



Ministerie van Veiligheid en Justitie

Audit Wpg politie Hollands-Midden

Rapport

Datum
Status

23 december 2011
Definitief

Colofon

Afzendgegevens

Departementale Auditdienst

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

Contactpersonen

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

T 070 370 65 60
M wpg@minvenj.nl

Projectnaam

Audit Wet Politiegegevens

Ons kenmerk

DDS/5719585/11

Auteurs

drs. D. van Ilpenhof RE CISA

Inhoud

Colofon 3

Assurance Verklaring 7

1 Samenvatting 9

2 Inleiding 23

- 2.1 Algemeen 23
- 2.2 Aanleiding 23
- 2.3 Doelstelling, aard en scope van de opdracht 23
- 2.4 Afbakening 24
- 2.5 Normenkader 24
- 2.6 Beperkingen voor de privacy audit 25
- 2.7 Onderzoeksmethoden en werkwijze 25
- 2.8 Doelgroep van het rapport 25

3 Bevindingen 26

- 3.1 Inleiding 26
- 3.2 Verantwoordelijke (artikel 1.f) 26
- 3.3 Kwaliteitsaspecten van politiegegevens (artikel 3 en 4) 27
- 3.4 Autorisatie (artikel 6) 34
- 3.5 Geautomatiseerd Vergelijken (GV)/In Combinatie Met Elkaar Verwerken (ICMEV)(artikel 11) 38
- 3.6 Ter beschikking stellen (artikel 15) 44
- 3.7 Verstrekken (artikel 16/24) 47
- 3.8 Rechten van betrokkenen (artikel 25/28) 54
- 3.9 Protocolplicht (artikel 32) 56
- 3.10 Audits (artikel 33) 57
- 3.11 Privacyfunctionaris (artikel 34) 58
- 3.12 Functionaris Gegevensbescherming (artikel 36) 60

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 maart 2011 is een privacy audit uitgevoerd bij het korps Hollands-Midden.

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 Hollands-Midden.

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 Hollands-Midden, naar de stand van ultimo maart 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 Hollands-Midden te nemen maatregelen. Ook is gebleken dat het korps Hollands-Midden voor het volledig kunnen voldoen aan de Wpg eisen mede afhankelijk is van besluiten die buiten het korps Hollands-Midden 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 Hollands-Midden, is, op grond van artikel 4 lid 1 van de Regeling Periodieke Audit Politiegegevens, verplicht binnen drie maanden een verbeterrapport op te stellen waarin de maatregelen worden beschreven die getroffen zijn ter verbetering van de in de privacy audit geconstateerde tekortkomingen. Op grond van artikel 4 lid 3 dient hercontrole plaats te vinden. Wij adviseren die hercontrole te laten uitvoeren door de interne auditors van het korps Hollands-Midden. Het verbeterrapport en de uitgevoerde hercontrole zullen in de navolgende jaren door de privacyauditor worden beoordeeld.

Den Haag, 23 december 2011

De Directeur van de Departementale Auditdienst

A handwritten signature in blue ink, consisting of a large, stylized 'J' followed by 'C. van Praat' and a long horizontal stroke.

J.C. van Praat RE RA

1 Samenvatting

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

Criteria:

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

Norm	Aspect		Bevinding en oordeel
Artikel 1.f, Verantwoordelijke			
1.f	Mandaatbesluit		Er is een mandaatbesluit waarin is aangetoond dat het bevoegde gezag het mandaat heeft verleend aan de Korpschef. Het mandaatbesluit bevat tevens een ondermandatering. 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 het intranet zijn de uitgangspunten van de Wpg gepubliceerd voor de medewerkers. Deze uitgangspunten gaan in op de noodzaak van de Wpg, alsmede op de verwerkingsdoelen van artikel 8 tot en met 13 Wpg. Hier wordt kort aangegeven wat wordt verstaan onder deze Wpg-artikelen, inclusief praktische voorbeelden. Tevens zijn werkafspraken gedocumenteerd voor artikel 8 en 9 Wpg politiegegevens. Hierin wordt ook het onderscheid tussen beiden duidelijk gemaakt. Een groot aantal trainingen zijn gegeven om voorlichting te geven over de Wet politiegegevens aan de medewerkers van Hollands-Midden. Hiermee wordt voldaan aan de Wpg.
3.1 t/m 3.3 (8) 4.1 (8)	Noodzakelijkheid (8) Doelbinding Rechtmatigheid Juistheid Volledigheid		Op het intranet zijn de uitgangspunten van de Wpg gepubliceerd voor de medewerkers. Deze uitgangspunten gaan in op de noodzaak van de Wpg, alsmede op de verwerkingsdoelen van artikel 8 tot en met 13 Wpg. Bij de invoer van politiegegevens in BVH is er sprake van verschillende invoercontroles om de juistheid en volledigheid van deze gegevens te controleren. De Regionale Dienst Informatie verzorgt de afhandeling en toetsing van informatieverzoeken. Hiermee wordt voldaan aan de Wpg.

Norm	Aspect		Bevinding en oordeel
3.1 t/m 3.4 (9) 4.1 (9)	Noodzakelijkheid (9) Doelbinding Rechtmatigheid Herkomst en wijze van verkrijging Juistheid Nauwkeurig Volledigheid		Op het intranet zijn de uitgangspunten van de Wpg gepubliceerd voor de medewerkers. Deze uitgangspunten gaan in op de noodzaak van de Wpg, alsmede op de verwerkingsdoelen van artikel 8 tot en met 13 Wpg. De Regionale Dienst Informatie verzorgt de afhandeling en toetsing van informatieverzoeken omtrent artikel 9 gegevens. Er wordt echter gebruik gemaakt van zowel SUMM-IT als BVO, waarbij niet altijd de gegevens in beide systemen worden geregistreerd. De belangrijkste gegevens staan in BVO, de verwerking vindt vaak plaats in SUMM-IT. Om een volledig beeld te verkrijgen moeten beide systemen worden geraadpleegd. Volledigheid is daarbij niet geborgd. In februari 2012 gaat HM volledig over naar het gebruik van Summ-IT. Blueview neemt deze gegevens mee in bevestigingen. Door het niet altijd invoeren van de zogeheten 'zachte gegevens' wordt mogelijk niet voldaan aan het volledigheidseisen van artikel 4.1 Wpg. Hiermee wordt niet geheel voldaan aan de Wpg.
3.4 (10 en 12) 4.1 (10 en 12)	Noodzakelijkheid (10 en 12) Doelbinding Rechtmatigheid Herkomst en wijze van verkrijging Juistheid Nauwkeurig Volledigheid		CIE: CIE maakt gebruik van het CIE-proceshandboek. Alle projectvoorstellen worden vooraf aan de CIE-Officier van Justitie voorgelegd. Een informatieofficier is al in de fase van preweging betrokken. De Officier van Justitie wordt bij elke in- en uitschrijving in het informantenregister betrokken. Tevens wordt een onderscheid gemaakt tussen bruto en netto informatie en wordt toegezien op de noodzaak tot inzicht in deze gegevens. RID: Gegevens inzake informanten (artikel 12 Wpg) worden elektronisch opgeslagen in een beveiligde ruimte. Hiermee wordt voldaan aan de Wpg.
4.3	Beveiliging (isolatie)		De mappenstructuur voldoet op meerdere punten vanuit beheersbaarheid niet aan de vereisten van de Wpg. In de opzet van de mappenstructuur wordt geen onderscheid gemaakt tussen artikel 8 Wpg en artikel 9 Wpg gegevens. Artikel 9 onderzoeken worden wel per map ingedeeld waarvoor men apart moet

Norm	Aspect		Bevinding en oordeel
			worden geautoriseerd. Door deze huidige opzet van de mappenstructuur kunnen de schoningstermijnen die betrekking hebben op deze gegevens niet juist worden toegepast. <i>Beveiliging CIE</i> De beveiliging en kwaliteit bij de CIE Hollands-Midden wordt echter gewaarborgd aan de hand van de landelijke CIE-richtlijn en het CIE-proceshandboek. Hiermee wordt niet volledig voldaan aan de Wpg.
Artikel 5, gevoelige gegevens			
	Gevoelige gegevens		Hollands-Midden hanteert een strikt beleid omtrent het vastleggen van gevoelige gegevens. Het korps is terughoudend in het registreren van gevoelige gegevens en doet dit enkel wanneer dit noodzakelijk is voor de uitvoering van de politietaak. Hiermee wordt voldaan aan de Wpg.
Artikel 6, Autorisatie			
	Korpsautorisatiematrix		Er wordt gebruik gemaakt van een korpsautorisatiematrix. De autorisatiematrix is middels intranet beschikbaar. De matrix bevat de belangrijkste systemen van Hollands-Midden, inclusief de regionale applicaties. Voor de overige systemen wordt er geautoriseerd conform landelijke afspraken. Indien wordt afgeweken worden hier aparte besluiten van opgesteld. Autorisaties buiten de standaardprofielen (maatwerkautorisaties) worden verleend op tijdelijke basis en worden voorgelegd aan de privacyfunctionaris. De privacyfunctionaris consulteert hiervoor bij de functionaris voor de gegevensbescherming. De directeur informatie geeft de uiteindelijke goedkeuring van de autorisatie. Dienst Informatie beheert de autorisaties. Hiermee wordt voldaan aan de Wpg.
	Aanvraagproces		De procedure met betrekking tot het autoriseren van medewerkers is bekend en voldoet aan de vereisten van zorgvuldigheid en evenredigheid van de Wpg. Hiermee wordt voldaan aan de Wpg.
	Wijzigingen en verwijderingen		In opzet is er een proces voor wijzigingen en verwijderingen. Wijzigingen dienen door de afdeling P&O te worden vermeld, dit blijkt in de praktijk vaak niet te gebeuren. Met de opzet van het veelal

Norm	Aspect	Bevinding en oordeel
		handmatige signaleren loopt men het risico dat functiewisselingen niet (tijdig) word(t)(en) gesignaleerd doordat het proces nog niet is geautomatiseerd. Men is afhankelijk is van 'oplettende medewerkers'. Hiermee wordt niet voldaan aan de Wpg.
	• Autorisatiebeheer CIE en RID	De CIE en RID autorisaties verlopen middels het regiobeleid Hollands-Midden. Hiermee wordt voldaan aan de Wpg.
32.1.c	Protocollering autorisaties	Aanvragen, wijzigingen en verwijderingen van autorisaties lopen volgens een procedure. De verzoeken worden vastgelegd in de tool 'Expertdesk'. Tijdelijke autorisatieverzoeken buiten het functieprofiel worden door de privacyfunctionaris bewaard. Hiermee wordt voldaan aan de Wpg.
32.3 voor 32.1.c	Bewaren protocolgegevens autorisaties	Aanvragen, wijzigingen en verwijderingen van autorisaties lopen volgens een procedure. De verzoeken worden vastgelegd in de tool Expertdesk. Tijdelijke autorisatieverzoeken buiten het functieprofiel worden door de privacyfunctionaris bewaard. Hiermee wordt voldaan aan de Wpg.
Artikel 11, Geautomatiseerd vergelijken en in combinatie zoeken		
	• Hanteerbare interpretatie	De CIE doet aan subjectanalyse. Met de OvJ is afgesproken dat er geen machtiging is vereist. Het Hoofd-CIE van het brononderzoek maakt een procesverbaal aan. Na voorafgaande toestemming van de CIE-Officier van Justitie, verstrekt hij dit aan het Hoofd-CIE waar het doelonderzoek plaats zou moeten vinden. Het Hoofd-CIE controleert vooraf of de te verstrekken tekst overeenkomt met de informatie. Tevens wordt gecontroleerd of deze rechtmatig is verkregen. Via een MRO (Melding Recherche Onderzoeken) worden data (personalia, telefoonnummer, kentekens) wekelijks geautomatiseerd landelijk vergeleken. Hiermee wordt er voldaan aan de Wpg.
	• Aangewezen functionarissen	De aangewezen functionarissen voor artikel 10 zijn personeel van de CIE, RID, themaregisters en in voorkomende gevallen medewerkers van Dienst Informatie (DI). DI-medewerkers mogen alleen deze handelingen verrichten bij goedkeuring door de desbetreffende Hoofd-CIE, RID, of

Norm	Aspect		Bevinding en oordeel
			themaverwerking. Hiermee wordt voldaan aan de Wpg.
11.4	Bevoegde gezag		De CIE-Officier van Justitie is het bevoegde gezag voor de verwerking van politiegegevens ex artikel 10 en 12 Wpg. Met toestemming van de Officier van Justitie kan er in combinatie met elkaar gezocht en verder worden verwerkt. Hiermee wordt voldaan aan de Wpg.
32.1.d en 32.1.h	Protocollering 11.1, 11.2, 11.4 en 11.5		Alle zoekslagen vinden plaats in BRAINS. De zoekresultaten worden aangehouden c.q. gelogd in BRAINS. In analyse reportages wordt aangegeven op welke wijze is gezocht. In de operationele analyse is beschreven hoe men tot het resultaat is gekomen. Er wordt echter geen actief toezicht gehouden op het geautomatiseerd vergelijken met niet-politiegegevens. Het toezicht op de protocolplicht is bovendien nog niet opgepakt. Hiermee wordt niet voldaan aan de Wpg.
32.3 voor 32.1.d en 32.1.h	Bewaren protocolgegevens 11.1, 11.2, 11.4 en 11.5		Er wordt geen actief toezicht gehouden op het geautomatiseerd vergelijken met niet-politiegegevens. Het toezicht op de protocolplicht is nog niet opgepakt. Hiermee wordt niet voldaan aan de Wpg.
Artikel 14, Bewaartermijnen			
8.2 en 8.3	(8) van 1 tot 5 jaar		Het schoningsscript van BVH (versie 1.2.2) is dit jaar bij Hollands-Midden geactiveerd. Hierdoor vindt het 'na een jaar achter schot plaatsen' van artikel 8 Wpg informatie automatisch plaats. De dagrapportage van BVH biedt in Hollands-Midden de mogelijkheid tot ongericht zoeken tot 1 jaar terug, maar elke medewerker die daarvoor geautoriseerd is heeft de mogelijkheid om op basis van bijvoorbeeld specifieke personen/kentekens/locaties hit/no-hitbevestigingen te doen op grond artikel 8.2 Wpg. Hiermee wordt voldaan aan de Wpg.
8.6	(8) verwijderen na 5 jaar		Het schoningsscript van BVH (versie 1.2.2) is dit jaar bij Hollands-Midden geactiveerd. Het verwijderen na vijf jaar hoeft pas in 2014 plaats te vinden omdat BVH (geheel leeg) in 2009 in gebruik is genomen. Hiermee wordt voldaan aan de Wpg.

Norm	Aspect		Bevinding en oordeel
14.1 (8)	(8) vernietigen na 5 jaar verwijderd		Het schoningscript van BVH (versie 1.2.2) is dit jaar bij Hollands-Midden geactiveerd. Politiegegevens in de applicatie BPS (voorganger BVH) worden geschoond na tien jaar. Er vindt nog geen vernietiging van informatie uit BVH plaats. Hiermee wordt voldaan aan de Wpg.
9.4	(9) verwijderen na OH plus ½ jaar		De bewaartermijn zoals deze is gesteld in de Wet politiegegevens is nog niet ingeregeld in BVO. Hierdoor blijven veel gegevens in het systeem staan die volgens de gestelde termijn al hadden moeten worden verwijderd of vernietigd. Het OH-moment kan niet worden bepaald omdat in de praktijk blijkt dat men (bijna) nooit een signaal van het OM ontvangt dat de zaak in kracht van gewijsde is gegaan, met als gevolg dat er in BVO nimmer een zaak wordt verwijderd. Hiermee wordt niet voldaan aan de Wpg.
14.1 (9)	(9) vernietigen na 5 jaar verwijderd		De bewaartermijn zoals deze is gesteld in de Wet politiegegevens is nog niet ingeregeld in BVO. Hierdoor blijven veel gegevens in het systeem staan die volgens de gestelde termijn al hadden moeten worden verwijderd of vernietigd. Het OH-moment kan niet worden bepaald omdat in de praktijk blijkt dat men (bijna) nooit een signaal van het OM ontvangt dat de zaak in kracht van gewijsde is gegaan, met als gevolg dat er in BVO nimmer een zaak wordt verwijderd. Hiermee wordt niet voldaan aan de Wpg.
10.6	(10) verwijderen na 5 jaar geen subjectwaardige registratie		Het Hoofd-CIE dient ervoor zorg te dragen dat het gegevensbestand regelmatig wordt gecontroleerd teneinde te beoordelen of de noodzaak voor de verwerking van gegevens nog steeds aanwezig is. Deze controle vindt elk half jaar plaats. Voor het verwijderen en vernietigen van artikel 10 Wpg-informatie volgt de CIE de procedure uit het landelijke CIE-proceshandboek. Hiermee wordt voldaan aan de Wpg.
14.1 (10)	(10) vernietigen na 5 jaar verwijderd		Het Hoofd-CIE dient ervoor zorg te dragen dat het gegevensbestand regelmatig wordt gecontroleerd teneinde te beoordelen of de noodzaak voor de verwerking van gegevens nog steeds aanwezig is. Deze controle vindt elk half jaar plaats.

