



Ministerie van Veiligheid en Justitie

Audit Wpg politie Zaanstreek Waterland

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

drs. [REDACTED] RE CISA
drs. [REDACTED] RO CIA

T [REDACTED]
M wpg@minvenj.nl

Projectnaam

Audit Wet Politiegegevens

Ons kenmerk

DDS/5719692/11

Auteurs

[REDACTED] MSc

I

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 (artikel 1.f) 25
- 4.3 Kwaliteitsaspecten van politiegegevens (artikel 3 en 4) 26
- 4.4 Gevoelige gegevens (artikel 5) 32
- 4.5 Autorisatie (artikel 6) 33
- 4.6 Geautomatiseerd Vergelijken (GV)/In Combinatie Met Elkaar Verwerken (ICMEV)(artikel 11) 35
- 4.7 Bewaartermijnen (artikel 14) 38
- 4.8 Ter beschikking stellen (artikel 15) 42
- 4.9 Verstrekken (artikel 16/24) 46
- 4.10 Rechten van betrokkenen (artikel 25/28) 51
- 4.11 Protocolplicht (artikel 32) 52
- 4.12 Audits (artikel 33) 54
- 4.13 Privacy functionaris (artikel 34) 55
- 4.14 Functionaris Gegevensbescherming (artikel 36) 56

1 Assurance Verklaring

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

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 Zaanstreek Waterland.

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 Zaanstreek Waterland, naar de stand van ultimo november 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 Zaanstreek Waterland te nemen maatregelen. Ook is gebleken dat het korps Zaanstreek Waterland voor het volledig kunnen voldoen aan de Wpg eisen mede afhankelijk is van besluiten die buiten het korps Zaanstreek Waterland 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 Zaanstreek Waterland, 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 Zaanstreek Waterland. Het verbeterrapport en de uitgevoerde hercontrole zullen in de navolgende jaren door de privacy auditor worden beoordeeld.

Den Haag, 3 januari 2012

De Directeur van de Departementale Auditdienst

J.C. van Praat RE RA

2 Samenvatting

Het korps Zaanstreek-Waterland heeft een aantal zaken in opzet goed opgepakt, zoals:

- Het korps Zaanstreek-Waterland heeft veel aandacht besteed aan de analyse van de Wet politiegegevens (Wpg). Er is zichtbaar veel werk gestoken in het toepassen van deze wet op de relevante werkprocessen en dit op een heldere manier inzichtelijk te maken voor de betrokken actoren binnen deze processen. Per functie heeft het korps een werkdocument ontwikkeld waarin de van toepassing zijnde Wpg-artikelen kort en bondig worden uitgelegd.
- Het implementatietraject dat gevolgd is om het korps Wpg-geschikt te maken heeft (in opzet) zichtbaar zijn vruchten afgeworpen.
- De privacyfunctionaris functioneert als vraagbaak voor het gehele korps. Voor alle Wpg-gerelateerde vragen kan men daar terecht zo blijkt uit de gehouden gesprekken.

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 opzet, bestaan en werking aan de vereisten van de Wpg.

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

Criteria:

- Groen = Er wordt in hoofdlijnen voldaan aan de norm.
- 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
Art. 1.f, Verantwoordelijke			
1.f	Mandaatbesluit		Er is een vigerend mandaatbesluit en ondermandaatbesluit van 22 juni 2011 krachtens welke het mandaat, het ondermaat en de volmacht zijn vastgelegd. Hierin wordt de Wpg expliciet genoemd. Hiermee wordt voldaan aan de Wpg.
Art. 3 en 4, Kwaliteitsaspecten van politiegegevens			
8.1 en 9.1	Onderscheid onderzoek Dagelijkse Politietaken (8) versus Bepaald geval (9)		Door middel van het protocol ' <i>aanwijzingen voor het gebruik van politiegegevens tijdens uw werk</i> ' wordt per functie bewustzijn gecreëerd omtrent het werken met politiegegevens. In dit protocol wordt uiteengezet met welke Wpg-applicaties men van doen heeft en wordt bewustgemaakt dat deze applicaties politiegegevens bevatten waarvoor speciale regels gelden. De

Norm	Aspect	Bevinding en oordeel
		verschillende verwerkingsdoelen worden beknopt uiteengezet en de daarbij behorende bewaartermijnen worden tevens vermeld. Kleine onderzoeken zijn artikel 8 onderzoeken en worden doorgaans binnen een week (40 uur) afgehandeld. Artikel 9 onderzoeken langer dan 40 uur of zijn onderzoeken met BOB-middelen. De grens tussen artikel 8 en artikel 9 Wpg informatie was in de praktijk niet altijd even duidelijk. Men heeft hierbij behoefte aan een eenduidige opvatting of een richtsnoer waar men op terug kan vallen. Korps Zaanstreek-Waterland heeft hiervoor vuistregels ontwikkeld, genaamd het 'AGGIE'. Deze vuistregels heeft men uitgebracht op een sticker om deze op alle notitieblokjes te plakken zodat Blauw deze vuistregels altijd met zich mee dragen. Hiermee wordt deels voldaan aan de Wpg.
3.1 t/m 3.3 (8) 4.1 (8)	Noodzakelijkheid (8) Doelbinding Rechtmatigheid Juistheid Volledigheid	De privacyfunctionaris controleert of aan de regelgeving voor digitale opslag, de toegankelijkheid door geautoriseerde personen alsmede de bewaartermijnen die gelden voor deze gegevens, wordt voldaan. Er zijn vuistregels voor Blauw vastgesteld ter informatie hoe men om hoort te gaan met politiegegevens. Deze vuistregels zijn door de privacyfunctionaris van het korps verspreid. Het korps gebruikt TrueBlue voor bewaking van de kwaliteit van een aantal velden in BVH. De Infodesk is dusdanig getraind om de inschatting te maken of het ter beschikking stellen noodzakelijk is en wanneer nodig door te vragen (zoals naar doelbinding). De noodzakelijkheid wordt getoetst aan de hand van de vraagstelling of een intake. Hiermee wordt voldaan aan de Wpg.
3.1 t/m 3.4 (9) 4.1 (9)	Noodzakelijkheid (9) Doelbinding Rechtmatigheid Herkomst en wijze van verkrijging Juistheid Nauwkeurig Volledigheid	Het rechercheproces bevat waarborgen voor deze aspecten. De PDCA-cyclus sluit via het OM en de rechter. De Infodesk geeft alleen artikel 9-informatie na goedkeuring van de betreffende bevoegd functionaris. De teamleider is bij Zaanstreek-Waterland de persoon om de kwaliteit van de politiegegevens onder artikel 9 te waarborgen. Tevens is de bevoegde functionaris verantwoordelijk voor de kwaliteit van artikel 9-gegevens. De gegevensverzameling in BVO wordt beheerd door de functioneel beheerder Informatie Management. De Infodesk controleert of de gegevens die verstrekt worden voldoen aan de informatievraag, en of de juistheid van de gegevens gewaarborgd is.

Norm	Aspect	Bevinding en oordeel
		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	Gesprekken met informanten worden zo snel mogelijk in bruto opgeslagen. Een medewerker voert de brutogegevens in het systeem in, een andere medewerker controleert deze gegevens op juistheid. De administratief medewerker CIE raadpleegt of de in de ZIR genoemde personen al subject zijn in de eigen artikel 10 Wpg-registratie. De CIE-chef beoordeelt of de betreffende ZIR voldoet aan de opname criteria conform de bepalingen van de registratie artikel 10 Wpg. Er wordt gehandeld conform het landelijke CIE-proceshandboek. De CIE wordt door de CIE-Officier van Justitie gecontroleerd op de rechtmatigheid van de handelingen. Hiermee wordt voldaan aan de Wpg.
4.3	Beveiliging	De toegankelijkheid en autorisatie van de groepsmappen is niet conform Wpg. Tevens vindt er geen / geen goede isolatie plaats binnen de publieke-mappenstructuur. Risico voor later onrechtmatig gebruik en bewaring. Bovendien voldoen niet alle landelijke applicaties aan de eisen van de Wpg. De public map is in zijn geheel in oktober 2011 verwijderd. Voor de verdere kantoorautomatisering is een project opgezet om dit in te richten conform de Wpg. Hiermee wordt deels voldaan aan de Wpg.
Art. 5, Gevoelige Gegevens		
• Gevoelige gegevens		Zaanstreek-Waterland hanteert een strikt beleid omtrent het vastleggen van gevoelige gegevens. Het korps is terughoudend in het registreren van gevoelige gegevens en doet dit enkel wanneer dit noodzakelijk is voor de uitvoering van de politietaak. Hiermee wordt voldaan aan de Wpg.
Art. 6, Autorisatie		
• Korpsautorisatiematrix		Autorisaties voor Wpg-applicaties worden uitsluitend op basis van de autorisatiematrix toegekend. Daarop wordt toegezien door de privacyfunctionaris. Hiermee wordt voldaan aan de Wpg.
• Aanvraagproces		De autorisatieprocedure bij korps Zaanstreek-Waterland is zorgvuldig uiteengezet conform de Wpg. De taken en verantwoordelijkheden zijn goed belegd. Een procedure is tevens aanwezig ingeval er sprake is van ontslag, schoring en bij overlijden. Hiermee wordt voldaan aan de Wpg.
• Wijziging en verwijdering		De autorisatieprocedure bij korps Zaanstreek-Waterland is zorgvuldig uiteengezet conform de Wpg. De taken en verantwoordelijkheden zijn goed belegd. Een procedure is tevens aanwezig ingeval er sprake is van ontslag, schoring en bij overlijden. Hiermee wordt voldaan aan de Wpg.

Norm	Aspect	Bevinding en oordeel
• Autorisatiebeheer CIE en RID.		Medewerkers en chefs van de afdelingen CIE en RID dienen alvorens zij autorisatie verkrijgen tot de politiesystemen aangaande informanten, themaverwerking ernstige misdrijven en verdere CIE- en RID-verwerkingen, de instemming te hebben van de Officier van Justitie. Hiermee wordt voldaan aan de Wpg.
32.1.c	Protocollering autorisaties	Een overzicht van de personen die de functies bekleden ligt bij Informatie Management. Een functioneel beheerder houdt een overzicht bij in Excel en wordt geactualiseerd wanneer er zich wijzigingen hebben voorgedaan. Wanneer de functioneel beheerder twijfelt over de rechtmatigheid van een autorisatie kan deze persoon terecht bij de privacyfunctionaris van het korps. Dit overzicht is altijd inzichtelijk voor de privacyfunctionaris. Hiermee wordt voldaan aan de Wpg.
32.3 voor 32.1.c	Bewaren protocolgegevens autorisaties	Een overzicht van de personen die de functies bekleden ligt bij Informatie Management. Een functioneel beheerder houdt een overzicht bij in Excel en wordt geactualiseerd wanneer er zich wijzigingen hebben voorgedaan. Wanneer de functioneel beheerder twijfelt over de rechtmatigheid van een autorisatie kan deze persoon terecht bij de privacyfunctionaris van het korps. Dit overzicht is altijd inzichtelijk voor de privacyfunctionaris. De privacyfunctionaris heeft wekelijks contact met de autorisatiebeheerder en heeft toegang tot de autorisatiematrix. Enkele keren per maand controleert de privacyfunctionaris de autorisaties. Hiermee wordt voldaan aan de Wpg.
Art. 11, Geautomatiseerd vergelijken en in combinatie zoeken		
• Hanteerbare interpretatie		Een interpretatie van artikel 11 is bij korps Zaanstreek-Waterland vastgelegd. Beschreven is hoe geautomatiseerd vergelijken en in combinatie met elkaar zoeken moet worden uitgevoerd, welke gegevens er mogen worden verwerkt en wie daarvoor is geautoriseerd. Tevens wordt vermeld wanneer toestemming van het bevoegde gezag vereist is. In de praktijk blijkt dat ondanks deze beschrijving de interpretatie lastig is en men behoefte heeft aan extra definitiebepaling. Hiermee wordt deels voldaan aan de Wpg.
• Aangewezen functionarissen		De artikel 11-zoekslagen mogen uitsluitend door personeel van CIE, RI, rechercheurs themaregisters en in bepaalde gevallen door medewerkers Infodesk worden uitgevoerd. Infodeskmedewerkers zijn alleen hiertoe bevoegd bij dringende noodzakelijkheid, na toestemming van het hoofd van de eenheid van CIE,

