



Ministerie van Veiligheid en Justitie

Audit Wpg politie Friesland

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
M

Projectnaam

Audit Wet Politiegegevens

Ons kenmerk

DDS/5719709/11

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) 27
- 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) 33
- 4.12 Audits (artikel 33) 35
- 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 maand augustus 2011 is een privacy audit uitgevoerd bij het korps Friesland.

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 Friesland.

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 Friesland, naar de stand van ultimo augustus 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 Friesland te nemen maatregelen. Ook is gebleken dat het korps Friesland voor het volledig kunnen voldoen aan de Wpg eisen mede afhankelijk is van besluiten die buiten het korps Friesland 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 Friesland, 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 Friesland. 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 Auditdienst 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 15 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 Politietak (8) versus Bepaald geval (9)		Het korps heeft criteria voor het verschil tussen artikel 8 en artikel 9 onderzoeken op intranet staan. Hiermee wordt voldaan aan de Wpg.
3.1 t/m 3.3 (8) 4.1 (8)	Noodzakelijkheid (8) Doelbinding Rechtmatigheid Juistheid Volledigheid		Het korps Friesland gebruikt TrueBlue voor de 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 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		Het rechercheproces bevat waarborgen voor deze aspecten. De PDCA-cyclus sluit via het OM en de rechter. Tevens is bij de recherche nu meer aandacht voor

Norm	Aspect		Bevinding en oordeel
	van verkrijging Juistheid Nauwkeurig Volledigheid		de vastlegging van bronnen en hoe informatie uit andere onderzoeken wordt verkregen. 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. Het handboek voor RID ligt ter goedkeuring bij de AIVD. Hiermee wordt voldaan aan de Wpg.
4.3	Beveiliging		Het korps heeft nog geen beleid voor de mappenstructuur. De landelijke en regionale applicaties 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 kantoorautomatisering 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. De privacyfunctionaris schoont jaarlijks de autorisaties voor applicaties. De privacyfunctionaris heeft een wettelijke taak om toezicht uit te oefenen, en schonen van autorisaties in dit kader is daarmee een oneigenlijke taak. Schoning behoort te worden uitgevoerd als een gedocumenteerd en controleerbaar proces via de lijn. Hiermee wordt niet voldaan aan de Wpg.
	• Autorisatiebeheer CIE, RID, OT, AT		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 geregistreerd. 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		Het Team Informatie is onder andere belast met 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 het Team Informatie binnenkomen worden geprotocolleerd. Hiermee wordt voldaan aan de Wpg.
32.3 voor 32.1.d en h	Bewaren protocolgegevens 11.1, 11.2 en 11.4		Aanvragen die via het Team Informatie binnenkomen worden bewaard. Hiermee wordt voldaan aan de Wpg.
Artikel 14, Bewaartermijnen			
8.2 en 8.3	(8) van 1 tot 5 jaar		Het korps Friesland maakte vanaf 1994 gebruik van bedrijfsprocessensysteem X-POL, in tegenstelling tot SSCN-partners Groningen en Drenthe. Voor X-POL was geen schoningsmodule beschikbaar. Hierdoor is veel oude informatie nog beschikbaar in BVH. 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. 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.

Norm	Aspect		Bevinding en oordeel
9.4	(9) verwijderen na OH plus ½ jaar		Het opschonen van artikel 9 onderzoeken gebeurt nog onvoldoende. Hierbij is de ketensamenwerking en specifiek de overdracht van informatie over afgesloten zaken van OM naar de politie een aandachtspunt. Hiermee wordt niet voldaan aan de Wpg.
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, waardoor er geen proces kan worden 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			
	Team Informatie voor bevraging		Er circuleert een Zicht op Zaken lijst om informatie te delen. Het Team Informatie verzamelt, veredelt, analyseert, stelt ter beschikking en verstrekt informatie. Er zijn echter nog geen nadrukkelijk toegekende taken en verantwoordelijkheden in de context van de Wpg. Inbedden van de Wpg in de werkprocessen is nog niet voltooid. Een deel van de politiegegevens van het korps Friesland zijn opgeslagen in persoonlijke en groepsmappen met een risico op onrechtmatig gebruik en bewaring. Het gebruik van de mappenstructuur binnen Opsporing belemmert de

