslân en Groningen" van 1 november 2009 staat dat bevoegd functionarissen zijn aangewezen, namelijk de unitchefs recherche, de chefs RID en CIE en de chefs districtsondersteuning.

Wij hebben vernomen dat de bevoegd functionarissen in 2009 een verplichte opleiding hebben gevolgd. Daarna zijn enkele nieuwe bevoegd functionarissen opgeleid. In de cursus is onder andere aandacht besteed aan de weigeringgronden conform artikel 15.2. Het cursusmateriaal omvatte onder andere:

- Wet politiegegevens;
- Memorie van toelichting WPG;
- Besluit Politiegegevens en toelichting;
- Handreiking Bevoegd Functionaris.

Tijdens de cursus is door de docent Wpg uitleg gegeven over de WPG en zijn onder andere individueel en klassikaal casussen gemaakt en besproken.

Wij hebben vernomen dat door het achterblijven van de ICT de Wpg-kennis van de bevoegd functionarissen is weggezaakt. Er zijn geen herhalingscursussen of opfriscursussen geweest in 2010 en 2011. In 2012 zal aan de bevoegd functionarissen een "opfris-cursus" worden aangeboden.

4.8.3 *Oordeel over ter beschikking stellen*

De Infodesk stelt informatie ter beschikking volgens vaste procedures. Een deel van de politiegegevens van het korps Drenthe zijn echter opgeslagen in persoonlijke en groepsmappen met een risico op onrechtmatig gebruik en bewaring. Het gebruik van de mappenstructuur binnen Opsporing belemmert de Infodesk met het zoeken en vergelijken met andere onderzoeken. Hierdoor kan informatie ook niet met andere korpsen worden gedeeld. Hiermee wordt niet voldaan aan de Wpg.

Bij CIE- en MRO-mutaties maakt men gebruik van de coderingen 00, 01 en 11. Hiermee wordt voldaan aan de Wpg.

Bevoegd functionarissen zijn aangewezen. Deze hebben in 2009 een verplichte opleiding gevolgd. Daarna zijn enkele nieuwe bevoegd functionarissen opgeleid. Door het achterblijven van de ICT is hun kennis weggezaakt. Er zijn geen herhalingscursussen of opfriscursussen geweest in 2010 en 2011. In 2012 zal aan de bevoegd functionarissen een "opfris-cursus" worden aangeboden. Hiermee wordt deels voldaan aan de Wpg.

In de cursus voor de bevoegd functionarissen is onder andere aandacht besteed aan de weigeringsgronden conform artikel 15.2. Hiermee wordt niet voldaan aan de Wpg.

4.9 **Verstrekken (artikel 16/24)**

4.9.1 *Norm*

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

4.9.2 *Bevindingen*

De landelijke verstrekkingwijzer is tijdens de opleiding voor bevoegd functionaris uitgereikt en is raadpleegbaar op intranet. Er is geen regionaal verstrekkingenschema. Het korps heeft op het intranet een gegevensbeheerlijst staan met de organisaties waaraan informatie mag worden verstrekt.

Verstrekkingen vinden doorgaans plaats via de Infodesk.

Binnen de CIE stelt het proceshandboek CIE regels aan het verstrekken van politiegegevens. Een gesignaleerde afwijking bij het verstrekken aan de driehoek via het district Assen is eerder in deze rapportage besproken.

Beheersmaatregelen die zijn gericht op het voldoen aan deze criteria en die in dit kader kunnen worden genoemd, zijn onder meer:

- Bij de informatie medewerkers is bekend hoe zij hun verstrekkingen moeten documenteren. Er is binnen het Infohuis een medewerker, die is opgeleid als Wpg kerninstructeur.
- Het werkproces Infodesk is beschreven; de status is echter nog steeds concept.

