



Ministerie van Veiligheid en Justitie

Audit Wpg politie Zuid-Holland Zuid
Rapport

Datum
Status

3 januari 2012
Definitief

Colofon

Afzendgegevens

Departementale Auditdienst

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

Contactpersonen

Senior Auditors

T 070 370 65 60
M wpg@minvenj.nl

Projectnaam

Audit Wet Politiegegevens

Ons kenmerk

DDS/5719621/11

Auteurs

Inhoud

Colofon 3

1 Assurance Verklaring 7

2 Samenvatting 9

3 Inleiding 22

3.1 Algemeen 22

3.2 Aanleiding 22

3.3 Doelstelling, aard en scope van de opdracht 22

3.4 Afbakening 23

3.5 Normenkader 23

3.6 Beperkingen voor de privacy audit 24

3.7 Onderzoeksmethoden en werkwijze 24

3.8 Doelgroep van het rapport 24

4 Bevindingen 25

4.1 Inleiding 25

4.2 Verantwoordelijke 27

4.3 Kwaliteitsaspecten van politiegegevens (artikel 3 en 4) 28

4.4 Gevoelige gegevens 40

4.5 Autorisatie (artikel 6) 41

4.6 Geautomatiseerd Vergelijken/In Combinatie Met Elkaar Verwerken (artikel 11) 44

4.7 Bewaartermijnen (artikel 14) 46

4.8 Ter beschikking stellen (artikel 15) 50

4.9 Verstrekken (artikel 16/24) 53

4.10 Rechten van betrokkenen (artikel 25/28) 58

4.11 Protocolplicht (artikel 32) 61

4.12 Audits (artikel 33) 63

4.13 Privacyfunctionaris (artikel 34) 64

4.14 Functionaris Gegevensbescherming (artikel 36) 65

1 Assurance Verklaring

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

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

Dit onderzoek is uitgevoerd conform de richtlijn 3600N, 'Assurance-opdrachten met betrekking tot de bescherming van persoonsgegevens (privacy audits)' van juni 2006, van de NIVRA en de NOREA.

Op grond van onze werkzaamheden concluderen wij dat het stelsel van maatregelen en procedures gericht op de bescherming van de politiegegevens, betrekking hebbende op de in de Wpg genoemde artikelen bij het korps Zuid-Holland Zuid, 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 Zuid-Holland Zuid te nemen maatregelen. Ook is gebleken dat het korps Zuid-Holland Zuid voor het volledig kunnen voldoen aan de Wpg eisen mede afhankelijk is van besluiten die buiten het korps Zuid-Holland Zuid dienen te worden genomen, bijvoorbeeld op landelijk niveau door de minister van VenJ, het KBB of de Raad van Korpschefs. Tekortkomingen op al deze vlakken hebben uiteindelijk geleid tot het geformuleerde oordeel.

De verantwoordelijke, zijnde de korpsbeheerder van het korps Zuid-Holland Zuid, is, op grond van artikel 4 lid 1 van de Regeling Periodieke Audit Politiegegevens, verplicht binnen drie maanden een verbeterrapport op te stellen waarin de maatregelen worden beschreven die getroffen zijn ter verbetering van de in de privacy audit geconstateerde tekortkomingen. Op grond van artikel 4 lid 3 dient hercontrole plaats te vinden. Wij adviseren deze hercontrole te laten uitvoeren door de interne auditfunctie van het korps Zuid-Holland Zuid. Het verbeterrapport en de uitgevoerde hercontrole zullen in de navolgende jaren door de privacyauditor worden beoordeeld.

Den Haag, 3 januari 2012

De Directeur van de Departementale Auditdienst

A handwritten signature in blue ink, consisting of several fluid, overlapping strokes, positioned above the printed name.

J.C. van Praat RE RA

2 Samenvatting

Het korps Zuid-Holland Zuid heeft veel aandacht besteed aan de analyse van de Wpg, de inrichting van processen voor compliancy aan de Wpg en trainingen van de sleutelpersonen in de Wpg. De Privacy Functionaris en de Bevoegd Functionarissen fungeren op hun beurt als vraagbaak voor het gehele korps. Tevens zijn de convenanten geïnventariseerd en het instrueren van de medewerkers over de protocolplicht heeft plaatsgevonden. Verder is veel energie gestoken in het opleiden van de medewerkers van het korps op het gebied van de wet- en regeling van de Wpg.

De korpsleiding toont hiermee en met andere initiërende activiteiten haar nadrukkelijke aandacht voor de Wpg. In opzet voldoet het korps grotendeels aan de Wpg. Niettemin voldoet het door ons beschouwde stelsel van maatregelen nog niet in bestaan en werking aan de vereisten zoals genoemd in de Wpg.

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

Criteria:

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

Norm	Aspect		Bevinding en oordeel
Artikel 1.f, Verantwoordelijke			
1.f	Mandaatbesluit		Er is een mandaatbesluit aanwezig. De verantwoordelijkheden zijn gedelegeerd aan de Korpschef en doorgemandateerd aan de districtscheffs. 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)		Er is een instructie voor Handhaving en Opsporing met het onderscheid tussen artikel 8 en artikel 9 Wpg onderzoeken. Deze is gecommuniceerd aan de bevoegd functionarissen. De stelregels voor deze instructie zijn helder geformuleerd. Hiermee wordt voldaan aan de Wpg.
3.1 t/m 3.3 (8) 4.1 (8)	Noodzakelijkheid (8) Doelbinding Rechtmatigheid Juistheid Volledigheid		Een trainingssessie heeft plaatsgevonden voor de chefs. De chefs rollen de kennis uit naar medewerkers en fungeren als vraagbaak. De zorg voor het voldoen aan de kwaliteitscriteria, zoals gesteld in artikel 3 en 4 Wpg, is opgemerkt en vindt via peer reviews achteraf plaats. Hiermee wordt voldaan aan de Wpg.
3.1 t/m 3.4 (9)	Noodzakelijkheid (9) Doelbinding Rechtmatigheid		Het proces van Opsporing bevat in opzet waarborgen voor de kwaliteitscriteria en worden uiteindelijk gecontroleerd via het Openbaar Ministerie en de

Norm	Aspect		Bevinding en oordeel
4.1 (9)	Herkomst en wijze van verkrijging Juistheid Nauwkeurig Volledigheid		rechter. De verantwoordelijkheden met betrekking tot de kwaliteit van de gegevens is bij korps Zuid-Holland Zuid goed belegd. Echter, uit de gesprekken blijkt dat er nog steeds zorgen bestaan omtrent de kwaliteit van de gegevens. Niet vooraf, maar achteraf vindt er controle plaats. De kwaliteitsreview vindt structureel binnen het gehele korps plaats. Incidenten worden teruggekoppeld aan coördinatoren en leidinggevenden voor het leereffect. Zij verzorgen de terugkoppeling en passende maatregelen. Hiermee wordt voldaan aan de Wpg.
3.4 (10 en 12) 4.1 (10 en 12)	Noodzakelijkheid (10 en 12) Doelbinding Rechtmatigheid Herkomst en wijze van verkrijging Juistheid Nauwkeurig Volledigheid		CIE: Alle projectvoorstellen worden vooraf aan de CIE-officier voorgelegd. Een informatie officier is al in de fase van prewering betrokken. De OvJ 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. Alleen de Chef RID en 1 medewerker RID hebben toegang tot deze gegevens. Hiermee wordt voldaan aan de Wpg.
4.3	Beveiliging		Kantoor Automatisering: Het korps beschikt over een proces voor de isolatie van de regimes op de O-schijf voor de Kantoor Automatisering en schoning van deze schijf. De opzet van de O-schijf voldoet aan de Wpg. Landelijke en regionale applicaties: Het korps Zuid-Holland Zuid heeft de Wpg geanalyseerd en de impact daarvan op de systemen en het autorisatiebeheer bepaald. Niet alle landelijke en regionale applicaties voldoen aan de vereisten vanuit de Wpg. Hiermee wordt niet voldaan aan Wpg.
Artikel 5, gevoelige gegevens			
	• Gevoelige gegevens		Binnen Zuid-Holland Zuid wordt een gegevensverzameling van veelplegers aangehouden. Deze gegevensverzameling bevat gevoelige gegevens. De opname van gevoelige gegevens is verdedigbaar doordat de noodzaak tot opname van gevoelige gegevens relateerbaar is met verhoogde risico's op incidenten als onder andere huiselijk geweld en eerwraak.

Norm	Aspect	Bevinding en oordeel
		De veelplegers informatie is opgenomen in Amazone, waarbij toegang is verleend op basis van 'need-to-know'. De gegevensverzamelingen van de CIE en RID bevatten ook gevoelige gegevens. Deze informatie is afgeschermd en noodzakelijk voor de uitvoering van de taak. Er zijn geen overige gegevensverzamelingen gebaseerd op gevoelige gegevens aangetroffen. Hiermee wordt voldaan aan de Wpg.
Artikel 6, Autorisatie		
	• Korpsautorisatiematrix	Een korpsautorisatiematrix is volgens de Role-based access control (RBAC) methode ontwikkeld. De matrix bevat de gebruikte applicaties en maakt inzichtelijk welke rollen rechten hebben op de applicaties. Hiermee wordt voldaan aan de Wpg.
	• Aanvraagproces	De autorisatieprocedure is uitgewerkt. Er zijn voldoende waarborgen in de procedure ingebouwd. De autorisatieverzoeken worden volgens een vast proces afgehandeld. Hiermee wordt voldaan aan de Wpg.
	• Wijziging en verwijdering	Indien een medewerker in een regio wordt gemuteerd, geschorst of ontslagen zorgt de regionale privacyfunctionaris van die regio ervoor dat een verzoek tot verwijdering van de interregionale autorisatie wordt verzonden aan de regio's waar de betreffende medewerker is geautoriseerd. De privacyfunctionaris heeft medio 2011 aangegeven dat hij onvoldoende zicht op het muteren van autorisaties via het loket ondersteuning. Ter verbetering heeft het korps de volgende procedure opgesteld: Voor internen houdt de privacyfunctionaris sinds ongeveer een jaar toezicht/controle door twee keer per jaar het autorisatieoverzicht van de gehele regio te updaten en met name te kijken naar de 'nieuwe autorisaties' en 'wijzigingen in bestaande autorisaties' die hij op deze lijst waarneemt. Hierdoor is de controle op reconciliatie, schoning en verwijdering in opzet compliant aan de Wpg, echter de werking kan nog niet worden aangetoond. Hiermee wordt deels voldaan aan de Wpg.
	• Autorisatiebeheer CIE, RID	CIE en RID beheren zelf de autorisaties op de systemen. Hiermee wordt voldaan aan de Wpg.
32.1.c	Protocollering autorisaties	Volgens de procedure wordt de aanvraag gedocumenteerd en is deze inzichtelijk voor de privacyfunc-

Norm	Aspect	Bevinding en oordeel
		tionaris. Deze functionaris voert een periodieke controle uit. Hiermee wordt voldaan aan de Wpg.
32.3 voor 32.1.c	Bewaren protocolgegevens autorisaties	Volgens de procedure wordt de aanvraag gedocumenteerd en is deze inzichtelijk voor de privacyfunctionaris. Deze functionaris voert een periodieke controle uit. Hiermee wordt voldaan aan de Wpg.
Artikel 11, Geautomatiseerd vergelijken en in combinatie zoeken		
	• Hanteerbare interpretatie	De regelgeving die wordt gehanteerd is: 1. Bij alle onderzoeken van enige omvang wordt voorafgaand aan het onderzoek een opdracht aan de OvJ gevraagd om 11.4 toe te passen; 2. Tot de systemen waarmee artikel-11 bevragingen zijn uit te voeren hebben slechts toegang de opgeleide medewerkers van de infodesk en analisten (inclusief Brainsanalisten), dan wel medewerkers van RID en CIE; 3. Analyseverzoeken worden centraal aangevraagd, afgestemd en goedgekeurd; 4. Gegevens worden bewaard op de O:schijf bij het onderzoek in kwestie of in BVO. Hiermee wordt voldaan aan de Wpg.
	• Aangewezen functionarissen	De bevoegde functionarissen (chefs), DREO en de Infodesk zijn op de hoogte van de korps specifieke handelwijzen en Wpg-aspecten. Hiermee wordt voldaan aan de Wpg.
11.4	Bevoegde gezag	Artikel 11 Wpg gecombineerd zoeken, analyseren wordt alleen ten behoeve van projectvoorbereiding door de analisten gedaan. Dit betreft dan artikel 11 lid 4 Wet politiegegevens. Aanvragen hiervoor dienen gedaan te worden bij de Officier van Justitie door middel van een opdrachtformulier. Een kopie van dit formulier van de OvJ wordt bij het betreffende onderzoeksteam bewaard. Hiermee wordt voldaan aan de Wpg.
32.1.d en 32.1.h	Protocollering 11.1, 11.2, 11.4 en 11.5	De gegevens worden opgeslagen in de map waar het onderzoek plaatsvindt (O-Schijf). In geval van grotere rechercheonderzoeken wordt bij aanvang van het onderzoek aan de Officier van Justitie opdracht gevraagd om gecombineerd gegevens te verwerken als bedoeld in artikel 11.4 van de Wet politiegegevens. Die opdracht wordt schriftelijk verleend volgens vast sjabloon en opgeslagen in de administratie van het onderzoeksteam.

Norm	Aspect		Bevinding en oordeel
			Hiermee wordt voldaan aan de Wpg.
32.3 voor 32.1.d en 32.1.h	Bewaren protocolgegevens 11.1, 11.2, 11.4 en 11.5		De gegevens worden opgeslagen in de map waar het onderzoek plaatsvindt (:O-Schijf). In geval van grotere rechercheonderzoeken wordt bij aanvang van het onderzoek aan de Officier van Justitie opdracht gevraagd om gecombineerd gegevens te verwerken als bedoeld in artikel 11.4 van de Wet politiegegevens. Die opdracht wordt schriftelijk verleend volgens vast sjabloon en opgeslagen in de administratie van het onderzoeksteam. De protocolleringen worden bewaard bij de desbetreffende onderzoeksdossiers en vormen een onderdeel van de dossiers inclusief de daarvoor geldende bewaartermijnen. Hiermee wordt voldaan aan de Wpg.
Artikel 14, Bewaartermijnen			
8.2 en 8.3	(8) van 1 tot 5 jaar		Tijdens ons onderzoek waren er geen geautomatiseerde faciliteiten aanwezig om het onderscheid tussen politiegegevens jonger dan 1 jaar versus tussen de 1 en 5 jaar af te dwingen. Hiermee wordt niet voldaan aan de Wpg
8.6	(8) verwijderen na 5 jaar		Verwijdering na 5 jaar is nog niet aan de orde aangezien de informatie in BVH van korps Zuid-Holland Zuid niet ouder is dan drie jaar in verband met de overgang van BPS naar BVH. De informatie van BPS (die ouder is dan 5 jaar) is zeer beperkt inzichtelijk. Er is echter nog geen proces opgesteld om politiegegevens te verwijderen. Het korps heeft wel een voorstel opgesteld om alle BPS-gegevens na 5 jaar te verwijderen waarna alleen de privacyfunctionaris en de Infodesk toegang tot hebben. Dit voorstel is nog niet geëffectueerd. Hiermee wordt deels voldaan aan de Wpg.
14.1 (8)	(8) vernietigen na 5 jaar verwijderd		Landelijk is geadviseerd het mechanisme voor vernietiging in BVH 1.2.2 niet te activeren. Het korps heeft een voorstel opgesteld om de gegevens van BPS na 5 jaar te verwijderen. Het voorstel voorziet niet in een vernietigingsproces. Hiermee wordt niet voldaan aan de Wpg.
9.4	(9) verwijderen na OH plus ½ jaar		Het Openbaar Ministerie heeft samen met het korps Zuid-Holland Zuid geen proces ingericht voor het afmelden van artikel 9 onderzoeken. Echter in afwezigheid van een initiatief vanuit het OM, verifieert het korps jaarlijks de status van on-

Norm	Aspect	Bevinding en oordeel
		derzoeken bij het OM. Dit is een goed initiatief, maar voldoet nog niet aan de frequentie van verwijdering maximaal na ½ jaar na het OH-moment. Het OM geeft geen consequente terugkoppeling. Hiermee wordt niet voldaan aan de Wpg. Het korps maakt hierbij de volgende kanttekening: <i>'Enerzijds is het praktisch onmogelijk om te schonen op onderzoeken. Het OM behandelt namelijk geen onderzoeken, maar vervolgt verdachten. Veel zaken worden gesplitst of gevoegd. Zo kan de ene verdachte snel worden geseponneerd, terwijl de andere voortvluchtig blijft. De wetgever heeft zich daarvan geen rekenschap gegeven. Ten tweede noemt de wet geen schoningstermijn. Gegevens kunnen worden verwerkt zolang als nodig is voor het onderzoek. De MvT geeft als voorbeeld dat kan worden gedacht aan verklaring of OH-vonnis. De auditor legt dit voorbeeld te eng uit. Geregeld beoordelen de recherchechefs of het nog nodig is om onderzoeken te bewaren en geregeld gaat men over tot vernietiging. Zo is recent heel RBS geschoond.'</i>
14.1 (9)	(9) vernietigen na 5 jaar verwijderd	Het Openbaar Ministerie heeft samen met het korps Zuid-Holland Zuid geen proces ingericht voor het afmelden van artikel 9 onderzoeken. Echter in afwezigheid van een initiatief vanuit het OM, verifieert het korps jaarlijks de status van onderzoeken bij het OM. Dit is een goed initiatief. Aangezien eenmaal per jaar bij het OM wordt geverifieerd of het OH-moment reeds heeft plaatsgevonden, is inzichtelijk welke zaken voor vernietiging in aanmerking komen. Aangezien het schoningsscript in BVO nog niet is geactiveerd, heeft het korps een eigen werkwijze ingericht. Zodra een artikel 9-onderzoek in BVO dient te worden geschoond, wordt de bevoegde functionaris van het desbetreffende onderzoek in kennisgesteld. Deze kan ervoor zorgen dat de map van dit onderzoek ook op de O-schijf wordt geschoond. Hiermee wordt voldaan aan de Wpg.
10.6	(10) verwijderen na 5 jaar geen subjectwaardige registratie	De chef RID en CIE binnen Zuid-Holland Zuid zijn aangewezen om er zorg voor te dragen dat artikel 10-vastleggingen op de O-schijf worden verwijderd binnen de hiervoor gestelde termijnen. Tevens zien ze ook toe op de doelmatigheid van vastgelegde informatie. Subjectmatige registratie wordt om de

Norm	Aspect	Bevinding en oordeel
		vier maanden nagelopen en beoordeeld op doelmatigheid en controle op tijdige verwijdering. Hiermee wordt voldaan aan de Wpg.
14.1 (10)	(10) vernietigen na 5 jaar verwijderd	De chef RID en CIE zijn binnen Zuid-Holland Zuid aangewezen om er zorg voor te dragen dat artikel 10-vastleggingen op de O-schijf worden verwijderd binnen de hiervoor gestelde termijnen. Hiermee wordt voldaan aan de Wpg.
14.3	Hernieuwde verwerking	Wanneer de wens is dat gegevens vanuit de archiefomgeving worden opgevraagd, dient dit te gebeuren middels een aanvraag bij de privacyfunctionaris. De privacyfunctionaris toetst deze aanvraag op doel en noodzaak voor de afweging om het wel of niet laten inzien van opgevraagde gegevens uit de archiefomgeving. Hiermee wordt voldaan aan de Wpg.
32.1.e	Protocollering 14.3	De protocolgegevens worden bewaard door de privacyfunctionaris en heeft alleen toegang tot deze gegevens. Hiermee wordt voldaan aan de Wpg.
32.3 voor 32.1.e	Bewaren protocolgegevens 14.3	De protocolgegevens worden bewaard door de privacyfunctionaris en heeft alleen toegang tot deze gegevens. De privacyfunctionaris heeft een overzicht vanaf 2007. Hiermee wordt voldaan aan de Wpg.
12.2	(12) verwerken na 4 maanden	Informatie wordt binnen een termijn van maximaal 4 maanden verwerkt en netto in een andere omgeving gezet. Dit zit vast in de werkwijze van de CIE. Hiermee wordt voldaan aan de Wpg.
12.6	(12) controleren en vernietigen	De chef RID en CIE zijn binnen Zuid-Holland Zuid aangewezen om er zorg voor te dragen dat de vastleggingen op de O-schijf worden verwijderd binnen de hiervoor gestelde termijnen. Hiermee wordt voldaan aan de Wpg.
Artikel 15, Ter beschikking stellen		
• Infodesk voor bevraging		De Infodesk maakt onderdeel uit van de Dienst Recherche Expertise en Ondersteuning (DREO). Deze is herkenbaar gepositioneerd met een eigen leiding. De afdeling Infodesk is in tweeën gesplitst waarvoor de chef Infodesk en de informatiecoördinator beide hun eigen takenpakket hebben. Bij de Infodesk wordt controle uitgevoerd op het Wpg-geschied van de informatie. Verzoeken worden gedaan middels een vast formulier beschikbaar op intranet, dit formulier bevat tevens de noodzaak voor doelomschrijving en reden van aanvraag. Hiermee wordt voldaan aan de Wpg.