Norm	Aspect	Bevinding en oordeel
		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.
	• Codering	Coderingen worden gebruikt bij CIE mutaties en voor MRO's. Hiermee wordt voldaan aan de Wpg.
	• Aanwijzing Bevoegd Functionaris	Bevoegd functionarissen zijn aangewezen en initieel opgeleid. Hiermee wordt voldaan aan de Wpg.
	• Opleiding Bevoegd Functionaris	Bevoegd functionarissen zijn vooral in 2009 opgeleid. Hun kennis van de Wpg is echter deels weggezaakt. In 2012 zal aan de bevoegd functionarissen een "opfris-cursus" worden aangeboden. Hiermee wordt deels voldaan aan de Wpg.
15.2	Weigeringgronden	De weigeringgronden zijn onderwezen aan de bevoegd functionarissen. Hiermee wordt voldaan aan de Wpg.
Artikel 16 t/m 24, Verstrekking		
	• Verstrekkingenwijzer (landelijk)	De landelijke verstrekkingenwijzer is tijdens de opleiding voor bevoegd functionaris uitgereikt en is raadpleegbaar op intranet. Het blijkt dat de verstrekkingenwijzer niet bij iedereen bekend is. Hiermee wordt deels voldaan aan de Wpg.
	• Proces voor convenanten	Er is centraal geen procedure vastgesteld voor verstrekkingen aan ketenpartners. Er is geen sturing op de noodzaak en de inhoud van convenanten. Een deel van de convenanten is niet rechtsgeldig wegens het ontbreken van de handtekening van de korpschef of ketenpartners, of de looptijd. De opgestelde convenanten voldoen niet in alle gevallen aan de gestelde criteria. Bij een aantal convenanten ontbreekt het artikel 20 besluit. Een totaaloverzicht van verstrekkingen binnen samenwerkingsverbanden ontbreekt. Eind 2011 zijn de korpsen Groningen, Friesland en Drenthe bezig met een inhaalslag. Hiermee wordt deels voldaan aan de Wpg.
	• Proces voor Artikel 20 Besluiten	Een aantal convenanten is niet rechtsgeldig en bij een aantal convenanten ontbreekt het artikel 20 besluit. De afweging wordt niet altijd gemaakt of de te verstrekken informatie wel past bij de doeleinden zoals die in artikel 20 zijn geformuleerd. Het verstrekken van informatie gebeurt in een aantal gevallen op een gevoelsmatige basis. Eind 2011 zijn de korpsen Groningen, Friesland en Drenthe bezig met een inhaalslag. Hiermee wordt deels voldaan aan de Wpg.

Norm	Aspect		Bevinding en oordeel
	• Verstrekkingenschema (regio)		Het korps heeft op het intranet een gegevensbeheerlijst staan met de organisaties waaraan informatie mag worden verstrekt. Verstrekkingen vinden doorgaans plaats via het Team Informatie of de Juridische dienst van het SSC Noord. Het is echter niet duidelijk wie verantwoordelijk is voor het proces in totaliteit. Verstrekkingen naar burgemeesters gaan via 11 teamchefs en op 4 verschillende manieren. Het is niet bekend of hierbij een en dezelfde lijn wordt gevolgd. 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		Aan de protocolplicht is slechts in beperkte mate invulling gegeven. Wat er precies geregistreerd moet worden, en op welke wijze is bij veel medewerkers niet bekend. In 2011 zijn 2.497 registraties met I90 gedaan. 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 leidinggevend op verstrekkingen en protocollering		Bij het Team Informatie is toezicht door de leidinggevende. Het vastleggen van verstrekkingen uit BVH met een I90 formulier gebeurt echter niet altijd door andere politiemedewerkers. Het invullen van het I90 formulier wordt als belastend ervaren. Daardoor worden niet alle verstrekkingen geregistreerd. Hieruit blijkt dat het toezicht door leidinggevend op verstrekkingen, met uitzondering van het Team Informatie, nog niet geheel voldoet.