- De CIE is bij het ter beschikking stellen en verstrekken van gegevens strak in de uitvoering met een extra waarborg door toezichthoudende taak van de CIE OvJ.
- De RID is hierin ook strak doch daar ontbreekt de rol van een check door een externe toezichthouder

Aanvullende informatie is door het korps Drenthe verstrekt: *'De korpsen Groningen, Friesland en Drenthe voeren thans een inhaalslag uit om de bestaande samenwerkingsverbanden WPG-proof te maken. Nieuwe besluiten worden door de gemandateerde leidinggevers gemaakt en voor een juridische toetsing aangeboden aan de Juridische afdeling. Indien akkoord bevonden wordt het besluit getekend door de partners en gearchiveerd bij de Juridische Dienst. Het besluit en het eventuele convenant worden intern gepubliceerd op Intranet en zijn aldus zichtbaar en beschikbaar voor de medewerkers.'*

Convenanten

Er is centraal geen procedure vastgesteld voor verstrekkingen aan ketenpartners. Er is geen sturing op de noodzaak en de inhoud van convenanten.

Er wordt soms te gemakkelijk van uitgegaan dat informatie altijd kan worden verstrekt als er een convenant is. De afweging wordt niet altijd gemaakt of de informatie wel wordt verstrekt voor de doeleinden zoals die zijn geformuleerd in artikel 20 van de WPG. Het verstrekken van informatie gebeurt in een aantal gevallen 'op gevoel'.

De conclusie van een afstudeeronderzoek luidt dat in 3 Noord een deel van de convenanten juridisch niet rechtsgeldig is: de handtekening van de korpschef of ketenpartners ontbreken, evenals de looptijd. Bij een groot aantal convenanten ontbreekt het besluit ex artikel 20 Wpg.

Het invullen van het I90 formulier in BVH wordt als belastend ervaren. Daardoor worden niet alle verstrekkingen geregistreerd en kan de privacyfunctionaris geen volledig toezicht houden op de verstrekkingen. In de periode van 1 januari 2010 tot en met 15 december 2011 zijn in BVH in totaal 170 mutaties met de maatschappelijke klasse I90 geregistreerd. Dit aantal staat niet in verhouding tot het aantal werkelijke verstrekkingen. (In de telling zijn niet begrepen de verstrekkingen die gedaan zijn door de informatieorganisatie en de verstrekkingen waarvoor een andersoortig formulier, zoals Meldingformulier Jeugdzorg, is opgesteld.)

In overleggen wordt ook mondeling informatie verstrekt. Deze verstrekkingen worden vaak niet vastgelegd.

Geautomatiseerde verstrekkingen

Volgens het korps vinden er momenteel geen geautomatiseerde verstrekkingen plaats, anders dan de in het Besluit politiegegevens toegestane verstrekkingen, zoals aan RDW bij het invorderen van een rijbewijs of kentekenbewijs. Abonnementen binnen Amazone worden uitsluitend intern gebruikt. Vanuit Amazone worden geen externe verstrekkingen gedaan.

4.9.3

Oordeel over verstrekkingen

De landelijke verstrekkingenwijzer is tijdens de opleiding voor bevoegd functionaris uitgereikt en is raadpleegbaar op intranet. De verstrekkingenwijzer is echter niet bij iedereen bekend. Het korps heeft op het intranet tevens een gegevensbeheerlijst staan met de organisaties waaraan informatie mag worden verstrekt. Hiermee wordt deels voldaan aan de Wpg.

Verstrekkings vinden plaats op basis van convenanten. Deze zijn niet allemaal WPG proof. Een intern onderzoek heeft aangetoond dat een aanzienlijk deel van de convenanten vermoedelijk juridisch niet rechtsgeldig is: de handtekening van de korpschef of ketenpartners ontbreken evenals de looptijd. Bij een groot aantal convenanten ontbreekt het besluit ex artikel 20 Wpg.

Er is centraal geen procedure vastgesteld voor verstrekkingen aan ketenpartners en er is geen sturing op de noodzaak en de inhoud van convenanten.

Er wordt soms te gemakkelijk van uitgegaan dat informatie altijd kan worden verstrekt als er een convenant is. De afweging wordt niet altijd gemaakt of de informatie wel wordt verstrekt voor de doeleinden zoals die in artikel 20 van de Wpg zijn geformuleerd. Het verstrekken van informatie gebeurt in een aantal gevallen 'op gevoel'.