Norm	Aspect		Bevinding en oordeel
			RI of recherche chef themaregisters. Hiermee wordt voldaan aan de Wpg.
11.4	Bevoegde gezag		Het in combinatie verwerken is alleen toegestaan in bijzondere gevallen en in opdracht van het bevoegd gezag (de OvJ respectievelijk de burgemeester). Hiermee wordt voldaan aan de Wpg.
32.1.d en 32.1.h	Protocollering 11.1, 11.2, 11.4 en 11.5		Vraagstellingen (vergelijkingen en combinatie zoekslagen) worden door de Infodesk vastgelegd in de BVO-Infodeskmodule. Zoekvragen worden tevens vastgelegd en gedurende vijf jaar bewaard. 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		Vraagstellingen (vergelijkingen en combinatie zoekslagen) worden door de Infodesk vastgelegd in de BVO-Infodeskmodule. Zoekvragen worden tevens vastgelegd en gedurende vijf jaar bewaard. Hiermee wordt voldaan aan de Wpg.
Art. 14, Bewaartermijnen			
8.2 en 8.3	(8) van 1 tot 5 jaar		In de nieuwe release van BVH (versie 1.2.2) is een schoningsmodule aanwezig, maar deze staat op landelijk verzoek van de voorzitter van de stuurgroep nog niet aan. Artikel 8 en 9 Wpg informatie wordt ook buiten BVH opgeslagen binnen de kantoorautomatiserings-omgeving, hier is een actieplan voor opgesteld. Hiermee wordt niet voldaan aan de Wpg.
8.6	(8) verwijderen na 5 jaar		In de nieuwe release van BVH (versie 1.2.2) is een schoningsmodule aanwezig, maar deze staat op landelijk verzoek van de voorzitter van de stuurgroep nog niet aan. Artikel 8 en 9 Wpg informatie wordt ook buiten BVH opgeslagen binnen de kantoorautomatiserings-omgeving, hier is een actieplan voor opgesteld. Hiermee wordt niet voldaan aan de Wpg.
14.1 (8)	(8) vernietigen na 5 jaar verwijderd		De BPS data heeft het korps omgezet naar '.txt-bestanden' welke alleen nog maar raadpleegbaar zijn door de informatie organisatie. In deze tekstbestanden is informatie van de periode 2011 tot 1998 beschikbaar. Artikel 8-gegevens ouder dan 10 jaar moeten worden vernietigd. Dat gebeurt op deze manier echter niet. De informatie wordt slechts achter een schot geplaatst en is nog steeds door een beperkt aantal medewerkers raadpleegbaar. Hiermee wordt niet voldaan aan de Wpg.
9.4	(9) verwijderen na OH plus ½ jaar		Het verwijderen van artikel 9 onderzoeken gebeurt nog onvoldoende. Hierbij is de ketensamenwerking en specifiek de overdracht van informatie over afgesloten zaken van OM naar de politie een aandachtspunt. In de praktijk blijkt dat men beperkt terugkoppeling

Norm	Aspect	Bevinding en oordeel
		krijgt van het OM door middel van afloopbriefjes wanneer een zaak in kracht van gewijsde is gegaan. Dit heeft als gevolg dat er in BVO geen structurele verwijdering van zaken plaatsvindt. Ook het achter het schot zetten vindt voor afgesloten zaken gebeurt niet. Korps Zaanstreek-Waterland heeft naar aanleiding van dit probleem het (landelijke) systeem BOSZ geïmplementeerd om op een eenvoudigere wijze terugkoppeling te ontvangen. BOSZ binnen OM is nog een pilot. Het korps is al wel live met BOSZ, maar het OM haakt aan per 10-1-2012. BOSZ is overigens een coördinatie en keten informatie systeem. Dan is het Openbaar Ministerie geautoriseerd zodat ze de status van de betreffende zaken hierin kunnen aangeven. Daarmee heeft het korps een actieplan paraat. Hiermee wordt deels voldaan aan de Wpg.
14.1 (9)	(9) vernietigen na 5 jaar verwijderd	Het vernietigen van artikel 9 onderzoeken gebeurt nog onvoldoende. Hierbij is de ketensamenwerking en specifiek de overdracht van informatie over afgesloten zaken van OM naar de politie een aandachtspunt. In de praktijk blijkt dat men beperkt terugkoppeling krijgt van het OM door middel van afloopbriefjes wanneer een zaak in kracht van gewijsde is gegaan. Dit heeft als gevolg dat er in BVO geen structurele verwijdering van zaken plaatsvindt. Ook het achter het schot zetten vindt voor afgesloten zaken gebeurt niet. Korps Zaanstreek-Waterland heeft naar aanleiding van dit probleem het (landelijke) systeem BOSZ geïmplementeerd om op een eenvoudigere wijze terugkoppeling te ontvangen. Vanaf vijf januari 2012 gaat dit systeem 'live' en is het Openbaar Ministerie geautoriseerd zodat ze de status van de betreffende zaken hierin kunnen aangeven. Daarmee heeft het korps een actieplan paraat. Hiermee wordt deels voldaan aan de Wpg.
10.6	(10) verwijderen na 5 jaar geen subjectwaardige registratie	Er is een procedure beschikbaar met betrekking tot het schonen van artikel 10 informatie. Controle hierop vindt plaats door de registratiebeheerder/administratief medewerker en vervolgens de CIE-chef. Tot eind 2010 werd periodiek (elke 3 maanden) nagekeken welke subjecten in aanmerking kwamen voor verwijdering. Thans is er sprake dat vanaf begin 2012 een nieuwe tool werkzaam wordt die automatisch een seintje gaat genereren wanneer een bepaald subject geschoond moet gaan worden.

Norm	Aspect		Bevinding en oordeel
			Hiermee wordt deels voldaan aan de Wpg.
14.1 (10)	(10) vernietigen na 5 jaar verwijderd		Er is een procedure beschikbaar met betrekking tot het schonen van artikel 10 informatie. Controle hierop vindt plaats door de registratiebeheerder / administratief medewerker en vervolgens de CIE-chef. Tot eind 2010 werd periodiek (elke 3 maanden) nagekeken welke subjecten in aanmerking kwamen voor vernietiging. Thans is er sprake dat vanaf begin 2012 een nieuwe tool werkzaam wordt die automatisch een seintje gaat genereren wanneer een bepaald subject geschoond moet gaan worden. Hiermee wordt deels voldaan aan de Wpg.
14.3	Hernieuwde verwerking		Een procedure met betrekking tot de hernieuwde verwerking van artikel 9 en 10 gegevens is vastgesteld. Hiervoor dient toestemming te worden gevraagd aan het bevoegd gezag (OvJ of burgemeester) door middel van een schriftelijke aanvraag. Hiermee wordt voldaan aan de Wpg.
32.1.e	Protocollering 14.3		Hernieuwde verwerking wordt schriftelijk vastgelegd in BVO. Hiermee wordt voldaan aan de Wpg.
32.3 voor 32.1.e	Bewaren protocolgegevens 14.3		De protocolgegevens worden opgeslagen in de BVO-Infodeskmodule. De privacyfunctionaris controleert regelmatig bij de Infodesk. Hiermee wordt voldaan aan de Wpg.
12.2	(12) gebruiken tot 4 maanden		RID: Tijdens het werkoverleg dat 1 keer per 2 weken met de gehele RID en het unithoofd plaatsvindt, worden onder andere informanten geëvalueerd. Als tijdens het overleg besloten wordt dat de informant geen meerwaarde meer oplevert, wordt het dossier afgebouwd. De dossiers worden aan het einde van de bewaartermijn overgedragen en opgeslagen in het archief van de politieregio Zaanstreek-Waterland. CIE: De CIE-OvJ voert controle uit op de opslag en bewaartermijnen van CIE-gegevens. Niet bekend is of tevens controle plaatsvindt op het gebruik van CIE-gegevens tot vier maanden. Hiermee wordt deels voldaan aan de Wpg.
12.6	(12) controleren en vernietigen		CIE: Het unithoofd Recherche Ondersteuning is verantwoordelijk voor de opslag en bewaartermijnen die gelden ten aanzien van CIE informatie. Controle vindt plaats door de CIE-OvJ. RID: Het unithoofd is verantwoordelijk voor de bewaartermijnen en de vernietiging van gegevens. De verwijderde politiegegevens worden gedurende een termijn van vijf jaar in RIDS bewaard ten behoeve van verwerking met het oog op de afhandeling van klachten en de verantwoording van

Norm	Aspect	Bevinding en oordeel
		verrichtingen en vervolgens door de geautoriseerde voor het Openbare Orde register vernietigd (art. 14 Wpg). Schoning van het artikel 12 register vindt plaats na 10 jaar. Alle handelingen worden geprotocolleerd in BVO bruto. Hiermee wordt voldaan aan de Wpg.
Art. 15, Ter beschikking stellen		
	Infodesk voor bevraging	Er zijn werkinstructies voor de Infodesk over hoe om te gaan met aanvragen vanuit Handhaving en Opsporing. De Infodesk geeft alleen artikel 9 informatie na goedkeuring van de betreffende bevoegde functionaris. Voordat door de Infodesk ter beschikking wordt gesteld, wordt gekeken of de gegevens juist zijn. Bovendien controleert de Infodesk of de gegevens die ter beschikking gesteld worden voldoen aan de aanvraag. Bij het verstrekken van de gegevens vermeldt de Infodesk de bron en vaak ook de zoekstring. Dit geeft inzicht in de gevolgde werkwijze bij het zoeken, daarmee is de herkomst van artikel 9-gegevens terug te vinden. Hiermee wordt voldaan aan de Wpg.
	Codering	Er is een werkinstructie voor codering in BVH en BVO. Dit is bekend bij de bevoegd functionaris en de medewerkers van de Infodesk. De CIE-codering wordt gebruikt. Hiermee wordt voldaan aan de Wpg.
	Aanwijzing Bevoegd Functionaris	Intern is een helpdesk voor de Wpg, namelijk de privacyfunctionaris. Op decentraal niveau en met name in het rechercheproces zijn de formeel aangewezen bevoegd functionarissen de contactpunten. Hiermee wordt voldaan aan de Wpg.
	Opleiding Bevoegd Functionaris	Alle bevoegde functionarissen van Zaanstreek-Waterland hebben een Wpg-cursus gehad. Daarnaast zijn een zelfstudie-cursus, modellen en de verstrekkingenwijzer op Intranet beschikbaar gesteld. De training wordt gegeven door de politieacademie en alle aspecten van de uitoefening van de functie bevoegd functionaris worden hierin meegenomen. Hiermee wordt voldaan aan de Wpg.
15.2	Weigeringsgronden	De bevoegd functionarissen zijn op de hoogte van de wettelijke weigeringsgronden in relatie tot de verplichting van het ter beschikking stellen. Dit is opgenomen in de opleiding voor bevoegde functionarissen. Hiermee wordt voldaan aan de Wpg.