Norm	Aspect	Bevinding en oordeel
• Codering		In BVO zijn coderingen vastgesteld die aan een mutatie gehangen dienen te worden. Hiermee wordt voldaan aan de Wpg.
• Aanwijzing Bevoegd Functionaris		De bevoegde functionarissen zijn aangewezen. Er is duidelijk aangegeven bij welke bevoegdheid de bevoegde functionarissen horen en dus welke personen kunnen worden geraadpleegd voor Wpg-vragen. Hiermee wordt voldaan aan de Wpg.
• Opleiding Bevoegd Functionaris		Er is geïnvesteerd in het personeel in het algemeen ten aanzien van de bekendheid van de Wpg. De bevoegde functionarissen zijn opgeleid en fungeren als Wpg-vraagbaak. Hiermee wordt voldaan aan de Wpg.
15.2	Weigeringgronden	De bevoegde functionarissen zijn getraind in de Wpg. De weigeringgronden zijn niet expliciet vastgesteld, maar door de noodzaak om informatieverzoeken te motiveren kunnen de Infodesk medewerkers de verzoeken toetsen op de noodzaak in relatie tot de doelbinding. Hiermee wordt voldaan aan de Wpg.
Artikel 16 t/m 24, Verstrekking		
• Verstrekkingwijzer (landelijk)		De landelijke verstrekkingwijzer wordt gehanteerd. Hiermee wordt voldaan aan de Wpg.
• Proces voor convenanten		Het korps heeft de convenanten geïnventariseerd. De convenanten zijn de afgelopen periode Wpg-geschikt gemaakt waarbij de wettelijk vereiste informatie is opgenomen. Het korps heeft een 10-stappenplan (het sjabloon) opgericht voor de totstandkoming van Wpg-geschikte convenanten, inclusief een geheimhoudingsclausule voor toekomstige convenanten. Daarmee is het proces voor convenanten in opzet, bestaan en werking aangetoond. Hiermee wordt voldaan aan de Wpg.
• Proces voor Artikel 20 Besluiten		Het korps heeft een handleiding opgesteld met de 10 geboden voor artikel 20-besluiten. De districtchefs zijn uiteindelijk verantwoordelijk voor de goedkeuring van een artikel 20-besluit. Het implementatieteam heeft bij inventarisatie geconstateerd dat een aantal artikel 20-besluiten niet Wpg compliant zijn. Het korps heeft een model ontwikkeld om een uitwisselingsbesluit ex artikel 20 Wpg te splitsen van samenwerkingsconvenanten (niet Wpg-relevant). Deze methodiek zal worden gebruikt voor de huidige convenanten die niet voldoen aan de Wpg. Het korps maakt de volgende kanttekening: 'In 2009 zijn alle convenanten geïnventariseerd conform het implementatieplan WPG. Veel daarvan waren niet WPG relevant, een ander deel werd niet meer gebruikt. Slechts één convenant bleek WPG-

Norm	Aspect	Bevinding en oordeel
		<i>proof. Dat is het enige convenant dat in stand is gebleven. Alle daarna afgesloten convenanten zijn en worden centraal getoetst door of namens de portefeuillehouder WPG en het OM.'</i> Hiermee wordt voldaan aan de Wpg.
• Verstrekkingenschema (regio)		Tijdens de opleidingen en in de interne communicatie is de verstrekkingprocedure steeds toegelicht. Daarbij is ook ingegaan op het vastleggen (het protocolleren) van deze verstrekking in BVH door middel van I90-formulieren. Artikel 19-verstrekkingen dienen volgens de Korps Zuid-Holland Zuid procedure te worden geregistreerd in zogeheten I90-formulieren. Voor een dergelijke verstrekking is toestemming van de burgemeester of Officier van Justitie nodig. Er vindt geen directe controle op incidentele gegevensverstrekking plaats binnen Zuid-Holland Zuid. De verzoeken die door externe partners aan de politie worden gedaan komen bij de privacyfunctionaris van het korps terecht. Deze verzoeken en eventuele verstrekkingen die hieruit voortvloeien worden opgeslagen en gearhiveerd in de applicatie Corsa. Hiermee wordt voldaan aan de Wpg.
• Proces voor geautomatiseerde verstrekking		Er vindt binnen politieregio Zuid-Holland Zuid geen geautomatiseerde verstrekking plaats. Deze bepaling is niet van toepassing.
7.2	Geheimhouding	Bij alle schriftelijke verstrekkingen wordt aangegeven dat de informatieontvanger een geheimhoudingsplicht heeft. De geheimhouding over de verstrekte informatie wordt bij de verstrekkingen geëist. Hiermee wordt voldaan aan de Wpg.
32.1.f	Protocollering verstrekking	Voor veel verstrekkingen is er een procedure zoals Haltverstrekkingformulieren, AMK-meldingsformulieren, bestuurlijke rapportages en externe informatieverzoeken in Corsa en het registratiesysteem van de infodesk (BIBOB) etc. Alleen verstrekkingen op basis van artikel 19 en soms 20 worden met I90 vastgelegd in BVH. In opzet is de protocollering van de verstrekking door middel van I90-formulieren goed geregeld. Een procesuitleg is beschikbaar voor Blauw. Echter bij toetsing van de werking blijkt dat het I90-formulier niet door iedereen structureel wordt ge-

Norm	Aspect		Bevinding en oordeel
			bruikt. 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. De privacyfunctionaris is wel betrokken bij het beoordelen van de binnenkomende verstrekkingverzoeken van buiten de politie. Deze verzoeken worden geregistreerd in Corsa. Het gebruik van het I90-formulier is summier. Het korps heeft hiertoe tijdens de opleidingen en trainingen extra aandacht aan besteed. Hiermee wordt deels voldaan aan de Wpg.
32.3 voor 32.1.f	Bewaren protocolgegevens verstrekking		Door de privacyfunctionaris wordt er een overzicht bijgehouden van artikel 18, 19 en 20 Wpg verstrekkingen. Deze protocolgegevens worden voor een periode van vijf jaar bewaard. Deze periode geldt tevens voor de verstrekkingen die worden aangehouden in Corsa. Hiermee wordt voldaan aan de Wpg.
	• Toezicht door leidinggevend op verstrekkingen en protocollering		Het toezicht van verstrekkingen wordt gedaan door de chefs en vormt onderdeel van het verstrekkingproces. Verstrekkingen dienen schriftelijk te geschieden en te worden ondertekend door een leidinggevende. Hiermee wordt voldaan aan de Wpg.
Artikel 25 t/m 31, Rechten van de betrokkene			
25.1	Verzoek om kennisgeving		De inzageprocedure bij korps Zuid-Holland Zuid is uitgewerkt en verloopt conform de Wet politiegegevens. De inzageverzoeken worden aan de privacyfunctionaris voorgelegd. Hiermee wordt voldaan aan de Wpg.
28.1 t/m 28.3	Correctie		De correctieprocedure bij korps Zuid-Holland Zuid is goed uitgewerkt en verloopt conform de Wet politiegegevens. Er zijn in 2010 twee klachten geweest, deze zijn beide afgehandeld. Echter, het korps heeft geen proces ex artikel 30 Wpg ingericht voor het op de hoogte stellen van alle partijen aan wie de initiële (niet-gecorrigeerde) verstrekking is gedaan. Het korps is hiervan op de hoogte. Hiermee wordt deels voldaan aan de Wpg.

Norm	Aspect		Bevinding en oordeel
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 rechercheonderzoek binnen Korps Zuid-Holland Zuid wordt aangevraagd middels een aanvraagformulier voor een BVO-registratie (MRO). Deze formulieren komen per e-mail terecht bij de privacyfunctionaris zodat deze formulieren worden bewaard. Op basis van de gegevens van de privacyfunctionaris werden er in 2009 (203) en in 2010 (109) rechercheonderzoeken (zogenaamde artikel 9 Wpg-zaken) aangemeld. Echter werden er geen artikel 9 Wpg-zaken afgemeld. De privacyfunctionaris geeft aan dat dit overzicht "verre van volledig" is. Echter, het korps heeft hier invulling aan gegeven door het opstellen van een 'CHECKLIST START ONDERZOEK art 9 WPG'. Hiermee wordt voldaan aan de Wpg.
32.3 voor 32.1.a	Bewaren protocolgegevens doel onderzoek		Het doel van onderzoek wordt vermeld in de MRO, tevens maakt de recherchecoördinator op de O-schijf (artikel 9-map) een map aan met het desbetreffende BVO-nummer. De gegevens van het doel van het onderzoek worden bewaard voor de termijn van vijf jaar. Hiermee wordt voldaan aan de Wpg.
13.4 en 32.1.b	Protocollering Artikel 13 gegevensverzamelingen		Voor protocollering van artikel 13-gegevensverzamelingen maakt korps Zuid-Holland Zuid gebruik van de applicatie Amazone. In Amazone worden doelgroepen gedefinieerd, inclusief het daarbij behorende Wpg-regime zoals artikel 13 Wpg. Hiermee wordt voldaan de Wpg.
32.3 voor 32.1.b	Bewaren protocolgegevens Artikel 13 gegevensverzamelingen		De aanvragen voor een doelgroep in Amazone worden gearhiveerd. Tevens wordt de termijn bepaald dat er gegevens van een dergelijke doelgroep worden vastgelegd in Amazone. Voor het aanvragen van een doelgroep wordt de format gebruikt zoals deze in Rotterdam-Rijnmond is ontwikkeld. Hiermee wordt voldaan aan de Wpg.
32.1.g	Protocollering onrechtmatige handeling		Wanneer verwerkingen hebben plaatsgevonden die door onbevoegden zijn gedaan of anderszins onrechtmatig zijn verricht, wordt dit gemeld bij de privacyfunctionaris. De privacyfunctionaris legt deze gemelde incidenten vast in het zogeheten 'zwartboek' waardoor een overzicht van deze meldingen aanwezig is.

Norm	Aspect		Bevinding en oordeel
			Hiermee wordt voldaan aan de Wpg.
32.3 voor 32.1.g	Bewaren protocolgegevens onrechtmatige handeling		Wanneer er verwerkingen hebben plaatsgevonden die door onbevoegden zijn gedaan of anderszins onrechtmatig zijn verricht, wordt dit gemeld bij de privacyfunctionaris. De privacyfunctionaris legt deze gemelde incidenten vast in het zogeheten 'zwartboek' waardoor een overzicht van deze meldingen aanwezig is. Het zogeheten 'Zwartboek' wordt door de privacyfunctionaris bijgehouden en bewaard. Hiermee wordt voldaan aan de Wpg.
32.2	Gemeenschappelijke verwerking		Er is geen gemeenschappelijke verwerking getroffen waar korps Zuid-Holland Zuid deel van uit maakt. Deze bepaling is hierbij niet van toepassing.
Artikel 33, Audits			
RPAP 3.1	Interne audit-functie		Ten tijde van de audit was geen interne audit-functie ingericht. Het korps heeft in november 2011 een interne auditor aangewezen die de interne privacy audits gaat uitvoeren in 2012. Deze gaat zich tevens bezighouden met het implementeren van de Wpg. Hiermee wordt deels voldaan aan art. 33 Wpg.
RPAP 3.4	Interne audit-plan		De afgelopen jaren is geen intern audit-plan opgesteld. Het korps stelt dat de bevindingen vanuit deze privacy audit mede zullen worden gebruikt voor het opstellen van het interne audit-plan. Hiermee wordt niet voldaan aan de Wpg.
RPAP 3.6	Interne audit-rapport		De afgelopen jaren is geen intern audit-rapport opgesteld. Hiermee wordt niet voldaan aan de Wpg.
Artikel 34, Privacyfunctionaris			
34.1 en 34.4	Benoemd en gemeld		Er is een privacyfunctionaris bij korps Zuid-Holland Zuid aangewezen in 2009 en aangemeld bij het CBP. Hiermee wordt voldaan aan de Wpg.
34.2	Overzicht over protocollering		De privacyfunctionaris houdt een aantal overzichten bij met betrekking tot de protocollering, maar deze is verre van compleet (in aantal) en volledig (in soorten protocollen). Het proces voor het verkrijgen van inzicht in de vastlegging van de protocollering is in opzet beschreven, echter de werking is niet geborgd. Dit is reeds opgemerkt door de privacyfunctionaris.

Norm	Aspect		Bevinding en oordeel
			De privacyfunctionaris heeft geen totaaloverzicht van alle artikel 11-verwerkingen. Deze worden decentraal aangehouden bij de desbetreffende onderzoeken. Hiermee wordt deels voldaan aan de Wpg.
34.3	Jaarverslag		De privacyfunctionaris heeft een concept jaarverslag opgesteld over 2009-2010 met daarin de bevindingen. Dit jaarverslag is echter niet aangeboden aan de korpsleiding, die daardoor niet heeft kunnen reageren op de gerapporteerde verbeterpunten. De privacyfunctionaris komt niet toe aan al de toezichthoudende taken. Hiermee wordt deels voldaan aan de Wpg.
Optioneel Artikel 36, Functionaris Gegevensbescherming			
36.1 en 36.2	Benoemd		Niet van toepassing. Er is geen functionaris gegevensbescherming benoemd.
Wbp 63.3	Gemeld		Niet van toepassing. Er is geen functionaris gegevensbescherming benoemd.
Wbp 64.1 t/m 64.4	Toezichthoudende rol		Niet van toepassing. Er is geen functionaris gegevensbescherming benoemd.

3 Inleiding

3.1 Algemeen

In opdracht van de landelijke stuurgroep Wpg, waarin de Directeur-Generaal Politie en het KBB zijn vertegenwoordigd, heeft de DAD van het ministerie van VenJ een privacy audit uitgevoerd bij het korps Zuid-Holland Zuid zoals de Korpsbeheerders deze, uit hoofde van de Wpg, twee jaar na inwerkingtreding van de wet dienen te laten uitvoeren (Wpg artikel 33 lid 1).

De opdracht is beschreven in het document 'Plan van aanpak Audit Wet Politiegegevens' d.d. 08-09-2011 met kenmerk DAD/DDS/2011/5706209. De audit is uitgevoerd bij het korps Zuid-Holland Zuid in 2011.

3.2 Aanleiding

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

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

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

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

3.3 Doelstelling, aard en scope van de opdracht

Doelstelling

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

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

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

korps Zuid-Holland Zuid beoogt te voldoen aan de beheersdoelstellingen die bij of krachtens de Wpg gelden.

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

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

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

3.4 Afbakening

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

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

3.5 Normenkader

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

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

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

3.6 Beperkingen voor de privacy audit

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

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

3.7 Onderzoeksmethoden en werkwijze

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

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

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

Het eindrapport is met inachtneming van het ontvangen commentaar vastgesteld.

3.8 Doelgroep van het rapport

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

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

De stuurgroep wordt voorgezeten door drs. 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 voor Politie Zuid-Holland Zuid.
- De korpschef van Politie Zuid-Holland Zuid.
- De Hoofd Officier van Justitie voor Politie Zuid-Holland Zuid.
- De privacyfunctionaris van Politie Zuid-Holland Zuid.
- De voorzitter van het College Bescherming Persoonsgegevens.

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

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

4 Bevindingen

4.1 Inleiding

De nieuwe Wet Politiegegevens (Wpg), die op 1 januari 2008 in werking is getreden, biedt meer armslag voor het gebruik van persoonsgegevens, voorziet in mogelijkheden om gegevens, die voor een bepaald doel zijn verwerkt, te gebruiken voor andere doelen en biedt meer mogelijkheden voor verstrekking van politiegegevens aan personen en instanties buiten de politiesector. Daarnaast voorziet de nieuwe wet in waarborgen voor de burger tegen ongerechtvaardigde inbreuken op diens persoonlijke levenssfeer.

4.1.1 *Regie en doorzettingsmacht voor de Wpg implementatie*

Het korps heeft een regionaal portefeuillehouder (plaatsvervangend KorpsChef, hierna: plv. KC) en een projectleider Wpg. De projectleider is aanspreekpunt voor Wpg-vragen, en bij velen bekend. De plv. KC is benoemd als portefeuillehouder voor de Wpg. De plv. KC heeft een projectleider aangesteld om de Wpg te implementeren en is tevens aanspreekpunt. De projectleider heeft hiervoor een implementatieteam van 12 personen aangesteld. In totaal zijn ongeveer 240 medewerkers van het korps Zuid-Holland Zuid opgeleid in de Wpg, dit betreft 20% van het korps. Een groot deel hiervan, de Wpg-sleutelfiguren zoals de teamchefs van de wijkpolitie en de beleidsmedewerkers, zijn door de projectleider zelf opgeleid.