Norm	Aspect		Bevinding en oordeel
			Voor het verwijderen en vernietigen van artikel 10 Wpg-informatie volgt de CIE de procedure uit het landelijke CIE-proceshandboek. Hiermee wordt voldaan aan de Wpg.
14.3	Hernieuwde verwerking		Er is nog geen invulling gegeven aan een procedure voor het hernieuwd verwerken van politiegegevens buiten de CIE om. Tevens zijn geen functionarissen aangewezen die deze verwerking mogen verrichten. Hiermee wordt niet voldaan aan de Wpg.
32.1.e	Protocollering 14.3		Er is nog geen invulling gegeven aan een procedure voor het hernieuwd verwerken van politiegegevens buiten de CIE om. Tevens zijn geen functionarissen aangewezen die deze verwerking mogen verrichten. Hiermee is de afhandeling van de protocollering niet geborgd. Hiermee wordt niet voldaan aan de Wpg.
32.3 voor 32.1.e	Bewaren protocolgegevens 14.3		Er is nog geen invulling gegeven aan een procedure voor het hernieuwd verwerken van politiegegevens buiten de CIE om. Tevens zijn geen functionarissen aangewezen die deze verwerking mogen verrichten. Hiermee is de afhandeling van de protocollering niet geborgd. Hiermee wordt niet voldaan aan de Wpg.
12.2	(12) gebruiken tot 4 maanden		Met het OM worden periodiek de subjecten en nieuwe bronnen doorgesproken. De Officier voert een steekproefsgewijze controle uit op de informatie onder artikel 12 Wpg. Tweemaal per jaar vindt schoning plaats van de informanten. Subjecten en bronnen worden getoetst en getekend door de Officier. Tevens vindt kascontrole plaats en worden de Processen Verbaal ingezien. De Officier van Justitie is elke 14 dagen aanwezig bij het werkoverleg. Voorts is elke week overleg met de teamleider. Hiermee wordt voldaan aan de Wpg.
12.6	(12) controleren en vernietigen		Met het OM worden periodiek de subjecten en nieuwe bronnen doorgesproken. De Officier voert een steekproefsgewijze controle uit op de informatie onder artikel 12 Wpg. Tweemaal per jaar vindt schoning plaats van de informanten. Subjecten en bronnen worden getoetst en getekend door de Officier. Tevens vindt kascontrole plaats en worden de Processen Verbaal

Norm	Aspect		Bevinding en oordeel
			ingezien. De Officier van Justitie is elke 14 dagen aanwezig bij het werkoverleg. Voorts is elke week overleg met de teamleider. Hiermee wordt voldaan aan de Wpg.
Artikel 15, Ter beschikking stellen			
	Infodesk voor bevraging		De Directie Informatie kent 7 businessunits: Functioneel beheer, Bedrijfsinformatiemanagement, Analyse, Veredeling, Gegevensverwerking, Afhandeling Bekeuring Systeem en Informatie coördinatie. Afdeling Gegevensverwerking is voor de enkelvoudige vragen en afdeling Veredeling voor de complexe vragen, waarbij een 14-tal systemen is betrokken. De coördinator beoordeelt de vraag, toetst de doelbinding en zet deze uit naar medewerker Gegevensverwerking of Veredeling. Alle vragen worden sinds 4 jaar geregistreerd in PLANON, waartoe alleen de business units Gegevensverwerking en Veredeling toegang hebben. Hiermee voldoet het korps aan de Wpg.
	Codering		CIE-informatie wordt gecodeerd in 00-informatie en 01-informatie belangrijke informatie wordt gecodeerd conform Wpg. Hiermee wordt voldaan aan de Wpg.
	Aanwijzing Bevoegde Functionaris		De bevoegde functionarissen zijn benoemd. Hiermee wordt voldaan aan de Wpg.
	Opleiding Bevoegde Functionaris		De functionarissen hebben een opleiding gevolgd om kennis van de Wpg op te doen. Hiermee wordt voldaan aan de Wpg.
15.2	Weigeringgronden		De bevoegde functionarissen zijn op de hoogte van de wettelijk toegestane weigeringsgronden. Deze gronden komen aan de orde in de genoten opleiding. Echter wij hebben geconstateerd dat doordat men veel in Word-documenten werkt deze informatie niet in de daarvoor bestemde systemen terechtkomt. Deze niet ingevoerde politiegegevens worden dus niet via deze systemen gedeeld. Hierdoor loopt men het risico dat er informatie in Word-documenten gehouden wordt daar waar het had moeten worden gedeeld. Hiermee wordt niet voldaan aan de Wpg.

Norm	Aspect	Bevinding en oordeel
Artikel 16 t/m 24, Verstrekking		
• Verstrekkingenwijzer (landelijk)		Het korps Hollands-Midden maakt gebruik van de landelijke verstrekkingwijzer. Hiermee wordt voldaan aan de Wpg.
• Proces voor convenanten		Nieuwe convenanten worden door de privacyfunctionaris van het korps getoetst aan de Wpg en daar waar nodig bijgesteld. District- en teamchefs worden in districtelijk verband geïnformeerd over de tekenbevoegdheid van de korpsbeheerder inzake convenanten en de (on)mogelijkheden van gegevensverstrekking wanneer zij op lokaal niveau samenwerking met partijen aangaan. Hollands-Midden heeft voor nieuwe artikel 20-besluiten een toetsingskader ontwikkeld om te waarborgen dat nog af te sluiten samenwerkingsverbanden voldoen aan de bepalingen van de Wpg. Hiermee wordt voldaan aan de Wpg.
• Proces voor Artikel 20 Besluiten		De nieuw te ondertekenen artikel 20-besluiten dienen ter toetsing te worden voorgelegd aan de privacyfunctionaris. Het besluit moet worden ondertekend door de korpsbeheerder en het bevoegde gezag. Geconstateerd is dat het opgestelde Modelbesluit de noodzakelijk gegevens bevat die op basis van artikel 20 Wpg zijn vereist. De afgesloten artikel 20-besluiten worden gepubliceerd op intranet zodat elke medewerker hiervan kan kennisnemen. Hiermee wordt voldaan aan de Wpg.
• Verstrekkingenschema (regio)		Uit de gehouden interviews blijkt dat de Wpg binnen het korps dusdanig wordt opgevat dat verstrekken niet is toegestaan, terwijl dit een onjuiste lezing is. Hiermee wordt niet voldaan aan de Wpg.
• Proces voor geautomatiseerde verstrekking		Het proces van geautomatiseerde gegevensverstrekking is niet beheersbaar doordat er geen inzicht is binnen het korps over deze verstrekkingen. Dit staat genoteerd als onderdeel van het verbeterpakket van Functioneel Beheer. Hiermee wordt niet voldaan aan de Wpg.
7.2	Geheimhouding	Er is geconstateerd dat de gegevens alleen onder geheimhouding worden verstrekt. Dit is conform de Wpg.

Norm	Aspect		Bevinding en oordeel
32.1.f	Protocollering verstrekking		In opzet is de protocollering van de verstrekking door middel van I90-formulieren goed geregeld. Een procesuitleg is beschikbaar. Echter, bij toetsing van de werking blijkt dat het I90-formulier niet door iedereen structureel wordt gebruikt. Vaak maakt men hiervan een losse vermelding in een mutatie. Doordat niet altijd gebruik wordt gemaakt van een I90-formulier kan het overzicht niet als compleet worden beschouwd. Daarmee kan de privacyfunctionaris zijn controlerende taak niet geheel effectief uitvoeren. Hiermee wordt deels voldaan aan de Wpg.
32.3 voor 32.1.f	Bewaren protocolgegevens verstrekking		In opzet is de protocollering van de verstrekking door middel van I90-formulieren goed geregeld. Een procesuitleg is beschikbaar. Echter, bij toetsing van de werking blijkt dat het I90-formulier niet door iedereen structureel wordt gebruikt. Vaak maakt men hiervan een losse vermelding in een mutatie. Doordat niet altijd gebruik wordt gemaakt van een I90-formulier kan het overzicht niet als compleet worden beschouwd. Daarmee kan de privacyfunctionaris zijn controlerende taak niet geheel effectief uitvoeren. Hiermee wordt deels voldaan aan de Wpg.
• Toezicht door leidinggevend op verstrekkingen en protocollering			De materiedeskundige, ploegchef en de informatiemedewerker gaan over de verstrekkingen van politiegegevens. De leidinggevend hebben tevens hierin een eigen verantwoordelijkheid dat er conform de Wpg wordt geprotocolleerd. De functionaris voor de gegevensbescherming houdt hier toezicht op en geeft wanneer nodig advies. Hiermee wordt voldaan aan de Wpg.
Artikel 25 t/m 31, Rechten van de betrokkene			
25.1	Verzoek om kennisneming		Sinds 2011 heeft Hollands-Midden een nieuwe procedure vastgesteld met betrekking tot het afhandelen van inzageverzoeken conform de Wpg. Eenvoudige verzoeken worden door een uitvoerend medewerker (de Wpg-functionaris) afgehandeld en de complexe verzoeken door de privacyfunctionaris. De medewerkers binnen het korps zijn middels een instructie 'Informatieverstrekking of privacyverzoek of WOB-verzoek' op de hoogte gebracht van deze procedure. Er blijken geen klachten te zijn binnengekomen. Hiermee wordt voldaan aan de Wpg.

Norm	Aspect		Bevinding en oordeel
28.1 t/m 28.3	Correctie		Verzoeken tot correctie worden door de privacyfunctionaris afgehandeld. De personen waarvan het inzageverzoek is ingewilligd worden middels een brief die men meekrijgt gewezen op dit recht van correctie. Om hiervoor in aanmerking te komen dient men het verzoek schriftelijk in te dienen en goed te motiveren. In 2010 is dit eenmaal voorgekomen. 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		Een nieuw onderzoek wordt aangemaakt door de rechercheur in een Word-sjabloon. Dit formulier stuurt automatisch een kopie naar de functionaris gegevensbescherming en ISC West. De functionaris voor de gegevensbescherming houdt sinds 2000 een overzicht bij van artikel 9 doelen. Tevens wordt nu gewerkt aan een tool op intranet voor eenduidige registraties. Hiermee wordt voldaan aan de Wpg.
32.3 voor 32.1.a	Bewaren protocolgegevens doel onderzoek		In een Excelbestand worden deze protocolgegevens bewaard door de functionaris voor de gegevensbescherming. Dit overzicht is inzichtelijk voor de privacyfunctionaris. Hiermee wordt voldaan aan de Wpg.
13.4 en 32.1.b	Protocollering Artikel 13 gegevensverzameling en		De gegevensverzamelingen op grond van artikel 13 zijn binnen Hollands-Midden geïdentificeerd. Het korps geeft aan geen gebruik te maken van regionale systemen en gegevensverzamelingen buiten de landelijke systemen. De protocollering van de landelijke artikel 13 systemen (zoals HKS) vindt op een landelijk niveau plaats middels standaard protocolformulieren. De protocollering van deze systemen wordt in de systemen aangehouden. Hiermee wordt voldaan aan de Wpg.
32.3 voor 32.1.b	Bewaren protocolgegevens Artikel 13 gegevensverzameling en		De gegevensverzamelingen op grond van artikel 13 zijn binnen Hollands-Midden geïdentificeerd. Het korps geeft aan geen gebruik te maken van regionale systemen en gegevensverzamelingen buiten de landelijke systemen. De protocollering van de landelijke artikel 13 systemen (zoals HKS) vindt op een landelijk niveau plaats middels standaard protocolformulieren. De protocollering van deze systemen wordt in de systemen aangehouden. Hiermee wordt voldaan aan de Wpg.

Norm	Aspect		Bevinding en oordeel
32.1.g	Protocollering onrechtmatige handeling		Er wordt een overzicht bijgehouden van de onrechtmatige verwerkingen door de functionaris voor de gegevensbescherming en de privacyfunctionaris. Dit betreft een aantal schendingen per jaar. Hiermee wordt voldaan aan de Wpg.
32.3 voor 32.1.g	Bewaren protocolgegevens onrechtmatige handeling		Er wordt een overzicht bijgehouden van de onrechtmatige verwerkingen door de functionaris voor de gegevensbescherming en de privacyfunctionaris. Dit betreft een aantal schendingen per jaar. Hiermee wordt voldaan aan de Wpg.
32.2	Gemeenschappelijke verwerking		Niet van toepassing. Het korps Hollands-Midden heeft geen gemeenschappelijke verwerkingen met andere korpsen.
Artikel 33, Audits			
RPAP 3.1	Interne audit-functie		Het korps heeft een senior controller aangewezen om de interne audit uit te voeren. Deze controller heeft de opleiding tot Wpg-auditor gevolgd. Hiermee wordt voldaan aan artikel 3.1 RPAP.
RPAP 3.4	Interne audit-plan		Het korps heeft een intern auditplan 2010 opgesteld. Het auditplan bevat een omschrijving van de minimale vereisten vanuit de RPAP, echter ontbreekt een uitwerking en toepassing van de wettelijke vereisten op de onderdelen van het korps Hollands-Midden. Het auditplan 2011 is uitgevoerd door een extern bureau en heeft zich gericht op het auditobject: de interne auditfunctie. Het korps gaat de bevindingen uit de externe auditrapportage gebruiken voor het auditplan 2012. Hiermee wordt voldaan aan artikel 3.4 RPAP.
RPAP 3.6	Interne audit-rapport		Het interne audit-rapport voldoet aan de minimumvereisten van de Wpg. De gevolgde audit-methodiek is opgesteld, de werkwijze is beschreven en tevens zijn de resultaten beschreven voorzien van een oordeel. Hiermee wordt voldaan aan artikel 3.6 RPAP.
Artikel 34, Privacyfunctionaris			
34.1 en 34.4	Benoemd en gemeld		De privacyfunctionaris is aangesteld en aangemeld bij het CBP. Hiermee wordt voldaan aan de Wpg. N.B: De privacyfunctionaris heeft meer een adviserende rol in het korps, terwijl de functionaris gegevensbescherming (FG) meer een toezichthoudende rol vervult. Deze taakverdeling is

Norm	Aspect		Bevinding en oordeel
			nog niet geheel helder en vergt nadere uitwerking in 2012, rekeninghoudende met de onafhankelijke rol die de FG dient te vervullen. Hiermee wordt voldaan aan de Wpg.
34.2	Overzicht over protocollering		De opzet en controle van protocolleringen vormt nog een aandachtspunt bij het korps Hollands-Midden. De protocolleringen vormt een van de centrale aandachtspunten voor het korps voor 2012. <i>Protocollering:</i> De nog niet geheel uitgekristalliseerde taakverdeling uit zich in het feit dat er geen heldere afbakening is van de taken die voortvloeien uit de protocolplicht. <i>Artikel 11:</i> De zoekresultaten worden aangehouden c.q. gelogd in BRAINS. In analyse rapportages wordt aangegeven hoe men heeft gezocht. In de operationele analyse is beschreven hoe men tot het resultaat is gekomen. Uit de praktijk blijkt dat nog onvoldoende controle plaatsvindt op de logging van artikel 11-verwerkingen. Hiermee wordt niet voldaan aan de Wpg.
34.3	Jaarverslag		De privacyfunctionaris heeft een jaarverslag over 2010 opgesteld. Tevens heeft functionaris voor de gegevensbescherming (FG), om begrijpelijke redenen, de taken van de privacyfunctionaris (in haar afwezigheid) deels overgenomen en vormt daarmee onderdeel van het proces. De overname van de privacytaken is door de FG medegedeeld aan het CBP. De FG heeft ook een jaarverslag 2010 opgesteld met daarin zijn bevindingen vanuit de rol als toezichthouder op naleving van de Wpg. Hiermee wordt voldaan aan de Wpg.
Optioneel Artikel 36, Functionaris Gegevensbescherming			
36.1 en 36.2	Benoemd		In het korps is een functionaris voor de gegevensbescherming (FG) aangesteld. Hiermee wordt voldaan aan de Wpg.
Wbp 63.3	Gemeld		De FG is aangemeld bij het CBP. Hiermee wordt voldaan aan de Wbp.

Norm	Aspect		Bevinding en oordeel
Wbp 64.1 t/m 64.4	Toezichthoudende rol		De FG heeft, om begrijpelijke redenen, de taken van de privacyfunctionaris (in haar afwezigheid) deels overgenomen en vormt daarmee onderdeel van het proces. De overname van de privacytaken is door de FG medegedeeld aan het CBP. De onafhankelijkheid van de FG kan door het meedraaien in het proces niet volledig worden gewaarborgd. Hiermee wordt deels voldaan aan de Wbp.