Norm	Aspect		Bevinding en oordeel
			Hiermee wordt deels voldaan aan de Wpg.
Artikel 25 t/m 31, Rechten van de betrokkene			
25.1	Verzoek om kennisneming		Het proces voor rechten van betrokkenen wordt goed doorlopen. Een aandachtspunt is dat de privacyfunctionaris verzoeken afhandelt in het kader van de rechten van betrokkenen, terwijl hij 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 een 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 Friesland 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 Friesland beschikt deels over een Artikel 13 Register. Hiermee wordt deels voldaan aan de Wpg.
32.1.g	Protocollering onrechtmatige handeling		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. 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

Norm	Aspect		Bevinding en oordeel
			oordeel vormen over het wel of niet voldoen aan de Wpg. Wij adviseren een nader onderzoek.
Artikel 33, Audits			
RPAP 3.1	Interne audit-functie		Er is een functionaris vrijgemaakt voor de uitvoering van een audit naar opzet en bestaan van het stelsel van beheersmaatregelen voor de Wpg. De interne Wpg audit-functie is echter 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 een interne Wpg audit-rapport opgesteld. Het rapport is echter oppervlakkig, vaktechnisch onvoldoende verantwoord en schiet tekort in het op systematische wijze toetsen van opzet, bestaan en werking van maatregelen en procedures. Hiermee wordt niet voldaan aan de Wpg.
Artikel 34, Privacyfunctionaris			
34.1 en 34.4	Benoemd en gemeld		De privacyfunctionaris voor het korps Friesland 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		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. Daarnaast komt de privacyfunctionaris niet toe aan de toezichthoudende taken. Bij de rechten van betrokkenen vindt bovendien onterechte vermenging van functies plaats omdat de privacyfunctionaris dit proces uitvoert en er tevens toezicht op zou moeten houden. Wpg-specifieke scholing, met name gericht op de toezichthoudende taak, is niet opgenomen in het opleidingstraject. 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 Friesland 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 Friesland 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 de 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 Friesland.

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 maart 2011, van maatregelen en procedures, waarmee het

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

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

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

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

3.4 Afbakening

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

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

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

Wij hebben onze werkzaamheden uitgevoerd in augustus en 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 drs.
- de korpschef mw.
- de Hoofd Officier van Justitie mr.
- de privacyfunctionaris drs.
- de voorzitter van het College Bescherming Persoonsgegevens.

Het rapport mag uitsluitend met toestemming van de korpsbeheerder dan wel de korpschef van korps Friesland 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 RMT plaatsgevonden, maar de implementatie is gestagneerd mede onder invloed van de vorming van het Shared Service Center (SCC).

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 Team Informatie / RIK.

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.

In opzet is er 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. Uit de interviews komt naar voren dat er op de werkvloer behoefte is aan praktisch gerichte werkinstructies, stroomschema's etc. waarin de regelgeving van de Wpg concreet en helder, gebruikersvriendelijk en functiegericht wordt beschreven. Dit biedt de medewerker handvatten bij het uitvoeren van de dagelijkse werkzaamheden conform de Wpg.

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)

Mandaatbesluit

- 4.2.1 *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.

- 4.2.2 *Bevindingen*
 Er is een vigerend mandaatbesluit van 15 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*
 Het voldoen aan de bepalingen van deze artikelen is een aangelegenheid waarin bijna alle geledingen van de politie zijn betrokken. Niettemin is in het bijzonder van belang dat het zwaartepunt van het voldoen aan deze criteria ligt bij de eerste vastlegging van gegevens.

Daarvoor dragen registratie- en gegevensbeheerders de verantwoordelijkheid. Er is niet beschreven op welke wijze de zorg voor het voldoen aan deze criteria dient plaats te vinden. In volgende schakels van de keten is er over het algemeen ook geen aandacht voor deze criteria.