Tevens zijn de bevoegde functionarissen aangewezen, zijn de convenanten geïnventariseerd en de medewerkers geïnstrueerd over de protocolplicht. Verder is veel energie gestoken in het opleiden van de medewerkers van het korps op het gebied van de wet- en regeling van de Wpg.

4.1.2 *Privacyfunctionaris*

De privacyfunctionaris is benoemd en aangemeld bij het CBP. De privacyfunctionaris voldoet niet aan alle vereisten van de Wpg en heeft zijn taken onvoldoende kunnen uitvoeren doordat teveel taken zijn belegd bij de privacyfunctionaris, waardoor onafhankelijk toezicht op de naleving van de Wpg in het gedrang is gekomen.

4.1.3 *Opzet en borging Wpg*

Opzet

Bij de beoordeling van de borging van de Wpg wordt een onderscheid gemaakt tussen opzet en bestaan enerzijds en de werking (borging in continuïteit) anderzijds. In opzet is de Wpg voldoende ingericht. Er is door het korps veel aandacht besteed aan het opzetten en inrichten van processen om te voldoen aan de Wpg. Op basis daarvan zijn onder andere convenanten, procedures en de autorisatiematrix opgesteld die aansluiten op de bepalingen van de Wpg.

Werking

Voor de toekomst moet nog aandacht worden besteed aan de borging in continuïteit van de opgezette processen. Dit houdt in dat moet worden vastgesteld dat de in opzet aanwezige procedures ook daadwerkelijk over een langere periode werken zoals die bedoeld zijn. Dit kan aan de hand van het opstellen van controlemaatregelen, audits en borging middels het INK-model, waarmee de werking van de Wpg in de politieprocessen aantoonbaar wordt gemaakt.

4.1.4 *Wpg met de praktijk*

De politiesystemen ondersteunen de Wpg onvoldoende:

1. Schoning vindt plaats in BVH en BVO.
2. Niet alle informatie kan in BVH of BVO worden opgeslagen (bijvoorbeeld foto's) waardoor uitwijk naar de kantoorautomatisering (O-schijf) nodig is om toch alle relevante gegevens te kunnen opslaan.
3. BVO bevat alleen artikel 9 informatie. BVH bevat artikel 8 informatie en artikel 9 informatie die door de bevoegd functionaris ter beschikking is gesteld voor verdere verwerking onder artikel 8. In de enkele gevallen waar dat niet zo is, wordt artikel 9 informatie in BVH-besloten verwerkt en hebben alleen direct geautoriseerden daar toegang toe.
4. Het registreren in BVH van het verstrekken van informatie via I90 wordt door sommige medewerkers als arbeidsintensief ervaren en gebeurt niet altijd.

Het kennisniveau van de Wpg bij Blauw op straat is niet optimaal. Blauw moet vooral weten onder welke voorwaarden een verstrekking kan worden gedaan en dat informatie zorgvuldig moet worden vastgelegd. Het vastleggen van de verstrekking gebeurt echter niet structureel. Dit is mede verklaarbaar doordat de protocolplicht door sommigen als arbeidsintensief wordt ervaren. Voornamelijk art. 11 lid 4 en 8 lid 3 Wpg worden in de praktijk niet als hanteerbaar beschouwd, mede door het ontbreken van een definitie van deze zoekmogelijkheden.

Doordat men onvoldoende op de hoogte is of informatie conform Wpg gedeeld mag worden, is men hierin te terughoudend. Dit speelt met name bij het Veiligheidshuis. Wanneer informatie met andere partijen moet worden gedeeld en men onzeker is welke informatie wel en welke informatie niet mag worden gedeeld dan komt het voor dat men zich voor de zekerheid hierin erg terughoudend opstelt.

4.2 Verantwoordelijke

Mandaatbesluit

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

Mandaat

De korpsbeheerder wordt in de Wpg aangewezen als verantwoordelijke. Eind 2007 heeft de korpsbeheerder mandaat verleend aan de korpschef, onder andere voor het ondertekenen van uitwisselingsbesluiten ex artikel 20 Wpg. In 2009 heeft de korpschef ondermandaat verleend aan de districtschefs voor wat betreft het ondertekenen van districtelijke besluiten. Verder heeft de korpsleiding een aanwijzingsbesluit genomen voor bevoegd functionarissen.

Ondermandatering

In januari 2011 is de mandaatregeling aangepast in die zin dat de bevoegdheid om uitwisselingsbesluiten ex artikel 20 Wpg namens de korpsbeheerder te ondertekenen is doorgemandateerd van de korpschef aan de districts- en divisiechefs.

Hiermee voldoet het korps aan de belegging van de verantwoordelijkheden conform de Wpg.

4.3 Kwaliteitsaspecten van politiegegevens (artikel 3 en 4)

4.3.1 Norm

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

4.3.2 Bevindingen

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

Onderscheid dagelijkse politietaak versus bepaald geval

Bij de start van een onderzoek wordt er op de O-schijf een aparte map aangemaakt. Via de zogeheten PAM-module maakt de bevoegde functionaris een map aan bestaande uit de onderzoeksnaam en het BVH-nummer dat de rechercheur aanlevert. Vervolgens hangt de bevoegde functionaris collega's eraan die in de map mogen werken.

Bij het Berovingen en Overvallen team (BOT) worden alle collega's aan alle zaken gehangen omdat ze aan meerdere zaken kunnen werken. Dit is nodig om flexibiliteit te bewerkstelligen. Indien een medewerker niet is geselecteerd voor een zaak, dan zijn de zaaksgegevens voor deze persoon niet inzichtelijk. Er worden ook recherche-assistenten toegevoegd om gegevens uit te lezen.

Bij Gerichte Opsporing (GO) wordt de digitale map minder gebruikt daar hier eenvoudiger of de 6 - uurszaken worden afgehandeld (art 8- zaken). Inmiddels is deze GO-afdeling ingericht als ZSM.

Bij het formeren van een Team Grootchalige Opsporing (TGO) worden zowel BVH, BVO als de digitale map op de O-schijf gebruikt.

Overgang artikel 8 naar 9

Wanneer een rechercheonderzoek start op het niveau van artikel 8 en overgaat naar artikel 9 wordt overlegd met de Officier van Justitie.

Afweging registratie BVH (8) versus BVO (9)

In BVO worden onder andere de taps geregistreerd. Er is een handleiding wanneer BVO moet worden toegepast. Als criteria worden gehanteerd voor artikel 9-zaken:

- Onderzoek duurt langer dan 40 uur
- En is gericht op feiten waarop in verzekeringstelling is toegestaan of
- er worden BOB-middelen ingezet.

Bij de uitrol c.q. overgang naar de O-schijf heeft korps Zuid-Holland Zuid deze criteria naar de medewerkers gecommuniceerd. Ook zijn deze criteria te vinden in de handreiking mappenstructuur.

De bevoegd functionaris maakt een startmutatie met een doel aan. De Officier van Justitie heeft dan reeds toestemming verleend. Voor de invoer is een standaard format aanwezig. Na de startmutatie wordt automatisch een Melding Recherche Onderzoek (MRO) gemaakt met personen, verdachten, locaties, telefoonnummers, voertuigen etc. Afhankelijk van de codering van de MRO wacht men eventuele vragen of een eventuele match af.

BVH wordt gezien als een werksysteem en bevat onder andere processen-verbaal (PV's) van bevindingen. BVO wordt gebruikt als registratiesysteem voor met name het gebruik van BOB-middelen. Het totaal maakt samen de zaak. Bij een TGO wordt alles wel dubbel gevuld. De TGO-verhoren worden in BVO geplakt.

Rechtmatigheid (8), Doelbinding, Noodzakelijkheid, Volledigheid, Juistheid

Rechtmatigheid

Het voldoen aan de bepalingen van de artikelen van de Wpg is een aangelegenheid waarin bijna alle geledingen van de politie zijn betrokken. Niettemin is in het bijzonder van belang dat het zwaartepunt van het voldoen aan deze criteria ligt bij de eerste vastlegging van gegevens. Daarvoor dragen registratie- en gegevensbeheerders de verantwoordelijkheid.

Uit de interviews blijkt dat men vooral doet aan 'gegevensbeheer achteraf'. Voor het samenstellen van een proces-verbaal vraagt men zich af: "kunnen we deze informatie gebruiken, ja of nee, is het 'betrouwbaar', ja of nee? Etc."

Doelbinding

De zorg voor kwaliteit in relatie tot de primaire processen krijgt vorm in een matrixmodel. De Infodesk heeft hierbij een makelaarsfunctie. Doordat het korps Zuid-Holland Zuid een relatief klein korps is, zijn de lijnen erg kort en is bijna iedereen binnen het korps op de hoogte van de lopende zaken.

De Infodesk controleert of informatievragen Wpg-proof zijn voordat deze worden beantwoord. Dit geschiedt zowel bij interne als externe verzoeken. Aangegeven wordt dat binnen BVH zowel artikel 8 als 9 politiegegevens staan. Om die reden is de afspraak gemaakt dat artikel 9 gegevens die in BVH staan impliciet door de bevoegd functionaris moeten zijn vrijgegeven voor verdere verwerking voor artikel 8.

Ten aanzien van gegevensbeheer en de kwaliteit van gegevens merken respondenten op dat daarover zorgen bestaan. Het delen van gegevens, het management van het beheer, criteria waaraan gegevens moeten voldoen en regelmatige controle zijn zaken die voor meer uitleg vatbaar zijn, zeker in de 'normale' processen. Respondenten merken op dat incidenten zijn voorgekomen voortvloeiend uit kwaliteitsproblemen met gegevens. De invoer wordt echter nu wel vrij strak gecoördineerd en gecontroleerd. Binnen de wijkpolitie is het nu nauwelijks nog een kwestie, binnen Opsporing zou het echter nog wel een probleem zijn.

De zorg voor het voldoen aan de kwaliteitcriteria zoals gesteld in artikel 3 en 4 Wpg is opgemerkt en vindt bij handhaving via *peer reviews* achteraf plaats.

DREO: Zoeken naar informatie via sporen

De technische recherche voert forensische onderzoeken uit en legt deze vast middels een proces-verbaal in BHV. Daarnaast worden de sporen uit het onderzoek vastgelegd op een cd-rom en overgedragen aan de betreffende teamleider van het onderzoek. De verschillende onderzoekstappen worden beschreven als: zoeken, vastleggen, verwerken, veredelen, dader bijhalen, PV opstellen en overdracht.

Met betrekking tot artikel 3 en 4 Wpg is hierbij relevant:

- De aangetroffen sporen tijdens een onderzoek worden middels een PV vastgelegd in BVH en Landelijk Sporen Volgsysteem (LSV). Dit zijn complexe systemen.

- Voorheen moesten de spoorgegevens dubbel worden ingevoerd. Met het huidige release van LSV worden de gegevens automatisch overgenomen, waardoor de volledigheid beter is geborgd.
- Omdat LSV voor 80% een management systeem is functioneert dit systeem binnen de politie onvoldoende. Als voorbeeld wordt aangegeven dat wanneer een spoor het pand verlaat dit niet eenvoudig is terug te vinden in het systeem. Het systeem biedt niet de mogelijkheid om een spoor eenvoudig uit te boeken.

Naast LSV wordt ook het TRIS, sporencoördinatie en sporenopslag systeem, binnen het korps Zuid Holland Zuid toegepast. Dit systeem wordt door bijna heel Nederland gebruikt.

Wanneer er een spoor wordt aangetroffen wordt deze voorzien van een sticker met een uniek nummer. Dit unieke nummer wordt vastgelegd in het LSV. De sporen (alleen vingerafdrukken en DNA) worden ingelezen bij Rotterdam / Zoetermeer en altijd als extra controle op de hit, nagekeken door een ander korps.

- Foto's van sporen worden door de 1 uur service, ter plaatste bij het korps Zuid Holland Zuid, afgedrukt en digitaal opgeslagen op cd-roms.
- De cd-rom wordt vervolgens overgedragen aan de betreffende teamleider van een onderzoek.
- Na teruggave van de cd-rom wordt deze opgeborgen in de hiervoor bestemde kluis.
- Audiovisueel materiaal mag maximaal tien jaar opgeslagen blijven. De medewerker ziet hier samen met de chef op toe.

Wpg-gegevens kluis

In de kluis wordt digitaal fotomateriaal opgeslagen van foto's die de Unit Forensische Opsporing (UFO) maakt op plaatsen delict / sporen op verzoek van de tactische recherche (opsporing). Hier staan geen persoonsgegevens op en/of gegevens die direct te herleiden zijn naar een natuurlijk- of rechtspersoon. Korps Zuid-Holland Zuid is van plan nog een extra controle uit te voeren op de inhoud van deze kluis om na te gaan of hier daadwerkelijk politiegegevens in de zin van de Wpg worden opgeslagen, en zodoende hier opvolgend waarborgen voor te organiseren in de lijn met de Wpg. Het team is verder verantwoordelijk voor de controle op bewaartermijnen.

Overdracht van informatie aan andere researcheteams en samenwerking

De technische recherche wordt regelmatig ingezet als ondersteuning bij de tactische recherche. Dit betreft regelmatig een inval die van te voren wordt ingepland.

- Middels een proces-verbaal in BVH, zoals bovenstaand beschreven worden de sporengegevens door de technische recherche vastgelegd.
- De vastlegging van het proces-verbaal wordt door twee functionarissen gecontroleerd op juistheid en volledigheid. Deze informatie wordt uiteindelijk gebundeld met de registratie van de tactische recherche.

Volledigheid en juistheid

De meeste informatie (meldingen) komt binnen bij de meldkamer en worden altijd geregistreerd in Geïntegreerd Meldkamer Systeem (GMS) op basis van de NAW-gegevens. Door de medewerker van de meldkamer wordt deze melding doorgezet naar een 'tussenbak', ofwel zogeheten GMS-meldingen. De collega's die zijn ingezet op de melding halen de melding op uit de tussenbak en zetten deze door naar de BVH met een Maatschappelijke klasse die van toepassing is op het incident. Dit laatste gebeurt handmatig.

Wanneer de melding in GMS is afgesloten wordt deze automatisch gekopieerd naar BVH. Dit gebeurt *continu*. Vanuit de meldkamer wordt zelf nauwelijks in BVH geregistreerd.

Gebruik van TrueBlue

TrueBlue is een tool waarmee BVH wordt gecontroleerd op invoerfouten. De chefs ICC hebben afspraken gemaakt over gegevensbeheer ten aanzien van BVH. De chefs accorderen de kennisregels van TrueBlue:

- Bij geconstateerde foutieve registraties wordt een signalering gestuurd naar de medewerker die de invoer heeft verricht. De desbetreffende medewerker dient zelf zorg te dragen voor de correctie van de foutieve invoer. De foutmeldingen gerelateerd aan de foutieve registraties worden automatisch verstuurd via TrueBlue;
- De districten ontvangen de lijsten met openstaande foutmeldingen. De districten geven aan welke medewerkers ziek, langdurig afwezig, of uit dienst zijn. De districten zijn verantwoordelijk om deze overzichten bij te houden.

Binnen alle diensten van de regio (district 1 t/m 3, DREO, DUO) is een controller aangewezen als kwaliteitscontroleur van BVH. Deze kwaliteitscontroleur loopt de rappellijst na van de TrueBlue-meldingen die openstaan binnen het desbetreffende district of dienst. Op deze manier ziet de kwaliteitscontroleur toe op het opvolgen van meldingen omtrent invoerfouten in BVH.

De kwaliteitscontroleurs zijn daarnaast aanspreekpunt voor de medewerkers die een TrueBlue melding ontvangen, en zijn hun vraagbaak wanneer het niet lukt om de invoerfouten te herstellen. Tevens rappelleert de kwaliteitscontroleur aan de leidinggevende van de medewerker wanneer deze al lange tijd een TrueBlue-melding heeft openstaan.

In de periode van juni tot oktober 2011 hebben alle gebruikers van BVH een verplichte kwaliteitsdag BVH gevolgd die tevens diende als BVH-opfriscursus. Tijdens deze dag zijn de medewerkers ook gewezen op het afhandelen van TrueBlue meldingen en is duidelijk gemaakt bij wie zij terecht kunnen mocht het niet lukken om een TrueBlue melding op te volgen.

Het korps Zuid-Holland Zuid heeft een front-backoffice (FOBO) gerealiseerd waar Formutra's worden vastgelegd voor de noodhulpeenheden. Bij de invoer door de FOBO wordt sterk gelet op kwaliteit. Dat heeft er onder andere toe geleid dat verkeerde toepassing van de code voor "overige zaken" is teruggebracht tot minder dan 1 procent.

Rechtmatigheid (9), Doelbinding, Noodzakelijkheid, Volledigheid, Juistheid

Doelbinding & noodzakelijkheid

Bij de Infodesk wordt er controle uitgevoerd op het Wpg-geschikt zijn van de informatie. Deze controle vindt steekproefsgewijs plaats.

Volledigheid en juistheid

Er wordt door de rechercheur altijd een startmutatie aangemaakt, waarin de (zaak) Officier van Justitie en de bevoegde functionaris/teamleider staan vermeld. De Officier van Justitie heeft in dit geval al toestemming verleend om met de zaak te starten.

Voor de invoer is een sjabloon aanwezig. Na de startmutatie wordt een MRO gemaakt welke wordt aangevuld met verdachten, locaties, telefoonnummers, voertuigen etc.

Personen met NAW-gegevens worden in BVO vastgelegd, inclusief het Burger Service Nummer (BSN). Door middel van het BSN heeft de politie een unieke zoeksleutel voor het vinden van relaties. Tevens kan het BSN worden gebruikt als controlemiddel. De politie kan in het GBA inloggen om via het BSN de gegevens van verdachten te controleren, echter gebeurt dit lang niet altijd wegens tijdgebrek. Ondanks het gebruik van de Personenserver kan er enige vervuiling ontstaan door verschrijvingen van de naam.

BVO is niet gebruikersvriendelijk en het is onduidelijk wat waar ingevuld moet worden om het systeem goed te laten functioneren. Tevens kost het veel moeite en kennis om bij bepaalde gegevens te komen. BVO is extra werk voor een rechercheur. Naast het opstellen van zijn proces-verbaal, moet de rechercheur sinds de komst van BVO ook zijn recherchegegevens ontsluiten voor anderen. Dit extra werk wordt als ongewenst beschouwd. Dat het moeite kost om bij de gegevens te komen heeft volgens het korps ook met een juiste toepassing van de WPG te maken. Rechercheurs mogen niet direct in andere onderzoeksgegevens. Daarvoor is tussenkomst nodig van de infodesk.

Tussen BVH en BVO kunnen geen gegevens worden overgehaald en kunnen er geen relaties worden aangelegd zodat automatisch van het ene systeem naar het andere kan worden gegaan. Indien het toch nodig geacht wordt gegevens van BVH over te zetten naar BVO dan dient dit handmatig te worden gedaan.