Norm	Aspect	Bevinding en oordeel
Art. 16 t/m 24, Verstrekking		
• Verstrekkingenwijzer (landelijk)		Het korps hanteert de landelijke verstrekkingwijzer. De wet (en het besluit) voorziet in aan wie verstrekt mag worden. De verstrekkingenwijzer is gepubliceerd op Intranet. Hiermee wordt voldaan aan de Wpg.
• Proces voor convenanten		Er is een convenantenloket. Het loket valt onder het kabinet korpsleiding (KKL). Het convenantenloket houdt alle afspraken bij met het oog op informatie-uitwisseling en houdt de looptijd van de afgesloten convenanten in de gaten. Een procedure en controlelijst is beschikbaar om de kwaliteit en rechtmatigheid van de convenanten (en artikel 20-besluiten) te waarborgen. De beoordeling en de controle van het convenant en het artikel 20 besluit wordt gedaan door de korpsleiding en/of de korpsjurist en worden daarbij door het convenantenloket ondersteund. De interne opdrachtgever adviseert welke politiegegevens worden uitgewisseld. De tekenbevoegdheid is door de korpsbeheerder gemandateerd aan de (plv.) korpschef. Binnen het korps is dit recht alleen gemandateerd aan de korpschef, daarom krijgt hij alle convenanten en artikel 20 besluiten onder ogen. Hiermee wordt voldaan aan de Wpg.
• Proces voor Art. 20 Besluiten		Er is een convenantenloket. Het loket valt onder het kabinet korpsleiding (KKL). Het convenantenloket houdt alle afspraken bij met het oog op informatie-uitwisseling en houdt de looptijd van de afgesloten convenanten in de gaten. Een procedure en controlelijst is beschikbaar om de kwaliteit en rechtmatigheid van de convenanten (en artikel 20-besluiten) te waarborgen. De beoordeling en de controle van het convenant en het artikel 20 besluit wordt gedaan door de korpsleiding en/of de korpsjurist en worden daarbij door het convenantenloket ondersteund. De interne opdrachtgever adviseert welke politiegegevens worden uitgewisseld. De tekenbevoegdheid is door de korpsbeheerder gemandateerd aan de (plv.) korpschef. Binnen het korps is dit recht alleen gemandateerd aan de korpschef, daarom krijgt hij alle convenanten en artikel 20 besluiten onder ogen. Hiermee wordt voldaan aan de Wpg.
• Verstrekkingenschema (regio)		Het korps Zaanstreek-Waterland heeft een eenduidig, gedocumenteerd proces hoe omgegaan dient te worden met verstrekkingen, welke functies hiervoor verantwoordelijk zijn. Hiermee wordt voldaan aan de Wpg.

Norm	Aspect	Bevinding en oordeel
• Proces voor geautomatiseerde verstrekking		Enkele leden van het Openbaar Ministerie van het parket Haarlem hebben toegang tot BVH (Basis Voorziening Handhaving), Hiervoor is een convenant afgesloten. Door toekenning van deze structurele toegang is de koppeling van een bevraging met de noodzaak en doelbinding <i>vooraf</i> niet toetsbaar. Een controle op bevragingen vooraf ontbreekt. Door rechtstreekse toegang tot BVH te verschaffen aan het OM ontbreekt de controle.. Hiermee wordt niet voldaan aan de Wpg.
7.2	Geheimhouding	Bij alle verstrekkingen wordt gewezen op de geheimhoudingsplicht conform artikel 7 lid 2 Wpg. Hiermee wordt voldaan aan de Wpg.
32.1.f	Protocollering verstrekking	Zowel de Infodesk als de overige medewerkers die verstrekkingen doen binnen het korps leggen de verstrekkingen vast in BVH of BVO. Voor Blauw is protocollering via I90 in BVH verplicht gesteld. De Infodesk protocolleert via Outlook, BVH of de BVO-Infodeskmodule. Het korps heeft de uitgangspunten voor (incidentele) verstrekkingen en de vastlegging daarvan bepaald. Er vindt geen structurele vastlegging plaats bij het proces handhaving. Hiermee wordt deels voldaan aan de Wpg.
32.3 voor 32.1.f	Bewaren protocolgegevens verstrekking	Zowel de Infodesk als alle overige medewerkers die verstrekkingen doen binnen het korps leggen de verstrekkingen vast in BVH of BVO, hier is ook nadrukkelijk binnen het korps bekendheid aan gegeven. Conform wettelijke eisen worden deze bewaard te worden tot een volgende audit en eventuele heraudit plaatsvindt. De bewaartermijn is vastgesteld op 5 jaar. Hiermee wordt voldaan aan de Wpg.
• Toezicht door leidinggevendenden op verstrekkingen en protocollering		Toezicht op verstrekkingen vormt onderdeel van de taken van de chefs. Voor verstrekkingen uit BVO is de bevoegde functionaris verantwoordelijk. De CIE OvJ is bij elke verstrekking betrokken en is zeer nadrukkelijk aanwezig wat betreft bevoegdheden en controle. Hiermee wordt voldaan aan de Wpg.
Art. 25 t/m 31, Rechten van de betrokkene		
25.1	Verzoek om kennisneming	De kennisnemingsverzoeken worden door de privacyfunctionaris en diens administratief medewerker in behandeling genomen en afgehandeld conform de Wpg. In 2010 zijn er 413 verzoeken (van externen) om informatie geweest. In 2011 ligt het aantal tot en met 12 december op 582 verzoeken. Over 2010

Norm	Aspect	Bevinding en oordeel
		waren er 32 daadwerkelijke inzageverzoeken, waarvan er 20 zijn gehonoreerd na overleg met de verzoeker(s). Hiermee wordt voldaan aan de Wpg.
28.1 t/m 28.3	Correctie	De correctieverzoeken worden door de privacyfunctionaris en diens administratief medewerker in behandeling genomen conform de Wpg. Er hebben zich echter geen correctieverzoeken voorgedaan. Hiermee wordt voldaan aan de Wpg.
Art. 32, Protocolplicht (32.1.c, d, e, f en h behandeld bij thema's)		
9.2 en 32.1.a	Protocollering doel onderzoek	Artikel 9-onderzoeken worden vastgelegd in BVO en via een MRO naar de landelijke verwijzingsindex VROS, onder beheer van het KLPD. Kleine onderzoeken worden niet structureel gemeld. Over de omvang van niet gemelde onderzoeken is geen kennis aanwezig. In de praktijk blijkt dat bij het protocolleren van artikel 9 verwerkingen in BVO regelmatig een wel héél korte doelomschrijving is gebruikt. Dergelijke omschrijvingen zijn te summier en voldoen daarom niet aan de wettelijke eisen. Hiermee wordt deels voldaan aan de Wpg.
32.3 voor 32.1.a	Bewaren protocolgegevens doel onderzoek	De privacyfunctionaris houdt een overzicht bij van alle (aangemelde) verwerkingen (en de doelen daartoe) die worden geopend voor artikel 9 Wpg. Hiermee wordt voldaan aan de Wpg.
13.4 en 32.1.b	Protocollering Art. 13 gegevensverzameling en	Per werkproces is aangegeven dat (aanvullende) protocollering verplicht is en wat de daarbij behorende bewaartermijnen zijn waarbij verwezen wordt naar artikel 13 en 32 Wpg. Er zijn zeven artikel 13-protocollen opgesteld en getekend door de gemandateerde korpschef. Dit zijn de landelijk opgestelde reglementen. In 2012 worden de overige reglementen aangeleverd en eveneens vastgesteld. Hiermee wordt voldaan aan de Wpg.
32.3 voor 32.1.b	Bewaren protocolgegevens Art. 13 gegevensverzameling en	Per werkproces is aangegeven dat (aanvullende) protocollering verplicht is en wat de daarbij behorende bewaartermijnen zijn waarbij verwezen wordt naar artikel 13 en 32 Wpg. Deze zijn per 1 november 2011 vastgesteld en nog niet middels een steekproef gecontroleerd. Hiermee wordt voldaan aan de Wpg.
32.1.g	Protocollering onrechtmatige handeling	Voor de verschillende gebruikte applicaties zijn verantwoordelijken aangewezen voor correcte afhandeling en melding van vermoedelijk onrechtmatige handelingen aan de privacyfunctionaris. Hiermee wordt voldaan aan de Wpg.

Norm	Aspect		Bevinding en oordeel
32.3 voor 32.1.g	Bewaren protocolgegevens onrechtmatige handeling		Er zijn geen onrechtmatige verwerkingen door de privacyfunctionaris geconstateerd. De privacyfunctionaris houdt indien van toepassing hiervan een overzicht bij. Hiermee wordt voldaan aan de Wpg.
32.2	Gemeenschappelijke verwerking		In het dossier beheersmaatregelen is een schriftelijke aanwijzing opgenomen en aan de bevoegd functionarissen uitgereikt. Deze geeft aanwijzing voor de (praktische) uitvoering van de protocolplicht ten aanzien van gemeenschappelijke verwerkingen. De bevoegde functionaris is verantwoordelijk voor het inlichten van het CBP en de privacyfunctionaris. Er zijn geen gemeenschappelijke verwerkingen geconstateerd. Hiermee wordt voldaan aan de Wpg.
Art. 33, Audits			
RPAP 3.1	Interne audit-functie		De Interne Wpg audit-functie is niet structureel belegd. De interne auditor is al wel intern aangewezen, echter is dit besluit nog niet geformaliseerd en hij heeft bovendien ook (nog) geen opleiding genoten. Hiermee wordt niet voldaan aan de Wpg.
RPAP 3.4	Interne audit-plan		Er is geen vaktechnisch verantwoord en meerjarig intern Wpg audit-plan. Er zijn Wpg-checklijsten voor de korpsleiding, unithoofden en (wijk)teamchefs. Tevens heeft de privacyfunctionaris een zogenaamde toezichtkalender ontwikkeld. Naar aanleiding van die toezichtkalender rapporteert de privacyfunctionaris aan de stuurgroep en de diensthoeften. Hiermee wordt niet voldaan aan de Wpg.
RPAP 3.6	Interne audit-rapport		Er is geen intern Wpg audit-rapport. Wel is er een student Management Economie en Recht ingezet om in een periode van 6 maanden te onderzoeken in welke mate het korps Zaanstreek-Waterland voldoet aan de eisen van de Wpg. Hiermee wordt niet voldaan aan de Wpg..
Art. 34, Privacyfunctionaris			
34.1 en 34.4	Benoemd en gemeld		De privacyfunctionaris is benoemd. Hij vervult deze rol naast het takenpakket vanuit het oogpunt van informatiebeveiliging. Hiermee wordt voldaan aan de Wpg.
34.2	Overzicht over protocollering		De privacyfunctionaris van Zaanstreek-Waterland is op de hoogte waar wordt geprotocolleerd en heeft de mogelijkheid protocolgegevens op te vragen en in te zien. De privacyfunctionaris heeft bovendien toegang tot de systemen voor controle op Wpg-compliance. Hiermee wordt voldaan aan de Wpg.
34.3	Jaarverslag		De privacyfunctionaris heeft een jaarverslag privacy 2008, 2009 en 2010 opgesteld. De

Norm	Aspect		Bevinding en oordeel
			privacyfunctionaris rapporteert bovendien regelmatig aan de stuurgroep Wpg. Hiermee wordt voldaan aan de Wpg.
Optioneel Art. 36, Functionaris Gegevensbescherming			
36.1 en 36.2	Benoemd		Er is geen functionaris gegevensbescherming benoemd.
Wbp 63.3	Gemeld		Niet van toepassing.
Wbp 64.1 t/m 64.4	Toezichthoudende rol		Niet van toepassing.