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 politietaken, 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 signaleerd, of de aanpak van de overlast bij een school of coffeeshop).
 - Een 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 n 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.

Uit de audit is gebleken dat doelbinding een lastig begrip is. Daarnaast is het ook niet altijd even gemakkelijk te bepalen wanneer politiegegevens relevant zijn. Verder is aangegeven dat de vastleggingen in BVO en BVH onvolledig zijn. Dit is onder meer te wijten aan de administratieve last voor het vastleggen en het ontbreken van koppelingen tussen applicaties.

Bij de informatieverwerkende afdelingen als de CIE en de RID wordt aan de kwaliteitsaspecten vanwege de bijzondere aard van hun taakstelling specifiek aandacht besteed. Daarbij is in de opzet het voldoen aan deze criteria zeker bij de CIE vanwege de toezichthoudende rol van het OM (de CIE OvJ) en het landelijk gebruik van het proceshandboek CIE goed verzorgd. Dit geldt in mindere mate bij de RID door het ontbreken van een toezichthoudende rol. Wel vindt toezicht plaats op de uitvoering door hoofd RID in afstemming met de korpschef.

Bij het Team Informatie is het voldoen aan deze criteria bij de eerste vastlegging van gegevens problematisch. Zij accepteren zonder nadere toetsing de ontvangen informatie zoals deze onder verantwoordelijkheid van registratie- en gegevensbeheerders wordt aangeleverd. Voor zover het in hun vermogen ligt, zullen zij wel aandacht besteden aan de vereiste criteria, doch de toetsing vanuit die positie is relatief beperkt te noemen. Bij het Team Informatie werkt men op basis van het concept "werkproces Infodesk 2008 handboek". Dit is gericht op het uitvoeren van een check door middel van een juridische bril of informatie aan de aanvrager ter beschikking mag worden gesteld.

De volgende beheersmaatregelen zijn geïmplementeerd:

- Een security beleidsplan, waarin de kwaliteit van gegevens aandacht krijgt, is opgesteld door de drie samenwerkende noordelijke korpsen.
- Een aantal procedures en checklisten is opgesteld om volledigheid en juistheid te waarborgen.
- Een aantal leidinggevenden bespreekt de onderwerpen van de Wpg tijdens interne overleggen.

- Registratiesystemen zoals BVH en BVO dwingen via de workflow bepaalde vastleggingen af. Op deze wijze wordt bijvoorbeeld volledigheid nagestreefd, zoals voor de MRO.
- Een aantal velden in BVH wordt gecontroleerd met behulp van de 'rules' in TrueBlue, resulterend in correctieve en repressie maatregelen waar nodig;
- Bij de recherche is er aandacht voor vastlegging van bronnen en hoe informatie uit andere onderzoeken is verkregen.
- Bij oplevering van een infoproduct (met disclaimer) wordt een bronnenlijst meegeleverd met als doel de kwaliteit te borgen bij de verzender (RIK) en de ontvanger (blauw/grijs).

Kwaliteitsbewaking met TrueBlue in BVH

Het korps Friesland 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 Friesland worden geen eigen kennisregels gemaakt. De beschikbare kennisregels zijn gedocumenteerd.

Informatievoorziening

Er bestaat nog geen vigerend beleid voor het beheer en de inrichting van de mappenstructuur. Er is een poging gedaan om bij 8Noord een uitrol te plegen. 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 voorsnog 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. Er wordt een gebrek aan doorzettingsmacht ervaren en er vindt geen monitoring plaats op de uitvoering van de Wpg.

Het korps Friesland gebruikt TrueBlue voor de bewaking van de kwaliteit van een aantal velden in BVH.

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

Het rechercheproces 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.

De CIE heeft een proceshandboek. De CIE OvJ houdt toezicht. Bij de RID liggen de kwaliteitscriteria al in het doel van de taak vast.