Binnen Opsporing zijn de researchecoördinatoren verantwoordelijk voor de kwaliteit van de invoer en het verwerken van gegevens. Bij hen berust tevens de taak om de medewerkers aan te spreken wanneer het ontbreekt aan kwaliteit betreffende de invoer en verwerking van politiegegevens van een medewerker. Incidenten met betrekking tot het invoeren van gegevens komen aan het licht via bijvoorbeeld de tool TrueBlue of via terugkoppeling vanuit het OM omtrent het aangeleverde PV of dossier.

De ICC-afdeling van de desbetreffende diensten zetten naar aanleiding van de invoer van gegevens de zaken uit aan de diverse afdelingen in de districten. De operationeel leidinggevenden coördineren de zaken, wijzen zaken toe aan medewerkers, bewaken de voortgang en toetsen de kwaliteit van de gegevens en spreken waar nodig de medewerkers aan wanneer er opmerkingen zijn met betrekking tot de kwaliteit van de gegevens. Hier behoort ook de controle op juistheid en nauwkeurigheid van politiegegevens thuis (artikel 4 lid 1 Wpg).

Daarnaast kan er vanuit het OM ook terugkoppeling plaatsvinden met betrekking tot de inhoudelijke kwaliteit van een product (in veel gevallen dus politiegegevens verwerkt in processen-verbaal die bij het OM zijn aangeleverd). Deze terugkoppeling is gericht aan de coördinatoren (leidinggevende) van het desbetreffende onderdeel dat het product heeft aangeleverd. Van deze leidinggevende wordt verwacht dat er opvolging gegeven wordt aan de op- of aanmerkingen die vanuit het OM gedaan worden.

Verantwoordelijkheid kwaliteit gegevens

Bij korps Zuid-Holland Zuid zijn verschillende verantwoordelijken aangewezen met betrekking tot de kwaliteitszorg. De afdeling Control Stafbureau korpsleiding is belast met de algehele controle op kwaliteitszorg. Binnen de korpsleiding is dat de

portefeuillehouder kwaliteitszorg. Binnen het staffbureau zijn diverse medewerkers met onderdelen van de kwaliteitszorg belast.

De zorg voor kwaliteit in de relatie tot de primaire processen krijgt vorm in een matrixmodel. De Districtchef is verantwoordelijk. Programmasturing is een belangrijke ontwikkeling dat op dit moment loopt in het korps.

Ten aanzien van gegevensbeheer en de kwaliteit van gegevens merken respondenten op dat daarover zorgen bestaan. Het delen van gegevens, het management van het beheer, criteria waaraan gegevens moeten voldoen en regelmatige controle zijn zaken die voor meer uitwerking vatbaar zijn, zeker in de 'normale' processen. Respondenten merken op dat incidenten zijn voorgekomen voortvloeiend uit kwaliteitsproblemen met gegevens.

Respondenten geven te kennen dat men doet aan 'gegevensbeheer achteraf'. Voor het samenstellen van een proces-verbaal vraagt men zich af: "kunnen we deze informatie gebruiken ja of nee, is het betrouwbaar".

Voor Team Grootschalige Onderzoeken (TGO's) zijn de journaals die in BVO gemaakt kunnen worden niet overzichtelijk. Daarom is besloten de vastlegging van de journaals vast te leggen op de O-schijf. Alleen functionarissen die geautoriseerd zijn voor een betreffend onderzoek kunnen bij deze map.

De verantwoordelijkheden met betrekking tot de kwaliteit van de gegevens is bij korps Zuid-Holland Zuid goed belegd. Echter, uit de gesprekken blijkt dat er nog steeds zorgen bestaan omtrent de kwaliteit van de gegevens. Niet vooraf, maar achteraf vindt er controle plaats waardoor het risico dat foute registraties niet worden gecorrigeerd bestaat. Middels preventieve kwaliteitsmaatregelen kunnen meer foute registraties worden voorkomen.

Hoewel er verantwoordelijken zijn aangewezen blijkt de maatregel niet effectief aangezien een aantal incidenten zijn geregistreerd. Er kan dan ook niet worden geoordeeld dat de kwaliteitszorg bij Zuid-Holland Zuid als effectief bestempeld kan worden. Hiermee wordt niet volledig voldaan aan de Wpg.

Reactie van het korps op het bovenstaande

Op 19 december 2011 heeft het korps de volgende reactie verstrekt, die wij hier integraal opnemen:

*Voor de controle op de kwaliteit van de invoer van gegevens zijn er binnen ZHZ een aantal **signaleringsinstrumenten** ingericht. Op het staffbureau van de korpsleiding zijn controllers aanwezig die zijn belast met de kwaliteitszorg. Steekproefsgewijs voeren zij controle uit op de kwaliteit van ingevoerde gegevens in BVH/BVO.*

Daarnaast zijn op de Informatie en Coördinatie Centra (ICC's) binnen de districten en diensten gegevensbewerkers aanwezig die als kwaliteitscontroleur van de ingevoerde mutaties in BVH toezicht op de kwaliteit van de invoer houden. Zij zien toe op een juiste invoer en signaleren onjuiste of dubbel ingevoerde persoonsgegevens of mutaties. Op de ICC's binnen de districten en diensten wordt alle invoer gecontroleerd, hier worden namelijk ook de zaken waar een vervolg op moet komen worden uitgezet naar de afdelingen binnen de districten.

Wanneer de kwaliteitscontroleurs van het stafbureau of op de ICC's incidenten waarnemen/signaleren met betrekking tot gegevensinvoer, dan wordt dit gecommuniceerd met de direct leidinggevende van de invoerende collega. Deze leidinggevende zorgt ervoor dat er opvolging wordt gegeven aan de melding van de kwaliteitscontroleurs.

Daarnaast wordt Trueblue als signaleringsinstrument gebruikt. Eerder in dit rapport is het gebruik van TrueBlue en de opvolging die aan de melding worden gegevens reeds toegelicht.

Tot slot is de BVH gekoppeld aan de Personenserver. Deze Personenserver kan ingevoerde persoonsgegevens automatisch controleren in de Gemeentelijke Basis Administratie (GBA). Bij geen overeenkomsten in GBA ontvangt de invoerende medewerker een melding om de door hem of haar ingevoerde gegevens op juistheid te controleren. De hiervoor genoemde kwaliteitscontroleurs op de districten zien er op toe dat er opvolging aan deze meldingen wordt gegeven.

Om de kwaliteit van de gegevens te verbeteren heeft Zuid-Holland-Zuid ook een aantal verbeterinstrumenten ingericht.

De afdeling HKD (onderdeel van ICC DREO) controleert en verbetert dubbele invoer in BVH en BVO. De HKD controleert en verbetert de ingevoerde persoonsgegevens en loopt alle gegevens van de zaken na die binnen BVH en BVO worden afgeboekt. Hiermee wordt voorkomen dat er onjuiste gegevensverwerking worden weggeschreven of worden ingezonden naar het OM. Dit betreft een controle achteraf.

Het korps heeft om de invoer van gegevens aan de voorkant te verbeteren voor alle gebruikers van BVH een terugkomdag georganiseerd. Dit betrof een verplichte lesdag om de kennis voor het invoeren van gegevens in BVH op te frissen en nog eens stil te staan bij de WPG en met name het vastleggen van verstrekkingen in de 190. Tevens is het belang van het opvolgen van TrueBlue-meldingen benadrukt op deze dag.

Om de medewerkers bij de invoer van gegevens te ondersteunen en de kwaliteit van gegevens te waarborgen is binnen ZHZ in april 2011 de regionale Front-office Back-office (FOBO) actief. Hier worden naar aanleiding van meldingen en informatie van collega's die naar een melding gestuurd worden, mutaties aangemaakt. Het voordeel hiervan is dat deze FOBO medewerker per incident precies weten binnen welke maatschappelijke klasse een mutatie moet worden opgestart. Op deze manier wordt foutieve invoer van gegevens voorkomen. Ook worden de persoonsgegevens die bekend worden binnen een incident direct op juistheid gecontroleerd. Op deze manier wordt aan de voorkant bij het verwerken van gegevens op kwaliteit gestuurd. De politiemedewerkers die bij een incident ter plaatse zijn geweest vullen de mutatie van de FOBO later aan en controleren deze. Op deze manier is er een dubbele check op de invoer van gegevens ingericht.

Herkomst en wijze van verkrijging, noodzaak en doelbinding

Technische Recherche

De meldingen voor de technische recherche komen binnen bij de Front-Office. Daarnaast wordt per melding binnen BVH een aanvraagformulier aangemaakt die via de e-mail verzonden wordt naar de technische recherche. In de aanvraagformulieren staat onder andere het doel van het onderzoek aangegeven, als het nodig is wordt aangegeven dat het spoedonderzoek betreft.

De mails met aanvraagformulieren worden in de e-mail map technische recherche bewaard. Aan de hand van de planning, die door de Front-Office in samenwerking met de Coördinator Forensische Recherche is opgesteld, worden de functionarissen gekoppeld aan een onderzoek.

Wanneer 's nachts meldingen worden gedaan, komen deze binnen bij de speciale pool die is ingericht in samenwerking met het korps Rotterdam-Rijnmond.

CIE

Alle projectvoorstellen worden vooraf aan de CIE-officier voorgelegd. Een informatieofficier is al in de fase van prewering betrokken. De Officier van Justitie wordt bij elke in- en uitschrijving in of uit het informantenregister betrokken.

- Als de CIE gegevens ter beschikking stelt voor verdere verwerking onder artikel 9 of 8, dan maakt de CIE daarvan een verstrekking PV. Die PV's worden opgeslagen op de O:schijf.
- 00-informatie is geheime informatie die alleen bij de politie en bij de informant bekend is (bruto informatie, artikel 12 Wpg). Dit zijn de meest vertrouwelijke gegevens die de CIE verwerkt. 00 betekent dat bij bekendwording van de info ook de bron bekend kan worden. Deze gegevens worden alleen binnen de CIE gedeeld.
- 00 informatie wordt geregistreerd in BVO. De leidinggevende en plaatsvervangend leidinggevende van de afdeling zijn de enige die erover kunnen beschikken. Alleen de functionarissen met een specifiek daartoe toegekende autorisatie kunnen deze informatie inzien.
- Daarnaast is er 01-informatie (artikel 10 Wpg). 01 betekent dat de info alleen mag worden benut voor artikel 8 of 9 verwerking als er specifieke toestemming wordt gegeven door de bron. Deze info wordt vastgelegd in BVO.
- Informatie volgens artikel 10 van de Wpg is netto-informatie opgeknipt per verdachte, gerubriceerd en er wordt aangegeven wat wel en wat niet operationeel mag worden verstrekt.

RID

Het verzamelen van informatie vindt ondermeer door RID-runners plaats via het bevragen van informanten. De runners maken hiervan verslagen, die 'bruto' in het informatiesysteem BVO-Rood worden verwerkt. Op basis van deze verslagen wordt de zogenoemde operationele informatie gefilterd. Deze gefilterde (netto-) informatie (artikel 10 Wpg) wordt verwerkt in het informatiesysteem BVO 'gewoon'.

- Als een burger bij balie politiebureau komt met operationele informatie, die mogelijk van belang is voor de RID, dan zal via de betrokken politieambtenaar de gegevens/informatie doorsturen naar RID.
- Gegevens inzake informanten (artikel 12 Wpg) worden elektronisch opgeslagen in een beveiligde ruimte. Alleen de Chef RID en één medewerker RID hebben toegang tot deze gegevens.

Oordeel over de kwaliteitspecten van politiegegevens

Het korps Zuid-Holland Zuid voldoet in hoofdlijnen aan de kwaliteitsaspecten zoals genoemd in de artikelen 3 en 4 van de Wpg.

Wpg impact regionale applicaties

De werkgroep heeft uit een lijst van circa 250 software systemen, 50 systemen geselecteerd die Wpg-relevant zijn. Daaronder 27 systemen ten aanzien waarvan de voorlopige inschatting is dat ZHZ aanpassingen moet doorvoeren in software, werkproces of databeheer.

In de implementatiefase heeft men onderzocht welke impact de Wpg heeft op de regionale applicaties en is er vervolgens een actieplan gedefinieerd om de applicaties in lijn te brengen met de Wpg. Inmiddels hebben alle regionale applicaties ech-

ter plaatsgemaakt voor landelijk gehoste applicaties. Hierdoor zijn er geen systemen meer actief die in eigen beheer zijn. Het laatste systeem dat in eigendom van het korps was betrof het JIS (Jongeren Informatie Systeem). Dit systeem werd gebruikt om jeugdgroepen aan de hand van de BEKE-lijst inzichtelijk te maken. Het JIS had tot 2010 geen autorisatiemodule. Iedere politiemedewerker met toegang tot intranet kon de gegevens benaderen. In 2010 is dat aangepast. Toegang is nu voorbehouden tot collega's die artikel 8 informatie mogen verwerken.

Op het intranet was ook een pagina te vinden waar de gegevens over Veelplegers werden bijgehouden. Ook die pagina was niet voorzien van een password. De Veelplegersite is in 2011 opgeheven en de informatie wordt nu ontsloten via het doelgroepsysteem Amazone. Daartoe hebben alleen politiemedewerkers toegang die zijn geautoriseerd voor verwerking onder artikel 8.

Tijdens de audit worden de regionale applicaties niet meer gebruikt. Gedurende de audit was het niet mogelijk dit vast te stellen. Het korps heeft de maatregelen getroffen om te voldoen aan de vereisten van de Wpg, echter de werking van de maatregel kon niet worden getoetst.



Functioneel gegevensbeheer

De Functioneel Beheerders (FB's) van Informatie Management (IM) kunnen gegevens fysiek van de database verwijderen via BVH. De medewerker die binnen BVH een foute registratie maakt, (bijvoorbeeld bij aanmaak van een verkeerde persoonskaart) kan, middels de helpdesk van de vtsPN en/of mailen naar Functioneel Beheer of kwaliteitscontroleurs van de districten, het verzoek tot verwijdering doen. De gegevens van de verwijdering worden gelogd (bijvoorbeeld op dienstnummer of registratienummer). De FB heeft een kijkfunctie op deze logging.

Verwijderen van gegevens

Binnen Zuid-Holland Zuid zijn geen strikte afspraken gemaakt (criteria) ten aanzien van het verwijderen van gegevens uit BVH. Binnen het korps zijn gegevensbewerkers (27 personen) aangewezen/geautoriseerd om gegevens uit BVH te verwijderen. Dit zijn vrijwel allemaal mensen vanuit de ICC's van alle districten die een rol spelen in de kwaliteitsbewaking van de invoer van gegevens in BVH. Daarnaast hebben een viertal personen toegang tot het functioneel beheerder menu van BVH. Dit zijn onder andere een tweetal functioneel beheerders uit Rotterdam-Rijnmond in verband met de bovenregionale samenwerking.

De verwijdering van gegevens wordt gelogd door vtsPN. Daarnaast heeft de functioneel beheerder van BVH in Zuid-Holland Zuid de mogelijkheid om te zien wie en wat er binnen BVH wordt verwijderd en aangepast. Dit maakt controle op aanpassingen/verwijderingen binnen BVH hierop voor de functioneel beheerder BVH mogelijk. De privacy ambtenaar wordt niet betrokken bij het verwijderen van gegevens uit BVH.

De verwijdering behoort formeel via de helpdesk bij de VTS aangevraagd te worden, wat tegelijk ook vastlegging van de aanvragen betekent via Expertdesk. In de praktijk wordt dit echter niet of nauwelijks gedaan doordat de helpdesk VTS maar acht uur per dag aanspreekbaar is. Vanwege het feit dat de politie een volcontinue dienst verstuurt men daarom het verzoek tot aanpassing of verwijdering vaker per mail naar een (aanwezige) gegevensbewerker of functioneel beheerder binnen de districten/diensten. Vaak gaat het om verwijderen (samenvoegen) van een (acteur)kaart.

Als het al gaat om het verwijderen van een (onjuiste) registratie is het binnen het korps de regel dat een aanvraag hiertoe in een mail wordt omschreven. De functioneel beheerder van BVH in Zuid-Holland Zuid bewaart deze mail. Als het gaat om wat meer omvangrijke registratie zal hier een opdracht van de chef voor moeten komen, dit is binnen het korps en het bestaan van BVH nog nooit aan de orde geweest.

Isolatie

De basis voor informatiebeveiliging in het korps wordt gevormd door de RIP, het BBNP, de Wet bescherming persoonsgegevens en de Wet en het Besluit Politieregistrars. De uitvoering van deze regeling wordt gedaan door middel van voorlichting, bijvoorbeeld in het personeelsblad. De functionele beveiligingsbehoefte van het korps is niet bekend. Het Informatiebeveiligingsbeleid wordt vastgesteld door het Regionaal Managementteam en voorbereid door de controller beveiliging. De volgende terreinen zijn de belangrijkste als het gaat om de getroffen maatregelen:

1. Fysieke toegangsbeveiliging
2. Autorisatiebeleid
3. Veiligheidsonderzoeken
4. P-onderzoeken.

Door participatie in het CIO overleg en het landelijk overleg informatiebeveiliging is het korps aangesloten op het landelijk beleid op het gebied van de informatiebeveiliging.

De Inspectie Openbare Orde en Veiligheid (IOOV) heeft onlangs een audit uitgevoerd naar de mate waarin het stelsel voor de aanpak van de informatiebeveiliging bij de Nederlandse politie is geïmplementeerd.

CIE

Informanten krijgen landelijk een unieke code zodat ze maar op 1 plek informant kunnen zijn. Als er over informanten wordt gesproken wordt deze code of een eigen kortere code gebruikt, maar nooit de naam van de informant. De naam staat wel in het informantenregister, artikel 12 in de zin van de Wpg. Binnen Zuid-Holland Zuid zijn twee medewerkers bevoegd met een raadpleegfunctie:

- Soms worden observatieteams ingezet in de zin van artikel 2 van de Politiewet. Dit is niet stelselmatig en wordt altijd van tevoren overlegd met de CIE officier.
- Informanten die iets vertellen over openbare orde horen bij de RID, over strafrechtelijke zaken horen ze bij de CIE.

RID

De RID is sinds vorig jaar (2010) op BVO overgegaan. De RID heeft daartoe alle gegevens van het eigen interne netwerk geconverteerd en geschoond overgezet naar BVO-Rood. Het interne netwerk (tevens KA-omgeving) wordt uitgefaseerd, maar wordt nu nog gebruikt voor KA-toepassingen en raadplegen. Het interne netwerk wordt op locatie beheerd door vtsPN (dus niet op afstand). Onbekend is of vtsPN werkzaamheden en activiteiten op dit interne netwerk worden gelogd. De vtsPN beheerder wordt echter altijd begeleid door iemand van de RID.