Hiermee wordt deels voldaan aan de Wpg.

Bij de CIE en de Infodesk is de vastlegging van verstrekkingen goed geregeld. Aan de basis gaat het niet altijd even goed.

Het vastleggen van verstrekkingen uit BVH met een I90 formulier gebeurt zeer beperkt. Het invullen van het I90 formulier wordt als belastend ervaren. Daardoor worden niet alle verstrekkingen geregistreerd en kan de privacyfunctionaris geen toezicht houden op de verstrekkingen.

In overleggen wordt ook mondeling informatie verstrekt. Deze verstrekkingen worden vaak niet vastgelegd.

Hiermee wordt deels voldaan aan de Wpg.

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

Er is een procesbeschrijving over verstrekken van gegevens aan burgers in verband met het inzagerecht. In korps Drenthe is deze taak vrijwel volledig bij de privacyfunctionaris belegd, die formeel is geplaatst bij de Juridische dienst van het SSC. Deze situatie is aan herinrichting onderhevig. De privacyfunctionaris houdt zich daar nu mee bezig en daarmee is er geen sprake van functiescheiding. In de oude organisatie waren er drie privacyfunctionarissen.

4.10.3 Oordeel over rechten van betrokkenen

De privacyfunctionaris is betrokken bij het behandelen van verzoeken in het kader van de rechten van betrokkenen. Dit is een ongewenste vermenging van functies, aangezien de privacyfunctionaris toezicht dient te houden op dit proces. Hierop komen wij terug bij het onderwerp "Privacyfunctionaris".

Niettemin wordt het proces voor de artikelen 25 en 28 goed doorlopen en wordt hierbij voldaan aan de Wpg.

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

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

Artikel 32.1.a

Een onderzoek conform Art. 9 wordt verwerkt in BVO, BVH of de mappenstructuur. Bij het starten van een onderzoek wordt een Melding Recherche Onderzoek (MRO) verstuurd naar de landelijke verwijsindex VROS, onder beheer van KLPD. Een overzicht van de meldingen is in een map geplaatst in de omgeving van de kantoorautomatisering, welke toegankelijk is voor de privacyfunctionaris.

Artikel 32.1.b

Het korps Drenthe beschikt over een Artikel 13 Register met de landelijke en regionale artikel 13 applicaties, inclusief doel etc. conform artikel 13.4. Dit overzicht is niet compleet, aangezien hierin alleen de volgende artikel 13 gegevensverzamelingen worden genoemd:

- VERONA;
- HKS;
- PAPOS;
- FOIS;
- VRIS;
- VROS;
- Arrestatie- en Ondersteuningseenheid (AOE);
- Politieonderhandelaars;
- Observatie Team (OT).

Het korps maakt gebruik van andere artikel 13 gegevensverzamelingen welke niet in het Register zijn opgenomen.

Artikel 32.1.g

Toezicht op het (on)geoorloofd en (on)deskundig gebruik van applicaties behoort in algemene zin tot de taken van de functioneel beheerorganisatie. Om de controle op de juistheid van de gegevens beter te borgen wordt aan de afdeling Functioneel beheer SSCN een audit-rol toegekend. Een overzicht van onrechtmatige verwerkingen ontbreekt echter.

4.11.3 *Oordeel over protocolplicht*

Bij het starten van een onderzoek wordt een Melding Recherche Onderzoek (MRO) verstuurd naar de landelijke verwijsindex VROS, onder beheer van KLPD. Er is een overzicht van deze meldingen beschikbaar voor de privacyfunctionaris.

Doelbinding conform artikel 9.2 wordt niet altijd op de juiste wijze vastgelegd.

De drie noordelijke korpsen hebben plannen BOSZ te implementeren, waarin onder andere het doel van een onderzoek wordt vastgelegd.

Hiermee wordt deels voldaan aan de Wpg.

Er is een gedeeltelijk Artikel 13 register.

Hiermee wordt deels voldaan aan de Wpg.

Een overzicht van onrechtmatige verwerkingen ontbreekt.