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

4.4 Gevoelige gegevens (artikel 5)

4.4.1 Norm

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

4.4.2 Bevindingen

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

Het korps heeft procedurele regels voor de omgang met gevoelige gegevens op intranet (PING) staan. Hierin is vastgelegd dat medewerkers van Politie Friesland gevoelige gegevens alleen mogen vastleggen als dat onvermijdelijk is voor het uitvoeren van de politietaak. 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

Er is een autorisatietabel van het Shared Service Centrum Noord (SSCN). Deze autorisatiematrix bevat de belangrijkste rollen binnen een korps en geeft initieel aan welke bevoegdheden in de basisvoorzieningen BVCM, BVH en BVO worden gekoppeld aan een rol, evenals autorisaties in andere systemen zoals GMS. Bij veel rollen heeft een medewerker actief toegang tot bijvoorbeeld BVH en BVO van het eigen korps, en mag raadplegen in de overeenkomstige basisvoorziening van de andere twee korpsen.

Het autorisatieproces in het korps Friesland wordt gezamenlijk uitgevoerd door het politiekorps, het SSCN en de vtsPN. Het beheer vindt plaats op basis van een procesbeschrijving voor autorisatiebeheer. Er is een procedure die de toekenning van autorisaties beschrijft. De privacyfunctionaris schoont jaarlijks de autorisaties voor applicaties.

De rechten op de mappenstructuur van de kantoorautomatiseringsomgeving zijn minder goed geregeld.

De CIE OvJ heeft een rol in het toetsen van de autorisaties van de CIE. Er bestaat op dit moment een proces waarbij de autorisaties van de CIE-medewerkers worden voorgelegd bij de OvJ. Dit proces is echter niet beschreven.

Er zijn 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 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 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 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.
- De autorisatieproblematiek voor BVH is eenvoudig. Er bestaat een discussie over toekenning van autorisaties aan stagiairs.
- 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..
- Bij het Team Informatie van het RIK wordt gebruik gemaakt van korps overstijgende systemen zoals Blueview. Reden is dat de interpretatie hier beter is geborgd.

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 voldoet het korps voor de autorisatiematrix 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.

De privacyfunctionaris schoont jaarlijks de autorisaties voor applicaties. Wij zijn van mening dat de privacyfunctionaris een wettelijke taak heeft toezicht uit te oefenen, en schonen van autorisaties in dit kader een oneigenlijke taak is. Schoning behoort te worden uitgevoerd als een gedocumenteerd en controleerbaar proces via de lijn.

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.

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

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 Team Informatie.

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.

Het Team Informatie is onder andere belast met het in combinatie met elkaar verwerken en geautomatiseerd vergelijken. Bij het Team Informatie zijn enkele medewerkers geautoriseerd voor Blueview. Nieuwe inzichten verkregen vanuit verschillende bronsystemen worden vastgelegd.

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.

Geïmplementeerde beheersmaatregelen zijn:

- Het werkproces Infodesk is beschreven. De status van deze werkinstructie is echter nog steeds concept.
- 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.

Het Team Informatie 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 Friesland.

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 Team Informatie binnenkomen worden geprotocolleerd.

4.7

Bewaartermijnen (artikel 14)

4.7.1

Norm

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

4.7.2

Bevindingen

Bij het gebruik en schonen van BVH kan geen onderscheid worden gemaakt tussen de artikelen 8 en 9 van de Wpg. Ook het ontbreken van een koppeling BVH en BVO wordt als knellend ervaren. Bewaartermijnen uit de Wpg worden eveneens als een belemmering ervaren, mede omdat BVO en BVH geen ondersteuning bieden om informatie als artikel 10 of 13 te classificeren. Nader onderzoek naar het Wpg-proof-zijn van BVH en BVO is noodzakelijk.

De regels voor schoning van bestanden met artikel 8 politiegegevens zijn weliswaar duidelijk gedefinieerd, maar zijn in de praktijk moeilijk uitvoerbaar. In de nieuwe release 1.2.2 van BVH zou dit wel tot de mogelijkheden behoren. Deze release op 15 december 2011 ingevoerd bij het korps Friesland. De schoningsscripts zijn daarbij niet aangezet. Friesland conformeert zich aan de visie van Noord-8 en zal na gezamenlijke besluitvorming de afgesproken scripts gaan uitvoeren.