Verwerken gegevens buiten BVO: Gegevensbeheer

In Zuid-Holland Zuid was het al gebruik om BPS-gegevens na 5 jaar te schonen. Dit gebruik blijft gehandhaafd met de inwerkingtreding van de Wpg. In BVH hoeft nog niet te worden geschoond. Er zijn twee omgevingen aangelegd in het oude BPS voor gegevens jonger dan 5 jaar (operationeel bruikbaar) en gegevens ouder dan vijf - jonger dan 10 jaar (archief). De laatste omgeving is zeer beperkt toegankelijk.

Het implementatieteam heeft bewerkstelligd dat ook ten aanzien van recherchegegevens een schoning is doorgevoerd. Oude tijdelijke registers zijn geïnventariseerd en waar nodig verwijderd. De grootste schoning is uitgevoerd ten tijde van de invoering van de O-schijf die bedoeld is voor de opslag van politiegegevens.

De O-schijf is ingericht volgens de Wpg-regimes en op informatieproduct. Aan de medewerkers is gevraagd om oude mappen op het netwerk te schonen (van 120.000 mappen naar 80.000) en vervolgens een scheiding aan te brengen tussen politiegegevens en overige gegevens. De politiegegevens zijn vervolgens geordend op Wpg-regime en soort van informatieproduct en daarna opgeslagen en regionaal bereikbaar gemaakt voor hen die daartoe geautoriseerd zijn.

Er is wel onwennigheid met het omgaan betreffende de opslag en onderhoud van gegevens. Iedere chef ICC heeft daarom enkele informatieproducten geadopteerd en organiseert daarop het gegevensbeheer. Er is een toelichting geschreven van hoe om te gaan met de O-schijf.

De chefs ICC zien toe op de juiste en tijdige afhandeling van de zaken.

Verdeling O-schijf

De politiegegevens worden in BPS/ BVH of BVO opgeslagen. Daarnaast worden politiegegevens op de O-schijf opgeslagen. Het korps heeft BVH-opleidingen georganiseerd van 4 dagen en een opleiding voor HOvJ's van 5 dagen, waarbij steeds 2 uur is stilgestaan bij de Wpg. Een onderwerp tijdens deze training was de invoering van de O-schijf waarvoor noodzakelijk was dat alle medewerkers hun oude kantooromgeving moesten nalopen op nog bruikbare politiegegevens en deze moesten classificeren naar product en Wpg-regime.

De O-schijf is onderverdeeld in:

- Artikel 8 Handhaving (dagelijkse politietaak).
- Artikel 9 Opsporing (rechtsorde concreet geval).
- Artikel 10 Informatie (alleen voor CIE/RID).
- Artikel 13.
- Artikel 14 Archief.

Veelplegers

De veelplegers worden gelabeld in OPS, HKS en BVH. Bij het invoeren van een mutatie in BVH, is inzichtelijk dat het om een veelpleger uit Zuid-Holland Zuid gaat. Ten tijde van onze audit werd alle informatie over veelplegers geplaatst op intranet van het korps. Deze informatie op intranet is voor iedereen die toegang heeft tot het intranet leesbaar via de zogenaamde veelplegerssite. Politie Zuid-Holland Zuid onderkent dat dit, uitgaande van de Wpg, niet voldoet aan de Wpg. De toenmalige versie van intranet biedt geen mogelijkheid om een filter aan te brengen. Het korps heeft dit medio 2011 aangepast. Sinds oktober 2011 zijn de veelplegerssites verwijderd van intranet. Deze informatie wordt nu ontsloten via Amazone (doelgroepen-systeem). Dit systeem is alleen toegankelijk voor BVH-geautoriseerden. Daarmee wordt voldaan aan de eisen van de Wpg.

Oordeel over beveiliging

Het korps Zuid-Holland Zuid heeft de Wpg geanalyseerd en de impact daarvan op de systemen en het autorisatiebeheer bepaald. Niet alle landelijke en regionale applicaties voldoen aan de vereisten vanuit de Wpg. Hiermee wordt niet voldaan aan artikel 4 lid 3 van de Wpg.

4.4 Gevoelige gegevens

4.4.1 Norm

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

4.4.2 Bevinding

RID/CIE

Bij de privacyfunctionaris is bekend dat de RID/CIE in sommige gevallen gevoelige informatie vastleggen. Deze informatie wordt vastgelegd op de afgeschermd O:schijf omgeving van deze afdelingen. De chefs van voornoemde afdelingen zien er op toe dat de vastlegging van gevoelige informatie slechts plaats vindt in aanvulling op andere politiegegevens en voor zover dit voor het doel van de verwerking onvermijdelijk is. Genoemde leidinggevenden zijn tevens verantwoordelijk voor de schoning van deze gegevens.

Veelplegers

Gevoelige gegevens kunnen worden verwerkt voor zover zij een duidelijke functie vervullen bij de uitvoering van de politietaak en voor zover dit nuttige informatie kan zijn voor de opsporing van een strafbaar feit.

Oordeel over gevoelige gegevens

Zoals ook in voorgaande secties is aangegeven, besteedt het korps Zuid-Holland Zuid veel aandacht aan de voorlichting van chefs en politiemedewerkers. Hierbij is ook aandacht gegeven aan hoe om te gaan met gevoelige gegevens.

4.5 Autorisatie (artikel 6)

4.5.1 Norm

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

4.5.2 Bevindingen

Korpsautorisatiematrix

Binnen Zuid-Holland-Zuid is een 'basismodel autorisatie' geformeerd. De autorisaties zijn rol gebaseerd en dit model geldt inmiddels als landelijk model. Aan de hand van deze rolbeschrijving hebben de oude autorisaties plaatsgemaakt voor nieuwe autorisaties voor de medewerkers van het korps.

Binnen Zuid-Holland Zuid zijn alle autorisaties van BVH, BVO en BlueView inzichtelijk voor de privacyfunctionaris middels een autorisatielijst. Deze lijst wordt twee keer per jaar (in het voor- en najaar) bijgewerkt door van voornoemde applicaties de autorisatielijsten te verversen. De privacyfunctionaris houdt binnen de regio met name de verschuivingen van medewerkers die het korps verlaten en medewerkers die met ontslag gaan in de gaten om zodoende autorisaties te kunnen laten blokkeren of op noodzakelijke wijzingen toe te zien.

Het korps heeft een rationale voor de Wpg-artikelen die van toepassing zijn op een functie en tevens op de rollen die aan een functie kunnen worden gekoppeld. Daarbij heeft het korps een aantal vertrouwelijkheidsniveaus gedefinieerd. Ook zijn de superuser-gebruikers gekoppeld aan functies.

Aanvraagproces interregionale autorisaties

Het Korps Zuid-Holland Zuid heeft dit jaar (2011) een autorisatieprocedure ontwikkeld. Deze procedure geldt voor externe (of interregionale) autorisaties en wordt als volgt weergegeven:

- De privacyfunctionaris ontvangt een aanvraagformulier (fysiek document), dit formulier wordt door de privacyfunctionaris bewaard en opgeslagen. Dit formulier wordt opgemaakt en ingezonden door de privacyfunctionaris van het aanvragende korps of bijvoorbeeld het OM.
- De privacyfunctionaris beoordeelt of de betrokkene in aanmerking komt voor een autorisatie. Hierbij worden door de privacyfunctionaris de volgende criteria gehanteerd:
 - Is betrokkene in dienst?
 - Wat zijn de werkzaamheden van betrokkenen?
 - Heeft betrokkene de eed of belofte afgelegd?
 - Gaat de chef/leidinggevende van betrokkene akkoord met autorisatie?
 - Wat is het doel van de autorisatie?
 - Is de autorisatie ten opzichte van het doel noodzakelijk?
- Indien betrokkene voldoet aan de bovenstaande criteria dan wordt de aanvraag door de privacyfunctionaris digitaal ondertekend en wordt deze doorgestuurd naar het Loket Ondersteuning van Zuid-Holland Zuid.
- Door Loket Ondersteuning wordt de aanvraag doorgezet van vtsPN. Deze maakt een account aan voor betrokkene.
- Nadat het account is aangemaakt, wordt door de privacyfunctionaris van het aanvragende korps of applicatiebeheer van het OM het account verstrekt aan betrokkene.

- De autorisatie van externen verloopt automatisch na 1 jaar.

De autorisatietermijn voor interregionale autorisaties geldt niet langer dan waarvoor deze noodzakelijk is met een maximale duur van één jaar. Daarna dient deze termijn telkens middels een autorisatieverzoek daartoe verlengd te worden. De verlengingsverzoeken worden via de e-mail aangevraagd.

De functionaris in de verzoekende regio dient in overeenstemming met de in die regio gebruikelijke wijze een autorisatieverzoek in bij zijn lijnchef. Hij maakt hierbij gebruik van het formulier 'interregionale autorisaties'.

Aanvraagproces intern

De autorisaties van medewerkers van korps Zuid-Holland Zuid lopen via een andere procedure. Tevens wordt er voor internen geen autorisatietermijn gehanteerd omdat dit door de grote hoeveelheid medewerkers ondoenlijk is.

Middels de autorisatielijsten van de systemen BVH, BVO en BlueView wordt er door de privacyfunctionaris op toegezien dat bij verschuivingen van medewerkers of ontslag de autorisaties worden geblokkeerd of beëindigd.

De procedure is als volgt beschreven:

- De directe chef kan middels een digitaal formulier de autorisatie van een medewerker aanvragen. Dit formulier wordt door Loket Ondersteuning doorgestuurd naar informatie management (IM).
- In dit formulier dient de aanvrager het doel en de noodzaak van de autorisatie aan te geven.
- De autorisatiemodule is gekoppeld aan het personeelssysteem Beaufort. Het systeem controleert of de aanvrager van de autorisatie wel bevoegd is tot het aanvragen ervan.
- De aanvragen worden vervolgens in behandeling genomen door het loket Ondersteuning of Informatie Management (IM). Hier wordt de aanvraag getoetst en verwerkt en waar nodig doorgezet naar vtsPN of de functioneel beheerder.
- Als er aan de autorisatie een besluit ten grondslag ligt, wordt dit geverifieerd bij R&A. Bij verplaatsingen worden oude autorisaties ingetrokken.
- IM of het Loket Ondersteuning verwerkt autorisatie en koppelt dit terug aan de aanvrager (chef betrokkene).

Werking

Met de invoer van het Loket Ondersteuning worden autorisatieaanvragen centraal verwerkt. Er is nog geen technische mogelijkheid om vanuit één punt autorisaties door te voeren. Het loket draagt daarom zorg dat de relevante functioneel beheerders worden geïnformeerd over de autorisatieaanvraag. Op dit moment is het loket doende om voorbereidingen te treffen om daadwerkelijk rol gebaseerd te gaan autoriseren. Autorisaties behoeven dan niet meer door de chef te worden aangevraagd, maar vloeien voort uit de werkzaamheden die een medewerker volgens het personeelssysteem uitvoert.

De privacyfunctionaris heeft een protocol geschreven voor de beoordeling van externe aanvragen op rechtstreekse toegang tot BVH.

Protocollering

Via intranet wordt een aanvraag gedaan, veelal is de leidinggevende de aanvrager. De aanvraag en de verdere procedure wordt vervolgens door Loket Ondersteuning verwerkt en vastgelegd in het systeem genaamd 'Planon'. Het Loket Ondersteuning

stuurt het aanvraagformulier door naar de afdeling die over de autorisatie gaat, dit kan vtsPN, Informatie Management (IM) van Zuid-Holland Zuid of de privacyfunctionaris zijn ect.

Alle stappen in de autorisatieprocedure worden via Loket Ondersteuning gecommuniceerd en in Planon vastgelegd. Alle stappen zijn in dit systeem op te vragen en in te zien voor Loket Ondersteuning en de privacyfunctionaris. De digitale aanvragen worden digitaal bewaard in Planon. Ze zijn voorzien van een status, te weten 'open' of 'afgehandeld'.

Zodra een autorisatieprocedure is afgehandeld, worden deze binnen Planon bewaard in de digitale archiefomgeving van Planon. Planon is pas een jaar actief en inmiddels zijn er 953 autorisatieverzoeken/autorisaties in Planon gearhiveerd. Er zijn nog geen afspraken vastgelegd omtrent de schoning van het digitale archief in planon (bewaartermijn).

De privacyfunctionaris heeft medio 2011 aangegeven onvoldoende zicht te hebben op het muteren van autorisaties via het Loket Ondersteuning. Ter verbetering heeft het korps de eerder genoemde procedure opgesteld.

Reconciliatie en schoning

Indien een medewerker in een regio wordt geschorst of ontslagen zorgt de regionale privacyfunctionaris van die regio er voor dat een verzoek tot verwijdering van de interregionale autorisatie wordt verzonden aan die regio's waar de betreffende medewerker is geautoriseerd.

De privacyfunctionaris heeft aangegeven dat hij onvoldoende zicht op het muteren van autorisaties via het loket ondersteuning. Hierdoor is de controle op reconciliatie, schoning en verwijdering niet aantoonbaar effectief.

Oordeel over autorisaties

Het korps Zuid-Holland Zuid voldoet in hoofdlijnen aan artikel 6 voor het beheer van autorisaties, met uitzondering van de processen voor reconciliatie, schoning en tijdige verwijdering. Voor deze processen is nog niet aangetoond dat de werking in continuïteit is geborgd.

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

4.6.1 Norm

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

4.6.2 Bevindingen

Hanteerbare interpretatie

De verantwoordelijke maakt inzichtelijk op welke wijze binnen het korps geautomatiseerd wordt vergeleken en in combinatie wordt verwerkt. Onderzoeksvragen worden geformuleerd door een onderzoeksteam, over het algemeen voor rechercheonderzoeken.

Aangewezen functionarissen

Als de verantwoordelijke onderscheid maakt tussen geautomatiseerd vergelijken en in combinatie verwerken, worden overeenkomstig functionarissen aangewezen die deze handelingen mogen uitvoeren. Dit betreft artikel 11.1 en 11.2 versus artikel 11.4 Wpg-verwerkingen.

De aanvraag verloopt via de chef. Dit kan via de e-mail, maar ook door middel van specifieke formulieren op intranet. De analisten worden aangewezen door de chef. De chef toetst de aanvragen. De gegevens worden opgeslagen in de map waar het onderzoek plaatsvindt (O-schijf).

Vragen uit de omgeving worden door middel van gebiedsscan aangeleverd. Elk district heeft een eigen analist. Wanneer informatie naar bijvoorbeeld de woningbouw gaat, moet er een convenant zijn.

Wanneer binnen rechercheonderzoeken gecombineerde zoekvragen plaatsvinden, wordt door het onderzoeksteam een artikel 11-verklaring gevraagd bij de zaaksofficier van Justitie. Deze verklaringen worden door het onderzoeksteam opslagen bij de fysieke documenten van het desbetreffende onderzoek.

Artikel 11.4: Bevoegde gezag

CIE

Artikel 11 lid 4 Wpg gecombineerd zoeken, analyseren wordt alleen ten behoeve van projectvoorbereiding door een analist gedaan. Aanvragen hiervoor dienen te worden gedaan bij de Officier van Justitie door middel van een opdrachtformulier. Een kopie van dit formulier wordt bij de CIE bewaard.

Tactisch strategisch analisten maken ook gebruik van de informatie van de CIE.

Er is één vaste CIE analist. Die brengt Criminele Samenstellings Verbanden (CSV) in kaart en beschrijft ze. Dit gebeurt volgens artikel 11.4 van de Wpg, gecombineerd zoeken. De analist maakt een rapport van bevindingen. De 00-informatie maakt

nooit deel uit van deze rapportage. Het rapport is een pre-document voor de regionale stuurploeg waarin ICC chefs, vervangende korpschef CIE leiding vertegenwoordigd zijn. In dit overleg wordt besloten of een onderzoek wordt gestart en zo ja, hoe en op welke onderdelen. Het Hoofd CIE toetst altijd of het rapport geen 00-informatie bevat.

Soms komt er via het VROS een melding dat een subject van de CIE in een Melding Recherche Onderzoek (MRO) voorkomt. Eventuele 01-informatie kan dan worden uitgewisseld.

Protocollering 11.1, 11.2 en 11.4 Wpg

Artikel 11 lid 4 Wpg gecombineerd zoeken en analyseren wordt alleen ten behoeve van projectvoorbereiding door een analist gedaan. Aanvragen hiervoor dienen te worden ingediend bij de Officier van Justitie door middel van een schriftelijk opdrachtformulier volgens een vast sjabloon. Deze verklaringen blijven in beheer van het desbetreffende onderzoeksteam.

Artikel 11-zoekacties worden middels een standaard opdrachtformulier vastgelegd. Deze worden echter niet centraal binnen het korps Zuid-Holland Zuid opgeslagen waardoor bijvoorbeeld bij privacyfunctionaris onvoldoende zicht heeft op het geheel aan artikel 11-protocollering. De privacyfunctionaris dient daarvoor te zoeken in de dossiers van de onderzoeken, aangezien de artikel 11-verwerking daar worden aangehouden.

Bewaren protocolgegevens 11.1, 11.2 en 11.4 Wpg

Er is binnen politieregio Zuid-Holland-Zuid geen protocollering aanwezig op het gebied van één verzamelpunt waar alle artikel 11-verklaringen worden opgeslagen. De zoekvragen worden opgeslagen bij de desbetreffende onderzoeken.

De Infodesk ontvangt/bewaart geen artikel 11 Wpg verklaringen afkomstig van de Officier van Justitie. Deze verklaringen blijven in beheer van het desbetreffende onderzoeksteam. De Infodesk verwerkt alleen gecombineerde zoekvragen afkomstig van de rechercheafdelingen. Bij een dergelijke aanvraag dient te worden aangegeven welke Officier een artikel 11-verklaring heeft afgegeven. Door Infodesk wordt van dergelijke aanvragen een verstrektingsrapport opgemaakt welke gekoppeld wordt aan het BVO-nummer van het desbetreffende onderzoek.

De bewaartermijn van artikel 11 Wpg formulieren is digitaal gelijk aan de schoning op de O:schijf (5 jaar). Fysiek gaat het document mee met het proces-verbaal dat bij het OM wordt aangeleverd. Wanneer er geen proces-verbaal wordt aangeleverd wordt deze opgeslagen bij de procesverbaaladministratie bij de overige fysieke stukken van het desbetreffende onderzoek.

Artikel 11.5 Wpg: andere gegevens

Het combineren van politiegegevens met niet-politiegegevens volgens artikel 11 lid 5 Wpg komt niet voor in het korps Zuid-Holland Zuid. Er wordt niet gecombineerd gezocht met behulp van automatische koppelingen naar externe bestanden. Wel kan het zijn dat een externe bron een databestand ter beschikking stelt voor verdere verwerking binnen de politie. De gegevens worden dan echter politiegegevens en er is sprake van 11.4 in plaats van 11.5.