3 Inleiding

3.1 Algemeen

In opdracht van de landelijke stuurgroep Wpg, waarin de Directeur-Generaal Politie en het KBB zijn vertegenwoordigd, heeft de DAD van het ministerie van VenJ een privacy audit uitgevoerd bij het korps ZAA NSTREEK-WATERLAND 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 Zaanstreek-Waterland in de maand mei 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 Zaanstreek-Waterland.

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

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

korps Zaanstreek-Waterland beoogt te voldoen aan de beheersdoelstellingen die bij of krachtens de Wpg gelden.

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

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

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

3.4 Afbakening

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

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

3.5 Normenkader

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

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

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

3.6 Beperkingen voor de privacy audit

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

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

3.7 Onderzoeksmethoden en werkwijze

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

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

Wij hebben onze werkzaamheden uitgevoerd in de maand mei 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 mr. G.H. Faber.
- De korpschef G.P.H.P. Huijser van Reenen.
- De Hoofd Officier van Justitie mr. C.J.L. van Dam MPM.
- De privacyfunctionaris [REDACTED]
- De voorzitter van het College Bescherming Persoonsgegevens.

Het rapport mag uitsluitend met toestemming van de korpsbeheerder dan wel de korpschef van korps Zaanstreek-Waterland 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*

Algemene aandachtspunten die bij de audit binnen politie Zaanstreek-Waterland naar voren zijn gekomen zijn:

- Er is voldoende bewustzijn bij politie Zaanstreek-Waterland omtrent de Wet politiegegevens. Sturing van de implementatie van de Wpg is gedaan door de stuurgroep Wpg met daarin vrijwel het voltallige Korps Management Team. Coördinatie van de implementatie is verricht door de kerngroep Wpg.
- Er is gebleken dat er behoefte is aan strakkere facilitering en regie voor het gebruik van informatiesystemen (BVO en BVH) op landelijk vlak.

Bij alle afdelingen zijn de rollen in kaart gebracht, wie wat doet en wat mag. Voor de autorisaties is Beaufort leidend.

4.1.2 *Bekendheid met de Wpg binnen de organisatie*

Politie Zaanstreek-Waterland heeft zichtbaar veel tijd en energie gestoken in het bekend maken van de Wet politiegegevens binnen alle geledingen van het korps. Dit heeft men gedaan door middel van het per functie inzichtelijk maken welke handelingen Wpg-relevant zijn en welke concrete consequenties dit heeft voor de dagelijkse praktijk voor deze functies. De privacyfunctionaris heeft hierbij een grote inbreng gehad.

4.1.3 *Wpg en de praktijk*

Er is een vertaalslag gemaakt van de Wet politiegegevens naar de dagelijkse politiepraktijk. Voor eventuele vragen kan men bij de privacyfunctionaris terecht.

Men blijkt voornamelijk problemen te hebben met de interpretatie van artikel 11 Wpg. De begrippen uit dit artikel zijn lastig te plaatsen waardoor er behoefte is aan een extra definitiebepaling.

4.2 Verantwoordelijke (artikel 1.f)

Mandaatbesluit

Net als onder de oude Wet Politiregisters (Wpolr) is ook in de Wpg de korpsbeheerder er verantwoordelijk voor, dat de nodige maatregelen worden getroffen zodat politiegegevens juist, nauwkeurig en proportioneel worden verwerkt en op tijd worden verwijderd.

4.2.1 *Bevindingen*

Er is een vigerend mandaatbesluit en ondermandaatbesluit van 22 juni 2011 krachtens welke het mandaat, het ondermaat en de volmacht zijn vastgelegd. Hierin wordt de Wpg expliciet genoemd.

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*

Onderscheid artikel 8 en artikel 9 gegevens

Voortraject Wpg

In 2009 en 2010 heeft korps Zaanstreek-Waterland op gezette tijden in Intercom en op intranet aandacht besteed aan de Wpg. In Intercom heeft de nadruk van de berichtgeving voornamelijk gelegen op achtergrondinformatie over de Wpg en een eerste kennismaking met de wet.

Met deze berichtgeving op intranet heeft men getracht de Wpg als onderwerp binnen het korps 'levend' te houden onder de medewerkers. Hierbij heeft men tevens gebruik gemaakt van zogenaamde Wpg-weetjes. Gedurende acht weken is elke week op een vast tijdstip een beschrijving gegeven van een herkenbare situatie uit de dagelijkse praktijk en hoe de Wpg daarop van toepassing is.

Gedurende acht weken is elke week op een vast tijdstip een beschrijving gegeven van een herkenbare situatie uit de dagelijkse praktijk en hoe de Wpg daarop van toepassing is. Intranet fungeert bovendien als een vraagbaak. Op de speciaal daarvoor ontwikkelde Wpg-pagina staat allerlei achtergrondinformatie over de wet.

Daarnaast is de film die vanuit de landelijke werkgroep is ontwikkeld op diverse momenten aan groepjes collega's getoond. De film geeft een herkenbaar beeld van de dagelijkse praktijk van de diender en de rol die de WPG daarin speelt.

Protocol aanwijzing gebruik van politiegegevens

Het korps Zaanstreek-Waterland heeft zichtbaar veel energie gestoken in het analyseren van de Wet politiegegevens en in de toepassing op de relevante werkprocessen en de daarbij betrokken zijnde functies. Deze inzet heeft geresulteerd in het protocol '*aanwijzingen voor het gebruik van politiegegevens tijdens uw werk*', waarbij er per functie bewustzijn wordt gecreëerd omtrent het werken met politiegegevens.

In dit protocol wordt uiteengezet met welke Wpg-applicaties men van doen heeft en wordt men bewust gemaakt dat deze applicaties politiegegevens bevatten waarvoor speciale regels gelden. De verschillende verwerkingsdoelen worden uiteengezet en de daarbij behorende bewaartermijnen worden tevens vermeld.

Tevens wordt er aangegeven dat het niet is toegestaan binnen korps Zaanstreek-Waterland om politiegegevens binnen de eigen kantoorautomatisering op te slaan buiten de specifiek daarvoor aangemaakte mappen om.

De privacyfunctionaris heeft tot taak om actief toe te zien op de naleving van bovenstaande regelgeving. Geconstateerde onregelmatigheden worden aan de verantwoordelijke chef gerapporteerd.

Dit protocol is opgesteld voor elke functie die te maken heeft met politiegegevens binnen het korps. Op deze manier heeft men op een overzichtelijke manier het onderscheid tussen artikel 8 en 9 (en meer) politiegegevens aangegeven.

Dagelijkse praktijk

Uit de gehouden gesprekken blijkt dat in de dagelijkse praktijk het echter niet altijd even duidelijk is wanneer men te maken heeft met artikel 8, 9 en 10 politiegegevens. De grens tussen artikel 8 en artikel 9 informatie is niet altijd even duidelijk. Men heeft hierbij behoefte aan een eenduidige opvatting of een richtsnoer waar men op terug kan vallen.

Korps Zaanstreek-Waterland heeft hierop vuistregels ontwikkeld, genaamd het 'AGGIE'. Deze vuistregels heeft men uitgebracht op een sticker om deze op alle notitieblokjes te plakken zodat Blauw deze vuistregels altijd met zich mee dragen.

Artikel 8 en 9 kwaliteit van de politiegegevens

De verantwoordelijkheid voor controle op de kwaliteit van het geleverde werk is bij korps Zaanstreek-Waterland belegd bij de leidinggevende functionaris, hierbij vindt tevens controle plaats of er aan de Wpg-regels wordt voldaan.

De privacyfunctionaris controleert of aan de regelgeving voor digitale opslag, de toegankelijkheid door geautoriseerde personen alsmede de bewaartermijn die gelden voor deze gegevens wordt voldaan.

Rechtmatigheid

Er zijn vuistregels voor Blauw vastgesteld ter informatie hoe men om moet gaan met politiegegevens. Deze vuistregels zijn door de privacyfunctionaris van het korps gecommuniceerd door middel van het aanschuiven bij het werkoverleg van de wijkteams en op deze manier gezamenlijk het Wpg-dossier door te nemen. Hierbij gaat veel aandacht uit naar de basisaspecten van de Wpg, gebruikmakende van praktische voorbeelden. Tevens kan men ook voor privacyvraagstukken terecht bij de privacyfunctionaris.

Alle interne informatieverzoeken gaan via de Infodesk. Doordat de korpsgrootte beperkt is vindt controle bij de Infodesk impliciet plaats. Aanvragers worden geïdentificeerd door middel van het e-mailadres, telefoonnummer (bij telefonische aanvraag) en de stem en / of naam herkenning. Anders wordt als extra controlemaatregel een vergelijking gemaakt tussen naam en dienstnummer.

De Infodesk geeft alleen artikel 9 informatie na goedkeuring van de betreffende bevoegde functionaris. Dit houdt in dat men altijd belt of mailt met een bevoegde functionaris om toestemming voor het verstrekken van de informatie.

Het rechteproces bevat tevens waarborgen voor deze rechtmatigheidsaspecten. De PDCA-cyclus sluit via het OM en de rechter.

Noodzakelijkheid

Dit wordt getoetst door de vraagstelling of door een intake. Echter vindt geen expliciete verdergaande controle plaats of de betreffende aanvrager daadwerkelijk met een zaak bezig is. De Infodesk is dusdanig getraind om de inschatting te maken

of het ter beschikking stellen noodzakelijk is en wanneer nodig door te vragen (zoals naar doelbinding).

Juistheid en volledigheid

De gegevensverzameling in BVH wordt via de kennisdatabase TrueBlue beheerd door twee medewerkers. Het betreft hier voornamelijk het controleren en doen corrigeren van de toegepaste kennisregels.

De teamleider is bij Zaanstreek-Waterland de aangewezen persoon om de kwaliteit van de politiegegevens onder artikel 9 te waarborgen. Daarbij is ook de bevoegd functionaris verantwoordelijk voor de kwaliteit van de artikel 9-gegevens.

De gegevensverzameling in BVO worden beheerd door de functioneel beheerder IM. De taakelementen van het gegevensbeheer maken deel uit van de functiebeschrijving. Het gegevensbeheer Personenserver wordt uitgevoerd door vtsPN Landelijk en kent derhalve geen regionaal beheer.

Voordat door de Infodesk ter beschikking wordt gesteld, wordt tevens gekeken of de juistheid van de gegevens toereikend is. Bovendien controleert de Infodesk of de gegevens die verstrekt worden voldoen aan de aanvraag.

Herkomst van artikel 9-gegevens

Bij het verstrekken van de gegevens vermeldt de Infodesk de bron en vaak ook de zoekstring. Dit geeft inzicht in de gevolgde werkwijze bij het zoeken en daarmee is de herkomst van artikel 9-gegevens terug te vinden.

Kwaliteit van artikel 10 en 12 informatie

Gesprekken met informanten worden zo snel mogelijk na het gesprek in bruto gespreksverslagen opgeslagen, de notities hiervan worden direct vernietigd. De bruikbare informatie komt uiteindelijk terecht in netto-verslagen, die voor operationele doeleinden gebruikt kunnen gaan worden.

Een medewerker voert deze gegevens in het systeem in, een andere medewerker controleert deze gegevens op juistheid. De administratief medewerker CIE raadpleegt of de in de ZIR genoemde personen al subject zijn in de eigen artikel 10 Wpg registratie. Wanneer dit het geval is accordeert de CIE-chef de opname van de verkregen externe informatie, ten behoeve van opname in de eigen artikel 10 Wpg registratie.

- Informatie uit de schriftelijk verkregen ZIR wordt overgenomen en verwerkt in BVO
- Informatie uit de digitaal verstrekte ZIR (gelabelde mutatie) wordt gekopieerd naar BVO.