2 Inleiding

2.1 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 Hollands-Midden 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 Hollands-Midden in 2011.

2.2 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.

2.3 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 Hollands-Midden.

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 Hollands-Midden 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.

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

2.5 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.

2.6 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.

2.7 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 Hollands-Midden en het Openbaar Ministerie, deelwaarnemingen in de procesbeschrijvingen en andersoortige documentatie en deelwaarnemingen in informatiesystemen.

Wij hebben onze werkzaamheden uitgevoerd in de periode maart 2011 en november/december 2011.

Het eindrapport is met inachtneming van het ontvangen commentaar vastgesteld.

2.8 Doelgroep van het rapport

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

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

De stuurgroep wordt voorgezeten door drs. J.J.M. Stikvoort.
mr. A.F. Gaastra neemt namens DG Politie deel aan de stuurgroep.
drs. H.M.F. Bruls neemt namens het KBB deel aan de stuurgroep.

De specifieke doelgroep waarvoor het rapport is bestemd bestaat uit:

- Onze opdrachtgever zoals bovengenoemd.
- De korpsbeheerder drs. H.J.J. Lenferink.
- De korpschef drs. J.J.M. Stikvoort.
- De Hoofd Officier van Justitie mr. C.A. Nooy.
- De privacyfunctionaris drs. [REDACTED] I
- De voorzitter van het College Bescherming Persoonsgegevens.

Het rapport mag uitsluitend met toestemming van de korpsbeheerder dan wel de korpschef van korps Hollands-Midden aan derden ter beschikking worden gesteld.

De opdrachtgever is verantwoordelijk voor de verspreiding, ook binnen de doelgroep, van het rapport.

3 Bevindingen

3.1 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.

3.1.1 Regie en doorzettingsmacht voor de Wpg implementatie

Het korps Hollands-Midden heeft kennisgenomen van de werkpakketten die het korps Rotterdam-Rijnmond heeft opgesteld. Deze werkpakketten bevatten voor de diverse afdelingen van een korps aandachtspunten gezien vanuit de Wpg. Deze werkpakketten zullen in 2012 door Hollands-Midden worden geanalyseerd en aangepast. De uit deze audit voortgekomen aandachtspunten worden gebruikt ter verdere aanvulling van deze werkpakketten.

De privacyfunctionaris heeft door omstandigheden haar taken het afgelopen half jaar onvoldoende kunnen uitvoeren waardoor onafhankelijk toezicht op de naleving van de Wpg in het gedrang is gekomen. De functionaris gegevensbescherming heeft zo goed mogelijk de taken van de privacy functionaris overgenomen. Deze tijdelijke verschuiving is bij het CBP kenbaar gemaakt.

Sinds voorjaar 2011 heeft het korps Hollands-Midden een nieuwe projectleider Wpg aangesteld.

3.1.2 Bekendheid met de Wpg binnen de organisatie

De bevoegde functionarissen binnen het korps Hollands-Midden pakken hun rol nog onvoldoende op. Enerzijds gebeurt dit doordat functionarissen te druk zijn met hun dagelijkse werkzaamheden. Anderzijds doordat men nog onvoldoende het belang van de Wpg wordt ervaren. Het is de verwachting dat wanneer meer aandacht voor het onderwerp Wpg ontstaat zal ook het bewustzijn onder de functionarissen toenemen, waardoor men de noodzaak zal inzien om hier tijd voor vrij te maken.

3.1.3 Wpg en de praktijk

De eisen vanuit de Wpg worden als beperkend beschouwd voor de uitvoering van de dagelijkse politietaken. Dit wordt met name bij 'Blauw' ervaren. Blauw wordt conform Wpg geacht om alle informatie die zij verstrekken vast te leggen en dit wordt als zeer bureaucratisch ervaren.

De termijnen (schonings- en bewaartermijnen) worden soms als knellend ervaren.

3.2 Verantwoordelijke (artikel 1.f)

Mandaatbesluit

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

Er is een mandaatbesluit waarin is aangetoond dat het bevoegde gezag het mandaat heeft verleend aan de Korpschef. Het mandaatbesluit bevat tevens een ondermandatering.

De mandatering bevat per dienst of afdeling een toelichting van het verleende mandaat aan de desbetreffende functies.

3.3 Kwaliteitsaspecten van politiegegevens (artikel 3 en 4)

3.3.1 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).

3.3.2 Bevindingen

3.3.2.1 Onderscheid onderzoek Dagelijkse Politietask versus Bepaald geval

Op het intranet zijn de uitgangspunten van de Wpg gepubliceerd. Deze uitgangspunten gaan in op de noodzaak van de Wpg alsmede de verwerkingsdoelen van artikel 8 tot en met 13 van de Wet politiegegevens (Wpg). Hier wordt kort aangegeven wat wordt verstaan onder deze Wpg-artikelen, inclusief praktische voorbeelden.

Tevens zijn werkafspraken gedocumenteerd voor artikel 8 en 9 Wpg verwerkingen. Hierin wordt ook het onderscheid tussen beide artikelen duidelijk gemaakt. Vuistregel die wordt gehanteerd is: Als grote hoeveelheden gegevens over verdachte en – met name – onverdachte personen worden verwerkt, is het regime van artikel 9 Wpg van toepassing. Onder het regime van artikel 8 Wpg valt de dagelijkse politietask.

Er is sprake van een artikel 8-verwerking als het opsporingsonderzoek door minder dan vier medewerkers wordt uitgevoerd óf als het onderzoek binnen 5 dagen kan worden afgerond, mits de inzet van BOB-bevoegdheden tot de artikelen 126n tot en met 126nd Sv kan worden beperkt.

Communicatie Wpg-regels naar de medewerkers

Een groot aantal trainingen zijn gegeven om voorlichting te geven over de Wet politiegegevens aan de medewerkers van Hollands-Midden.

Bevoegde functionarissen

De bevoegde functionarissen hebben een uitnodiging gekregen om deel te nemen aan een gezamenlijke training met korps Haaglanden. Nieuw aangestelde bevoegde functionarissen ontvangen geen extra training omtrent de Wpg.

Tevens schuift de privacyfunctionaris aan bij werkoverleggen van – met name – wijkagenten aan om aan de hand van casuïstiek de Wpg uit te leggen en vragen te beantwoorden.

De trainingen die bevoegde functionarissen moeten volgen zijn in een planning opgenomen. Op de planning is aangegeven welke bevoegde functionarissen op welke datum de opleiding volgen of hebben gevolgd. Tevens is hierbij een onderscheid gemaakt welke training verplicht is voor welke functionaris. Indien een bevoegde functionaris niet op is komen dagen op een training is dit ook in het overzicht opgenomen.

Vuistregels van Rotterdam-Rijnmond

Het korps Hollands-Midden heeft een uiteenzetting gemaakt tussen artikel 8 en 9 Wpg en daarbij ook duidelijke voorbeelden gegeven. Als verdere handreiking aan met name het Blauw op straat zullen de vuistregels vanuit Rotterdam-Rijnmond worden overgenomen.

Infodesk bij toetsen kwaliteit gegevens

De Regionale Dienst Informatie (RDI) verzorgt de afhandeling van informatieverzoeken. Wanneer het een ingewikkeld informatieverzoek betreft wordt deze in behandeling genomen door een informatiespecialist.

Er zijn drie mogelijkheden waarop men informatie bij de RDI kan aanvragen:

1. Deze verzoeken komen binnen via een sjabloon van Hollands-Midden. Bij het invullen van dit standaardformulier dient men naast de gegevens van de aanvrager tevens het doel van het informatieverzoek aan te geven. Dit zijn verplichte velden. De e-mails worden ingeboekt in programma PLANON (een tool waardoor inzichtelijk is wat de status van de afhandeling van een verzoek is).
2. Een andere mogelijkheid is het aanvragen van informatie door middel van het sturen van een e-mail. Hierbij dient men ook aan te geven wat het doel van de informatieaanvraag is en dient de identiteit van de verzoeker tevens te worden vastgesteld. Deze berichten worden vastgelegd in PLANON, exclusief de bijlagen.
3. Het is mogelijk om – bij spoed – het verzoek per telefoon in te dienen. Men spreekt van spoed wanneer met gegronde reden de informatie eerder geleverd te willen zien dan de door het systeem aangegeven verwachte levertijd.

De toetsing van het ter beschikking stellen van artikel 9 Wpg gegevens vindt plaats door de desbetreffende bevoegde functionaris. De Infodesk informeert bij moeilijke zaken de bevoegde functionaris, laatstgenoemde kan de verzoeken eventueel weigeren.

Artikel 8 Rechtmatigheid, volledigheid, juistheid en beveiliging

De borging van de rechtmatigheid, volledigheid, juistheid en beveiliging is impliciet opgenomen in de politieprocessen. Op onderdelen voldoet de politie aan de Wpg zonder dat er een vastlegging van de opzet aanwezig is. Dit komt door controlemaatregelen die al in de processen bestaan, tevens door het wetboek van strafvordering en de samenwerking met het Openbaar Ministerie.

Juistheid, volledigheid

Bij de invoer van politiegegevens in BVH is sprake van verschillende invoercontroles om de juistheid en volledigheid van deze gegevens te controleren. Dit gebeurt door middel van een controle achteraf met behulp van de tool 'Trueblue' waardoor fout- en verbeterregistrering plaatsvindt. Bovendien houdt gegevensbeheer ook controle op de gegevens binnen BVH.

Iedere nacht draait de tool TrueBlue en de gegevens belanden bij gegevensbeheer in Leiden. De functionaris die de gegevens heeft ingevoerd, krijgt vervolgens een signaal dat hij moet aanvullen of wijzigen. Eventueel volgt een rappel. Na aanvulling van deze gegevens volgen geen nieuwe rappels. De 'kennisregels' voor TrueBlue worden door VtsPN aangeleverd. TrueBlue wordt alleen gebruikt voor BVH en wordt niet gebruikt voor bijvoorbeeld systemen als BVO, Beaufort, etc.

KA-Omgeving

Er wordt nog veel gewerkt in Word-documenten binnen de KA-omgeving. Dit heeft als gevolg dat deze informatie niet beschikbaar is voor andere politieonderdelen. Dit heeft tevens invloed op de volledigheid van de informatiesystemen omdat deze Word-document niet in de daarvoor bestemde systemen terechtkomen. Daarmee zijn deze gegevens niet beschikbaar voor andere politieonderdelen.

Artikel 9 BVO Juistheid, volledigheid

Het rechercheproces bevat waarborgen voor deze kwaliteitsaspecten. De borging van de rechtmatigheid, volledigheid, juistheid en beveiliging is impliciet opgenomen in de politieprocessen. Op onderdelen voldoet de politie aan de Wpg zonder dat er een vastlegging van de opzet aanwezig is. Dit komt door controlemaatregelen die al in de processen bestaan, tevens door het wetboek van strafvordering en de samenwerking met het Openbaar Ministerie.

De applicatie BVO kent geen hulpmiddelen of toepassingen voor een kwaliteitscontrole op de juistheid en volledigheid van de (politie-)gegevens. De kennis van rechercheurs op het gebied van Wet politiegegevens blijkt niet optimaal.

Koppeling BVO met Summ-IT

BVO is gekoppeld met een andere applicatie die Hollands-Midden in gebruik heeft, namelijk Summ-IT. Informatie dat in BVO wordt ingevoerd wordt tevens in Summ-IT geregistreerd, andersom vindt er geen geautomatiseerde informatieoverdracht plaats. Dit heeft te maken met het feit dat BVO minder soorten informatie kan registreren (zoals foto's) dan met Summ-IT mogelijk is.

Om te kunnen controleren of men daadwerkelijk alle gegevens zowel in BVO als Summ-IT (in plaats van alleen Summ-IT) wordt er een automatische gegevensvergelijking gegenereerd door Summ-IT. Dit gegenereerde rapport wordt door de functioneel beheerder gecontroleerd.

In de praktijk wordt echter gebruik gemaakt van zowel SUMM-IT en BVO, waarbij niet altijd de gegevens in beide systemen worden geregistreerd. De belangrijkste gegevens staan in BVO, de verwerking vindt vaak plaats in SUMM-it. Om een volledig beeld te verkrijgen, moeten beide systemen worden geraadpleegd. Volledigheid is daarbij niet geborgd.

In februari 2012 gaat Hollands-Midden volledig over naar het gebruik van Summ-IT. Blueview neemt deze gegevens mee in bevestigingen.

Door niet altijd invoeren van zogeheten 'zachte gegevens' wordt mogelijk niet voldaan aan het volledigheidseisen van artikel 4.1 Wpg.

Koppelingen met VROS

Wekelijks worden alle nieuw ingevoerde gegevens van BVO (dus van alle regio's) gekopieerd om vervolgens middels de toepassing/applicatie VROS van deze nieuwe gegevens vast te stellen of het subject ook bij andere korpsen voorkomt.

Artikel 10 en 12 Rechtmatigheid, volledigheid, juistheid en beveiliging

Kwaliteitscriteria CIE

Artikel 10 gegevens worden binnen de eigen omgeving opgeslagen, hier kan niemand buiten de CIE bij. Controle op autorisaties op deze mappen vindt regelmatig plaats.

Op onderdelen voldoet de politie aan de Wpg zonder dat er een opzet aanwezig is. Dit komt door de controles die al in de processen bestaan en door het wetboek van strafvordering en de samenwerking met het OM.

Er is een CIE-instructie aanwezig met betrekking tot de verwerking van politiegegevens waarin is vastgelegd wat de CIE-Officier van Justitie (CIE-OvJ) moet controleren met duiding van de subjecten, controle van de journaals en de frequentie van de controles. Volgens de CIE-OvJ voert het CIE meer controles uit dan dat is voorgeschreven.

De chef-CIE heeft een wekelijks overleg met de runners waardoor er een betere sturing kan plaatsvinden. Bovendien controleert de chef-CIE op wekelijkse basis aan de hand van processen-verbaal of de inschrijvingen aan de voorwaarden voldoet. Dit houdt onder meer in dat er controle plaatsvindt of de aanduiding van het subject klopt, of de netto informatie overeenkomt met de bruto-informatie en of de veredeling juist heeft plaatsgevonden. Voorts vindt er controle plaats op de verlengingen. Doorgaans zijn de verlengingen voor een half jaar.

De verwerkingen van artikel 12 Wpg gegevens moeten maximaal (bruto) te volgen zijn. De Wpg vereist dat er transparantie is in de verwerkingen en een *audittrail* aanwezig is van de verwerkingen. Het is niet wenselijk om voor alle veredelingsvormen openheid te geven tijdens terechtzitting, in verband met het afbreukrisico voor de informant. Een voorbeeld hiervan is veredeling aan de hand van 00-informatie (bruto-informatie).

Als zaken verder CIE-matig worden onderzocht, vindt een dusdanige vastlegging plaats in artikel 12 dat de volledige routing van het onderzoek/ de veredeling te volgen en te herleiden is. De inzet van een Observatie team vindt altijd plaats na overleg met hoofd CIE en eventueel met machtiging van een Officier van justitie als er sprake is van stelselmatigheid. Resultaat wordt altijd vastgelegd, echter niet altijd in een procesverbaal. De registratie dient wel bruto plaats te vinden. Pas als sprake is van een stelselmatige actie dan wordt een machtiging van de Officier van Justitie gevraagd, die in de kluis wordt bewaard om aan te geven dat voor het volgen, af luisteren, etc. een opdracht aanwezig is. Hiermee wordt geborgd dat, indien noodzakelijk, verkregen bewijs te toetsen is door de rechter.

Informatie ouder dan zes maanden wordt doorgaans niet voor operationele doelen gebruikt.

Kwaliteitscriteria RID

Bij de RID wordt tevens een controle uitgevoerd op de verkregen informatie. Bij deze controle komt het toetsen van de betrouwbaarheid van de informatie en de herkomst van de informatie aan de orde. Hierbij wordt ook de afhandelingsurgentie beoordeeld.

De runners die de informanten spreken maken hiervan verslagen (bruto-verslag) op. Deze informatie valt onder artikel 12 Wpg en wordt opgeslagen in een digitaal systeem binnen een standalone omgeving. Er worden geen hard copy verslagen

aangehouden. De gespreksverslagen hebben de hoogste codering van geheimhouding.

De runners hebben alleen toegang tot de eigen verslagen. Informatie die wordt gebruikt voor analysedoeleinden wordt uit de eerdergenoemde bruto-verslagen geabstraheerd en opgeslagen in een ander informatiesysteem. Dit informatiesysteem is gekoppeld aan het netwerk. De opgeslagen informatie is van het niveau 10 en betreft een artikel 10 Wpg verwerking. Na het analyseren van de informatie wordt eventueel na toestemming van het Hoofd-RID informatie verstrekt aan de Infodesk.