4.7 Bewaartermijnen (artikel 14)

4.7.1

Norm

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

4.7.2

Bevindingen

Van BPS naar BVH

Het korps Zuid-Holland Zuid maakte vanaf 1992 gebruik van het Bedrijfsprocessen-systeem (BPS). In 1998 is een begin gemaakt met het archiveren van de (persoons) gegevens in dit systeem. Onder de werking van de Wet politieregister was de maximale bewaartermijn 5 jaren. Men heeft toen gekozen om de archiefbestanden van de regio onder te brengen in een archiefbestand BPS. Dit is gedaan met het oog op het bewaren van gegevens van zaken die nog niet tot een oplossing waren gebracht. Inmiddels is er een archief opgebouwd van 11 jaren (1992-2002), dat niet meer algemeen toegankelijk is. Het fysieke (papieren) archief wordt tien jaar bewaard.

De Wet politiegegevens staat toe dat gegevens die worden gebruikt voor de dagelijkse politietaak (artikel 8 Wpg) maximaal vijf jaar kunnen worden verwerkt en daarna vijf jaar worden bewaard voor verantwoordingsdoeleinden. Anders is dat met gegevens die zijn verwerkt in belang van grotere rechercheonderzoeken (artikel 9 Wpg). Dergelijke gegevens worden bewaard tot aan de verjaring van het feit of tot aan een onherroepelijk vonnis. Beide gegevenssoorten worden opgeslagen in BPS. Het is niet eenvoudig om bij de schoning van BPS onderscheid te maken tussen beide gegevenssoorten.

Om bovenstaande redenen heeft de implementatiecommissie het volgende voorgesteld:

- Verwijder alle BPS-gegevens na vijf jaar uit BPS en plaats deze in een afzonderlijk bestand.
- De Infodesk en de privacyfunctionaris hebben toegang tot dit bestand.
- Stel een procedure op dat het bestand slechts mag worden geraadpleegd in het kader van art 9 Wpg en dat daaruit slechts gegevens worden verstrekt over niet-verjaarde misdrijven of misdrijven die nog niet tot een onherroepelijk vonnis hebben geleid.
- Alleen de privacyfunctionaris heeft nog toegang tot het papieren archief. Indien nodig beoordeelt hij of mogelijkheden bestaan om gegevens uit het papieren archief opnieuw ter beschikking te stellen voor de politietaak.

BVO schoning

Voor BVO en de artikel 9 onderzoeken is het volgende geregeld:

De functioneel beheerder BVO (FB) ziet toe op de openstaande onderzoeken in BVO. De functioneel beheerder schrijft geregeld de bevoegde functionarissen aan om na te gaan of een onderzoek nog wel in BVO mag staan, of dat de termijn van 5 jaar bijna is verstreken. De functioneel beheerder ontvangt van de bevoegde functionaris of van het OM een schriftelijke opdracht tot verwijderen/vernietigen van gegevens.

De bevoegde functionaris geeft aan dat het aantal schriftelijke opdrachten dit jaar wel licht toe nam maar dekt absoluut nog niet de gehele lading.

Met name vanuit het OM wordt weinig terugkoppeling gegeven naar aanleiding van een OH-vonnis. Om deze reden ziet de functioneel beheerder periodiek toe op dat de bevoegde functionarissen van een nog openstaand artikel 9-onderzoek wordt geactiveerd om na te gaan of dit onderzoek wel/niet verwijderd/vernietigd moet worden. Het probleem bij het terugkoppelen is dat de politie zaakgericht werkt en het OM persoonsgericht. Bij vervolging van verdachten uit één onderzoek komt het vaak voor dat zaken ten aanzien van individuele personen worden gesplitst of juist worden samengevoegd. De ene verdachte kan worden geseponeerd, terwijl een andere wordt vervolgd maar ook voor enkele soortgelijke feiten. Weer een andere verdachte weet uit handen van de politie te blijven.

Aangezien het schoningsscript in BVO nog niet werkzaam is, heeft het korps de volgende werkwijze ingericht:

- 1 De FB BVO stuurt periodiek een lijst rond naar alle recherche afdelingen met de vraag of er nog onderzoeken op staan die verwijderd c.q. kunnen worden vernietigd.
- 2 Zo ja, dan dient de bevoegde functionaris een vernietigingsformulier op te maken en te ondertekenen. (Uiteraard na overleg met OvJ / RC).
- 3 Als het formulier binnen is voegt de FB BVO de te vernietigen registratie samen met de door mij daarvoor ingerichte registratie genaamd "18SCHONING".
- 4 Zodra alle informatie in "18SCHONING" staat. Dit kunnen dus ook meerdere onderzoeken tegelijk zijn. De functioneel beheerder BVO geeft de VMS-beheerder de opdracht deze registratie te verwijderen.
- 5 Hiermee wordt de gehele registratie van de BVO database verwijderd, inclusief de inhoud van het/de vernietigen onderzoek(en). Hierna maakt de functioneel beheerder BVO weer een nieuwe, lege 18SCHONING registratie aan en kan de procedure weer worden herhaald.
- 6 Tot slot stuurt de functioneel beheerder BVO hierna een e-mail naar de bevoegde functionaris met daarin de dag en het tijdstip waarom zijn of haar onderzoek(en) werd(en) vernietigd. Met deze informatie dient de bevoegde functionaris weer een vernietigingsproces-verbaal op te maken voor het OM.

Als een artikel 9-onderzoek wordt verwijderd of vernietigd, ziet de bevoegde functionaris van het desbetreffende onderzoek erop toe dat ook de O-schijf gegevens van dit onderzoek worden geschoond.

Artikel 8: Bewaartermijn 1-5 jaar

In BVH worden de gegevens automatisch na 5 jaar geschoond. De teamleider van het onderzoek is verantwoordelijk het schonen van de mappen op de O-schijf.

CIE

In aanvulling op de aandacht die in trainingen is besteed aan het belang van een zorgvuldige verwerking van politiegegevens, zijn daarover diverse publicaties verschenen in de Interpol en de Blauwe Link. Het meeste effect mag echter worden verwacht van het feit dat zo een 900 politiemedewerkers tijdens de opleidingen 2 uur hebben kennigemaakt met de Wpg met als boodschap: 'leg je informatie zorgvuldig vast en laat verstrekken over aan daartoe bevoegde medewerkers'.

ANPR Kentekens

Het korps bewaart alle middels ANPR gefotografeerde kentekens volgens een door het RMT vastgestelde procedure die de noodzaak voor inzet van ANPR beschrijft. Dit

beleid is ingevoerd. ANPR wordt alleen ingezet voor gerichte acties. Kentekens die niet matchen worden binnen 24-uur vernietigd.

Artikel 8: Verwijderen na 5 jaar

BVH wordt gebruikt om meldingen te registreren, aangiftes te verwerken en incidenten af te handelen. Artikel 8 Wpg is hierop van toepassing. De BVH wordt het meest gebruikt voor Artikel 8 Wpg zaken maar is nog niet voorzien van een termijnbewaking. Na vijf jaar zou er echter 'schoning' moeten plaatsvinden, maar het is niet bekend of dit daadwerkelijk gebeurt.

Men geeft aan dat Zuid-Holland Zuid nog geen vijf jaar met de O-schijf werkt zodat dit (nog) niet valt te controleren.

De O-schijf is de schijf binnen de kantoorautomatisering die bestemd is voor de opslag van politiegegevens. De O-schijf is per jaar ingedeeld. Na 5 jaar zal schoning plaatsvinden. Het korps werkt nog geen 5 jaar met O-schijf.

Bij het inrichten van de O-schijf is bewust rekening gehouden met het feit dat het schonen aan de hand van termijnen mogelijk moet zijn. Om deze reden is de O-schijf per onderwerp/onderdeel in jaartallen ingedeeld (zie de handreiking mappenstructuur), waardoor er handmatig per jaartal kan worden geschoond. De projectleider implementatie WPG is binnen het korps Zuid-Holland Zuid verantwoordelijk om er op toe te zien dat na vijf jaar de O-schijf handmatig wordt geschoond en de politiegegevens worden verwijderd.

Zodra een artikel 9-onderzoek in BVO dient te worden geschoond, wordt de bevoegde functionaris van het desbetreffende onderzoek (veelal de recherchecoördinator) hiervan in kennis gesteld. Deze kan zorgen dat de map van dit onderzoek ook op de O-schijf wordt geschoond.

De unit forensische ondersteuning (voorheen technische recherche) heeft een eigen omgeving waar ze foto's van plaats delict, processen-verbaal van bevindingen, onderzoeksresultaten en dergelijke opslaan. Dit zou over moeten naar de recherche map. Dit gebeurt niet altijd.

Vernietigen na 5 jaar verwijderd

Landelijk is dringend geadviseerd het mechanisme voor vernietiging in BVH 1.2.2 niet te activeren. Hiermee wordt niet voldaan aan de Wpg, onder andere door een landelijk advies. Ondanks dat niet wordt voldaan aan de Wpg, heeft het korps de voorkeur gegeven aan de borging van de werkbaarheid van de primaire taken. Het korps wacht op een landelijke sluitende technische oplossing.

Artikel 9: Verwijderen na OH plus ½ jaar

Zoals hierboven toegelicht, wordt het korps Zuid-Holland Zuid door het OM niet altijd op de hoogte gehouden als het *onherroepelijk moment* (OH) is aangebroken. Er kan dan ook niet worden gegarandeerd dat de politiegegevens uiterlijk een half jaar na het OH-moment worden verwijderd. Het korps heeft hiervoor een eigen procedure uitgewerkt.

Artikel 9: vernietigen na 5 jaar verwijderd

RID: Het RID geeft aan dat in BVO ook een schoningsmodule zou komen. Deze is (nog) niet verwezenlijkt. Daardoor kan niet worden geschoond in BVO. Het probleem is dan dat volgens RID daarmee niet kan worden voldaan aan de Wpg-

vereisten. Derhalve worden er door RID handmatig codes/ "datum eerste verwerking" aangebracht in BVO om zo de bewaartermijn te kunnen controleren.

Artikel 10: verwijderen na vijf jaar geen subjectwaardige registratie

De chef RID en CIE zijn binnen Zuid-Holland Zuid aangewezen om zorg te dragen dat artikel 10-vastleggingen worden verwijderd binnen de hiervoor gestelde termijnen. Tevens zien zij toe op de doelmatigheid van vastgelegde informatie. De subjectmatige registratie wordt om de vier maanden nagelopen en beoordeeld op doelmatigheid en gecontroleerd op tijdige verwijdering.

Artikel 10: vernietigen na vijf jaar verwijderd

De chef RID en CIE zien toe op tijdige vernietiging na vijf jaar verwijdering.

Hernieuwde verwerking artikel 14.3 Wpg

Binnen BVH en voorheen BPS worden gegevens ouder dan vijf jaar geplaatst naar de archiefomgeving. Deze omgeving is alleen toegankelijk voor de privacyfunctionaris van het korps. Gegevens die zijn verwijderd uit BPS/BVH en nog binnen de archiefomgeving aanwezig zijn, kunnen worden opgevraagd bij de privacyfunctionaris.

Indien gegevens uit de archiefomgeving worden opgevraagd, dient dit te gebeuren middels een aanvraag bij de privacyfunctionaris. Deze aanvraag gaat middels een e-mail aan de privacyfunctionaris waarin door de aanvrager moet worden aangegeven wat de redenen, doel en noodzaak zijn van het opvragen van archiefbestanden. De privacyfunctionaris hanteert een scherpe toetsing bij het wel of niet laten inzien van opgevraagde gegevens uit de archiefomgeving.

Alle aanvragen en de eventuele verstrekkingen die hieruit voorkomen zijn opgeslagen en gearhiveerd door de privacyfunctionaris. Alleen de privacyfunctionaris heeft toegang tot dit archief. De privacyfunctionaris heeft de afgelopen jaren de volgende aantallen aanvragen ontvangen en in behandeling genomen:

- 2007: 39 aanvragen
- 2008: 35 aanvragen
- 2009: 30 aanvragen
- 2010: 20 aanvragen
- 2011: 21 aanvragen

Artikel 12: verwijderen na vier maanden

Er is een lijst met voorlopig geregistreerde informanten. Hiervan moet nog worden bepaald of de politie verder wil gaan met deze informanten. Zo ja dan volgt inschrijving in het informantenregister.

Bij de CIE wordt elk jaar het informantenregister geschoond. Als er de afgelopen twee jaar geen informatie van een informant is ontvangen wordt die uitgeschreven uit het informantenregister.

4.8 Ter beschikking stellen (artikel 15)

4.8.1

Norm

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

4.8.2

Bevindingen

Infodesk voor bevraging

De Infodesk maakt onderdeel uit van het Informatie Coördinatie Centrum (ICC) van de Dienst Recherche Expertise en Ondersteuning (DREO). Elke regio heeft een eigen infodesk.

De afdeling Infodesk is in tweeën gesplitst, waarbij de chef Infodesk en informatiecoördinator beide hun eigen takenpakket hebben. Bij afwezigheid nemen ze elkaar waar. Bij de Infodesk werken onder andere analisten en procescoördinatoren. Daarnaast beschikt de desk over een E-loketfunctie.

De procescoördinatoren worden per thema (zoals bijvoorbeeld woninginbraken) aangesteld. De thema's blijven de komende jaren gehandhaafd.

Proces

De verzoeken aan Infodesk worden gedaan middels een vast formulier op het intranet van Zuid-Holland Zuid. Middels dit formulier dient de aanvrager te motiveren en verantwoorden met welke reden en doel hij of zij deze informatie heeft opgevraagd/bevraagd.

De Infodesk verwerkt deze aanvragen middels een vaste werkwijze. Alle aanvragen en de antwoorden/gegevens die de Infodesk hierop verstrekt, worden per jaartal digitaal opgeslagen op de O-schijf. Deze gegevens worden na vijf jaar geschoond.

Vragen vanuit onder andere de meldkamer

De Infodesk werkt vraaggericht voor afhandeling van de binnenkomende vragen. Er wordt nagegaan wie de aanvrager is en wat de bevoegdheden van deze aanvrager zijn om een bepaalde vraag te stellen. Bij handhaving betreft het artikel 8 informatie en rechercheurs mogen artikel 9 informatie in BVO bekijken.

Vragen politie op straat

Bij een vraag van de straat om bijvoorbeeld een auto na te checken kan de meldkamer alleen in BHV (artikel 8) en het Herkenningsdienst Systeem (HKS) kijken. De Infodesk wordt niet bij de vraag betrokken.

Voor verzoeken om informatie over verdachten wendt een vrager zich tot de Infodesk of ICC-medewerkers belast met deze taak. Vermoedelijk vanaf eind mei 2011 komt er een centrale afhandeling arrestanten afdeling. Hierbij komt Dit is een back-office waar verschillende taken samen komen van onder andere de Infodesk en ICC.

Op 16 december 2011 heeft het korps Zuid-Holland Zuid de volgende aanvullende informatie verstrekt: *'Inmiddels is er een centrale afhandeling van arrestanten gerealiseerd in Dordrecht. Deze afdeling werkt onder de naam ZSM. Daarnaast is er een Front Office Back Office (FOBO) actief die blauw en opsporing ondersteunen op het gebied van het verwerken van informatie en het bevragen hiervan'.*

Controle Wpg-geschiktheid

Bij de Infodesk wordt controle uitgevoerd op het Wpg-geschikt zijn van de informatie. Dit vindt steekproefsgewijs plaats.

De Infodeskmedewerker (informatierechercheur) die de aanvraag in behandeling neemt toetst de noodzakelijkheid van het verzoek en neemt bij twijfel contact op met de leidinggevende van de Infodesk (welke als bevoegde functionaris is aangewezen). Niet in alle gevallen vindt er dus controle van de Bevoegd functionaris plaats op een aanvraag omdat ook een informatierechercheur in staat is om een aanvraag op noodzaak te toetsen.

Samenwerking met de rechercheur

De Infodesk levert lijsten met onderzoeken aan voor de recherche. De lijsten bevatten artikel 9 informatie, bijvoorbeeld woninginbraken.

Wanneer een rechercheonderzoek start op artikel 8 (BVH), en overgaat naar artikel 9 (BVO) en/of informatie uit anderen onderzoeken wordt geraadpleegd, is er toestemming vereist van de OvJ (zaaksofficier en de officier die een zaak voorbereid) en bevoegde functionaris(bij grote zaken). Bij kleinere onderzoeken kan de teamleider zelf toestemming geven.

Codering

De Infodesk levert lijsten met onderzoeken aan voor de recherche. Dit betreft artikel 9 Wpg informatie, bijvoorbeeld woninginbraken. In BVO worden de CIE coderingen gehanteerd. De infodesk kent die wel, maar ziet de informatie met deze coderingen niet.

Deze werkafspraken zijn tijdens de BVO-opleidingen gecommuniceerd met de medewerkers van Opsporing die hiermee te maken krijgen. Ook is dit behandeld bij de terugkomdagen. De researchecoördinatoren zorgen ervoor dat de juiste codering wordt gebruikt. Deze researchecoördinatoren zijn in de artikel 9-onderzoeken veelal de bevoegde functionaris.

Bevoegde functionaris

In 2009 heeft Korps Zuid-Holland Zuid leidinggevendenden vanaf de rang van inspecteur van de politie als 'bevoegde functionaris'. Hierbij is er rekening gehouden met de Wpg en het Besluit Politiegegevens.

De bevoegde functionarissen zijn binnen Zuid-Holland Zuid als volgt ingedeeld:

Voor artikel 9 lid 3 Wpg / art. 11 lid 1 en 3 Wpg / artikel 13 lid 3 Wpg
Hoofd DREO en diens vervanger
Leider TGO en plaatsvervangend tactisch coördinator
Chef Zware Criminaliteit, chef Vreemdelingenrecherche, chef Zedenpolitie, chef ABPM en chefs districtsrecherche
Recherche coördinatoren
ICC-coördinatoren die belast zijn met de dagelijkse leiding aan zaaks keuzevoorbereiding
Chef bureau Veelplegers / PGA en één schriftelijk aangewezen vervanger
Chef Bureau Interne Zaken, voor zover het betreft de gegevens uit onderzoeken die (mede) onder hun aansturing worden verricht

Voor artikel 9 lid 3 Wpg / artikel 11 lid 2 en 4 Wpg / artikel 13 lid 3 Wpg

Chef CIE en diens vervanger, voor zover het betreft politiegegevens die worden verwerkt onder het regime van artikel 10 eerste lid onder a

Voor artikel 10 lid 5 Wpg / artikel 11 lid 2 en 4 Wpg / artikel 13 lid 3 Wpg

Chef RID en één schriftelijk aangewezen vervanger, voor zover betreft politiegegevens die worden verwerkt onder het regime van artikel 10 lid 1c Wpg

Opleiding bevoegd functionaris

Circa 20 leidinggevend en projectleden hebben de 5-daagse Landelijke Wpg-training gevolgd. Meer dan 50 bevoegd functionarissen zijn opgeleid middels een in het korps ontwikkelde eendaagse training. Datzelfde geldt voor zo'n 70 informatie-medewerkers, 15 beleidsadviseurs 40 operationeel leidinggevend, 6 medewerkers post & archief en 25 kerninstructeurs BVH. In totaal zijn zo'n 240 mensen opgeleid en zo'n 900 voorgelicht. De in het korps ontwikkelde trainingen zijn de basis geweest voor de trainingen die nu landelijk worden aangeboden.