De CIE-chef beoordeelt of de betreffende ZIR voldoet aan de opnamecriteria conform de bepalingen van de registratie artikel 10 Wpg.

De uiteindelijke informatie wordt in het systeem geplaatst onder "groepen personen", hier is sprake van wanneer zij de openbare orde in het geding kunnen brengen. De informatie wordt enkel gebruikt ter ondersteuning bij opsporingen, niet als bewijs. Ten behoeve van de openbare orde handhaving heeft dit grotendeels een preventief karakter.

Naast het runnen van informanten voor informatie wordt tevens gebruik gemaakt van openbare bronnen. Deze informatie wordt in het systeem BVO opgenomen en met het unithoofd besproken, en is op doelgroep raadpleegbaar.

Er wordt gehandeld conform het landelijke CIE-proceshandboek. De CIE wordt door de CIE-Officier van Justitie gecontroleerd op de rechtmatigheid van de handelingen.

Beveiliging

Proceseigenaar automatiseringsorganisatie

In het kader van de implementatie van de Wpg is het unithoofd Informatiemanagement aangewezen als proceseigenaar van de automatiseringsorganisatie. Hij is verantwoordelijk voor het ICT dienstverleningsproces (applicatie-, systeem-, netwerk-, datacommunicatie-, functioneel- en gegevensbeheer) in het korps, waaronder het bevorderen van de beveiliging van de politiegegevens en de informatiesystemen van het korps.

Gebruik kantoorautomatisering

Informatie van onderzoeken wordt, naast BVO en BVH, ook in groepsmappen vastgelegd. Dit brengt het risico met zich mee dat deze in de KA-omgeving opgeslagen informatie later onrechtmatig wordt gebruikt en bewaard.

Sectiemappen worden in artikel 9 of soms artikel 10 mappen opgeslagen. Daar hebben ook nog steeds dezelfde mensen toegang toe. Er is tevens gebleken dat met name de *publieke*-map een veelheid aan politiegegevens bevat. Dit is te verklaren door de beperkte mogelijkheden die de applicatie BVH biedt om documenten te bewerken. Hierdoor maakt men eerder gebruik van Microsoft Word om procesverbalen in te voeren om vervolgens deze informatie naar BVH te kopiëren. Het is dan aan de verbalisant zelf of deze het aangemaakte Word-bestand verwijderd.

Het gebruik van de kantoorautomatiseringsomgeving (KA-omgeving) voldoet nog niet aan de Wet politiegegevens, zo constateert tevens korps Zaanstreek-Waterland. Wel heeft het korps een plan van aanpak opgesteld om dit in het vervolg te gaan verbeteren. Van de Public map zijn alle autorisaties geheel verwijderd en nu nog alleen toegankelijk voor de privacyfunctionaris. In plaats daarvan wordt er gebruik gemaakt van een O:\-schijf met daarop aparte opslagmappen per artikel ingedeeld.

Personeel wordt erop gewezen niets binnen de KA-omgeving op te slaan. Als men toch gegevens moet opslaan binnen deze omgeving wordt men in de instructie erop gewezen dit te doen in de publieke map. Per aangemaakte map moet in dat geval het mutatienummer aan het BVO-nummer gekoppeld zijn, waardoor een koppeling met BVO plaatsvindt en de gegevens altijd herleidbaar zijn naar BVO.

Beheer van gegevens

Het korps Zaanstreek-Waterland heeft naar aanleiding van de implementatie van de Wpg uitgebreid in kaart gebracht wat de stand van zaken is met betrekking tot de structurering en beheer van gegevens. Uit dit document blijkt het volgende:¹

¹ De volgende tekst is afkomstig uit het Dossier beheersmaatregelen van korps Zaanstreek-Waterland. Projectleider WPG, dateert van 17 maart 2010.

Structurering van gegevens

In de praktijk blijkt dat er veelal sprake is van de verwerking van politiegegevens in ongestructureerde vorm. Hierbij wordt bedoeld op politiegegevens welke middels de diverse kantoorautomatiserings-omgevingen in verschillende (afdelings)mappen /privémappen en binnen talrijke applicaties worden verwerkt en waarbij de diverse data en/of pagina's tekst tezamen processen-verbaal, rapportages, etc. vormen.

Verzamelingen van politiegegevens, verwerkt in dergelijke documenten en binnen de diverse applicaties zijn niet zonder meer van elkaar, maar ook niet van andersoortige gegevens, te onderscheiden.

Gegevensverzamelingen binnen de overige afdelingsapplicaties

De gegevensverzamelingen binnen deze politiestystemen kennen diverse varianten met betrekking tot het beheer. Applicaties zoals LIST en VROS zijn landelijke applicaties, maar worden regionaal beheerd door de functioneel beheerder IM. Voor HKS wordt, naast het functioneel beheer door IM, gegevensbeheer uitgevoerd door een aangewezen functionaris bij de sectie AI.

Diverse applicaties kennen binnen de betreffende secties een zogenoemde 'super-user' als beheerder. Voorbeelden daarvan zijn PSH-V (Vreemdelingenzaken) en PSH-TM (ADO). Het betreft hier zowel functioneel beheer als het uitvoeren van elementen van gegevensbeheer. Het beheer van een gesloten politiestysteem als RIDS (afdelingsapplicatie RI) wordt volledig in eigen beheer gevoerd.

Er is inzicht wie welke applicatie functioneel beheerd, echter dit is met de kleine applicaties decentraal en gefragmenteerd belegd. Dus niet centraal bij bijvoorbeeld IM. Er is wel bekend wie de functioneel beheerders zijn. Het uitvoeren van (taakelementen) gegevensbeheer is een zaak van 'handelen naar goed inzicht'.

Gegevensverzamelingen binnen kantoorautomatisering

De verzamelingen van gegevens binnen de KA-omgeving kunnen worden onderverdeeld in drie categorieën:

a. Groepsdata

Binnen groepsdata zijn momenteel ongeveer 6000 autorisaties verleend aan medewerkers voor het verwerken van gegevens in naar schatting 400 mappen die daarvoor door vtsPN zijn aangemaakt. De mappen kennen geautoriseerde gebruikers, maar in veel gevallen zijn er geen 'eigenaren' van deze mappen aangewezen/bekend.

Gegevensbeheer in deze map is niet georganiseerd. Er is geen zicht op de inhoud van deze mappen, maar aangenomen kan worden dat het merendeel van de mappen politiegegevens bevatten.

b. Public

Public is een map welke voor alle medewerkers toegankelijk is en gebruikt wordt voor opslag van gegevens met het doel om deze gegevens te delen. Vastgesteld is dat deze map ook gebruikt wordt voor de opslag van politiegegevens, waarbij deze gegevens beschikbaar komen voor medewerkers die daarvoor niet geautoriseerd mogen zijn (o.a. burgerpersoneel en stagiaires).

c. Privé mappen

Binnen de persoonlijke bestanden worden door de medewerkers mappen aangemaakt waarin zij diverse gegevens opslaan die in het kader van de politietaak worden verkregen. Er is geen zicht op de inhoud van deze mappen, maar

aangenomen kan worden dat een groot deel van deze persoonlijke mappen politiegegevens bevatten. Deze gegevens worden naar alle waarschijnlijkheid dan ook niet conform de Wpg 'verplicht gedeeld'.

[REDACTED]

[REDACTED]

[REDACTED]

Onderzoeksmap Team Grootschalige Onderzoek (TGO)

Onderzoeksmappen worden geautoriseerd voor de onderzoeksteams recherche. Deze staan op de groepsschijf van betreffende afdeling. TGO heeft een eigen afgeschermd schijfruimte waarop per team/onderzoek autorisaties worden toegekend.

Informatie uit eigen werk staat op de groepsmap. Alleen de afdeling analyse heeft hiertoe toegang, rechercheurs en blauw kunnen er niet in. De mappen worden persoonlijk geautoriseerd en zijn voldoende afgeschermd. Informatie waarvan men niet wil dat anderen inzage hebben kan men ook in de persoonlijke map kwijt.

Hierbij is gebleken dat voornamelijk de publieke map een veelheid aan politiegegevens bevat. Op dit moment vindt herinrichting van de kantoorautomatisering plaats.

Mobiele gegevensdragers

- De in gebruik zijnde handhelds zijn beveiligd door middel van een pincode. Wanneer de handheld vijf minuten niet wordt gebruikt wordt deze automatisch vergrendeld en dient opnieuw deze pincode te worden ingevoerd.
- Opgenomen filmpjes worden na verwerking uit de voertuigen gehaald en opgeslagen in het politiebureau, dat fysiek beveiligd is door middel van een toegangscontrolesysteem en een alarminstallatie.
- Er wordt functiescheiding toegepast. De teamchef, coördinatoren en medewerkers hebben hun eigen rol in de processen.
- Overdracht van de PSH-TM gegevens vindt plaats met een USB-stick, omdat er geen koppeling met het politiedomein mogelijk is. Een extern bedrijf (aangemerkt als bewerker) heeft toegang tot het systeem na toestemming van een medewerker VHT, die achter het systeem zit en meekijkt wat er gebeurt. Gegevens worden door het systeem leesbaar gemaakt voor het politiesysteem PSH-TM en voor verdere afhandeling middels interne post verzonden naar de administratieve organisatie aan het politiebureau te Zaandijk.

Logging

In BVH wordt alles gelogd; alleen wijzigingen in de tekst zijn niet terug te zien, wel wijzigingen in tabellen. Dat is een landelijke voorziening. In de logging is tevens te zien wie wat heeft verwijderd. Er is geen periodieke controle op de logging, dat gebeurt alleen in bijzondere gevallen op verzoek van BIO of de PF. In BPS moest de logging specifiek worden aangezet. Er is niet de mogelijkheid om terug te kijken.

Techniek

Vanuit vtsPN is er een 'achterdeur' om in het BVH systeem te komen. Als men met een dienstnummer in de tabellen van BVH is opgenomen, bestaat in principe de mogelijkheid om op afstand in het systeem te kijken. Zo is bekend dat een persoon uit Meppel toegang kan krijgen tot het systeem. Zaanstreek-Waterland is daar tegen. Echter de overige korpsen zijn daarvan voorstander. Op die manier kunnen dus aanpassingen verricht worden in het systeem.

Vanuit BVH zijn er koppelingen met heel wat systemen. Alleen niet met BVO en dat wordt als onhandig ervaren. BVO is geen productiesysteem, daarvoor is SUMM-It in het leven geroepen.

CIE Informanten

De verzameling met informanten staat fysiek los van andere informatie. De runners leveren aan de hand van de input van de informanten een bruto verhaal op.

4.3.3

Verbeterpunten

Als verbeterpunten zijn te noemen:

- Opstellen van procedures, richtlijnen voor het inrichten van een mappenstructuur die voldoet aan de vereisten vanuit de Wpg.
- Controle op de bewaartermijnen van de aangehouden informatie binnen de KA-omgeving.
- Opstellen van procedures en richtlijnen voor toetsing van de kwaliteitsaspecten op de informatie aangehouden in de KA-omgeving.
- Met betrekking tot de reeds afgeronde *pilot* met PDA's: creëer bewustzijn binnen het korps met betrekking tot de (privacy-)risico's die het werken met handhelds met zich meebrengen.

4.4 Gevoelige gegevens (artikel 5)

4.4.1 Norm

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

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

4.4.2 Bevindingen

Het team belast met artikel 10-onderzoeken legt gevoelige gegevens vast indien dat noodzakelijk is (direct met de zaak te maken heeft). Deze informatie is tevens beperkt toegankelijk. De bevoegde functionaris van de betreffende zaak is degene die uiteindelijk bepaalt of het opnemen van de gevoelige informatie noodzakelijk is of niet.