Hiermee wordt niet voldaan aan de Wpg.

4.11.4 *Bevinding gemeenschappelijke verwerking*

Het Shared Service Center Noord (SSCN) is een gemeenschappelijk onderdeel van drie korpsen. De processen, lokale infrastructuur en lokale gegevensverzamelingen worden gedeeld tussen medewerkers van deze drie korpsen. In de stukken hebben wij geen bevestiging kunnen vinden dat wordt voldaan aan artikel 32.2 Wpg, namelijk dat een verantwoordelijke is aangewezen en dat deze het SSCN als een gemeenschappelijke verwerking heeft gemeld bij het CBP.

Navraag bij het korps leverde het volgende antwoord: "*Directie SSCN: De drie korpsleidingen zijn verantwoordelijk, het is niet een zelfstandige entiteit. De medewerkers zijn in dienst van een van de drie korpsen. De privacy functionaris is bijvoorbeeld ondergebracht bij de JD van SSC, maar valt onder korps Drenthe en is ook als zodanig aangemeld bij CBP.*"

Vervolgens is door het korps meegedeeld: "*In SSCN zijn een aantal ondersteunende werkzaamheden samengevoegd, zoals de salaris- en personeelsadministratie, de juridische dienst en de facilitaire dienst. Ook de forensisch-technische recherche en enkele recherche specialiteiten zijn samengevoegd, waaronder de digitale recherche en de financiële recherche. Feitelijk zijn deze ondersteunend aan de drie korpsen. Wanneer er sprake zou zijn van een gemeenschappelijke verwerking zal deze niet plaatsvinden onder de verantwoordelijkheid van de SSCN, maar onder verantwoordelijkheid van een korps.*"

4.11.5 *Oordeel over gemeenschappelijke verwerking*

SSCN is een gemeenschappelijke activiteit van drie korpsen, waarbij iedere medewerker onder een van de drie korpschefs valt. Door het ontbreken van een landelijke richtlijn voor het positioneren een gemeenschappelijk onderdeel in relatie tot de Wpg, kunnen wij ons vooralsnog geen onderbouwd oordeel vormen over het wel of niet voldoen aan de Wpg.

Wij adviseren nader onderzoek, zowel landelijk om tot een richtlijn te komen over het positioneren van een gemeenschappelijke activiteit, als regionaal om de informatiestromen binnen SSCN in beeld te brengen en aan de Wpg te toetsen.

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*

Het korps Drenthe heeft geen interne auditor voor de Wpg. Er is geen structurele interne Wpg audit functie, geen intern Wpg audit plan en geen interne Wpg audit rapportage. Hiermee wordt niet voldaan aan de Regeling Periodieke Audit Politiegegevens (RPAP).

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*

De privacyfunctionarissen bij het SSC voeren andere taken uit dan de toezichhoudende. Er is geen overzicht van geautomatiseerde vergelijkingen, geen overzicht van onrechtmatige verwerkingen, geen overzicht van verstrekkingen en geen overzicht van mutaties op autorisaties.

De privacyfunctionaris is betrokken bij het afhandelen van verzoeken in het kader van de rechten van betrokkenen en eventuele daarmee samenhangende correcties conform de artikelen 25 en 28. Hiermee vindt onterechte vermenging van functies plaats omdat de privacyfunctionaris dit proces uitvoert en er tevens toezicht op zou moeten houden.

Over 2010 is geen jaarverslag beschikbaar. Het was de intentie één rapport op te stellen voor Groningen, Friesland en Drenthe. Door een veranderende prioriteitstelling in het korps is dit verslag echter niet opgesteld. Hiermee wordt niet voldaan aan de Wpg voor wat betreft de toezichhoudende en de signalerende rol.

4.13.3 *Oordeel over de privacyfunctionaris*

Er wordt voldaan aan de eis vanuit de Wpg dat er een privacyfunctionaris moet zijn, maar de invulling van deze taak is niet in overeenstemming met de Wpg.

4.14 Functionaris Gegevensbescherming (artikel 36)

De optionele functionaris Gegevensbescherming bestaat niet als functie bij korps Drenthe.