Er is een opleidingsprogramma opgesteld voor de bevoegde functionaris met specifieke aandachtspunten voor hun werkgebied en specifieke verdeling van wetsartikelen uit de Wpg.

In een aantal sessies zijn bevoegde functionarissen getraind in de Wpg. Hiermee wordt voldaan aan de Wpg.

Weigeringsgronden

De bevoegd functionarissen zijn getraind in de Wpg. De weigeringsgronden zijn daarbij behandeld. Hiermee wordt voldaan aan de Wpg.

Oordeel over ter beschikking stellen

Het korps Zuid-Holland Zuid voldoet in hoofdlijnen aan artikel 15 Wpg voor het intern delen van politiegegevens.

4.9 Verstrekken (artikel 16/24)

4.9.1

Norm

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

4.9.2

Bevindingen

Verstrekkingenwijzer (landelijk)

De RID stelt gegevens ter beschikking middels de afgesproken NIK/RIC lijn (NIC betreffen de Landelijke Verstreking en RIC betreffen de Regionale Verstreking). De verstrekte informatie is voor operationeel gebruik.

De RID zegt alleen gegevens en informatie aan het bevoegd gezag (i.c. burgemeester) te verstrekken.

Artikel 19-verstrekkingen

In het document *'Toetsing samenwerking en incidentele verstrekkingen 2010'* heeft korps Zuid-Holland Zuid het nodige onderzoek verricht om artikel 19 Wpg toe te lichten en daaromtrent helderheid te verschaffen. Het document bevat een toelichting op artikel 19 Wpg, de afwegingen volgend uit artikel 19 Wpg en een beschrijving van een voorbeeld ter toelichting van de wetpassages. In deze beschrijving wordt ook het gebruik van het I90-formulier in BVH toegelicht.

Artikel 19-verstrekkingen dienen te worden geregistreerd in I90-formulieren.

Er vindt geen directe controle op incidentele gegevensverstrekking plaats binnen het korps. De verzoeken die door externe partners aan de politie worden gedaan komen bij de privacyfunctionaris van het korps terecht. Deze verzoeken en eventuele verstrekkingen die hieruit voortvloeien worden opgeslagen en gearcheeerd in Corsa.

Convenanten (artikel 20 besluiten)

Het korps Zuid-Holland Zuid heeft een inventarisatie uitgevoerd van bestaande convenanten. De inventarisatie heeft 25 convenanten opgeleverd, waarvan er 16 als Wpg-relevant zijn aangemerkt. Een convenant bleek Wpg-geschied, een tiental ver-eiste aanpassing of opzegging.

Er zijn 16 convenanten van kracht. De privacyfunctionaris houdt een overzicht van de actieve convenanten. In dit overzicht zijn ook de betrokken partijen inzichtelijk gemaakt en staat de looptijd.

Niet alle originele convenanten zijn echter gearcheeerd en in beheer bij de privacy-functionaris, zo blijkt uit het overzicht. Tevens blijkt dat van 4 van de 16 actieve convenanten geen origineel exemplaar aanwezig is.

Implementatieteam

Het implementatieteam heeft voorgesteld om nieuwe convenanten te splitsen in een document met samenwerkingsafspraken (convenant) en een besluit ex artikel 20 Wpg (uitwisselingsbesluit). Door een splitsing aan te brengen wordt het mogelijk om de voorbereiding van een samenwerkingsverband bij een partner te beleggen. Tevens wordt de politie-inzet beperkt tot het maken van een eenvoudig besluit om in

het kader van het samenwerkingsverband gegevens te kunnen verstrekken. Voor een dergelijk uitwisselingsbesluit heeft het team een opzet ontwikkeld, dat tot landelijk model is verheven.

Dit implementatieteam heeft vervolgens de niet Wpg-geschikte convenanten waar nodig aangevuld. Voorheen waren er convenanten met bijvoorbeeld scholen en zwembaden waar de politie alleen informatie van ontving en geen eigen informatie mee uitwisselde. In dit soort situaties zijn geen nieuwe convenanten gemaakt. Andere convenanten die wel Wpg-relevant waren, zijn verder onderzocht. Er is gekeken of de oude convenanten nog in gebruik waren en welke aanvullingen noodzakelijk waren om te voldoen aan de Wpg. Aan de bestaande of nieuwe convenanten is een Besluit Wpg toegevoegd. De verouderde convenanten zijn beëindigd.

Nadat het implementatieteam opgehouden is te bestaan, is de verantwoordelijkheid voor het afsluiten van convenanten neergelegd bij het lijnmanagement. De districts- hoofden hebben een brief ontvangen waaruit blijkt dat de verantwoordelijkheid in de lijn kwam te liggen en dat de werkgroep/implementatieteam ophield te bestaan. In het vervolg worden nieuwe convenanten voorgelegd aan de portefeuillehouder WPG en aan het OM, voordat ze worden ondertekend door of namens de korpsbeheerder.

Het verstrekken van gegevens aan ketenpartners vindt tegenwoordig plaats aan de hand van een door korps Zuid-Holland Zuid opgesteld samenwerkingsconvenant (ex art. 20 WPG) dat alle ketenpartners hebben ondertekend. Het convenant wordt getoetst door de projectleider Wpg en de privacyfunctionaris van het korps Zuid-Holland Zuid. Het getekende convenant behoort in het bezit te zijn van de privacyfunctionaris korps Zuid-Holland Zuid.

Er is een mandateringsregeling met betrekking tot het tekenen van convenanten. Dit mandaat gaat niet verder dan de districtchef.

Proces voor artikel 20 besluiten

Voor het aangaan van samenwerkingsverbanden en het opstellen van nieuwe convenanten is binnen Zuid-Holland Zuid een procesbeschrijving '*stappenplan t.b.v. structurele samenwerkingsverbanden*' opgesteld. Deze beschrijving is voorzien van een checklist welke dient te worden nagelopen wanneer men voornemens is een samenwerkingsverband aan te gaan. Alle relevante zaken zoals deze worden gesteld in de Wpg komen in deze checklist aan bod.

Aanvullend hierop zijn enkele richtlijnen binnen Zuid-Holland Zuid vastgesteld onder de noemer: '*de 10-geboden artikel 20 WPG*'. De bedoeling hiervan is het aantal personen te beperken dat bevoegd is om politiegegevens te verstrekken aan samenwerkingsverbanden. Die beperking is noodzakelijk om te borgen dat aan verstrekking een noodzakelijkheidstoets voorafgaat, dat de ontvanger bekend wordt met de geheimhoudingsplicht en dat de verstrekking wordt vastgelegd. Dat laatste moet gebeuren op een wijze waardoor de privacy functionaris op ieder moment kan beschikken over een totaaloverzicht.

De meeste convenanten worden opgemaakt door tussenkomst van de wijkpolitie. Men zegt dat de wijkpolitie Wpg-opgeleid zijn en de convenantprocedure kennen. Tevens is er in de regio een klein begeleidingsteam beschikbaar om te adviseren over convenanten.

Vastgesteld is dat de opzet met betrekking tot de informatieverstrekking met derden goed is vastgelegd. Het korps heeft veel aandacht besteed om de vele niet

Wpg-geschikte convenanten om te zetten naar convenanten die wel als Wpg-proof kunnen worden aangewezen.

Het proces voor opstellen van convenanten heeft aantoonbaar gewerkt.

Inhoud convenanten

De convenanten die volgens de nieuwe opzet van korps Zuid-Holland Zuid zijn ingericht voldoen aan de wettelijke vereisten van artikel 20 lid 2 Wet politiegegevens.

Overzicht verstrekkingen aan derde partijen

Binnen het korps Zuid-Holland-Zuid is met betrekking tot de artikel 19 en artikel 20 verstrekking een procesbeschrijving geformeerd. In deze beschrijving wordt ook het gebruik van het I90-formulier in BVH toegelicht. Voor een dergelijke verstrekking moet op het formulier worden verwezen naar het onderliggende convenant.

De protocolgegevens van de verstrekking worden bewaard in de vorm van de I90-formulieren in BVH of indien de privacyfunctionaris verstrekt als document in Corsa. Zowel voor de I90-formulieren in BVH als de stukken die onder verstrekkingen in Corsa worden opgeslagen, wordt een bewaartermijn van 5 jaar gehanteerd.

Beleid bij de Politie Zuid-Holland Zuid is dat alle individuele verstrekkingen worden vastgelegd conform de eisen in de Wpg. In het geval van bijvoorbeeld het Veiligheidshuis worden (individuele) verstrekkingen aan de ketenpartners niet vastgelegd in een BVH-mutatie. De verslagen vanuit de PGA-overleggen dienen als verantwoording van de gegevensverstrekking.

Veiligheidsregio

Meldkamer

Vanuit de Gemeenschappelijke Meldkamer worden alle partijen op de hoogte gesteld van de melding in GMS. Alle partijen kunnen immers in GMS en zijn in dienst van de politie. Echter is dit strijdig met artikel 15 Wpg. Medewerkers van Ambulance en/of Brandweer kunnen ook informatie lezen over politiezaken wanneer dit gekoppeld is aan een actie van de Ambulance en/of Brandweer. Het korps dient juiste afspraken te maken over het beschikbaar stellen van informatie onderling in het kader van de Wpg. Momenteel is dit namelijk nog niet waterdicht.

Er is geen samenwerkingsconvenant tussen de diensten op de Gemeenschappelijke Meldkamer Centrale (GMC) van regiopolitie Zuid-Holland-Zuid. Er vindt dan ook niet vanzelfsprekend uitwisseling van politiegegevens plaats richting de ambulancedienst en/of de brandweer op de GMC. De politiegegevens worden alleen in uiterste noodzaak uitgewisseld aan de brandweer of ambulancedienst.

Bandopnames op de GMC worden voor de duur van 10 jaar bewaard. Er wordt gebruik gemaakt van het systeem EVA en is alleen voor geautoriseerde medewerkers toegankelijk. Een centralist kan tijdens een lopende dienst tot zes uur terug bandopnames beluisteren. Daarna kunnen deze opnames alleen via een aanvraagformulier worden opgevraagd via de leidinggevende van de GMC.

RIEC

Zie voor de werking van het RIEC de aangeleverde RIEC-brochure. Het RIEC ontvangt informatie van de het korps door middel van een verstrekkingformulier. Deze informatie is meestal van de reguliere Infodesk bij het korps. Eén medewerker van het RIEC (gedetacheerd vanuit politie Zuid-Holland Zuid aan de RIEC) is feitelijk op locatie werkzaam bij de reguliere Infodesk van het korps en verzameld informatie.

Het RIEC werkt er naar toe om deze medewerker RIEC om te zetten naar Informatiecoördinator bij de Infodesk Zuid-Holland Zuid.

Het verstrekken van deze informatie aan RIEC gebeurt na toestemming van de coördinator Infodesk, die door de korpsleiding is aangewezen als bevoegd functionaris. Deze filtert voor elke verstrekking op basis van het vereiste van "zwaarwegend belang". Het hoofd Infodesk ondertekent mede het verstrekkingformulier.

Indien het Wpg artikel 9 informatie betreft zal ook de betreffende teamleider van de zaak, die door de korpsleiding als bevoegde functionaris is aangewezen, toestemming verlenen voor het verstrekken van de informatie. De coördinator Infodesk is de functionaris die hierop toeziet en zorgt voor de vereiste toestemming van de teamleider van de zaak.

Convenantendatabank

Door de privacyfunctionaris van het korps Zuid-Holland Zuid wordt er een (geactualiseerd) overzicht bijgehouden van de convenanten en besluiten voor verstrekkingen op grond van artikel 20 Wet politiegegevens. In totaal zijn er 16 convenanten geïdentificeerd en opgenomen in dit overzicht.

De volgende gegevens worden hierin per convenant vermeld:

- Naam van het convenant.
- De betrokken partijen.
- Doel van de gegevensverstrekking.
- Welk zwaarwegend algemeen belang er aan het convenant ten grondslag ligt.
- Welke gegevens er worden verstrekt.
- Wat de looptijd van het convenant is.
- Wanneer de convenant is ondertekend.
- Of de convenant Wpg-proof is.

Verstrekkingenschema (regionaal)

Tijdens de opleidingen en in de interne communicatie is deze procedure steeds toegelicht. Daarbij is ook ingegaan op het vastleggen, het protocolleren van deze verstrekking in BVH via I-90.

Op basis van de beschikbare informatie kan niet worden vastgesteld welk onderdeel van het district informatie verstrekt zoals vastgelegd in de landelijke verstrekkingenwijzer.

Proces voor geautomatiseerde verstrekking

Er vindt binnen politieregio Zuid-Holland Zuid geen geautomatiseerde verstrekking plaats. Wanneer er politiegegevens worden verstrekt zit daar altijd een persoon tussen.

Geheimhouding verstrekking informatie

Het verstrekken van gegevens vindt plaats aan de hand van een door het korps Zuid-Holland Zuid vastgesteld model 'bestuurlijke rapportage'. In dit model wordt ook voorzien dat degene aan wie politiegegevens worden verstrekt, wordt gewezen op de geheimhouding.

Binnen het ontwikkelde format voor de artikel 20 besluiten/convenanten is ook de geheimhouding opgenomen. Op deze manier zijn alle partijen gewezen op de geheimhouding. In het format van de bestuurlijke rapportage (ook binnen de I90 aanwezig) dat gebruikt wordt voor de verstrekking (zowel de art. 19 als art. 20 verstrekkingen) is eveneens deze geheimhouding opgenomen.

Protocollering verstrekking

Voor de verstrekkingen aan derden is een procedureafspraken gemaakt hoe deze te registreren in BVH. Dit schriftelijk vastleggen gebeurt middels een I90-formulier. Er wordt geconstateerd dat slechts in een enkel geval aan deze afspraak wordt voldaan.

In 2010 zijn er binnen BVH 12-tal I90-formulieren opgemaakt en in 2011 zijn dit er tot op heden 20. Omdat het vastleggen van verstrekkingen middels het I90-formulier niet consequent is gebeurd, wordt hier tijdens de BVH-kwaliteitsdagen extra aandacht aan besteed en is de noodzaak van het opmaken van het I90-formulier benadrukt.

Een deel van de verstrekkingen geschiedt al jaar en dag via een standaard procedure, bijvoorbeeld de verstrekkingen aan de Stichting processen verbaal, BIBOB, HALT etc. Voor de verstrekkingen aan het bestuur is een format bestuurlijke rapportage ontwikkeld. Bij besluiten ex artikel 20 Wpg staat de wijze van verstrekking en vastlegging beschreven in het besluit. Daar waar geen standaardprocedure is, geldt dat verstrekkingen worden vastgelegd in BVH onder de maatschappelijke klasse I90.

Momenteel worden door de interne auditor de verstrekkingen binnen de actieve convenanten getoetst, om zodoende ook hierin het vastleggen van de verstrekkingen in een bestuurlijke rapportage (I90), voor zover dit nog niet gebeurt, te realiseren binnen het korps Zuid-Holland Zuid.

Jeugdzorg

Volgens artikel 18 Wet politiegegevens mag structureel worden verstrekt aan derden die bij Algemene Maatregel van Bestuur zijn aangewezen, zoals bureau HALT en de Raad voor de Kinderbescherming. Hiervan wordt door Korps Zuid-Holland Zuid een proces-verbaal Minderjarige (PVM) opgemaakt. Verstrekkingen aan Jeugdzorg vinden structureel plaats via een zorgformulier en vastgelegd in BVH.

Er zijn 1894 [2009] en 1561 [2010] zorgmeldingen verstrekt aan Jeugdzorg.

Bewaren protocolgegevens verstrekking

Verstrekkingen die worden vastgelegd in BVH middels het I90-formulier worden bewaard voor een termijn van 5 jaar. Na de termijn worden deze formulieren geschoond. De verstrekkingen die de privacyfunctionaris verricht worden opgeslagen in Corsa en eveneens voor 5 jaar bewaard).

Toezicht leidinggevend op verstrekkingen en protocollering

Binnen het korps zijn voor de art. 19 en art. 20 Wpg-verstrekkingen zogenaamde 10-geboden samengesteld die zijn gecommuniceerd met de medewerkers. Deze 10-geboden worden gebruikt als leidraad bij het beoordelen van een verstrekking door een leidinggevende. Daarnaast wordt ook de landelijk opgestelde verstrekkingenwijzer gehanteerd.

4.10 Rechten van betrokkenen (artikel 25/28)

4.10.1 Norm

De verantwoordelijke deelt een ieder op diens schriftelijk verzoek binnen zes weken mede of, en zo ja welke, deze persoon betreffende politiegegevens zijn vastgelegd.

4.10.2 Bevindingen

Inzagerecht

Binnen Korps Zuid-Holland Zuid is er een procedure uitgewerkt om de verzoeken van betrokkenen in goede banen te leiden. De procedure gaat uit van een centrale regie. De verzoeken worden gericht aan de verantwoordelijke met betrekking tot de verwerking van politiegegevens, de korpsbeheerder. De verzoeken zullen namens de korpsbeheerder moeten worden afgehandeld. Overigens heeft de korpsbeheerder deze bevoegdheid gemandateerd aan de korpschef.

Jaarlijks komen er tussen de 20 á 30 inzageverzoeken binnen bij de privacyfunctionaris van Zuid-Holland Zuid. Het kan voorkomen dat er inzage verzoeken worden afgewezen. Tot op heden is dit echter nog niet gebeurd in Zuid-Holland Zuid.

De privacyfunctionaris beoordeelt de inzageverzoeken aan de hand van de formulering van artikel 25 Wpg (criteria). De privacyfunctionaris reageert binnen 4 weken op een inzageverzoek. De termijnen voor de inzagen worden gehaald, en met betrekking tot deze termijnen zijn er geen klachten bekend binnen Zuid-Holland Zuid.

Alle verzoeken en de hierop volgende handelingen worden gerapporteerd in Corsa. Er is in 2011 één keer een klacht ingediend welke ongegrond werd verklaard. Dit betrof een klacht over het feit er wel stukken ter inzage werden aangeboden, maar dat van deze stukken geen kopieën werden verstrekt aan de verzoeker.

In 2010 ontving het korps Zuid-Holland Zuid 1.696 verzoeken. Dit zijn onder andere verzoeken van advocaten, verzekeringsmaatschappijen, gemeenten en betrokkenen. Al deze verzoeken zijn in Corsa gearcheeerd.