CIE en RID

De runners hebben alleen toegang tot hun eigen gespreksverslagen. Het hoofd van de RID kan autorisaties verlenen om bij gespreksverslagen van andere runners te kunnen. Hoofd-RID is de enige die autorisaties mag toekennen en intrekken. De autorisatieprocedure wordt bovendien gelogd. Het CIE werkt al langer conform deze procedure.

De analisten zijn geautoriseerd voor het inzien van artikel 10 Wpg informatie. Wanneer nodig kan artikel 12 Wpg informatie hieraan door het hoofd van de RID tijdelijk worden toegevoegd.

Afschermprocedure CIE (niet zijnde informatie van informanten)

Landelijk zijn afspraken gemaakt omtrent het afschermen van informatie uit een onderzoek, waarbij is gekozen voor een werkwijze via de CIE-lijn.

De afscherming van informatie vindt plaats onder een aantal strikte voorwaarden. Een van deze voorwaarden is dat overleg of communicatie tussen opsporingsambtenaren van bron- en doelonderzoek niet (of slechts bij zeer hoge uitzondering en altijd na overleg met de zaakofficier) is toegestaan teneinde 'kennis van extra informatie en gevaar voor afscherming' te voorkomen. Met name bij hoog embargo (bron)onderzoeken is dit het geval. Uitgangspunt is dat de CIE-Officier van Justitie degene is die de informatieoverdracht vanuit het brononderzoek coördineert via het Hoofd-CIE. Na tussenkomst van de CIE-Officier en het Hoofd-CIE van het brononderzoek wordt de informatie vervolgens overgeheveld naar het doelonderzoek. Daarbij geldt als uitgangspunt dat binnen de OM-lijn enkel op voorhand contact plaatsvindt tussen zaakofficier en CIE-OvJ.

In de afscherming van de informant is de regel dat afspraken (werkregels) strikt worden nagekomen. Verder is het regel dat een informant maar bij één informatiedienst actief mag zijn. Dat betekent dat soms overschrijving moet plaatsvinden uit artikel 12 Wpg informatie naar de AIVD of RID. Er is een controle via ICS-code bij de NCIE of potentiële informanten reeds voorkomen bij RID of CIE-elders in den lande.

De werkregels worden voor inschrijving met de informant doorgenomen en in ieder geval door de runners ondertekend. Dit 'contract' wordt bewaard in het persoonsdossier van de informant.

De zogeheten 01-informatie (netto-informatie) is slechts beschikbaar voor een beperkt aantal functionarissen. Zij zijn geautoriseerd in het BVO door het Hoofd CIE, en met instemming van de CIE-Officier.

Voorheen ging er een Excel CIE-lijst naar veel medewerkers. Omdat deze informatie niet in een procesverbaal stond, kon dat wel eens fout gaan. Als daarvan gebruik

wordt gemaakt, dan moet een procesverbaal worden opgemaakt. Deze pv's voor de CIE hebben landelijk een vaste indeling. Het korps Hollands-Midden heeft daaraan de volgende tekst toegevoegd:

"Eerdergenoemde informatie is door mij voor strafrechtelijk onderzoek ter beschikking gesteld aan het onderzoek (naam onderzoek) van de regiopolitie Hollands Midden en mag slechts na voorafgaande schriftelijke toestemming van het hoofd C.I.E., voornoemd, worden verstrekt aan een ander."

De vrees is dat anders doeldoorbreking plaatsvindt bij andere onderzoeken zonder dat daarvoor conform de Wpg toestemming is verkregen van de bevoegde functionaris...

Beveiliging

Elk district heeft een eigen map waarbinnen elk team een eigen map krijgt waar alleen het team toegang tot heeft. In deze mappen bevinden zich artikel 8 informatie. Wanneer het een artikel 9-onderzoek betreft worden deze in een apart per onderzoek aangemaakte map geplaatst. Medewerkers moeten per map worden geautoriseerd waardoor niet iedereen toegang heeft tot alle onderzoeksmappen. Op basis van 'need-to-know' heeft men de toegang gereguleerd.

Er is in de mappenstructuur een onderscheid gemaakt tussen artikel 8 en artikel 9 onderzoeken. Beide omgevingen zijn gescheiden van elkaar, zowel op districtsniveau als op onderzoeksniveau.

Pilot Blackberry's

Hollands-Midden draait op het moment een proef met Blackberry's voor het Blauw. Voor het gebruik van deze toestellen wordt er niet gebruik gemaakt van de servers van de producent RIM zoals dit normaliter wel het geval is. In plaats daarvan draaien de PDA's op de servers van vtsPN.

De toestellen zijn allen beveiligd met een geautomatiseerde pincode-blokkering wanneer het toestel enige tijd niet actief is. Bovendien kunnen de toestellen bijvoorbeeld bij verlies op afstand worden gewist.

Er vindt geen lokale opslag van politiegegevens op de Blackberrys plaats. Opslag is óf in de bronsystemen, óf op een speciaal voor de pilot ingerichte server (UCM) bij VtsPN.

Regionale applicaties

De regionale applicaties die bij Hollands-Midden worden gebruikt zijn in het kader van de Wpg geïnventariseerd. Functioneel beheer heeft deze inventarisatie uitgevoerd en de controle uitgevoerd of deze systemen als Wpg-proof kunnen worden beoordeeld. Een voorbeeld van een Wpg-relevante regionale applicatie is de Briefing-tool. In deze applicatie kan bijvoorbeeld de Infodesk dia's klaarzetten die voor briefings voor Blauw worden gebruikt. Niet uitgesloten wordt dat hiermee tevens politiegegevens worden gedeeld tijdens een dergelijke briefing.

Ingerichte mappenstructuur

Ten behoeve van Opsporing (bijvoorbeeld rechercheonderzoeken) kunnen dossiers worden vastgelegd door middel van een ingerichte mappenstructuur. De afscherming van deze dossiers gebeurt door middel van de in Windows beschikbare afschermvoorzieningen.

Op het moment heeft ieder district de beschikking over een eigen map waarbinnen de teammappen kunnen worden opgeslagen. Artikel 9 onderzoeken worden apart per onderzoek in een aparte map opgeslagen, autorisatie vindt per onderzoeksmap plaats.

Functioneel beheer zal op basis van een melding/mail tijdelijke register via de Service Desk van VtsPN zorgdragen dat de mappenstructuur beschikbaar wordt gesteld voor het betreffende onderzoek. De feitelijke realisatie van de mappenstructuur evenals de autorisaties hieromtrent vindt plaats door VtsPN.

De aanvraag van mappen in de mappenstructuur blijkt goed te gaan. Echter, het verwijderen van deze mappen blijkt een probleem. [REDACTED]

II

Logging

BVH kent een aparte log-database. Het laagste niveau waarop wordt gelogd is schermniveau met een permissie. Tevens worden de activiteiten van functioneel beheer gelogd. BVO is uitgerust met een centrale log waarin zowel de zoekacties (veelal gebaseerd op tekst), de dag/tijd en de zoeker alsook de zoekresultaten worden gelogd. Echter blijkt deze logfunctie niet bij alle processen aan te staan.

Toegang beheerders tot de informatie

De beheerders zijn vanzelfsprekend geautoriseerd voor die systemen die zij beheren. Het is voor de beheerders mogelijk om de data in te zien binnen het domein Hollands-Midden. De gegevens die behoren tot de artikel 12-categorie zijn hiervan uitgezonderd.

Ook draaien de beheerders piketdienst (avonduren en weekend). Dit wordt gedaan via een speciale doelgroep laptop. Middels deze laptop is het mogelijk op afstand toegang te verkregen tot de politiesystemen. De verbinding met het politiedomein is versleuteld.

Beveiliging CIE

De beveiliging bij het CIE Hollands-Midden wordt gewaarborgd aan de hand van de landelijke CIE-richtlijn. Bovendien brengt de aard van de gegevens mee dat er extra zorg betracht wordt in de beveiliging hiervan, en dat de CIE hier zelf ook alle belang bij heeft.

Binnen de afdeling CIE Hollands Midden is er beperkt toegang tot de volledige informatie met betrekking tot artikel 12 WPG informatie. *Alle* artikel 12 WPG informatie is slechts toegankelijk voor het Hoofd CIE en diens plaatsvervangers.

Overeenkomstig artikel 2:3 lid 6 Bpg is het hoofd van de CIE en diens plaatsvervanger geautoriseerd tot identificerende gegevens van een informant en is binnen de CIE Hollands-Midden geen toegang verleend aan administratief personeel tot identificerende gegevens.

Verbeterpunt

- Hollands-Midden werkt mee aan de pilot voor het gebruiken van PDA's in het politieproces. Het is wenselijk om tijdens de pilotfase mee te nemen hoe men de gebruikers het bewustzijn creëert van de risico's die het gebruik van een datadrager met daarop politiegegevens met zich meebrengt.

Gevoelige gegevens (artikel 5)

Norm

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

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

Bevindingen

Hollands-Midden hanteert een strikt beleid omtrent het vastleggen van gevoelige gegevens. Het korps is terughoudend in het registreren van gevoelige gegevens en doet dit enkel wanneer dit noodzakelijk is voor de uitvoering van de politietaak.

Binnen het proces van handhaving worden geen structurele gegevensverzamelingen van gevoelige gegevens aangehouden. Uiteraard bevinden zich gevoelige gegevens in politiesystemen, zoals in de Briefing-tool dat wordt gebruikt voor projectbriefings. Deze tool biedt de mogelijkheid om bepaalde informatie te voorzien van een aflooptermijn waardoor gevoelige gegevens niet langer dan noodzakelijk beschikbaar zijn. Toegang tot gevoelige gegevens verloopt op basis van 'need-to-know'.

Indien vragen zijn omtrent het gebruik van gevoelige gegevens kan men terecht bij de privacyfunctionaris van het korps.

3.4 Autorisatie (artikel 6)

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).

Autorisatiematrix

Een autorisatiematrix is in korps Hollands-Midden aanwezig. In deze matrix is elke afdeling uitgesplitst per functie, en per functie worden de bijbehorende toegestane autorisaties vermeld. Afwijkende autorisaties dienen bij de privacyfunctionaris te worden aangevraagd middels een tijdelijk besluit. Hier wordt bij Hollands-Midden strikt op gemonitord. De autorisatiematrix is specifiek ingericht op Hollands-Midden, zowel qua gebruik van autorisatirollen als de gehanteerde naamgevingen.

Er zijn twee soorten autorisaties:

1. Autorisaties welke zijn gekoppeld aan functies genoemd in het functiehuis van Hollands-Midden (functie gebonden autorisaties).
2. Autorisaties welke op tijdelijke basis als maatwerk aan een bepaald persoon zijn verleend (persoonsgebonden autorisaties).

Het proces en de verantwoordelijkheden rondom het toekennen van deze autorisaties worden hierna verder uitgewerkt.

Functie gebonden autorisaties

Per functie wordt vastgesteld welke autorisaties een medewerker nodig heeft om deze functie naar behoren uit te kunnen oefenen. Deze zijn vastgelegd in de autorisatiematrix op het intranet.

Autorisaties voor een nieuw te creëren functie

Dienst personeel stelt een functiebeschrijving aan en de betreffende lijnchef levert vervolgens input voor de benodigde rechten op de systemen. De privacyfunctionaris brengt advies uit in overleg met de functionaris voor de gegevensbescherming. Vervolgens neemt de proceseigenaar op basis van dit advies een beslissing. Bij akkoord wordt deze opgenomen in de autorisatiematrix. Het autorisatiebeheer wordt uitgevoerd door de Dienst Informatie.

Aanvullende autorisaties

De lijnchef signaleert indien aanvullende rechten benodigd zijn. De aanvraag voor aanvullende autorisaties wordt aan de privacyfunctionaris (en de functionaris voor gegevensbescherming) voorgelegd. Het is aan de proceseigenaar ter finale beslissing of de aanvullende autorisaties moeten worden verleend. Beheer wordt tevens door Dienst Informatie uitgevoerd.

Functieverandering

De dienst personeel weet wanneer een medewerker van functie verandert. Dit wordt in het personeelssysteem aangepast en kan gevolgen hebben voor het salaris, de (gewelds)middelen waarover een medewerker beschikt, en voor de autorisaties die zijn toegekend aan de medewerker.

De dienst personeel signaleert een functieverandering en hoort deze te melden aan de Dienst Informatie. Na de melding trekt de Dienst Informatie alle autorisaties in die bij de oude functie horen, en verleent vervolgens de autorisaties die behoren bij de nieuwe functie. In geval van een overlappende periode kunnen tijdelijke autorisaties worden verleend.

In de praktijk worden in het geval van functiewisselingen en verwijderen de autorisaties niet automatisch aangepast. Binnen Korps Hollands-Midden is dit nog steeds afhankelijk van oplettende mensen zoals de Personeels Management Adviseur. Laatstgenoemde regelt de aanpassing en stuurt dit naar ISC-West.

Een chef is op zijn beurt weer verantwoordelijk voor het intrekken van autorisaties. Echter beschikken de chefs niet over een overzicht van de actuele werkelijke autorisaties. Als reden wordt aangevoerd dat het niet mogelijk is om (snel) een lijst van autorisaties samen te stellen, mede verklaarbaar door de grote hoeveelheid aan systemen. Bovendien bezitten veel systemen de functionaliteit niet voor het extraheren van de actuele autorisaties, aldus Korps Holland-Midden.

Voor BVH blijkt het echter eenvoudig te zijn om een rapport te genereren door middel van Cognos met daarin een overzicht van de personeelsleden van Hollands-Midden en de daaraan gekoppelde functies.

Het korps is op de hoogte van het feit dat bij functiewijzing de autorisatiemutaties niet tijdig plaatsvinden. Dit is als een aandachtspunt gesteld voor 2012.

Persoonsgebonden autorisaties

Dit betreffen de autorisaties buiten het standaardprofiel. Voor persoonsgebonden autorisaties geldt dat de lijnchef de aanvullende autorisaties kan aanvragen. Deze aanvraag wordt voorgelegd aan de privacyfunctionaris. De privacyfunctionaris geeft

vervolgens advies uit na de functionaris voor de gegevensbescherming hierover te hebben geconsulteerd.

De Directeur Informatie neemt uiteindelijk het besluit over het verzoek op basis van het advies. Bij akkoord wordt een autorisatie verleend voor maximaal zes maanden. Het is aan de gebruiker zelf het verzoek in te dienen om deze autorisaties te laten verlengen. De privacyfunctionaris houdt een overzicht bij van deze verzoeken. De Dienst Informatie beheert deze persoonsgebonden tijdelijke autorisaties.

Toetsing

De Functionaris Gegevensbescherming (FG) toetst de toegekende autorisaties. De interregionale autorisaties worden getoetst door de privacyfunctionaris van het verzoekende korps en de privacyfunctionaris van Hollands-Midden.

Functiewisselingen en verwijderen

In de praktijk blijkt dat functiewisselingen niet tijdig worden gesignaleerd waardoor het verwijderen van niet-tijdelijke autorisaties niet structureel tijdig gebeurt.

Aanvraagprocedure

Aanvragen, wijzigingen en verwijderen van autorisaties verlopen volgens een procedure. Door het systeem wordt afgedwongen dat - alvorens toegang/gebruik te kunnen maken van BVO, SUMM-IT of Mappenstructuur - eerst een 'melding tijdelijke register' moet worden ingevuld.

De leider van het onderzoek is verantwoordelijk voor wie welke autorisaties krijgt. Autorisaties mogen dan ook alleen door de desbetreffende chef worden aangevraagd. Autorisaties voor mappen worden per onderzoek geregeld. De Directeur Informatie is eindverantwoordelijke die uiteindelijk bepaalt of een autorisatie verlengd wordt. De privacyfunctionaris (en indirect de functionaris voor de gegevensbescherming) heeft hierin een adviserende rol.

Interregionale autorisaties verlopen via de privacyfunctionaris en worden getoetst door de privacyfunctionaris van de betreffende regio.

Alle aanvragen worden door de privacyfunctionaris opgeslagen. Per medewerker is bij de privacyfunctionaris bekend welke autorisatie deze persoon heeft. Ongeveer eens per kwartaal vindt er een steekproefsgewijze controle hierop plaats. Bovendien vraagt de privacyfunctionaris via functioneel beheer eens per jaar een uitdraai van alle autorisaties binnen BVH. Samen met de Functionaris voor de Gegevensbescherming vindt er hierop terugkoppeling plaats naar de chef.

De aangemaakte 'melding tijdelijk register' gaat vervolgens naar de Servicedesk van vtsPN om te worden verwerkt in de communicatieapplicatie Expertdesk. Deze zorgt ervoor dat vtsPN een nieuwe gebruiker registreert *zonder* de bijbehorende rollen. Expodesk genereert alleen een ticket: er worden werkopdrachten gegenereerd voor Functioneel Beheer BVO.¹

Elke betrokken partij meldt vervolgens na uitvoering van de opdracht dat hij gereed is. Vervolgens meldt vtsPN aan de opdrachtgever en de betrokken medewerker dat de autorisatie is voltooid.