Zaanstreek-Waterland hanteert een strikt beleid omtrent het vastleggen van gevoelige gegevens. Het korps is terughoudend in het registreren van gevoelige gegevens en doet dit enkel wanneer dit noodzakelijk is voor de uitvoering van de politietaak. De privacyfunctionaris heeft richting de medewerkers altijd benadrukt hiermee zorgvuldig om te gaan.

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

Inrichting autorisatieproces applicaties Regiopolitie Zaanstreek-Waterland

Naar aanleiding van de inwerkingtreding van de Wet politiegegevens heeft korps Zaanstreek-Waterland een autorisatieprocedure uitgewerkt die aan de vereisten van de Wpg voldoet.

Opzet autorisatieprocedure

Onder verantwoordelijkheid van het unithoofd Personeel & Organisatie worden personeelsgegevens beheerd in het personeelsregistratiesysteem Beaufort. Het proces is dusdanig ingericht dat mutaties binnen dit systeem tijdig worden doorgevoerd en alle personen gekoppeld zijn aan een functie.

Onder verantwoordelijkheid van het hoofd Kwaliteitszorg Korpsleiding (KKL) wordt het functiehuis van de organisatie actueel gehouden.

Het hoofd Algemene bedrijfsvoering is verantwoordelijk voor het per functie vaststellen van de autorisaties per Wpg-relevante applicatie.

Elke autorisatie bevat een duidelijke omschrijving van;

- de verwerkingen waartoe de medewerker wordt geautoriseerd.
- de onderdelen van de politietaak ter uitvoering waarvan de verwerkingen worden gedaan.

De functionaris IM is benoemd tot regionaal autorisatiebeheerder. Autorisaties voor (Wpg) applicaties worden uitsluitend op basis van de autorisatiematrix toegekend. Deze matrix is in beheer bij IM. Daarop wordt toegezien door de privacyfunctionaris.

Bevoegd gezag

De aanvraag van een autorisatie gaat altijd via de lijnchef, deze is verantwoordelijk voor de goedkeuring. Medewerkers en chefs van de afdelingen CIE en RID dienen instemming te hebben van de OvJ, alvorens zij autorisatie verkrijgen tot de politiesystemen aangaande informanten, themaverwerking ernstige misdrijven en verdere CIE- en RID-verwerkingen.

Standaardautorisaties op systemen

Er zijn een aantal autorisaties vastgesteld die worden aangemerkt als standaardautorisaties. Dit zijn autorisatie op de systemen BVH, BVO, GVA-Online en RI-Online.

Bijzondere autorisaties op systemen

Er kunnen ook bijzondere autorisatie worden verleend. Deze worden op basis van de Wpg en na beoordeling van de privacyfunctionaris toegekend.

Bijzondere autorisaties zijn autorisaties voor medewerkers die niet in dienst zijn, zoals onderzoekers of stagiaires. Ook betreft het autorisaties die buiten het functieprofiel van de medewerker vallen.

De autorisatiebevoegde functionaris (unithoofd of hoger) geeft duidelijk aan voor welke bedrijfsapplicaties autorisatie nodig is en mailt dit naar de privacyfunctionaris. Deze beoordeelt de aanvraag en mailt de aanvraag voor verdere afhandeling rechtstreeks naar IM.

Autorisaties op Servers en mappen

De autorisatiebevoegde functionaris vraagt de autorisatie voor servers of mappen rechtstreeks aan bij de Functioneel beheerder IM. De functioneel beheerder IM maakt hierop een ticket aan en stuurt het verzoek naar vtsPN met *carbon copy* (controlefunctie) aan de privacyfunctionaris. VtsPN voert het verzoek uit. Interregionale autorisaties dienen door middel van een aanvraagformulier te worden aangevraagd door de autorisatiebevoegde lijnchef (unithoofd of hoger) en moeten worden gemaild naar de privacyfunctionaris van het eigen korps. Deze neemt contact op met de privacyfunctionaris van de andere regio die daarop de aangevraagde autorisatie verzorgt.

Mutaties

Er is tevens een procedure vastgesteld met betrekking tot het doorgeven van bijvoorbeeld functiewijzigingen. Personeelsmanagement dient de eventuele wijziging (ook i.v.m. in- en uitdiensttreding) vast te leggen in het aanstellings- of wijzigingsbesluit. Dit formulier gaat vervolgens naar de afdeling personeelsadministratie die deze mutatie doorgeeft aan functioneel beheer. Laatstgenoemde partij zorgt voor de aanpassing in de autorisatie.

Een procedure is aanwezig ingeval er sprake is van ontslag, schorsing en overlijden.

Autorisatie-instructies

Voor alle te verlenen autorisaties is ten behoeve van de bevoegde chefs een overzichtelijke instructie/handleiding vervaardigd.

Toezicht door de privacyfunctionaris

Een functioneel beheerder van IM houdt in Excel een overzicht bij van welke personen welke functies bekleden. Dit overzicht wordt geactualiseerd indien zich wijzigingen hebben voorgedaan. Wanneer de functioneel beheerder twijfelt aan de rechtmatigheid van een autorisatie, dan kan deze persoon terecht bij de privacyfunctionaris van het korps. Dit overzicht is altijd inzichtelijk voor de privacyfunctionaris.

De privacyfunctionaris heeft conform de Wpg een toezichthoudende rol met betrekking tot autorisaties. De privacyfunctionaris:

- toetst aanvragen voor het verlenen van autorisaties aan de regels;
- geeft opdracht tot het verlenen of intrekken van autorisaties en verifieert de daadwerkelijke uitvoering ervan;
- controleert de toepasselijkheid van verleende autorisaties en geeft zo nodig opdracht tot het intrekken van autorisaties;
- houdt toezicht op de administratie van verleende en ingetrokken autorisaties.

De privacyfunctionaris heeft wekelijks contact met de autorisatiebeheerder en heeft tevens zelfstandig toegang tot de autorisatiematrix. Enkele keren per maand controleert de privacyfunctionaris de autorisaties. Vaak is dat ad hoc, naar aanleiding van bijvoorbeeld een gebeurtenis of een vraag.

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

4.6.1 Norm

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

4.6.2 Bevindingen

Uit de gesprekken komt naar voren dat men sommige Wpg-termen lastig vindt te interpreteren. Men blijkt voornamelijk problemen te hebben met de interpretatie van artikel 11 Wpg. De begrippen uit dit artikel zijn lastig te plaatsen waardoor er behoefte is aan een extra definitiebepaling.

De uitleg/toepassing van art 11 lid 4 blijft een punt waarover men verschillend denkt. Er moet per doelstelling toestemming zijn van het bevoegd gezag, waardoor meerdere zoekslagen mogen worden gedaan. Daarvan worden verschillende interpretaties gehanteerd. Men kan voor vragen hierover bij de privacyfunctionaris van het korps terecht.

In de praktijk blijkt het echter niet werkbaar te zijn om voor elke zoekslag dit te melden en ter goedkeuring voor te leggen. Dit speelt voornamelijk in het geval van het zogeheten 'bulk werk' van artikel 8 en 9 informatie. Desalniettemin heeft men artikel 11 verwerkingen procesmatig uitgewerkt en uiteengezet welke functionarissen bevoegd zijn deze zoekacties uit te voeren.

Geautomatiseerd vergelijken

Het geautomatiseerd vergelijken is erop gericht vast te stellen of bepaalde gegevens uit de ene verzameling van gegevens ook voorkomen in andere verzamelingen van gegevens binnen het Wpg-domein, zonder dat daarbij meteen alle onderliggende gegevens zichtbaar zijn. Daarmee wordt het zoeken dus uitgevoerd op de voor de persoonlijke levenssfeer minst bezwaarlijke wijze, zoals dat ook ingevolge artikel 4, derde lid Wpg vereist is.

Bij de dagelijkse uitvoering van de politietaak zijn dat de gegevens die langer dan een jaar worden verwerkt en derhalve inmiddels niet langer 'vrij mogen worden verwerkt'. Deze gegevens mogen wel aan de hand van een (op-)nieuw in het kader van de dagelijkse politietaak verkregen gegeven, door middel van geautomatiseerde vergelijking op hit no hit-basis, weer worden opgeroepen om, indien dat noodzakelijk is, opnieuw gebruikt te worden bij de uitvoering van de dagelijkse politietaak.

Het geautomatiseerd vergelijken op 'hit-no hit' basis kan ook gedaan worden ten behoeve van zoekslagen voor gerichte gegevensverwerkingen voor de handhaving

van de rechtsorde in een bepaald geval (art. 9), of voor het verkrijgen van inzicht in de betrokkenheid van personen bij bepaalde ernstige bedreigingen van de rechtsorde (art. 10). Deze zoekbevoegdheid is geregeld in artikel 11, eerste respectievelijk tweede lid, Wpg.

Bij de geautomatiseerde vergelijking mogen alleen gegevens worden gebruikt die voor het doel waarvoor de vergelijking wordt uitgevoerd al zijn verkregen. Het Bpg regelt hoe de resultaten van een geautomatiseerde vergelijking zichtbaar worden. Dit is in de eerste plaats afhankelijk van het doel waarvoor de gerelateerde gegevens worden verwerkt.

Gecombineerd met elkaar verwerken

Met betrekking tot het in combinatie verwerken heeft Zaanstreek-Waterland artikel 11.4 Wpg uiteengezet in een procesbeschrijving.

Alle beschikbare politiegegevens kunnen hierbij worden geraadpleegd, doorzocht en gecombineerd, bijvoorbeeld door het stellen van samengestelde zoekvragen of door analyse aan de hand van bepaalde profielen van daders, slachtoffers of feiten. De resultaten ervan zijn direct en volledig zichtbaar.

Hierbij komen ook gerelateerde gegevens naar voren die bij geautomatiseerd vergelijken (deels) onzichtbaar blijven, omdat de betrokken bevoegd functionaris ze middels codering (deels) aan het oog heeft onttrokken.

Het gecombineerd verwerken is de meest verstrekende bevoegdheid om over te gaan tot het onbeperkt analyseren van alle beschikbare politiegegevens, waarbij zeer geavanceerde zoekmethoden kunnen worden toegepast.

Uit een oogpunt van proportionaliteit en subsidiariteit heeft de wetgever in de eerste plaats overwogen dat deze zoekmogelijkheden pas mogen worden ingezet, nadat gebruik is gemaakt van de verwerking van politiegegevens ter ondersteuning van de politietaken, zoals geregeld in artikel 13 Wpg.

Met betrekking tot gegevens die worden verwerkt ten behoeve van de uitvoering van de dagelijkse politietaken als bedoeld in artikel 8 Wpg, is in het derde lid bepaald dat uitsluitend die categorie gegevens – ook die ‘achter het schot’ van het tweede lid – in combinatie mogen worden verwerkt, indien dat voor datzelfde doel noodzakelijk is. Gedacht moet worden aan analyses om uit dit soort gegevens trends te ontdekken die aanleiding vormen om gericht gegevens te gaan verwerken als bedoeld in artikel 9 Wpg. De autorisaties voor deze zoekhandelingen zijn geregeld in artikel 2:1 Besluit politiegegevens.

De zoekmogelijkheden van in combinatie verwerken kunnen alleen worden gebruikt ten behoeve van onderzoeken in bepaalde gevallen in het kader waarvan politiegegevens worden verwerkt op grond van artikel 9 Wpg en ten behoeve van het verkrijgen van inzicht in de betrokkenheid van personen bij bepaalde ernstige bedreigingen van de rechtsorde als bedoeld in artikel 10 Wpg. Ten behoeve van een onderzoek in een bepaald geval mag niet door middel van geautomatiseerde vergelijking worden gezocht in CIE- en RID-gegevens.