Verzoeken over 2010

	Aantal
Inlichting verzoek uit proces-verbaal	503
Verzoek inlichting uit politieregister	1.026
Inzageverzoeken	167

De procedure

- 1 Verzoeken om kennisneming van de eigen gegevens van betrokkene dienen schriftelijk en onder vermelding van naam, volledige voornamen, volledig adres en geboortedatum per post te worden gericht aan:

De korpschef van het regionaal politiekorps Zuid-Holland-Zuid,
t.a.v. de privacyfunctionaris,
Postbus 1070,
3300 BB te DORDRECHT

- 2 De privacyfunctionaris neemt het verzoek in behandeling en laat aan de aanvrager een ontvangstbevestiging sturen.

- 3 De privacyfunctionaris stuurt een brief aan de verzoeker en biedt de mogelijkheid om het wettelijk vastgestelde bedrag van € 4,50 te storten op het centrale bankrekeningnummer van de politie Zuid-Holland-Zuid. Na ontvangst van dit bedrag is het inzageverzoek ontvankelijk.
- 4 Na ontvangst van het bedrag van € 4,50 wordt het verzoek binnen zes weken afgehandeld door de privacyfunctionaris. Eventuele verdaging met vier, dan wel zes weken is mogelijk. Hij draagt zorg voor een deugdelijke vaststelling van de identiteit van de verzoeker.
- 5 De privacyfunctionaris maakt bij inzageverzoeken onderscheid naar "zuivere" en "onzuivere" inzageverzoeken. Met een "zuiver" inzageverzoek wordt bedoeld een verzoek van een belanghebbende om te weten komen of er persoonsgegevens over hem/haar bij de politie worden verwerkt. Met een "onzuiver" inzageverzoek wordt bedoeld een verzoek om informatie van bijvoorbeeld een advocatenkantoor of een woningstichting. Dergelijke verzoeken worden veelal doorverwezen naar het secretariaat van de districtsleiding, tenzij er spoed bij de afhandeling gewenst is. Dan neemt hij de afhandeling van een dergelijk informatieverzoek zelf ter hand.
- 6 Aan het verzoek wordt geen gevolg gegeven/afgewezen wanneer het belang van artikel 27 Wpg in het geding is. Een gehele of gedeeltelijke afwijzing vindt steeds schriftelijk plaats.

Inzageverzoeken worden geregistreerd in het postregistratiesysteem (Corsa).

De privacyfunctionaris heeft geen vervanger als hij bijvoorbeeld met vakantie gaat. Een procedure/werkinstructie met betrekking tot inzage-/correctieverzoeken is beschikbaar, dus indien nodig kan dit door iemand anders worden overgenomen.

Recht op correctie

Ook met betrekking tot het recht op correctie is er een procedure vastgesteld. Deze wordt als volgt weergegeven:

- 1 Degene aan wie overeenkomstig artikel 25 Wpg kennis is gegeven van hem betreffende politiegegevens, kan de verantwoordelijke schriftelijk verzoeken deze te verbeteren, aan te vullen, te verwijderen of af te schermen. Het verzoek wordt gericht aan:

De korpschef van het regionaal politiekorps Zuid-Holland-Zuid,
t.a.v. de privacyfunctionaris,
Postbus 1070,
3300 BB te DORDRECHT.

- 2 De adviseur beveiliging & privacy toetst het verzoek op ontvankelijkheid.
- 3 Indien ontvankelijk, pleegt de privacyfunctionaris overleg met degene die de "dagelijkse leiding" heeft over het betreffende verwerking en legt een advies met betrekking tot het recht op verbetering, aanvulling, verwijdering of afscherming van gegevens voor aan het Hoofd Politiezonele Bedrijfsvoering. Het Hoofd Politiezonele Bedrijfsvoering bepaalt of, en in welke mate, gevolg wordt gegeven aan het verzoek. Het verzoek wordt binnen vier weken na binnenkomst van het verzoek door de privacyfunctionaris afgehandeld. Hij legt de afhandeling vast in een verslag dat wordt gearhiveerd bij de privacyfunctionaris. Een weigering dient gemotiveerd en schriftelijk te geschieden en is een besluit in de zin van de Algemene wet bestuursrecht.

- 4 Indien een verzoek leidt tot verbetering, aanvulling, verwijdering dan wel afscherming, wordt het bedrag van € 4,50, dat betaald is voor het inzageverzoek, teruggestort op de bank- of girorekening van betrokkene. De privacyfunctionaris draagt hier ten spoedigste zorg voor.
- 5 Indien een verzoek leidt tot verbetering, aanvulling, verwijdering, dan wel afscherming, dient aan degenen, aan wie foutieve gegevens zijn verstrekt in het jaar, voorafgaand aan de datum van het verzoek, en in de sinds dat verzoek verstreken periode, daarvan mededeling te worden gedaan.

Logboek van gedane verstrekkingen

Degene die belast is met de dagelijkse leiding over de verwerking van politiegegevens is hiervoor verantwoordelijk. Voor het Herkenningsdienstsysteem(HKS) is de coördinator regiobeveiliging HKS belast met de dagelijkse leiding.

Mededeling van verbetering, aanvulling, verwijdering of afscherming

Er vindt geen mededeling van verbetering, aanvulling, verwijdering of afscherming plaats bij korps Zuid-Holland Zuid. Men geeft hiervoor de volgende reden:

'Controle op gegevens die naderhand worden gewijzigd is handmatig ondoenlijk en ICT-technisch niet mogelijk. Er wordt binnen ZHZ dan ook niet op toegezien dat wijzigingen van gegevens worden gecommuniceerd met derden die inzage hebben gehad dan wel politiegegevens verstrekt hebben gekregen. Het handmatig nalopen om na te gaan of er binnen verstrekte of ter inzage aangeboden politiegegevens wijzigingen hebben plaatsgevonden is dermate arbeidsintensief dat dit onmogelijk is uit te voeren.'

4.11 Protocolplicht (artikel 32)

4.11.1

Norm

De verantwoordelijke draagt zorg voor de schriftelijke vastlegging van:

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

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

4.11.2

Bevindingen

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

Protocollering doel onderzoek

Voor de vastlegging van een artikel 9-onderzoek is binnen het korps Zuid-Holland Zuid afgesproken dat deze middels een MRO wordt gemeld. Deze meldingen komen per e-mail bij de privacyfunctionaris terecht. Deze bewaart de meldingen.

Op basis van de gegevens van de privacyfunctionaris werden er in 2009 en 2010 respectievelijk 203 en 109 artikel 9 Wpg-zaken aangemeld. Er worden echter geen artikel 9 Wpg-zaken afgemeld. De privacyfunctionaris geeft aan dat het overzicht *verre van volledig* is.

Binnen ZHZ is een protocol 'opstarten artikel 9-onderzoek' in de vorm van een checklist opgesteld en gecommuniceerd naar de medewerkers, met name naar de recherchecoördinatoren. Deze checklist is een hulpmiddel om te voorkomen dat iets wordt overgeslagen of wordt vergeten wanneer er wordt aangevangen met een artikel 9-onderzoek. Deze checklist (die is aangeleverd bij de DAD) bestaat uit de onderstaande acties.

CHECKLIST START ONDERZOEK artikel 9 WPG

- Bevoegd functionaris benoemen.
- BVO-verwerking starten en doel onderzoek vastleggen.
- Teamleden en ondersteuners autoriseren.
- MRO aanmaken en onderhouden.
- Afspraken maken over opslag onderzoeksgegevens.
 - DCS-bestanden.
 - Analysebestanden.
 - Gegevensopslag op netwerk ZHZ.
 - BVO-BVH.
- Afspraken maken over coderen van onderzoeksgegevens.
 - Operationeel bruikbare informatie.
 - BOB-gegevens.

- Desgewenst opdracht 11.4 vragen aan OM.
- Regeling treffen voor vastleggen van verstrekkingen.
- Afspraken maken over schoning van gegevens.

Deze checklist wordt binnen Opsporing gebruikt om er voor te zorgen dat er tijdige en juiste vastlegging van artikel 9-onderzoeken plaatsvindt en er afspraken worden gemaakt over de schoning van gegevens.

Bewaren protocollering doel onderzoek

Bij de start van een artikel 9-onderzoek, wordt door de researchcoördinator een BVO registratie voorzien van startmutatie en wordt er een MRO aangemaakt. In Zuid-Holland Zuid zijn al deze coördinatoren aangewezen als bevoegd functionaris. In de MRO wordt het doel van het onderzoek verantwoord. Op deze manier zijn alle artikel 9-onderzoeken binnen het korps inzichtelijk voor de privacyfunctionaris. Deze voert echter geen steekproeven uit op de vastlegging van doelen van onderzoek.

Daarnaast maakt de researchcoördinator op de O-schijf in de artikel 9 map een map ten behoeve van dit onderzoek aan en autoriseert hier alleen de medewerkers van de recherche voor die belast zijn met dit onderzoek. Deze map is voorzien van het desbetreffende BVO-nummer zodat deze gelijktijdig met de BVO-registratie in BVO kan worden geschoond. De gegevens met betrekking tot het vastleggen (MRO voorzien van startmutatie) van het doel van een onderzoek worden in BVO bewaard voor een termijn van 5 jaar.

Protocollering artikel 13 gegevensverzameling

Binnen het korps Zuid-Holland Zuid wordt gebruik gemaakt van de applicatie Amazone. Het aanmaken van doelgroepen binnen deze applicatie dient voorzien van een motivatie te worden aangevraagd bij de chef Intelligence/ korpsprojectleider Wpg. De laatstgenoemde toetst aan de hand van het doel en de categorie personen of verwerking van een doelgroep binnen Amazone mogelijk is. De beheerder van Amazone ziet er op toe dat Amazone op de juiste manier wordt gebruikt en niet wordt vervuild. Verder maakt het korps gebruik van de volgende (landelijke) artikel 13 systemen:

- Amazone
- HKS
- NSYS
- OPS
- PAPOS
- BVI

Bewaren protocolgegevens artikel 13 gegevensverzameling

De aanvragen voor een doelgroep in Amazone worden gearchiveerd. Wanneer een nieuwe doelgroep wordt aangemaakt, wordt schriftelijk vastgelegd wie de verantwoordelijke medewerker (eigenaar) wordt van de doelgroep, de beheerder van de doelgroep en welke regime van toepassing is. Tevens wordt de termijn vastgelegd en wordt bepaald dat er gegevens van een dergelijke doelgroep worden vastgelegd in Amazone. Voor het aanvragen van een doelgroep wordt de format gebruikt zoals deze in Rotterdam-Rijnmond is ontwikkeld.

Protocollering onrechtmatige handeling

Wanneer er verwerkingen hebben plaatsgevonden die door onbevoegden zijn gedaan of anderszins onrechtmatig zijn verricht, wordt dit gemeld bij de privacyfunctionaris.

De privacyfunctionaris legt deze gemelde incidenten vast in het zogeheten 'Zwartboek' waardoor een overzicht van deze meldingen aanwezig is. Zo wordt bij de PF bijvoorbeeld gemeld dat iemand met het password van iemand anders heeft ingelogd en gegevens heeft vastgelegd/verwerkt.

Deze meldingen die de functionaris ontvangt, zijn geanonimiseerde meldingen en bevat geen persoonsgegevens in de zin van de Wpg. Aan de hand van het overzicht van de privacyfunctionaris wil het korps kunnen zien of dergelijk onrechtmatig handelen af of toeneemt.

Wanneer er sprake is van onrechtmatig handelen waarvan een leidinggevend/districtchef meent dat er hierop disciplinaire maatregelen genomen moeten worden, neemt de Districtchef zelf disciplinaire maatregelen of wordt dit gemeld bij BIZ (Bureau Interne Zaken).

Bewaren protocolgegevens onrechtmatige handeling

Het 'Zwartboek' wordt door de privacyfunctionaris bijgehouden en bewaard.

Gemeenschappelijke verwerking

Het korps heeft geen gemeenschappelijke verwerking met een ander korps.

4.12 Audits (artikel 33)

4.12.1

Norm

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

4.12.2

Bevindingen

Interne audit functie

Interne auditfunctie

Uit de gesprekken en de ondersteunende documentatie is gebleken dat veel tijd en moeite is gestoken in het Wpg-geschied maken van Korps Zuid-Holland Zuid. Middels het Project Initiatie Implementatie Wet politiegegevens heeft men een zorgvuldig uitgewerkt plan opgesteld om de Wpg gefaseerd te implementeren.

Bovendien heeft het korps jaarlijks de voortgang van deze implementatie middels voortgangsverslagen bijgehouden. Het laatste verslag dateert uit 2009. Er is echter op het moment van rapporteren (media 2011) geen auditor aangewezen en er zijn de afgelopen jaren geen interne audits verricht die de vorderingen intern heeft getoetst.

Vanaf het vierde kwartaal van 2011 heeft Korps Zuid-Holland Zuid een interne auditor aangewezen die zich tevens bezig gaat houden met de verdere implementatie van de Wpg.

Intern audit-plan

Er zijn geen interne audits verricht in de afgelopen jaren. Ook ontbreekt een intern audit-plan. Het korps Zuid-Holland Zuid heeft op 16 december 2011 meegedeeld dat een auditplan zal worden opgesteld aan de hand van het auditrapport van de externe privacy auditor, dat zal worden voorgelegd aan de korpsleiding.

Interne audit rapport

Er zijn geen interne audits verricht in de afgelopen jaren. Interne audit rapporten zijn derhalve ook niet beschikbaar.

4.13 Privacyfunctionaris (artikel 34)

4.13.1 Norm

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

4.13.2 Bevindingen

Benoeming en melding

Er is een privacyfunctionaris in het korps Zuid-Holland Zuid aangewezen onder de Dienst Stafbureau Korpsleiding. Zijn officiële functie is controller beveiliging (categorie beleidsadviseur).

De privacyfunctionaris is in 2009 aangemeld bij het College Bescherming Persoonsgegevens.

De rol van de privacyfunctionaris

Er is niet voorzien in procedures en/of werkinstructies die voor de privacyfunctionaris van toepassing zijn. De handreiking privacyfunctionaris worden als uitgangspunt gebruikt. Uit het gesprek blijkt echter dat ten tijde van de audit de taakomschrijving nog niet geheel was uitgekristalliseerd.

De privacyfunctionaris geeft aan dat er onvoldoende tijd beschikbaar is voor de toezichthoudende rol als privacyfunctionaris. Hij kan niet aan alle taakvereisten van de Wpg voldoen. Het takenpakket wordt dan ook – naar eigen zeggen – slechts gedeeltelijk uitgevoerd.

Goedkeuring autorisaties

De privacyfunctionaris keurt via de e-mail binnenkomende aanvragen van het OM voor autorisaties voor het systeem BVH goed alvorens deze door te zetten naar functioneel beheer. Hiertoe heeft de privacyfunctionaris een procedure opgesteld. Tevens controleert de privacyfunctionaris de autorisaties periodiek op actualiteit.

Advisering

Uit de interviews blijkt dat de privacyfunctionaris binnen het korps bekend is en men hem, waar nodig, om advies vraagt betreffende privacy gerelateerde zaken. Ook worden er veel vragen gesteld aan de voormalig Wpg-projectleider, die nog fungeert als informele vraagbaak.

Protocollering

Hieronder volgt een overzicht van de schriftelijke vastlegging van de privacyfunctionaris:

- De privacyfunctionaris houdt een overzicht bij van de autorisaties van de korpsleden voor de hoofdsystemen als BVH, BVO. Hij controleert de autorisaties periodiek op actualiteit. Er is echter geen recent overzicht beschikbaar van de toekenning van autorisaties als bedoeld in artikel 6 Wpg. De privacyfunctionaris heeft bovendien geen goed zicht op het muteren van autorisaties via het loket ondersteuning.
- Er wordt een overzicht bijgehouden van de convenanten en besluiten voor verstrekingen op grond van artikel 20 Wpg.

- Overige verstrekkingen aan derden op grond van artikel 18 en 19 van de Wpg worden geregistreerd in Corsa, een postregistratiesysteem. Daarbij houdt de PF in een eigen registratie bij aan wie hijzelf welke informatie heeft gestuurd.
- De privacyfunctionaris houdt een overzicht bij van onrechtmatige verwerkingen in het Zwartboek.
- De privacyfunctionaris houdt geen overzicht bij van geautomatiseerde vergelijkingen op basis van artikel 11 Wpg. Hij krijgt daarover geen informatie aangeleverd.
- Er zijn 2009 twee en in 2010 drie personen geweest die daadwerkelijk inzage hebben gehad in hun persoonsgegevens. Dit zijn verzoeken op basis van artikel 25 van de Wpg.
- In 2009 zijn 203 en in 2010 zijn 109 artikel 9-onderzoeken aangemeld. De privacyfunctionaris geeft echter aan dat dit overzicht verre van volledig is.

Jaarverslag

Privacyfunctionaris van Korps Zuid-Holland Zuid heeft over de jaren 2009 en 2010 een gecombineerd jaarverslag afgeleverd met daarin zijn bevindingen met betrekking privacy-gerelateerde zaken. Ook bevat het een verslag van de werkzaamheden voor het korps. Het jaarverslag 2009 en 2010 is door de privacyfunctionaris niet officieel aangeboden aan de korpsleiding van Zuid-Holland Zuid. Om deze reden heeft het korps dan ook nog niet kunnen acteren op de verbeterpunten die door de privacyfunctionaris worden aangedragen in zijn jaarverslag.

De centrale bevindingen zijn:

- Een zorgpunt is dat nog niet inzichtelijk te maken is welke geautomatiseerde vergelijkingen plaatsvinden.
- Er is in 2009 is nog niet begonnen met het inzichtelijk maken en vaststellen van de doelstellingen van artikel 13 verwerkingen.
- Nog niet iedereen heeft de Wpg tussen de oren. Er is echter wel progressie. Inmiddels voldoet het korps Zuid-Holland Zuid op hoofdlijnen aan de eisen van de Wpg, zoals:
 - De inbedding van beheersmaatregelen.
 - Een borging door middel van beschrijvingen van werkprocessen met koppeling naar de Wpg vindt plaats.
 - Het korps heeft een privacyfunctionaris aangewezen en benoemd.
 - De Bevoegde Functionarissen zijn benoemd en opgeleid.

De privacyfunctionaris heeft een jaarverslag opgesteld met daarin zijn bevindingen. Daarmee is aan de formele vereisten voor een jaarverslag voldaan conform artikel 34 lid 3 van de Wpg. Doordat het rapport niet is aangeboden aan de korpsleiding, wordt niet voldaan aan artikel 34 lid 1, waarin is gesteld dat de privacyfunctionaris namens de verantwoordelijke toeziet op de verwerking van politiegegevens. Hieraan wordt alleen voldaan als de verantwoordelijke ook daadwerkelijk wordt ingelicht over eventuele verbeterpunten. Hierdoor is de opvolging van de aangedragen verbeterpunten en daaruit voortvloeiende actiepunten nog niet inzichtelijk gemaakt.

4.14 Functionaris Gegevensbescherming (artikel 36)

De functionaris gegevensbescherming bestaat niet als functie bij korps Zuid-Holland Zuid.