De regels voor de verwijdering van oude gegevens zijn duidelijk bij de leidinggevendenden. Echter in de praktijk zijn ze moeilijk uitvoerbaar omdat het verwijderen handmatig moet gebeuren. Daardoor krijgt het verwijderen en schonen

nog onvoldoende prioriteit. Ook is niet voor iedereen helder wie verantwoordelijk is voor deze activiteiten.

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. Het OM heeft inzicht in de wijze van afdoening van zaken en moet dit delen met de politie om aan te geven wanneer WPG verwijderingstermijnen gaan lopen

Informatie van onderzoeken wordt bij de politie Friesland, naast in BVO en in BVH, ook in eigen persoonlijke en groepsmappen vastgelegd. Hierdoor ontstaat het risico op onrechtmatig gebruik en bewaring. De aanbeveling is om de schoning en uitfasering van groepsmappen voor onderzoeksdoelstellingen voort te zetten en het gebruik van aangewezen politiesystemen te stimuleren.

Tenslotte worden meldkamergesprekken na 3 maanden vernietigd.

Geïmplementeerde beheersmaatregelen zijn onder meer:

- Binnen het kantoor zijn Wpg-posters met informatie over bewaartermijnen opgehangen.
- Medewerkers van de Team Informatie zien toe op bewaartermijnen bij verstrekken van informatie.
- CIE OvJ voert periodiek controles uit waarbij ook naar de bewaartermijnen wordt gekeken.

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.

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.

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.

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

Voor het realiseren van artikel 15 Wpg is een aantal maatregelen getroffen bij Politie Friesland.

Het Team Informatie valt onder de divisie Informatie. Dit Team Informatie stelt informatie ter beschikking volgens vaste procedures. Op andere niveaus in het korps bestaat minder structuur in de informatie-uitwisseling. Er is aangegeven dat sommige medewerkers gebruik maken van informatie die volgens de Wpg had moeten worden verwijderd. Dit is moeilijk te voorkomen als de informatie niet wordt afgeschermd in de systemen. Ook het protocolleren van het ter beschikking stellen van informatie is een aandachtspunt. Uit de audit komt naar voren dat leidinggevendenden niet altijd goed zicht hebben op welke informatie ter beschikking wordt gesteld.

Bij CIE- en MRO-mutaties maakt men gebruik van de coderingen 00, 01 en 11. De door het korps gehanteerde omschrijving is:

- 00 = niet operationeel te gebruiken;
- 01 = slechts te gebruiken na overleg met de CIE;
- 11 = operationeel te gebruiken.

Informatie van onderzoeken wordt bij het korps Friesland, naast BVO en BVH, ook in eigen persoonlijke en groepsmappen vastgelegd. Hierbij ontstaat een risico op onrechtmatig gebruik en bewaring. Daarnaast is deze lokale opslag niet bevorderlijk voor het delen van informatie. Met name restinformatie wordt niet gedeeld, omdat dit nauwelijks in BVO wordt vastgelegd.

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 weigeringsgronden conform artikel 15.2. Het cursusmateriaal omvatte onder andere:

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

De cursus is door een docent WPG. Tijdens de cursus werd door hem uitleg gegeven over de WPG en werden 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.

Geïmplementeerde beheersmaatregelen zijn onder meer:

- De Infodesk hanteert elektronische formulieren met een check op de behoefte aan informatie gericht op "need to know". Telefonische vragen worden normaliter niet behandeld.
- De Infodesk werkt met een disclaimer bij het ter beschikking stellen van politiegegevens.
- Het werkproces Infodesk is beschreven. De status van deze werkinstructie is echter nog steeds concept.
- Iedereen die voor BVO is geautoriseerd kan zien als iemand een object is van onderzoek, maar niet de specifieke informatie. Voor specifieke informatie is toestemming nodig van de teamleider van dat onderzoek.
- De CIE is bij het ter beschikking stellen van gegevens strak in de uitvoering, met als extra waarborg de toezichthoudende taak van de CIE OvJ.
- RID gaat zorgvuldig om met het ter beschikking stellen van informatie. Zie ook het thema Verstrekkingen verderop in dit rapport. Hoofd RID ziet toe op de omzetting van bruto naar netto informatie. Hier ontbreekt echter de rol van een check door een externe toezichthouder.