¹ Voor VG West bijvoorbeeld UNIX-beheer, databasebeheer en Windowsbeheer (t.b.v. icoon).
Pagina 36 van 61

De Service Desk is door Functioneel Beheer geïnstrueerd dat bij twijfel of afwijkingen geen autorisaties worden toegekend, maar dat het verzoek/melding tijdelijk register zonder pardon teruggaat naar de verantwoordelijke onderzoeksleider. De Service Desk heeft een lijst van namen die gemandateerd zijn voor het indienen van autorisatieverzoeken.

Een functieverandering en vertrek van een medewerker worden op dezelfde manier aangevraagd door de daarvoor geautoriseerde P-medewerker. De verwerking van de melding is gelijk aan die van een aanvraag.

Toezicht op autorisaties door privacyfunctionaris

De privacyfunctionaris van korps Holland-Midden is tevens betrokken in de procedure voor autorisaties. De privacyfunctionaris houdt een Excelbestand bij met alle autorisaties per functie. Ingeval er afwijkingen zijn geconstateerd is het aan deze privacyfunctionaris om te beoordelen of deze geoorloofd is of niet. Vervolgens geeft de privacyfunctionaris advies uit aan het hoofd van de dienst en maakt laatstgenoemde de uiteindelijke beslissing.

Er zijn verschillende titels waarop iemand wordt geautoriseerd:

- politieambtenaar.
- niet in dienst van korps Holland-Midden, maar wel een van de andere korpsen (deze mensen worden tijdelijk geautoriseerd).
- als specialist bij een onderzoek betrokken (deze specialisten worden tijdelijk geautoriseerd).

Protocollering autorisaties

Zoals reeds aangegeven verlopen aanvragen, wijzigingen en verwijderen van autorisaties volgens een procedure waarbij afgedwongen wordt dat alvorens gebruik te kunnen maken van BVO, SUMM-IT of Mappenstructuur eerst een "melding tijdelijke register" wordt ingevuld. De Service Desk is hierbij geïnstrueerd streng op toe te zien of de autorisatieverzoeken kloppen.

Bewaren protocollering autorisatie

De autorisatieverzoeken worden vastgelegd in de tool 'Expertdesk'. Tijdelijke autorisatieverzoeken buiten het functieprofiel worden door de privacyfunctionaris bewaard.

Autorisatiebeheer CIE en RID

De toekenning van autorisaties onder het regime van het nieuwe landelijke functiehuis is een zorgpunt. De functieomschrijving voor een CIE-medewerker en een RID-medewerker is dan gelijk waardoor toekenning van autorisaties aan personen met eenzelfde functieomschrijving zou dan tot verkeerde uitkomsten kunnen leiden. Door de korpschef is hiervoor nu voor enkele personen (bijvoorbeeld de 2 analisten) al een aanwijzing gegeven. Echter deze voorziening is niet waterdicht en vraagt nog verdere uitwerking.

Overzicht autorisaties CIE

Voor het gebruik van gegevens zijn verschillende niveaus van autorisatie aanwezig. De chef, diens plaatsvervangers en één medewerker van Functioneel Beheer zijn geautoriseerd op niveau 8. De runners op niveau 6 en een zeer beperkt aantal medewerkers van de Dienst Informatie op niveau 4. Die laatste kan dan wel zien dat er een hit is op een bepaald persoon (hit/no hit), maar niet de achterliggende

informatie. Voor de taakuitvoering zijn 2 medewerkers van de RID geautoriseerd op 6, zij hebben toestemming nodig voor verder gebruik van het Hoofd-CIE.

Autorisaties SUMM-IT

Autorisatiebeheer voor Summ-IT verloopt via Functioneel Beheer van Dienst Informatie. De medewerkers van Functioneel Beheer hebben hiervoor een aparte opleiding gehad. Tevens houdt Functioneel Beheer een overzicht bij van de autorisaties, dit overzicht is inzichtelijk voor de privacyfunctionaris.

Op de G-schijf wordt van SUMM-IT gebruik gemaakt.

- SUMM-IT bevat een tool waarmee in korte tijd over alle mappen en dus onderzoeken kan worden gescand op de G-schijf.
- Formeel moet de runner door de projectleider aan een onderzoek worden toegevoegd aan een project om dit te kunnen raadplegen.
- Bij de CIE vindt men dit echter niet wenselijk. Nu is er mogelijkheid om met behulp van SUMM-IT alle informatie te raadplegen.
- Het is tevens niet bekend welke functionaris deze autorisaties heeft toegekend. Vastleggingen hiervan zijn ook niet bekend. In de toekomst is dat afgedekt door de zinsnede op het projectformulier.

3.4.1 Verbeterpunten

Als verbeterpunten zijn te noemen:

- Het in gebruik nemen van een tool en/of een proces om autorisaties in een geautomatiseerde vorm vast te leggen en te beheren;
- Een proces inrichten om veranderingen in functies tijdig te signaleren, zodat acties kunnen worden ondernomen;
- Het realiseren van zicht op autorisaties in de KA-omgeving;
- Het hanteren van overzichten waarmee leidinggevend in staat zijn de autorisatie van hun medewerkers te beoordelen.

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

3.5.1 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 Wpg. Dit om vast te stellen of verbanden bestaan tussen de betreffende gegevens. De gerelateerde gegevens kunnen - na instemming van de daartoe bevoegde functionaris - voor dat onderzoek verder worden verwerkt. De bevoegde functionarissen zijn in dit geval de leider van het betreffende onderzoek of diens plaatsvervanger.

Indien politiegegevens in combinatie met elkaar worden verwerkt, worden van die verwerking nader genoemde gegevens vastgelegd (protocolplicht).

In combinatie met elkaar zoeken

Voor ICMEV verwerking moet volgens artikel 11 lid 4 Wpg een machtiging worden afgegeven. Het is bij de CIE niet altijd duidelijk wanneer dat nodig is. De CIE-analisten kunnen bij informatie van artikel 8, 9, 10 en 12 Wpg.

Voor elke aanvraag zou een aparte machtiging nodig zijn. Met de OvJ is afgesproken dat de CIE niet doet aan datamining en dat daarom geen machtiging is vereist. De

CIE doet aan subjectanalyse. In het geval van informatie over woninginbraken is wellicht wel een machtiging van de OvJ nodig.

Niet duidelijk is in hoeverre het CIE primair artikel 11-verwerkingen verricht teneinde vast te stellen of er verbanden bestaan tussen gegevens. Indien dergelijke verbanden bestaan, gaat CIE over tot subjectanalyse; inhoudende verdere verwerking van de datagegevens. Daarbij zoekt CIE gericht in de voor haar beschikbare systemen en doet daarbij dus aan datamining.

Proces GV-ICMEV

De tekst die van brononderzoek naar doelonderzoek wordt verstrekt, wordt door de projectleider en zaakofficier van het brononderzoek vastgesteld op basis van de onderliggende stukken en in een zogenaamd kluisproces-verbaal vastgelegd. Het Hoofd-CIE van het brononderzoek maakt een proces-verbaal met deze tekst en na voorafgaande toestemming van de CIE-OvJ, verstrekt hij dit aan het Hoofd-CIE waar het doelonderzoek plaats zou moeten vinden.

Het Hoofd-CIE controleert vooraf of de te verstrekken tekst overeenkomt met de informatie en of deze rechtmatig is verkregen. Via MRO (Melding Recherche Onderzoeken) worden data (personalia, telefoonnummer, kentekens) wekelijks geautomatiseerd landelijk vergeleken. Als data in verschillende onderzoeken in het land voorkomen, of deze data opgenomen zijn in een artikel 10 Wpg registratie van de CIE vinden er zogenaamde 'hits' plaats. Partijen die informatie hebben op gelijke data nemen contact met elkaar op om de waarde van deze 'hit' te beoordelen. Dit kan leiden tot uitwisseling van informatie. Vanuit de CIE worden 'hits' in VROS 'onderzocht' door runners nadat zij door de medewerkster informatievoorziening ter beschikking zijn gesteld.

Bevoegde gezag

De CIE Officier van Justitie is het bevoegde gezag voor de verwerking van politiegegevens ex artikel 10 en 12 Wpg. Het takenpakket bestaat uit onder meer:

- Beoordelen of inschrijving van informanten noodzakelijk / rechtmatig is.
- Het toezien op het verloop van het informatie traject.
- Het toezien op de schriftelijke vastleggingen.
- Het beoordelen van de uitschrijving van de informanten.

De aangewezen functionarissen voor artikel 10 zijn personeel van de CIE, RID, themaregisters en in voorkomende gevallen medewerkers van Dienst Informatie (DI). DI-medewerkers mogen alleen deze handelingen verrichten bij goedkeuring door de desbetreffende Hoofd-CIE, RID, of themaverwerking.

Rol van de Officier van Justitie

Elke week is er overleg met de runners waarbij onder andere de sturing wordt afgestemd. Tevens wordt eenmaal per week gecontroleerd aan de hand van een proces-verbaal of de inschrijving aan de volgende voorwaarden voldoet:

- de aanduiding van het subject dient te kloppen;
- de tekst netto moet in overeenstemming zijn met wat bruto is vastgelegd;
- de veredeling is gegaan conform de Wpg, aangezien het soms schort aan de traceerbaarheid naar de bron.

De CIE-mensen zien het nut van deze invulling van het toezicht. De controle door de Officier van Justitie wordt gedaan omdat deze zich verantwoordelijk acht voor een

goede uitvoering van het proces. Voorts vindt er controle plaats op de verlengingen die doorgaans een half jaar duren. Bij voorkeur zijn de runners ook zelf bij de besprekingen, en niet alleen de coördinatoren.

Protocollering artikel 11

Er wordt geen actief toezicht gehouden op het geautomatiseerd vergelijken met niet-politiegegevens. Het toezicht op de protocolplicht is bovendien nog niet opgepakt.

Van elke geautomatiseerde vergelijking en gecombineerde verwerking van politiegegevens, worden volgens de procedure de volgende gegevens vastgelegd:

- a. de gegevens die voor de rechtstreekse raadpleging zijn gebruikt.
- b. de identiteit of het kenmerk van de politieambtenaar die de rechtstreekse raadpleging heeft uitgevoerd.
- c. de gegevens op grond waarvan kan worden nagegaan welke gegevens ter beschikking zijn gesteld voor verdere verwerking voor een doel, als bedoeld in artikel 9 of 10 van de Wpg.

In verband met de protocolplicht wordt vanuit het proces opgelegd het volgende te registreren:

- a. De verwerking die is verricht met de betreffende politiegegevens;
- b. Wie (functie en naam/user name) de politiegegevens heeft verwerkt en op welke datum;
- c. De grondslag van de initiële vastlegging van het politiegegeven;
- d. De inhoud van de ter beschikking gestelde informatie (bijvoorbeeld de naam, kenteken, telefoonnummer).
- e. Indien van toepassing, bij instemming; een bevestiging dat het bevoegde gezag heeft ingestemd met beslissing tot verstrekking.

De applicatie BRAINS wordt gebruikt voor artikel 11-verwerkingen. In deze applicatie worden de zoekvragen en resultaten aangehouden (gelogd). Tevens worden de zoekresultaten aangehouden / gelogd in BRAINS. In analyse reportages wordt aangegeven hoe is gezocht. In de operationele analyse is beschreven hoe men tot het resultaat is gekomen.

Uit de praktijk blijkt echt dat nog onvoldoende controle plaatsvindt op de logging van artikel 11-verwerkingen.

Bewaartermijnen (artikel 14)

3.5.2 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.

3.5.3 Bevindingen

Algemeen

Termijnen (schoning- en bewaartermijnen) worden soms als knellend ervaren. Het komt voor dat een crimineel zich een bepaalde periode stil houdt, bijvoorbeeld vanwege het stichten van een gezin. Wanneer hij na 5 jaar weer actief wordt dan ben is bijvoorbeeld de politierechercheur alle voorgaande informatie over deze crimineel kwijt.

Gebruik van de kantoorautomatisering

Doordat de politiesystemen (o.a. BVH en BVO) onvoldoende toegankelijk zijn, worden gegevens in de kantoorautomatisering vastgelegd. Deze kantoorautomatisering wordt in het kader van de Wpg niet gecontroleerd. Zolang er, naast de bestaande politiesystemen, gebruik wordt gemaakt van kantoorautomatisering, dient hierop een controle plaats te vinden.

Er is geen schoningsmodule binnen BVO. Ook de mappenstructuur die binnen het korps in de kantoorautomatisering voor Opsporing wordt gehanteerd voldoet niet aan de Wpg-vereisten omtrent bewaar- en vernietigingstermijnen.

Tevens blijkt het binnen de KA-omgeving een probleem te zijn om mappen uit deze omgeving te verwijderen. Dit is uiteraard niet bevorderlijk om te kunnen voldoen aan de door de Wpg gesteld bewaartermijnen.

Meldkamergegevens (GMS)

Het GMS-bestand is gekoppeld met het systeem EVA, en bevat gegevens die zowel betrekking hebben op Politie, Brandweer als Ambulance (waaronder ook medische gegevens).

Uit de documentatie blijkt dat meldkamer gesprekken – welke politiegegevens (kunnen) bevatten – van twee jaar geleden nog kunnen worden teruggeluisterd. Alle gesprekken worden opgeslagen met als naam tijdstip en datum.

Het is niet bekend hoe vaak het archief van GMS waarin deze gesprekken worden geregistreerd, wordt geschoond.

Als de melding in GMS wordt afgesloten gaan alle gegevens naar BVH. BVH wordt verder aangevuld door de agenten die door de mobilofonist naar de locatie zijn gestuurd. GMS kent een archief. Het archief is raadpleegbaar. De gegevens zijn beschermd tegen wijzigingen. De registraties van een half jaar terug kunnen zijn nog zichtbaar. In het archief kun je ook zien welke diender heeft gemeld. In BVH is dat echter niet zichtbaar.

Bewaartermijnen artikel 8

'Het achter schot zetten na 1 jaar'

Sinds juni 2009 heeft Hollands-Midden BVH in gebruik genomen. Ondanks de recente ingebruikname heeft men in juni 2010 al de eerste politiegegevens op grond van artikel 8 lid 1 Wpg 'achter een schot' hebben moeten plaatsen. Het schoningsscript van BVH (versie 1.2.2) is dit jaar bij Hollands-Midden geactiveerd. Hierdoor vindt het na een jaar achter schot plaatsen van artikel 8 Wpg informatie automatisch plaats.

De dagrapportage van BVH biedt in Hollands-Midden de mogelijkheid tot ongericht zoeken tot 1 jaar terug, maar elke medewerker die daarvoor geautoriseerd is heeft de mogelijkheid om op basis van bijvoorbeeld specifieke personen/kentekens/locaties hit/no-hitbevragingen te doen op grond artikel 8.2 Wpg.

Verwijderen na vijf jaar

Het verwijderen na vijf jaar hoeft pas in 2014 omdat BVH in 2009 in gebruik is genomen. Er is gestart met een lege database. Voorheen maakte het korps gebruik van BPS. Op een zeer select groepje mensen na is BPS afgeschermd, dus ook BPS gaat maximaal vijf jaar terug, en BPS-gegevens ouder dan 10 jaar worden vernietigd.

Hard copy archieven

De bekendheid van de bewaartermijnen van de papieren archieven bij de verschillende bureaus is niet overal even groot. Het korps heeft als insteek dat de expertise omtrent bewaartermijnen geconcentreerd is bij de afdeling Document Informatie Voorziening (DIV). DIV is verantwoordelijk voor de bewaartermijnen, dit is geen verantwoordelijkheid van de bureaus zelf. DIV werkt aan een notitie wijziging bewaartermijnen, maar deze is nog niet geheel gereed.

Het korps Hollands-Midden is zich bewust van de problematiek rondom het hard copy archief en participeert in een expertisegroep om dit te adresseren. Bovendien zijn de decentrale hard copy archieven door de afdeling DIV geïnventariseerd, waarbij de dossiers ouder dan 2 jaar centraal worden gearhiveerd, dus niet meer op de Wijkbureaus.

Vernietigen na vijf jaar

Ter beschikkingstellingen worden in maandmappen opgeslagen binnen de KA-omgeving. Deze mappen worden na 5 jaar vernietigd. De mappen bevatten alleen maar veredelingsinformatie. De 'echte' informatie staat in de primaire systemen waarvoor het artikel 8 Wpg bewaarregime telt.

Bewaartermijnen artikel 9

De bewaartermijn voor artikel 9-gegevens zoals deze is gesteld in de Wet politiegegevens is nog niet ingeregeld in het informatiesysteem BVO. Hierdoor blijven veel gegevens in het systeem staan die volgens de gestelde termijn al hadden moeten worden verwijderd of vernietigd. BVO gegevens hebben betrekking op artikel 9 tot en met 12 Wpg politiegegevens.

BVO-gegevens worden tevens compleet gekopieerd naar andere toepassingen zoals VROS. Hierdoor loopt men het risico dat men niet tegemoet kan komen aan de wettelijke bewaartermijnen.