De Wpg eisen met betrekking tot geautomatiseerd vergelijken en in combinatie verwerken worden niet afgedwongen door het systeem, maar er dient wel toestemming gegeven te worden.

Het in combinatie verwerken is alleen toegestaan in bijzondere gevallen en in opdracht van het bevoegd gezag (de OvJ respectievelijk de burgemeester).

Autorisatie en protocollering GV-ICMEV

In geval van een onderzoek inzake handhaving rechtsorde bepaald geval en om inzicht te verkrijgen in betrokkenheid van personen bij bepaalde ernstige bedreiging van de rechtsorde, mogen aangewezen functionarissen langs geautomatiseerde weg zoeken naar verbanden tussen politiegegevens, namelijk het geautomatiseerd vergelijken en het in combinatie verwerken.

Deze zoekslagen mogen binnen het korps alleen door personeel van CIE, RI en rechercheurs themaregisters (mensenhandel, mensensmokkel en terrorisme) en in voorkomende gevallen door medewerkers Infodesk worden uitgevoerd. Medewerkers Infodesk mogen deze zoekslagen alleen uitvoeren bij dringende noodzakelijkheid en na toestemming van het hoofd van de eenheid van CIE, RI of recherchechef themaregisters.

Om toestemming te verkrijgen van het bevoegd gezag heeft korps Zaanstreek-Waterland een sjabloon van een proces-verbaal ontwikkeld die door de betreffende bevoegd functionaris dient te worden opgemaakt. Het betreft hier een proces-verbaal 'Aanvraag opdracht in combinatie verwerken' en is beschikbaar op intranet.

Daarbij dient vastgelegd te worden:

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

Het opmaken van het proces-verbaal, zoals hierboven beschreven blijft echter achter, en voor zover de privacyfunctionaris bekend, is die nog nimmer opgemaakt. Dit wordt gezien als een te grote administratieve last.

De logging functionaliteit, die de genoemde zoekslagen in een logverslag bijhoudt, is nog niet door de vtsPN beschikbaar gesteld. De vraagstellingen (vergelijkingen en combinatie zoekslagen) worden tot die tijd door de Infodesk vastgelegd in de BVO-Infodeskmodule. De zoekvragen worden tevens hierin vastgelegd, en bewaard voor vijf jaar. De privacyfunctionaris heeft weliswaar geen zelfstandige toegang, doch indien noodzakelijk wordt hem door de Infodesk of functioneel beheerder inzage verleend.

Er heeft nog geen formele steekproef plaatsgevonden op geautomatiseerd vergelijken met andere dan politiegegevens. Doordat de privacyfunctionaris zeer regelmatig bij de Infodesk is en daar vragen beantwoordt en met de werkzaamheden meekijkt heeft hij daar zicht op.

4.6.3

Verbeterpunten

- De procedures en richtlijnen met betrekking tot artikel 11 zoekacties op een begrijpelijke manier communiceren naar betrokkenen. Met geeft aan dat men behoefte heeft aan heldere richtsnoeren.
- Het gebruik van het zelf ontwikkelde sjabloon proces-verbaal te stimuleren onder de betrokken medewerkers.

4.7 Bewaartermijnen (artikel 14)

4.7.1

Norm

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

4.7.2

Bevindingen

De bewaartermijnen zijn zowel in BVH als BPS bekend, maar kunnen niet (meer) toegepast worden. Voor BVH geldt dat de functionaliteit binnen de applicatie nog niet is ingericht. Er is in de nieuwe release van BVH (versie 1.2.2) weliswaar een schoningsmodule in aanwezig, maar deze staat op landelijk verzoek van de voorzitter van de stuurgroep nog niet aan.

Voor BPS geldt dat de functionaliteit door verschil in applicatie-versies (tussen actuele en historische omgeving) niet meer gebruikt kan worden. BPS voorziet dus wel in de mogelijkheid, echter kan op dit moment niet door een functioneel beheerder uitgevoerd worden.

Hiervoor is begin 2011 opdracht aan vtsPN gegeven om de BPS versies gelijk te gaan trekken teneinde de noodzakelijke schoning te kunnen toepassen.

Met behulp van een maandelijkse monitorlijst bepaalt de bevoegde functionaris of een onderzoek kan worden afgesloten. Als een onderzoek kan worden afgesloten wordt een sluitdatum ingevoerd op aangeven van de teamleider. Dat gebeurt met enige regelmaat.

Sectie Algemene Inlichtingen is verantwoordelijk voor het toezicht op de bewaartermijnen, maar hier is tot nog toe niet echt naar gekeken. Zo is het niet duidelijk hoe lang preweeg-documenten na het opstellen in BVO blijven staan en hoe lang registraties bij de Infodesk worden bewaard. Met betrekking tot de registraties zijn tot nu toe geen gegevens verwijderd.

Tevens geeft men aan dat er dit jaar dossiers digitaal aangeleverd zijn aan de Officier van Justitie en aan de HKD. Er komen ongeveer 30 dossiers per dag binnen en er is een achterstand opgebouwd van ongeveer 400 á 500 dossiers ten aanzien van het verwerken van die dossiers in HKS. HKD levert maandelijks schoningsverslagen aan.

Er is geen toezicht op de schoningsactiviteiten van de analisten, zo blijkt uit de ontvangen documentatie.

Het schoningsproces van artikel 8 en 9 politiegegevens bij Zaanstreek-Waterland is niet conform Wpg. De overdracht van informatie over afgesloten zaken van OM naar politie is een aandachtspunt.

BPS

Het oudere systeem BPS is alleen nog toegankelijk voor de privacyfunctionaris en de infodesk en wordt uitgefaseerd. De Infodesk is ervan op de hoogte dat er in dat geval toestemming nodig is van de Officier van Justitie.

Sinds 12 december 2011 is de BPS-data geheel verwijderd, waarmee informatie van vóór april 2009 niet meer toegankelijk is. Deze data heeft het korps omgezet naar '.txt-bestanden', welke alleen nog maar raadpleegbaar zijn door de informatie organisatie. In deze tekstbestanden is informatie van de periode tot 1998 beschikbaar. Personeel van deze afdeling is Wpg-opgeleid en op de hoogte van de beperkingen van de Wpg met betrekking tot historischevragingen.

Zolang ten aanzien van deze gegevensverzameling geen onderscheid gemaakt wordt tussen artikel 8 en artikel 9 politiegegevens (en dus door elkaar wordt opgeslagen) is dit voor korps Zaanstreek-Waterland de best mogelijke oplossing.

Desalniettemin, gegevens ouder dan tien jaar moeten vernietigd worden. Dat gebeurt echter niet. Ze worden achter een schot geplaatst en de informatie tot 1998 is nog steeds – weliswaar beperkt – raadpleegbaar.

Kleinschalige rechercheonderzoeken

Bij het korps Zaanstreek-Waterland is gebleken dat teveel kleinschalige recherche onderzoeken op de plank zijn blijven liggen. Er was geen zicht op lopende / niet afgeronde zaken. Om bedrijfsprocessen voor dit soort onderzoeken inzichtelijker te maken heeft het korps binnen haar organisatie een tweetal afdelingen ingericht. Deze afdelingen zijn organisatorisch opgenomen onder de unit Zaanstreek Noord en de unit Purmerend.

Met de implementatie van BOSZ zal dit probleem (geen zicht hebben op plankzaken) grotendeels worden opgelost.

Artikel 9 half jaar na OH-moment

Het Openbaar Ministerie dient zorg te dragen voor het bericht aan het korps dat een zaak in kracht van gewijsde is gegaan. Wanneer het korps hierover is bericht is een zaak afgesloten, maar gedurende een half jaar nog wel te raadplegen. Dit wordt dan weggezet in de zogeheten 'artikel 14-map' en die mag nog vijf jaar worden bewaard.

Bij gebruik moet apart toestemming worden gevraagd aan de OvJ. De bij de start van het onderzoek aangemaakte Melding Recherche Onderzoek (MRO) wordt dan tevens afgesloten. Na een half jaar stopt de levering van en naar VROS automatisch. De levering naar BlueView blijft ongewijzigd aanstaan.

In de praktijk blijkt dat men weinig – af en toe – terugkoppeling krijgt van het OM door middel van afloopbriefjes wanneer een zaak in kracht van gewijsde is gegaan. Dit heeft als gevolg dat er in BVO geen structurele verwijdering van zaken plaatsvindt. Ook het achter het schot zetten voor afgesloten zaken gebeurt niet.

Korps Zaanstreek-Waterland heeft naar aanleiding van dit probleem het (landelijke) systeem BOSZ geïmplementeerd om op eenvoudigere wijze terugkoppeling te ontvangen. Vanaf 10 januari 2012 gaat dit systeem 'live' en is het Openbaar Ministerie geautoriseerd zodat ze de status van de betreffende zaken hierin kunnen aangeven.

Cold-case zaken

In het geval van een cold-case moordzaak moet men nog bij oude informatie kunnen zodra er weer nieuwe informatie beschikbaar komt. Om deze reden moet het niet worden vernietigd. In dit geval wordt in een paar zinnen beschreven waarom er niet wordt vernietigd. Men stelt dan beschikbaar onder voorwaarden (bijvoorbeeld middels een machtiging), waarbij de Officier van Justitie fungeert als poortwachter.

BVO informatie mag gebruikt worden zolang een zaak niet verjaard is. In het geval van een moord is wordt geen verjaringstermijn gehanteerd. Als een zaak in kracht van gewijsde is geweest, dienen de gegevens verwijderd te worden en vallen deze onder art. 14 (bewaartermijn van extra vijf jaar), daarna moet het vernietigd worden. Het systeem is echter nog niet zo oud. Bevoegde functionarissen zijn er nu ook wel van bewust dat je niet alles kunt blijven bewaren.

De Infodesk treedt op als poortwachter en kan de relevante informatie opzoeken en vervolgens melden dat de zoekactie resultaat heeft opgeleverd, maar dat toestemming door de OvJ moet zijn verleend alvorens deze informatie beschikbaar wordt gesteld.

Artikel 10 informatie

De Criminele Inlichtingen Eenheid heeft een procedure uitgewerkt met betrekking tot het schonen van artikel 10 informatie.

De registratiebeheerder/administratief medewerker CIE stelt een lijst samen van de te schonen subjecten. Deze medewerker stelt vervolgens de lijst ter beschikking aan de CIE-chef.

Tot eind 2010 werd periodiek (elke drie maanden) nagekeken welke subjecten in aanmerking kwamen voor verwijdering. Omdat sprake zou zijn van de verlenging van de termijnen van vijf naar tien jaar werd in afwachting daarvan vanaf begin 2011 gestopt met het periodiek verwijderen van de daarvoor in aanmerking komende subjecten. Een bijkomend probleem was dat de medewerker de lijsten met daarop de subjecten die voor schoning in aanmerking zouden komen sinds eind 2010 niet meer kon leveren. Die betreffende functionaliteit was van deze persoon afgenomen. Dat gold voor alle vier de regio's binnen het verzorgingsgebied van Zaanstreek-Waterland. Thans is er sprake dat vanaf begin 2012 een nieuwe tool werkzaam wordt die automatisch een melding genereert indien een bepaald subject geschoond dient te worden.

De CIE-chef controleert deze lijst van de te schonen objecten, en geeft de opdracht tot schoning aan de administratief medewerker CIE. De te schonen informatie wordt volgens de richtlijnen van artikel 10 verwijderd. Praktisch gezien betekent dit dat alle mutaties die aan het betreffende subject hangen worden verwijderd. Tevens werd het kenmerk subject weggehaald. Dit kan worden aangemerkt als verwijderen, maar niet als vernietigen.