4.8.3

Oordeel over ter beschikking stellen

Het Team Informatie stelt informatie ter beschikking volgens vaste procedures.

Een deel van de politiegegevens van het korps Friesland zijn echter opgeslagen in persoonlijke en groepsmappen met een risico op onrechtmatig gebruik en bewaring. Het gebruik van de mappenstructuur binnen Opsporing belemmert het Team informatie met het zoeken en vergelijken met andere onderzoeken. Hierdoor kan informatie ook niet met andere korpsen worden gedeeld.

Bij CIE- en MRO-mutaties maakt men gebruik van de coderingen 00, 01 en 11.

De bevoegd functionarissen 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.

In de cursus voor de bevoegd functionarissen is onder andere aandacht besteed aan de weigeringsgronden conform artikel 15.2.

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 verstrekkingenwijzer 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 het Team Informatie of de Juridische dienst van het SSC Noord. Dat loopt niet goed. Het is niet duidelijk wie verantwoordelijk is voor het proces in totaliteit. Verstrekkingen naar burgemeesters gaan via 11 teamchefs en via 4 verschillende manieren. Het is niet bekend of hierbij een en dezelfde lijn wordt gevolgd.

Vragen van de gemeente gaan via de teamchef "blauw" naar de privacyfunctionaris. In beginsel toetst de privacyfunctionaris de vraag en verstrekt. De teamchef "blauw" moet weten wat er speelt. Verstrekkingen naar de gemeente lopen te allen tijde via deze functionaris.

Aanvullende informatie is door het korps Friesland verstrekt op 16 december 2011: *'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 leidinggevendenden 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.'*

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 art 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. Er zijn over 2011 aan ons 2.497 registraties met I90 overlegd.

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

Voor wat betreft het Veiligheidshuis geldt dat er in 2011 een apart onderzoek van de CBP heeft plaatsgevonden naar het Wpg-proof zijn, in het bijzonder op de JCO support. Door het CBP zijn conclusies getrokken. Er zijn maatregelen getroffen ter verbetering. In oktober 2011 wordt hierover een hoorzitting gehouden.

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.

Bij het Veiligheidshuis hebben de ketenpartners getekend voor geheimhouding. CIE benadrukt dat de door hen verstrekte gegevens niet verder mogen worden doorverstrekt.

Het proces voor convenanten en artikel 20 besluiten loopt niet conform de daaraan te stellen eisen.

Verstrekkingen vinden doorgaans plaats via het Team Informatie of de Juridische dienst van het SSC Noord. Dat loopt niet goed. Het is niet duidelijk wie verantwoordelijk is voor het proces in totaliteit. Verstrekkingen naar burgemeesters gaan via 11 teamchefs en via 4 verschillende manieren. Het is niet bekend of hierbij een en dezelfde lijn wordt gevolgd.

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. Vanuit Amazone vinden geen externe verstrekkingen plaats.

De Team Informatie legt alle verstrekkingen vast. Het vastleggen van verstrekkingen door andere medewerkers via een I90 in BVH verloopt echter niet altijd goed, mede door onvoldoende bewustzijn en doordat dit als een administratieve last wordt ervaren.

De wel vastgelegde gegevens over verstrekkingen worden bewaard.

Bij de Team Informatie is toezicht door de leidinggevende. Bij andere medewerkers is niet altijd voldoende toezicht op het gebruik van de I90 in BVH.