Wel is er geconstateerd dat er sinds acht maanden op verzoek en in nauw overleg door de Functioneel Beheer wekelijks een schoning / vernietiging wordt op CIE-gegevens. Het blijkt tevens dat het schonen lastig is doordat het systeem veel gecombineerde documenten bevat.

OH-Moment

In de praktijk blijkt dat men niet of nauwelijks een signaal van het Openbaar Ministerie ontvangt dat de zaak in kracht van gewijsde is gegaan, met als gevolg dat er niet tijdig in BVO een zaak wordt verwijderd.

Het korps heeft (mede) om dit probleem te ondervangen de applicatie BOSZ geïmplementeerd. Hiermee is het mogelijk om de voortgang van een zaak bij te houden. In 2012 zal ook justitie aansluiten bij het gebruik van BOSZ. Middels deze aansluiting is het beoogd doel dat het korps structureel op de hoogte wordt gesteld van het onherroepelijke moment.

Artikel 10 Verwijderen en vernietigen na 5 jaar geen subjectwaardige registratie
De CIE van korps Hollands-Midden werkt volgens het landelijke CIE-proceshandboek waarin ook de aanpak met betrekking tot de bewaartermijnen procedureel zijn geregeld.

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

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

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

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

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

RID

In 2003/2004 is de RID begonnen met een nieuw informatiesysteem maar dit systeem is echter verouderd en 'sterft nu uit'. In het nieuwe BVO schijnen hiervoor mogelijkheden te zitten maar doordat dit informatiesysteem pas 4,5 maand actief is, is nog onbekend of dit werkt.

In de praktijk wordt veelal voordat er bewaard of gearchiveerd gaat worden een lijst uitgedraaid waarop staat wat in de toekomst vernietigd gaat worden.

Hernieuwde verwerking

Er is nog geen invulling gegeven aan een procedure voor het hernieuwd verwerken van politiegegevens buiten de CIE om. Tevens zijn ook geen functionarissen aangewezen die deze verwerking mogen verrichten.

CIE

Voor het hernieuwd verwerken van artikel 9 en 10 Wpg gegevens heeft het CIE aan de hand van het landelijke CIE-proceshandboek voorwaarden vastgesteld om verwijderde en bewaarde gegevens voor hernieuwd gebruik beschikbaar te stellen:

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

Bewaartermijn artikel 12 informatie

Er is op het moment geen schoningsmodule binnen CIE. Dat betekent dat nu met informatievragen voor wat betreft de ouderdom van informatie kritisch wordt omgegaan en een handmatige controle wordt uitgevoerd. In bijzondere gevallen vindt overleg plaats met de Officier van Justitie en/of de parketsecretaris.

Met het Openbaar Ministerie worden periodiek de subjecten en nieuwe bronnen doorgenomen. De Officier voert vervolgens een steekproefsgewijze controle uit op de informatie onder artikel 12 Wpg.

Tweemaal per jaar vindt schoning plaats van de informanten. Subjecten en bronnen worden getoetst en getekend door de Officier. Ook vindt kascontrole plaats en worden de pv's ingezien. De OvJ is elke 14 dagen aanwezig bij het werkoverleg. Voorts is elke week overleg met de teamleider.

3.5.4 Verbeterpunten

- Stel de bewaartermijnen vast voor de diverse gegevensverzamelingen conform de artikel specifieke wettelijk gestelde bewaartermijnen;
- Richt schoningsprocedures in voor de diverse gegevensverzamelingen aangehouden in de kantoorautomatisering en laat deze uitvoeren.

3.6 Ter beschikking stellen (artikel 15)

3.6.1 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.

3.6.2 Bevindingen

De Infodesk

Bij de afdeling Dienst Informatie is de Infodesk Hollands-Midden gepositioneerd. De Infodesk Hollands-Midden bestaat uit 5 afdelingen. Deze 5 business units vormen Regionaal Informatie Centrum (RIC), dat bij ieder korps aanwezig is. De zogenoemde RIC's staan met elkaar in verbinding en tevens met het Nationaal Informatie Knooppunt (NIK).

Afdeling Gegevensverwerking is voor de enkelvoudige vragen en afdeling Veredeling voor de complexe vragen, waarbij een 14-tal systemen is betrokken.

Binnen Veredeling worden verschillende taakaccenten onderscheiden, waaronder taakaccent opsporing, taakaccent RID (1 aparte medewerker), taakaccent CIE (2

aparte medewerkers), taakaccent internetsurveillanten, taakaccent preventie in het kader van de openbare orde.

Procesgang

Vragen kunnen binnenkomen via de telefoon, een digitaal intakeformulier of een email afkomstig van blauw, rechercheur, teamchef, interregionale Infodesk en BOD.

De Interregionale Infodesk en BOD vragen echter alleen informatie op per e-mail. Het aantal vragen per maand is ongeveer 1200. De coördinator beoordeelt de vraag en toetst ook doelbinding en zet deze uit naar medewerker BU Gegevensverwerking of Veredeling. De medewerker handelt de vraag af en verstrekt de informatie per e-mail richting klant. Als disclaimer wordt aan de mail de volgende tekst toegevoegd:

"Dit document en de eventuele bijlagen bevat(ten) politiegegevens in de zin van de Wet politiegegevens. Deze gegevens zijn uitsluitend bestemd voor het doel waarvoor deze hier worden verstrekt. Verdere verwerking van deze gegevens is toegestaan, maar uitsluitend voor zover een wet daarin voorziet of een goede taakuitvoering dit noodzakelijk maakt. Voor elke andere handeling met deze gegevens geldt, ook nadat u deze hebt ontvangen, geheimhouding zoals bedoeld in artikel 7 van de Wet politiegegevens. Overtreding van deze geheimhoudingsbepaling is strafbaar gesteld in artikel 272 van het Wetboek van Strafrecht, waarvan lid 2 hier niet van toepassing is."

Alle klanten vallen binnen het Wpg-domein. De behandeltijd varieert en is afhankelijk van de complexiteit van de analyse die noodzakelijk is.

Registratie vraag en antwoord

Alle vragen worden sinds 4 jaar geregistreerd in PLANON, waartoe alleen de businessunits Gegevensverwerking en Veredeling toegang hebben. Tevens worden de aantallen bijgehouden voor de statistieken van bedrijfsvoering.

De antwoorden op artikel 8 niveau komen in een maand map op de G-schijf van NT. Na 5 jaar bewaring worden mappen verwijderd. Antwoorden op artikel 9 en 10 Wpg-niveau worden in BVO geplaatst binnen het afgeschermd gedeelte voor het specifieke onderzoek. Interregionale vragen en antwoorden worden geregistreerd in de eerder genoemde maand map op de G-schijf van NT. De meeste vragen hebben echter een artikel 8 karakter.

Vragen vanuit opsporing

Er bestaat een recherche op korpsniveau en op districtsniveau. Vanuit deze niveaus komen vragen per e-mail of telefoon binnen bij de coördinator, die deze vervolgens toewijst aan taakaccent opsporing. Een andere manier waarop vragen binnenkomen is via de opdrachtenbank in BVO. In de opdrachtenbank worden de verzoeken van de rechercheurs vanuit de verschillende lopende opsporingsonderzoeken geplaatst. De vragen die afkomstig zijn van de opdrachtenbank worden niet geregistreerd in PLANON, maar uitsluitend in BVO.

Taakverdeling bij informatievoorziening ten behoeve van opsporing

Enkelvoudige vragen dienen gesteld te worden bij Gegevensverwerking. Complexere vragen gaan naar Veredeling die uit politiesystemen informatie veredelt.

Binnen rechte teams kan de verkregen informatie worden gecombineerd met andere registraties na het ontvangen van een machtiging van Officier van Justitie. Hierbij moet bijvoorbeeld gedacht worden aan telecomgegevens,

kentekenregistraties etc. Bovendien beschikken de opsporingsteams over internet- en telecomspecialisten. De rechercheurs hebben geen toegang tot de systemen waaruit Veredeling zijn informatie haalt.

Onderscheid digitale functies

De internetsurveillanten gebruiken openbare bronnen zoals YouTube, Hyves en Twitter om informatie te ontsluiten. Een digitaal rechercheur onderzoekt informatiedragers zoals SIM-kaarten, USB-sticks, diskettes, harde schijven e.d. De eerste is geplaatst in BU V en de tweede binnen de recherche.

Codering

Er is een strikte scheiding tussen de CIE en tactische recherche. Dit heeft te maken met interne en externe openbaarheid en daarmee gepaard gaande afschermingsbelangen. De rechter moet kunnen controleren op basis van welke informatie tactisch onderzoek is verricht en of dat rechtmatig is gegaan.

Nu de CIE ook beschikt over zogenaamde 00-informatie – informatie die rechtstreeks kan leiden tot de bron – zou tactisch handelen door de CIE kunnen leiden tot niet-ontvankelijkheid omdat de rechter zijn controlerende taak niet in volle omvang kan uitvoeren. Om die reden geeft de CIE alleen informatie aan de tactische recherche die bekend mag worden en dus door de rechter gecontroleerd kan worden, de zogenaamde 01-informatie.

Bevoegde functionarissen

Er is een landelijke één week durende Wpg-cursus geweest op het hoofdbureau in Leiderdorp verzorgd door het landelijke Project Implementatie WPG. Hier zijn ongeveer 10 medewerkers van Hollands-Midden naartoe geweest. [REDACTED] II

[REDACTED] Uit de cursus kwam naar voren dat de impact van de Wpg groot zal zijn.

De bevoegde functionarissen hebben tevens een uitnodiging gekregen om deel te nemen aan een gezamenlijke training met Haaglanden. Nieuw aangestelde bevoegde functionarissen ontvangen echter geen extra training omtrent de Wpg omdat dit reeds tijdens de opleiding aan de orde is gekomen.

Tevens heeft men bekendheid van de Wpg bij de functionarissen weten te bewerkstelligen door middel van het aanschuiven van de privacyfunctionaris bij werkoverleggen van met name wijkagenten aan om aan de hand van casuïstiek de Wpg uit te leggen en vragen te beantwoorden.

Weigeringsgronden ter beschikking stellen

De bevoegde functionarissen zijn op de hoogte van de wettelijke toegestane weigeringsgronden. Deze gronden komen aan de orde in de opleiding die alle functionarissen hebben genoten.

Echter is er geconstateerd dat doordat men veel in Word-documenten werkt en daardoor deze informatie niet in de daarvoor bestemde systemen terechtkomen, deze politiegegevens dus niet via deze systemen worden gedeeld. Hierdoor loopt men het risico dat er informatie in Word-documenten achtergehouden wordt daar waar het had moeten worden gedeeld.

Artikel 10

Bij artikel 10 onderzoeken is de leidende gedachte dat er risico bestaat voor de informant. Als de CIE informatie verstrekt voor analyse wil men dat dat formeel

plaatsvindt op basis van een PV. Zo niet dan weigert zij de informatie. Er is geen protocol dat hierin de weg wijst.

Door de komst van twee nieuwe Chefs-CIE is sprake van een aanscherping. Informatie wordt thans niet meer geleverd zonder een proces-verbaal. Men wordt wel scherper hierin en grensgevallen worden steeds meer getest.

CIE

Bij de vraag om informatie uit een artikel 9-onderzoek van een ander korps voor een artikel 12 onderzoek van Hollands-Midden moet expliciet de toestemming worden verkregen van de projectleider van het artikel 9 onderzoek van het andere korps. De CIE gaat er echter van uit dat als de Officier van Justitie autorisatie heeft toegekend om zaaksinformatie te gebruiken, in overleg met de privacyfunctionaris ook impliciet toestemming is verkregen voor overheveling van artikel 9 informatie.

Overigens is het platform CIE in een landelijke werkgroep bezig met deze materie. De voorgestelde oplossing ligt erin dat bij de melding van een artikel 9-zaak, expliciet een zinsnede in het formulier wordt opgenomen waarin toestemming wordt gegeven voor het gebruik van de artikel 9 informatie voor andere doeleinden.

De processen-verbaal voor de CIE hebben landelijk een vaste indeling. Korps Hollands-Midden heeft daaraan de volgende tekst toegevoegd:

Eerdergenoemde informatie is door mij voor strafrechtelijk onderzoek ter beschikking gesteld aan het onderzoek (naam onderzoek) van de regiopolitie Hollands Midden en mag slechts na voorafgaande schriftelijke toestemming van het hoofd C.I.E., voornoemd, worden verstrekt aan een ander.

De bovenstaande oplossing door expliciet op het formulier is lijkt een goede oplossing om bewustwording bij het CIE te creëren omtrent het vragen van schriftelijke toestemming bij het ter beschikking stellen van gegevens aan een ander.

Ter beschikking stellen artikel 13 tweede lid

Doordat er veelvuldig gebruik wordt gemaakt van regionale en/of lokale systemen wordt daarmee de informatiedeling en verdere verwerking van politiegegevens met korpsen uit andere regio's uitgesloten. De antwoorden op informatieverzoeken die nu in de lokale mappen komen worden nu per definitie niet politie-Nederland breed gedeeld zoals dit wel op grond van artikel 13 lid 2 Wpg mogelijk moet zijn. Dit betreft antwoorden op heel specifieke vragen die vanuit de reguliere systemen komen.

Alleen informatie in de primaire systemen (kunnen) worden gedeeld met politie-Nederland breed.

3.7 Verstrekken (artikel 16/24)

3.7.1 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 van de Wpg worden deze verstrekkingen nader uitgewerkt. Artikel 20 regelt de omstandigheden en voorwaarden voor de verstrekkingen aan derden structureel voor samenwerkingsverbanden.

3.7.2 Bevindingen

Verstrekkingswijzer

Landelijk is er een verstrekkingswijzer opgesteld waarin overzichtelijk is gemaakt welke gegevens naar welke wettelijk vastgestelde partijen mogen worden vertrekt. De landelijke verstrekkingswijzer kan dienen als onderliggende documentatie om deels invulling te geven aan artikel 16 t/m 24 Wpg. De centraal opgestelde procesbeschrijving geeft weer welke informatie aan welke partijen mag worden verstrekt.

Het korps Hollands-Midden maakt gebruik van de landelijke verstrekkingswijzer.

Er zijn de volgende verstrekkingen geconstateerd die voorkomen in deze landelijke verstrekkingswijzer:

- De Wpg regelt verstrekking van politiegegevens aan het Openbaar Ministerie in artikel 16 lid 1c Wpg. In deze situatie verstrekt en ontvangt het korps Hollands-Midden privacygevoelige gegevens, zoals de veelplegerslijst. Het risico bestaat dat de interne afspraken tussen Chef Gegevensverwerking en het Openbaar Ministerie in strijd zijn met artikel 3 Wpg.
- Verstrekkingen aan burgemeesters (i.c. het bevoegde gezag) vindt plaats op grond van artikel 18 Wpg en is alleen dan toegestaan voor de daarin genoemde doeleinden.
- Verstrekkingen aan de Penitentiare Inrichting (PI) vinden er tevens plaats. Mogelijk wel in strijd met protocolplicht vastgelegd in artikel 32 Wpg.
- De voorzitter van het College heeft ingestemd met een directe toegang van de Regionale Inlichtingen Dienst tot CIE-informatie. Dat is in een soort convenant vastgelegd. Het Landelijk Platform van CIE officieren en ook dat van Recherche officieren hebben aan deze inzage een aantal voorwaarden verbonden:
 - geen gebruik zonder overleg;
 - een beperkte mogelijkheid tot raadplegen van gegevens; alleen door chef RID en zijn plaatsvervanger.

Convenanten

Het Veiligheidshuis

In Leiden bestaat een zogenoemd Veiligheidshuis waar informatie gedeeld wordt met partners. Dit zijn allerlei instanties die een rol spelen bij jeugd en jongerenwerk en hulpverlening. Bij periodieke besprekingen komen concrete casussen ter sprake, waarbij de politie in een spagaat zit als het aankomt om informatie te delen. Politie is hierbij terughoudend en kan lang niet in alle details treden.

Voor dit samenwerkingsverband heeft het korps sinds november 2011 een artikel-20 besluit opgesteld, genaamd 'Besluit informatie uitwisseling Politie Hollands Midden in het kader van Het samenwerkingsverband Veiligheidshuis'.

In dit besluit is uiteengezet:

- welk doel de samenwerking en gegevensverstrekking noodzakelijk;
- het zwaarwegend belang van de verstrekking;
- de uit te wisselen gegevens;
- de geheimhoudingsplicht conform artikel 7 Wpg;
- de looptijd van het besluit van 1 jaar met mogelijkheid tot stilzwijgende verlenging

Het besluit is ondertekend door de korpsbeheerder, burgemeester en het bevoegde gezag.

Bewerkersovereenkomsten

Er zijn geen bewerkersovereenkomsten met ICT leveranciers (hierdoor is het recht om te auditen bij die leveranciers ook niet geregeld).

Proces voor artikel 20 besluiten

In 2009 heeft korps Hollands-Midden een inventarisatie gemaakt van de bestaande samenwerkingsverbanden. Hierbij is gebleken dat een deel van de convenanten zoals naar verwachting niet als Wpg-proof konden worden beschouwd. Mede op basis daarvan heeft het Korps Management Team (KMT) in datzelfde jaar een besluit genomen betreffende:

1. het opstellen van een algemeen toetsingskader dat voor de totstandkoming van nieuwe convenanten gebruikt dient te worden.
2. het vaststellen van het 'Modelbesluit artikel 20-verstrekkings' als regionale standaard en het vanuit de Wpg juridische kader voor gegevensverstrekking door de politie.
3. een regionale doorlichting van de bestaande convenanten van PHM teneinde:
 - a) de afspraken over informatie-uitwisseling te toetsen aan de vereisten van de Wpg en deze zo nodig aan te passen.
 - b) de juridische consequenties van de overige samenwerkingsafspraken op grond van andere wet- en regelgeving in kaart te brengen.
 - c) de convenanten op hoofdlijnen te toetsen aan het vast te stellen toetsingskader.
 - d) te komen tot een eenduidige definitie en een regionaal standpunt over de gewenste inzet en reikwijdte van convenanten binnen het korps.

Het afsluiten van convenanten

Nieuwe convenanten worden door de privacyfunctionaris van het korps getoetst aan de Wpg en daar waar nodig bijgesteld. District- en teamchefs worden in districtelijk verband geïnformeerd over de tekenbevoegdheid van de korpsbeheerder inzake convenanten en de (on)mogelijkheden van gegevensverstrekking wanneer zij op lokaal niveau samenwerking met partijen aangaan.

Hollands-Midden heeft voor nieuwe convenanten een toetsingskader ontwikkeld om te waarborgen dat nog af te sluiten samenwerkingsverbanden voldoen aan de bepalingen van de Wpg. Tevens heeft men hiervoor het 'Modelbesluit artikel 20 verstrekkings' ontwikkeld dat als juridisch kader kan dienen voor alle gegevensverstrekkingen door het korps binnen een samenwerkingsverband.

Het modelbesluit kan pas ondertekend worden wanneer sprake is van een structureel samenwerkingsverband dat in een convenant geformaliseerd is waarnaar het besluit verwijst. Nieuwe partijen kunnen zich middels een bijlagenconstructie als deelnemer aansluiten en conformeren zich daarmee aan de bepalingen zoals neergelegd in het convenant.

Gelet op de mandaatregeling en de Aanwijzing Wpg voor het OM vindt ondertekening van het modelbesluit (artikel 20-verstrekkings) namens de politie plaats door de korpsbeheerder, de (fungerend) hoofdofficier van justitie en het bevoegde gezag.

Proces voor artikel 20 besluiten

Voordat wordt besloten tot het sluiten van artikel 20-besluit wordt een afweging gemaakt of het aparte vastleggen van de taak noodzakelijk is, of de wettelijke bepalingen dwingen tot het gebruik van een ander instrument of een ander instrument eventueel de voorkeur verdiend wat betreft de uitvoerbaarheid en handhaafbaarheid.

Inhoudelijke vereisten met betrekking tot de gegevensverwerking zijn volgens het toetsingskader:

- Pas wanneer een samenwerkingsverband geformaliseerd is in een schriftelijke vastlegging, kan de korpsbeheerder besluiten tot het verstrekken van politiegegevens aan de deelnemende partijen.
- Afspraken over gegevensverstrekking door de politie worden in een 'Modelbesluit artikel 20 verstrekkingen' opgenomen dat als bijlage bij het algemene convenant wordt gevoegd.
- Het 'Modelbesluit artikel 20 verstrekkingen' wordt ondertekend door de korpsbeheerder en het bevoegde gezag.
- Het artikel 20 besluit wordt in alle gevallen vooraf ter toetsing aan de privacyfunctionaris van het korps voorgelegd die toeziet op naleving van Wet en het Besluit Politiegegevens (Wpg en Bpg).
- De privacyfunctionaris ontvangt het ondertekende convenant en 'Modelbesluit'.
- Van elke verstrekking wordt in de Basisvoorziening Handhaving (BVH) vastgelegd welke gegevens aan wie, wanneer en voor welk doel verstrekt worden.

De afgesloten convenanten worden gepubliceerd op intranet en daarmee inzichtelijk gemaakt voor de medewerkers. Wanneer een nieuw convenant is ondertekend wordt hiervan door middel van een bericht melding op intranet gemaakt. Indien alleen van de zakelijke inhoud van het besluit mededeling wordt gedaan, wordt vermeld waar en wanneer de gehele tekst ter inzage ligt.

Modelbesluit

Geconstateerd is dat het opgestelde Modelbesluit de noodzakelijke gegevens bevat die op basis van artikel 20 Wpg zijn vereist. Dit betekent dat men het zwaarwegend algemeen belang dient te motiveren en aan dient te geven welke van de limitatief genoemde doeleinden in artikel 20 van toepassing is.

Bovendien heeft Hollands-Midden in het model opgenomen dat men de wijze van strekking aangeven en de te verstrekken gegevens dient vast te leggen. Tevens wordt er conform artikel 7 Wpg gewezen op de geheimhouding en is een standaardlooptijd van een jaar vastgesteld.

Verstrekkingenschema (regionaal)

De verstrekkingen worden altijd in een proces-verbaal in BVH vastgelegd. Verstrekking vindt steeds terughoudend plaats: tot persoon herleidbaar vindt nauwelijks plaats. Verstrekkingen gaan vaak over minder belangrijke dingen. Met name bij verstrekkingen aan burgemeesters komt dit prangend naar voren.

Er wordt mondeling meer informatie verstrekt, welke niet (structureel) wordt geregistreerd. Men geeft aan dat het belang van informatieverstrekking prevaleert

boven het niet verstrekken. Er is een trend zichtbaar dat advocaten en verzekeringsmaatschappijen informatie opvragen.

CIE

Alleen met uitdrukkelijke instemming van het HoofdCIE mag informatieverstrekking worden verricht door de informatieanalisten van DI aan derden binnen de politie. Bij afwezigheid van het Hoofd-CIE is de betreffende plaatsvervanger bevoegd om de informatie te verstrekken. Informatiedeling aan NCIE wordt zo nu en dan gedaan, bijvoorbeeld informatie over motorclubs.

Met informatieaanvragen vanuit het buitenland wordt terughoudend omgegaan. Voorheen werden collega's uit het buitenland ontvangen door de CIE. Het onbewust delen van informatie leidde dan tot rechtshulpverzoeken (RHV) die gebaseerd waren op eerder (informeel) gedeelde informatie. Dat gebeurt inmiddels niet meer. Er wordt nu alleen ingegaan op informatieverzoeken als deze voldoende relevantie bevatten en via Rechtshulpverzoeken worden ingediend.

De tekst die van brononderzoek naar doelonderzoek wordt verstrekt wordt door de projectleider en zaakofficier van het brononderzoek vastgesteld op basis van de onderliggende stukken en in een zogenaamd kluisproces-verbaal vastgelegd. Het Hoofd-CIE van het brononderzoek maakt een proces-verbaal met deze tekst en na voorafgaande toestemming van de CIE-OvJ, verstrekt hij dit aan het Hoofd-CIE waar het doelonderzoek plaats zou moeten vinden.

Ter beschikking stellen en verstrekken

Het Hoofd-CIE controleert vooraf of de te verstrekken tekst overeenkomt met de informatie en bekijkt of deze informatie rechtmatig is verkregen. Via MRO (Melding Recherche Onderzoeken) worden data (personalia, telefoonnummer, kentekens) wekelijks geautomatiseerd landelijk vergeleken.

Als data in verschillende onderzoeken in den lande voorkomen of deze data opgenomen zijn in artikel 10 Wpg-registraties van de CIE, vinden er zogenaamde 'hits' plaats. Partijen die informatie hebben op gelijke data nemen contact met elkaar op om de waarde van deze 'hit' te beoordelen. Dit kan leiden tot uitwisseling van informatie. Vanuit de CIE worden 'hits' in VROS onderzocht door runners. De informatie moet daarvoor door de medewerkster informatievoorziening ter beschikking zijn gesteld.

De processen-verbaal voor de CIE hebben landelijk een vaste indeling. Korps Hollands-Midden heeft daaraan de volgende tekst toegevoegd:

Eerdergenoemde informatie is door mij voor strafrechtelijk onderzoek ter beschikking gesteld aan het onderzoek (naam onderzoek) van de regiopolitie Hollands Midden en mag slechts na voorafgaande schriftelijke toestemming van het hoofd C.I.E., voornoemd, worden verstrekt aan een ander.

De vrees is dat anders doeldoorbreking plaatsvindt bij andere onderzoeken zonder dat daarvoor conform de Wpg toestemming is van bevoegde functionaris.

RID

Het RID runt de informanten activiteiten en beoordeelt de verkregen informatie op betrouwbaarheid en de wijze van verkrijging van de informatie. Het RID beoordeelt de afhandelingsurgentie op basis van de verkregen informatie.

De runners maken een gespreksverslag op van het gesprek met de informant, dit is het zogenaamde brutoverslag en kan worden geschaard onder artikel 12 Wpg. Het brutoverslag wordt elektronisch opgeslagen in een digitaal systeem op een standalone-pc. Het systeem is tevens logisch beveiligd. Er worden geen papierverslagen aangehouden.

Voordat de informatie wordt gedeeld met de Infodesk, vindt er altijd een beoordeling plaats. Als criterium geldt: als de informant door de deling bekend wordt dan wordt de informatie niet verder verspreid. Binnen de RID wordt alle verstrekte informatie altijd bekeken en ondertekend door het bevoegde gezag (in dit geval het Hoofd-RID).

De informatiewinning gebeurt in artikel 12, vervolgens wordt het overgenomen in TEAM artikel 10 en daarna wordt het overgenomen in 9 of 8. De Infodesk verricht dan de verdere verstrekking. De achterliggende gedachte is dat de Infodesk de informatie kan verrijken en/of veredelen.

Voor zowel CIE als RID wordt informatie ter beschikking gesteld aan de Infodesk. Deze draagt zorg voor verdere verspreiding van de informatie.

Proces voor geautomatiseerde verstrekking

Het korps verricht automatische verstrekkingen. Ten tijde van de audit was echter geen algeheel inzicht in deze automatische verstrekkingen of het beheer van die geautomatiseerde verstrekkingen.

De chef Gegevensverwerking heeft onvoldoende inzicht in de getroffen of noodzakelijke beveiligings- en betrouwbaarheidsmaatregelen voor de geautomatiseerde en elektronische berichtenuitwisseling tussen Chef Gegevensverwerking en het Openbaar Ministerie.

Door het ontbreken van een inzicht in de geautomatiseerde verstrekkingen bestaat het risico dat de geautomatiseerde verstrekking in de loop der tijd niet langer noodzakelijk is, of de aard van de gegevensverstrekking uit de pas loopt met de noodzaak. Het proces van geautomatiseerde gegevensverstrekking is daarmee niet beheersbaar. Dit staat genoteerd als onderdeel van het verbeterpakket van Functioneel Beheer.

Geheimhouding verstrekking informatie

Bij het antwoord op een informatievraag wordt een disclaimer meegestuurd. Middels de disclaimer wordt de ontvanger geattendeerd op het feit dat hij politiegegevens alleen voor een bepaald doel mag gebruiken en dat geheimhouding daarbij verplicht is.

Protocollering verstrekking

Het hangt van de verstrekking af welk soort protocollering er wordt gebruikt. Bij Hollands-Midden maakt men gebruik van zowel de I90-formulieren als de E-62 formulieren.

Voor informatieverzoeken die bijvoorbeeld bij de wijkagent of de baliemedewerker worden gesteld, bestaat een protocolplicht voor vastlegging in BVH (code I90). De functionaris voor de gegevensbescherming (FG) zou in BHV moeten controleren wat daar op dit gebied is vastgelegd. Dat heeft voor de FG nu niet de hoogste prioriteit.

De verstrekkingen aan Penitentiaire Inrichting (PI) valt te scharen onder art 18 Wpg en is conform Wpg/BPG.

Vastlegging BVO-Infodeskmodule

De Infodesk gebruikt voor het protocolleren van de verstrekkingen de Infodeskmodule in BVO. De Infodeskmodule in BVO is een voorziening waarmee het werkproces van de Infodesk wordt ondersteund.

De Criminele Inlichtingen Eenheid (CIE) voert vanuit hun specifieke taakstelling een eigen administratie rondom verstrekkingen en heeft hiertoe tevens de beschikking over een verstrekkingmodule in de BVO.

Verstrekking via formulieren in BVH en BVO

Verstrekking kan plaatsvinden via een vast formulier in BVO of BVH. Deze formulieren worden opgeslagen in het systeem, waarmee voldaan is aan de protocolplicht. Echter niet alle verstrekkingen worden middels deze formulieren geprotocolleerd.

Verstrekking binnen GMC aan rode en witte kolom

In de omgeving van het gemeenschappelijk meldcentrum worden gegevens verstrekt aan de partners binnen het GMC. Deze verstrekking vindt alleen plaats binnen de operatie. Wanneer een dergelijke verstrekking plaats vindt, wordt in een bepaald vak in de melding een bepaald teken geplaatst, waaruit duidelijk blijkt dat gegevens verstrekt zijn aan of de witte of aan de rode kolom. Later is hier een uitdraai van te maken.

Verstrekking in alle overige gevallen via I90 en E62

Wanneer een verstrekking van politiegegevens plaatsvindt, en niet onder één van bovengenoemde manieren zijn verstrekt, dan dient van deze verstrekking een vastlegging in BVH plaats te vinden middels een I90-formulier of een E62-formulier.

Hierbij valt te denken aan:

- verstrekkingen van politiegegevens in een samenwerkingsverband (in geval dat een besluit artikel 20 is opgemaakt) tijdens een overleg onafhankelijk of van dit overleg (wel/geen) een verslag wordt gemaakt;
- verstrekkingen van politiegegevens middels een brief.

Binnen de maatschappelijke klasse I90 kan een formulier verstrekkingen worden opgehaald en ingevuld.

Minimale vereisten vastleggingen

De gegevens die op grond van de 'instructie administreren van gegevensverstrekkingen aan externe partijen' minimaal moeten worden vastgelegd zijn:

- de identiteit van de ontvanger;
- een omschrijving van de verstrekte gegevens;
- het doel waarvoor de gegevens verstrekt worden;
- op basis van welk Wpg-artikel men verstrekt (artikel 16 – 25 Wpg).

Daarbij wordt tevens de volgende kanttekening gemaakt dat artikel 9 en 10-gegevens niet met alle partijen mogen worden gedeeld en daarnaast er altijd overleg met de bevoegde functionaris nodig is.

Bewaren protocolgegevens verstrekking

In de praktijk blijkt men niet structureel de I90-verstrekkingformulieren in te vullen. Deze mutaties zijn echter wel zichtbaar in het systeem waardoor in feite er

wel een vastlegging van de verstrekking plaatsvindt. Het is echter niet mogelijk om een overzicht van deze vastleggingen te genereren.

Toezicht leidinggevenden op verstrekkingen en protocollering

De materiedeskundige, ploegchef en de informatiemedewerker gaan over de verstrekkingen van politiegegevens.

De leidinggevenden hebben tevens hierin een eigen verantwoordelijkheid dat er conform de Wpg wordt geprotocolleerd. De functionaris voor de gegevensbescherming houdt hier toezicht op en geeft wanneer nodig advies.

3.7.3 Verbeterpunten

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

- Zorg voor beheersmaatregelen die gericht zijn op een volledige registratie van verstrekkingen door middel van I90 formulieren uit BVH;

3.8 Rechten van betrokkenen (artikel 25/28)

3.8.1 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.

3.8.2 Bevindingen

Informatieverzoeken van burgers of namens burgers:

Informatieverzoeken van burgers (of instanties of advocaten namens burgers) aan de korpschef kunnen uitmonden in verstrekkingen. Eén van de taken van de functionaris gegevensbescherming is om die verzoeken te beoordelen en van een memo te voorzien.

- In de memo neemt de functionaris gegevensbescherming op dat de Wpg van toepassing is en geeft hij de termijnen aan waarop moet worden gereageerd. De verzoeken gaan dan ter behandeling naar één Wpg-functionaris die het als taak erbij heeft gekregen. Per 01-01-2012 is de betreffende persoon vrijgemaakt van overige werkzaamheden en zal het in behandeling nemen van informatieverzoeken de hoofdtaak zijn;
- De Wpg-functionaris kijkt wat er aan informatie aanwezig is en bepaalt of het verstrekken wel of niet kan, en verstrekt ook namens de lijnchef (teamchef) de informatie;
- De Wpg-functionaris en privacyfunctionaris rapporteren bij art. 25 verzoeken aan de functionaris gegevensbescherming terug wat er is verstrekt. Bij een verwijderverzoek bij art. 25 gaat het verzoek naar de privacyfunctionaris en dat wordt centraal afgedaan door de Korpschef;
- De uitkomst van verwijderverzoeken wordt weer aan de functionaris gegevensbescherming voorgelegd door de privacy functionaris. Daarmee controleert de functionaris gegevensbescherming of de privacyfunctionaris het werk goed heeft gedaan;
- De privacyfunctionaris stuurt inhoudelijk de informatiecoördinatoren aan op het gebied van die verzoeken.