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 niet goedgekeurde procesbeschrijving over verstrekken van gegevens aan burgers in verband met het inzagerecht. In korps Friesland pakt het Team Informatie dit op en in principe niet de privacyfunctionaris. Uitvoering vindt plaats door de Juridische dienst bij het SSC. Die is echter aan herinrichting onderhevig. De privacyfunctionaris houdt zich daarom nu bezig met de afhandeling van de rechten van betrokkenen.

De werkprocessen voor verbetering, aanvulling, verwijdering of afscherming van politiegegevens gegevens zijn niet formeel belegd. In de praktijk richt de privacyfunctionaris een verzoek aan de CIO, waarna de aanpassingen door functioneel beheer worden uitgevoerd.

Voor het jaar 2011 wordt het aantal af te handelen verzoeken op grond van ex art. 25, 28 en 30 (Kennisneming, correctie etc.) geschat op ongeveer 400.

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.

4.11 Protocolplicht (artikel 32)

4.11.1 Norm

De verantwoordelijke draagt zorg voor de schriftelijke vastlegging van:

- a. de doelen van Art. 9 onderzoeken;
- b. gegevens die op grond van ondersteunende taken worden vastgelegd (Art. 13.4);
- c. de toekenning van autorisaties (Art. 6);
- d. de geautomatiseerde vergelijking of het in combinatie met elkaar verwerken van politiegegevens (Art. 8.3 en 11.1, 11.2 en 11.4);
- e. de hernieuwde verwerking van politiegegevens op grond van Art. 9 of 10 (Art. 14.3);
- f. de verstrekking van politiegegevens (Paragraaf 3);
- g. signalen van onbevoegde of onrechtmatige verwerkingen;
- h. de geautomatiseerde vergelijking van gegevens met openbare bronnen (Art. 11.5).

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 verwijsex 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 Friesland beschikt over een Artikel 13 Register met de landelijke en regionale artikel 13 applicaties, inclusief doel etc. conform artikel 13.4. Naar onze mening is dit overzicht 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*

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

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

Er is een gedeeltelijk Artikel 13 register.

Een overzicht van onrechtmatige verwerkingen ontbreekt.

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 Groningen 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*

Op het gebied van de audit heeft Friesland een eigen koers gevaren. Er is een functionaris vrijgemaakt voor de uitvoering van een audit. De auditfunctie ten aanzien van de Wpg is echter niet structureel belegd. Daarnaast is geen vaktechnisch verantwoorde en meerjarige audit ingericht. Tenslotte is geen auditdossier opgesteld.

Geïmplementeerde beheersmaatregelen zijn onder meer:

- Er is een audit uitgevoerd die heel praktisch is gericht op het zicht krijgen op bestaande knelpunten in de uitvoering van de Wpg, maar niet voldoet aan de vaktechnische vereisten.

4.12.3 *Oordeel over interne audit*

Er is weliswaar een eenmalige actie uitgevoerd, maar er is geen structurele interne Wpg audit functie, geen intern Wpg audit plan en geen interne Wpg audit rapportage.

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 toezichthoudende. 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 toezichthoudende en de signalerende rol.

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 functionaris Gegevensbescherming bestaat niet als functie bij korps Friesland. Wel is er een Informatie Beveiligings Functionaris (IBF-er).

Informatiebeveiliging is in uitvoerende zin ondergebracht bij het Cluster Interne Veiligheid (BIV). Het hoofd van dit organisatieonderdeel legt rechtstreeks verantwoording af aan de Korpschef. Het beveiligingsbeleid is vastgelegd in een door de korpsbeheerder vastgesteld informatiebeveiligingsplan (d.d. 30 juni 2006). De IBF-er heeft zowel een adviserende als een toezichthoudende taak. De IBF-er heeft een tweedaagse WPG opleiding gevolgd.

De invoering van de WPG heeft niet geleid tot een aangepaste taakstelling of specifieke werkinstructies voor de IBF.

Het beveiligingsbeleid is niet aangepast aan de huidige organisatie-inrichtingen en ook niet op aansluiting op de WPG.