Werking inzagerecht begin 2011

De afhandeling van informatieverzoeken van burgers of namens burgers is begin 2011 nog niet goed belegd. Er zijn 18 informatiecoördinatoren die hebben aangegeven dit werk niet te willen doen.

- Als reden wordt aangegeven dat zij niet goed zijn opgeleid in de Wpg voor het verrichten van de werkzaamheden. Bovendien vinden zij dat het meer verzoeken zijn dan aanvankelijk gedacht (ongeveer 300 verzoeken in het kader van art. 16/24 en 20 verzoeken in het kader van art. 25);
- Er is alleen een Wpg-presentatie geweest en er zijn hand-outs uitgedeeld. Inzageverzoeken in het kader van privacy werden voorheen decentraal afgehandeld door contactpersonen in de districten. Inzageverzoeken moeten in principe via de Dienst Informatievoorziening worden ingestoken;
- Sinds mei worden deze verzoeken door één vervanger (de Wpg-functionaris) uitgevoerd die dit werk naast zijn andere werkzaamheden uitoefent. De functionaris kan indien nodig de privacyfunctionaris raadplegen. De uiteindelijke belegging van de inzageverzoeken wordt bepaald door de Directeur Informatie en de functionaris gegevensbescherming geeft uitvoering aan diens keuze.

Complexe art 25 verzoeken worden door, of onder supervisie van de privacyfunctionaris afgehandeld.

Nieuwe procedure

Inzageverzoeken

Sinds medio 2011 heeft Hollands-Midden een nieuwe procedure vastgesteld met betrekking tot het afhandelen van inzageverzoeken conform de Wpg. De medewerkers binnen het korps zijn middels een instructie 'Informatieverstrekking of privacyverzoek of WOB-verzoek' op de hoogte gebracht van de procedure.

Volgens de procedure dient de betrokkene het inzageverzoek schriftelijk in te dienen. Het verzoek tot een kennisname of -correctie moet worden gericht aan de korpschef, ter attentie van de privacyfunctionaris. In dit verzoek moet de personalia en telefoonnummer worden vermeld alsmede een toelichting om welk soort informatie het zou moeten gaan. Aangegeven wordt dat er *geen* kopieën worden verstrekt en de aanvrager alleen gegevens te horen krijgt die op de persoon zelf betrekking hebben.

Eenvoudige verzoeken worden door een uitvoerend medewerker afgehandeld, de complexe verzoeken door de privacyfunctionaris. Voor het klachtenbeheer is tevens een persoon aangewezen. Wanneer medewerkers vragen hebben of advies hieromtrent kunnen gebruiken kan men terecht bij de privacyfunctionaris of functionaris voor de gegevensbescherming van het korps.

Ontevredenheid ten opzichte van de procedure probeert men eerst op te lossen door middel van een gesprek. Bij geen oplossing wordt de klager verzocht de verzoeker de klacht op schrift te zetten en de zenden naar de korpschef t.a.v. Klachtenbeheer.

Er blijken geen klachten te zijn binnengekomen.

Verzoek tot correctie

Verzoeken tot correctie worden door de privacyfunctionaris afgehandeld. De personen waarvan het inzageverzoek is ingewilligd worden middels een brief die men meekrijgt gewezen op dit recht van correctie. Om hiervoor in aanmerking te komen dient men het verzoek schriftelijk in te dienen en goed te motiveren. In 2010 is dit eenmaal voorgekomen.

De uitvoering van de correctie blijkt in de praktijk wel eens lastig doordat diverse bevragingssystemen de gewijzigde brongegevens niet goed over nemen.

Verbeterpunten

- Duidelijkheid scheppen in de uiteindelijke werking van de inzageprocedure;
- De Functionaris gegevensbescherming blijvend inzetten in de toezichhoudende en adviserende rol en waar mogelijk onttrekken uit de reguliere procesgang.

3.9 Protocolplicht (artikel 32)

3.9.1 Norm

De verantwoordelijke draagt zorg voor de schriftelijke vastlegging van:

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

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

3.9.2 Bevindingen

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

Protocollering doel onderzoek

De functionaris voor de gegevensbescherming houdt sinds 2000 een overzicht bij van alle aan- en afgemelde onderzoeken. Bevoegde functionarissen moeten de start van een nieuw onderzoek aangegeven (aanmaken). Dit aanmaken van een onderzoek kan worden gedelegeerd. Het afsluiten en/of overdragen van een onderzoek echter niet worden, dit mag alleen gebeuren door de betreffende bevoegde functionaris. De functionaris voor de gegevensbescherming houdt controle op de aan- en afgemelde onderzoek. Dit overzicht van de FG is tevens in te zien voor de privacyfunctionaris. Overigens wordt nu gewerkt aan een tool op intranet om eenduidige registraties mogelijk te maken.

Proces

De rechercheonderdelen starten een nieuw onderzoek. De rechercheur maakt in een Word sjabloon een nieuw onderzoek aan voor artikel 9 Wpg. In de sjablonen van Word is geregeld dat het formulier dan automatisch naar de functionaris gegevensbescherming en ISC West wordt gestuurd.

Vervolgens beoordeelt de functionaris gegevensbescherming het ingevulde sjabloon en voert het de gegevens in een Excelbestand in waarin de doelen van de onderzoeken worden bijgehouden. In een Excelbestand worden onder andere de volgende gegevens opgenomen:

- naam van het onderzoek;
- de eindverantwoordelijke;
- locatie, stad;
- wat er is gebeurd;
- waar het dossier zich bevindt;

- de wetscategorie te worden vermeld die wordt geschonden.

Tevens wordt opgenomen in de melding op welke applicaties de informatie wordt vastgelegd, zoals afgeschermd BVH, onderzoeksomgeving BVO, G-schijf, standalone PC, laptop.

Afmelden van onderzoeken

De afmeldingen van onderzoeken via het sjabloon vertonen een stijgende lijn in het melding ophefregister. Opname in het ophefregister houdt in dat het onderzoek wordt afgesloten. De functionaris voor de gegevensbescherming geeft een bevestiging terug en vermeldt in het Exceloverzicht dat het onderzoek is afgesloten. De daadwerkelijke vernietiging van het dossier wordt niet meer gemeld in het overzicht.

De zaken die niet tot een oplossing komen blijven echter openstaan. De afloopberichten van het Openbaar Ministerie lopen via de Dienst Informatie (veredeling).

Protocollering artikel 13 gegevensverzameling

De gegevensverzamelingen op grond van artikel 13 zijn binnen Hollands-Midden geïdentificeerd. Het korps geeft aan geen gebruik te maken van regionale systemen en gegevensverzamelingen buiten de landelijke systemen. De protocollering van de landelijke artikel 13 systemen (zoals HKS) vindt op een landelijk niveau plaats middels standaard protocolformulieren. De protocollering van deze systemen wordt in de systemen aangehouden.

Protocollering onrechtmatige handeling

Er wordt door de privacyfunctionaris een overzicht bijgehouden van onrechtmatige verwerkingen. Er is een Excelbestand waarin privacyschendingen worden vastgelegd. De functionaris gegevensbescherming en de privacyfunctionaris vullen de Excelsheet samen in wanneer ze tegen schendingen aanlopen. Het gaat om een aantal schendingen per jaar.

Uit het rapport 2010 van de functionaris gegevensbescherming blijkt dat in 2010, drie onrechtmatige verstrekkingen zijn geconstateerd. Dit betrof twee informatieverstrekkingen die zijn gedaan aan woningeigenaren bij geclaimde overlast. Echter de overlast was te gering voor rechtvaardiging van de verstrekking, en/of er was geen toestemming aan het bevoegde gezag gevraagd.

Gemeenschappelijke verwerking

Niet van toepassing. Het korps Hollands-Midden heeft geen gemeenschappelijke verwerkingen met andere korpsen.

3.10 Audits (artikel 33)

3.10.1 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.

3.10.2 Bevindingen

Interne audit functie

Het korps Hollands-Midden heeft in het kader van de Wet politiegegevens (Wpg) drie medewerkers een interne Wpg-audit laten uitvoeren in 2010. Een extern bureau heeft een appreciatie uitgevoerd op de gehanteerde werkmethode en rapportage.

De Regeling Periodieke Audit Politiegegevens (RPAP) stelt in artikel 3 dat ten minste jaarlijks een interne Wpg-audit dient plaats te vinden in de vorm van een IT-audit, welke betrekking heeft op één dan wel een aantal onderdelen van de wet. De doelstelling van deze audit is het op systematische wijze toetsen of op adequate wijze uitvoering is gegeven aan de bepalingen van de wet, gericht op:

- a) de opzet en het bestaan van maatregelen en procedures die in de borging van de wettelijke eisen moeten voorzien;
- b) de werking van de getroffen maatregelen en procedures.

Het korps Hollands-Midden heeft een pioniersrol vervuld met de uitvoering van de interne Wpg-audit. Tijdens de interne audit zijn de politieprocessen onderzocht, met name de artikelen 8 tot en met 12 Wpg.

Al tijdens de uitvoering van de interne audit groeide het besef dat dit geen echte IT-audit was. Het extern bureau heeft de interne audit beoordeeld en concludeerde dat zowel audit-technisch als inhoudelijk de kwaliteit van de audit niet voldoende was.

Interne audit plan

Het korps heeft een intern auditplan 2010 opgesteld. Het auditplan bevat een omschrijving van de minimale vereisten vanuit de RPAP, echter ontbreekt een uitwerking en toepassing van de wettelijke vereisten op de onderdelen van het korps Hollands-Midden. Het auditplan 2011 is uitgevoerd door een extern bureau en heeft zich gericht op het auditobject: de interne auditfunctie.

Het korps gaat de bevindingen uit de externe auditrapportage gebruiken voor het auditplan 2012.

Interne audit rapport

Aan de hand van het appreciatierapport van 2011 is vastgesteld dat de gevolgde interne audit methodieken inclusief bevindingen zijn opgesteld. De werkwijze is beschreven, tevens zijn de resultaten van de privacy audit beschreven.

3.10.3 Verbeterpunten

- Beleg structureel de auditfunctie ten aanzien van de Wpg;
- Richt een vaktechnisch verantwoorde en meerjarig gerichte audit in;
- Stel een auditdossier op.

3.11 Privacyfunctionaris (artikel 34)

3.11.1 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.

3.11.2 Bevindingen

Benoeming en melding

De PF heeft een cursus Wpg doorlopen. Na deze cursus te hebben gevolgd formeel is zij benoemd als privacyfunctionaris (PF) in 2009. Vanaf aanstelling is de privacyfunctionaris het korps ingetrokken om de medewerkers te informeren over de implementatie van de Wpg.

De functionaris gegevensbescherming (FG) is ook een tijdje waarnemend privacyfunctionaris geweest (en is tevens bij het CBP aangemeld). Daarna is de huidige PF aangenomen als privacy functionaris. Vanaf half december 2010 is zij door ziekte uitgevallen en is de FG haar functie van privacyfunctionaris weer gaan oppakken.

De rol van de privacyfunctionaris

De privacyfunctionaris heeft door omstandigheden haar taken begin 2011 tot medio 2011 onvoldoende kunnen uitvoeren. Daardoor is onafhankelijk toezicht op de naleving van de Wpg in het gedrang gekomen.

Er zou door de privacyfunctionaris een overzicht moeten worden bijgehouden van onrechtmatige verwerkingen. Er is een Excelbestand waarin privacyschendingen worden vastgelegd. De functionaris gegevensbescherming en de privacyfunctionaris vullen de Excelsheet samen in als zij tegen schendingen aanlopen. Het gaat om een aantal schendingen per jaar.

Voor de privacyfunctionaris is het heel moeilijk om toezicht op de autorisaties te houden:

- De benodigde overzichten kunnen niet worden gegenereerd, en;
- De privacyfunctionaris maakt zelf onderdeel uit van het autorisatieproces en voldoet niet aan haar toezichthoudende rol;
- Idealiter zou de privacyfunctionaris een afwijkingenrapportage krijgen van de autorisaties die niet zijn ingericht conform de autorisatierichtlijnen vanuit de autorisatiematrix.

Privacyfunctionaris ziet met betrekking tot een aantal uitvoeringsaspecten bij de Infodesk niet toe (mogelijk in strijd met artikel 34 WPG).

Opleiding

De privacyfunctionaris heeft een cursus gevolgd voorafgaand aan haar aanstelling.

Protocollering

De privacyfunctionaris houdt een overzicht bij van alle artikel 9 doelen. Vanaf 2000 is dat al door de functionaris gegevensbescherming bijgehouden.

De rechercheonderdelen starten een nieuw onderzoek. De rechercheur maakt in een Word-sjabloon een nieuw onderzoek aan voor artikel 9. In de sjablonen van Word is geregeld dat het formulier dan automatisch naar de functionaris gegevensbescherming en ISC West wordt gestuurd. ISC West is een onderdeel van de politie, ten behoeve van Hollands-Midden en Haaglanden waar de servers staan. Vervolgens beoordeelt de FG het ingevulde sjabloon en voert het de gegevens in het Excelbestand in.

De verantwoordelijke dient zorg te dragen dat veel zaken schriftelijk worden vastgelegd, waaronder alle verstrekkingen aan externen, autorisaties, doelen van

onderzoeken, samenwerkingsverbanden, etc. Dit is specifiek vastgelegd in artikel 32 van de Wpg. Alle rechercheonderzoeken worden correct gemeld door de "tijdelijke register aanmelding" in 2008, 2009 en 2010 door te laten lopen. Controle vindt plaats door de FG.

In de sturingscyclus wordt viermaandelijks een overzicht gepresenteerd, waarbij het aantal meldingen artikel 9 Wpg en BVO-meldingen staat vermeld. Het aantal meldingen wordt regelmatig besproken met bureauchefs en de directie. Op deze wijze is er inzicht en controle op verwerking en opslag van opsporingsgegevens. Daarnaast wordt regelmatig bekeken of de onderzoeken ook geheel in BVO worden verwerkt. Het korps hanteert het uitgangspunt: om informatie te kunnen delen is het noodzakelijk om de informatie ook beschikbaar te stellen in een landelijk systeem (BVO).

Aandachtspunten protocollering

De opzet en controle van protocolleringen vormt nog een aandachtspunt bij het korps Hollands-Midden. De protocolleringen vormen een van de centrale aandachtspunten voor het korps voor 2012. De nog niet geheel uitgekristalliseerde taakverdeling uit zich in het feit dat er geen heldere afbakening is van de taken die voortvloeien uit de protocolplicht.

De zoekresultaten van artikel 11-zoekacties worden aangehouden / gelogd in BRAINS. In analyseportages wordt aangegeven hoe is gezocht. In de operationele analyse is beschreven hoe men tot het resultaat is gekomen. Uit de praktijk blijkt echter dat nog onvoldoende controle plaatsvindt op de logging van artikel 11-verwerkingen.

Jaarverslag

De FG heeft een jaarverslag 2010 opgesteld met daarin zijn bevindingen vanuit de rol als toezichthouder op naleving van de Wpg.

3.12 Functionaris Gegevensbescherming (artikel 36)

In het korps is een functionaris gegevensbescherming (FG) aangesteld. De FG helpt de privacyfunctionaris in haar takenpakket vanuit de Wpg.

Aanmelding

De FG is aangemeld bij het CBP.

Toezichthoudende rol

De functionaris ziet toe op de verwerking van persoonsgegevens overeenkomstig het bij en krachtens de wet bepaalde. Het toezicht strekt zich uit tot de verwerking van persoonsgegevens door de verantwoordelijke die hem heeft benoemd of door de verantwoordelijken die zijn aangesloten bij de organisatie die hem heeft benoemd.

Het is de FG toegestaan om aanbevelingen te doen aan de verantwoordelijke voor een verbeterde bescherming van de gegevens. De FG heeft, om begrijpelijke redenen, de taken van de privacyfunctionaris (in haar afwezigheid) deels overgenomen en vormt daarmee onderdeel van het proces. De overname van de PF-taken door de FG is medegedeeld met het CBP.

3.12.1 Verbeterpunten

Als volgende verbeterpunten zijn te noemen:

- Wij bevelen aan om de taken van de privacyfunctionaris en de functionaris gegevensbescherming duidelijk af te bakenen om vermenging van de

adviesfunctie en de toezichthoudende rol van de Functionaris
gegevensbescherming gescheiden te houden van de taken van de PF.