De verwijderde politiegegevens worden gedurende een termijn van vijf jaar bewaard ten behoeve van verwerking met het oog op de afhandeling van klachten en de verantwoording van verrichtingen en worden vervolgens vernietigd (artikel 14).

Hernieuwde verwerking

Politiegegevens die na hun verwerking zijn verwijderd en die gedurende vijf jaar worden bewaard, mogen in bepaalde gevallen en onder strikte voorwaarden beschikbaar worden gesteld voor hernieuwde verwerking. Deze hernieuwde verwerking van politiegegevens dient schriftelijk te worden vastgelegd.

Er is een schriftelijke aanwijzing uitgereikt aan de bevoegd functionarissen waarin de praktische uitvoering van de protocolplicht ten aanzien van deze verwerkingen wordt beschreven.

In de schriftelijke aanwijzing wordt gewezen op het feit dat politiegegevens uit artikel 9 en 10 die na hun verwerking zijn verwijderd en gedurende vijf jaar worden bewaard in bepaalde gevallen beschikbaar mogen worden gesteld voor hernieuwde verwerking. Hiervoor is toestemming vereist van het bevoegde gezag (OvJ of burgemeester).

De praktijk wijst uit dat men aan de beschikbare vijf jaar BPS/BVH gegevens doorgaans voldoende heeft en (indien mogelijk) uitwijkt naar het artikel 13-reglement van HKS. Men heeft nog niet meegemaakt dat men toch informatie, ouder dan vijf jaar nodig heeft en dus toestemming van het bevoegde gezag is vereist.

Indien er toch sprake is van hernieuwde verwerking wordt dit vastgelegd en gedurende vijf jaar bewaard in de BVO-Infodeskmodule.

Restinformatie CIE

De aangeleverde restinformatie dient te voldoen aan de volgende voorwaarden:

- Restinformatie dient voorzien te zijn van het door de Zaakofficier van justitie voor akkoord getekende formulier "Rapport tot verstrekking van onderzoeksgegevens".
- Restinformatie dient middels een BVO mutatie te worden aangeleverd.

De administratief medewerker CIE verzamelt de verkregen restinformatie, welke middels een gelabelde BVO mutatie is verkregen. De CIE-chef controleert vervolgens of de verkregen restinformatie voldoet aan de opnamecriteria voor de artikel 10 Wpg registratie en accordeert deze. De gelabelde BVO mutaties met betrekking tot restinformatie worden overgezet naar de artikel 10 registratie.

Tevens draagt de administratief medewerker zorg voor koppeling van eventuele onderliggende stukken met de restinformatie in BVO. Deze onderliggende stukken dienen echter wel meerwaarde te hebben.

Men heeft intern afgesproken geen fysieke levering te laten plaatsvinden van een PV restinformatie. Dit PV wordt pas aangeleverd indien een strafrechtelijk opsporingsonderzoek wordt opgestart.

Artikel 12 informatie

RID

Het unithoofd is verantwoordelijk voor de bewaartermijnen en de vernietiging van gegevens. Het RID-systeem is bekeken en een kast met papieren dossiers is het afgelopen half jaar volledig geschoond.

Wanneer een informant gegevens aanbiedt wordt het in zijn dossier (hangmap) bewaard, dit is de laatste jaren echter niet voorgekomen. De dossiers worden bewaard in een kluis die in een beveiligde ruimte staat. Om toegang tot deze ruimte te verkrijgen dient men in het bezit te zijn van een code en een geautoriseerde toegangspas.

Tijdens het werkoverleg dat één keer per twee weken met de gehele RID en het unithoofd plaatsvindt, worden onder andere informanten geëvalueerd. Als tijdens het overleg besloten wordt dat de informant geen meerwaarde meer oplevert, wordt het dossier afgebouwd. De dossiers worden aan het einde van de bewaartermijn

overgedragen en opgeslagen in het archief van de politieregio Zaanstreek-Waterland.

De verwijderde politiegegevens worden gedurende een termijn van vijf jaar in RIDS bewaard ten behoeve van verwerking met het oog op de afhandeling van klachten en de verantwoording van verrichtingen en vervolgens door de geautoriseerde voor het Openbare Orde register vernietigd (artikel 14 Wpg).

CIE

Digitale informatie wordt bewaard in BVO bij de bewerker organisatie vtsPN. Dossiers, aantekeningen en processen-verbaal worden opgeslagen in een kluis op de afdeling. Het unithoofd Recherche Ondersteuning is verantwoordelijk voor de opslag en de bewaartermijnen die gelden ten aanzien van CIE informatie. De sectie CIE gaat zorgvuldig om met de Wpg-verplichtingen. De CIE-OvJ voert hierop controle uit.

De lijst instemming OvJ is nog niet aan de chef CIE overhandigd, maar verblijft nog onder de hoede van de CIE-OvJ, een en ander in verband met interregionale afstemming.

Schoning van het artikel 12 register vindt plaats na maximaal 10 jaar. Alle handelingen worden geprotocolleerd in BVO-bruto. De applicatie Ask Sam is inmiddels uitgefaseerd en wordt alleen nog geraadpleegd. De politiegegevens in Ask Sam worden momenteel inzichtelijk gemaakt en ter vernietiging voorgelegd aan de CIE-OvJ.

4.7.3

Verbeterpunten

- Houd beheersmaatregelen voor verwijdering en vernietiging in de systemen BVH en BVO landelijk op de agenda

4.8 Ter beschikking stellen (artikel 15)

4.8.1

Norm

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

4.8.2

Bevindingen

Infodesk

De sectie Infodesk gaat serieus om met de Wpg-verplichtingen. Een verdere verdieping van Wpg-kennis is wenselijk en zal worden georganiseerd.

De Infodesk bestaat uit zes tot zeven medewerkers. Daarnaast zijn er ongeveer tien analisten met verschillende achtergronden. Er is een strategisch analist die zich bezighoudt met de algemene veiligheid, er zijn drie tactische analisten, ongeveer zes operationele analisten, een CIE analist en tenslotte een operationele analist uit het korps.

De operationele analisten worden veelal aan onderzoeken toegevoegd. Tactische analisten maken gebiedsscans en worden ingezet voor de sturing van blauw en grijs. Een van de tactische analisten is tevens scenario-analist en wordt ingezet bij TGO's (teams grootschalig onderzoek) om scenario's op te stellen. De CIE beschikt

over een analist die zich onder andere bezighoudt met de beoordeling van informanten.

Daarnaast beschikken de units over informatievoorzieners die onder andere briefings assisteren bij de Infodesk. Zo is er een informatievoorzieners Zaanstreek (ICZ) en een informatievoorzieners Purmerend (ICP).

De afdeling bestaat uit een coördinator RID, twee inlichtingenrechercheurs en een administratief medewerker. De regionale informatievoorzieners is unithoofd van de afdeling en ontvangt als zodanig informatie van Zaanstreek-Waterland. Het unithoofd is tevens hoofd CIE, Infodesk, RID, Analyse en Onderzoek en Projectvoorbereiding.

Toetsing door de Infodesk

Alle interne informatieverzoeken gaan via de Infodesk waar negen mensen werkzaam zijn. Doordat de korpsgrootte beperkt is vindt controle bij de Infodesk impliciet plaats. Aanvragers worden geïdentificeerd door middel van het e-mailadres, telefoonnummer (bij telefonische aanvraag) en stem- en/of naamherkenning. Anders wordt als extra controlemaatregel een vergelijking gemaakt tussen naam en dienstnummer.

De Infodesk geeft alleen artikel 9 informatie na goedkeuring van de betreffende bevoegde functionaris. Dit houdt in dat men altijd belt of mailt met een bevoegde functionaris om toestemming voor het verstrekken van de informatie.

Voordat door de Infodesk ter beschikking wordt gesteld wordt de juistheid van de gegevens beoordeeld. Bovendien controleert de Infodesk of de gegevens, die ter beschikking worden gesteld of worden verstrekt, voldoen aan de aanvraag.

Bij het verstrekken van de gegevens vermeldt de Infodesk de bron en vaak ook de zoekstring. Dit geeft inzicht in de gevolgde werkwijze bij het zoeken en daarmee is de herkomst van artikel 9-gegevens terug te vinden.

Informatiesystemen

- BVO (basis voorziening opsporing).
- BVH (basis voorziening handhaving).
- BlueView.
- HKD (systeem waar datadossiers in zijn verwerkt aan de hand van coderingen).
- HKS (ouder landelijk bruikbaar systeem).
- BOSZ (coördinatie + keten informatie systeem)

Het merendeel van de gegevens wordt uit de systemen BVH of BVO gehaald. Middels BlueView wordt bovenregionale informatie geraadpleegd.

De Infodesk doet een intake bestaande uit vragen vanuit blauw en grijs en geven opgevraagde informatie. Deze informatie komt binnen via de mailbox. De antwoorden worden vastgelegd in BVO, BVH of in de Infodesk registratie (module van BVO).

Werkprocessen

Alle werkprocessen staan in een handboek, opvraagbaar bij de privacyfunctionaris.

Alle medewerkers kunnen een aanzet geven tot het maken van een preweeg-document, de recherchechef dient hierover goedkeuring te geven. Dit document bestaat ongeveer uit anderhalf A4 waarin in het kort de casus staat beschreven.

Eén keer in de vier weken vindt er een overleg van de stuurgroep plaats waarin deze preweeg-documenten worden besproken. Van deze overleggen worden notulen gemaakt welke in de map projectvoorbereiding bewaard worden. Het preweeg-document wordt vervolgens in BVO gezet.

Achtergrond Unit Recherche Ondersteuning (RIO)

De unit bestaat uit 3 secties, namelijk de Algemene (Infodesk), Criminele (CIE) en Regionale Inlichtingen (OOV).

CIE processtappen ter beschikking stelling

De administratief medewerker CIE controleert of de betreffende persoon als subject geregistreerd staat. Wanneer dat niet het geval is, kan geen ter beschikking stelling of verstrekking plaats vinden)

- De administratief medewerker CIE registreert in BVO een verstrekkingsmutatie (VSTZW).
- De administratief medewerker CIE stelt de ter beschikking te stellen informatie beschikbaar aan de CIE-chef ter accordering.
- De CIE-chef controleert, zonodig, de informantenstatus. Dit is het geval indien de ter beschikking stelling niet direct plaatsvindt nadat de informant zijn informatie heeft gegeven.
- De CIE-chef accordeert en parafeert de ter beschikking te stellen informatie van de ZIR aan de externe CIE (welke buiten het verzorgingsgebied is gesitueerd).

De administratief medewerker CIE registreert wanneer en aan wie de ZIR ter beschikking is gesteld.

De administratief medewerker CIE verstuurt de ZIR:

- Digitaal, door de ZIR te labelen naar de externe CIE binnen hetzelfde verzorgingsgebied.
- Schriftelijk (op papier) indien de CIE niet behoort tot het verzorgingsgebied.
- De administratief medewerker CIE maakt de ter beschikking stelling definitief.

Voor de RI geldt dat de bevoegd functionaris/unithoofd Recherche Ondersteuning toestemming verleent voor het ter beschikking stellen van de gegevens.

Codering

Het systeem BVO-rood is vorig jaar (2010) in gebruik genomen en maakt gebruik van een vertrouwelijkheidscode ten aanzien van de informatie. De CIE-codering wordt gebruikt, namelijk de 00/01/11-codering.

Voor de invoering van BVO werden alle gesprekken vastgelegd in het oude systeem RIDS. In dat systeem was nog geen onderscheid mogelijk tussen bruto- en netto-informatie. Deze gegevens worden niet meer overgezet naar BVO tenzij nieuwe informatie een vervolg is op bestaande informatie vanuit RIDS, die dientengevolge mag worden overgezet (gelet op de "schuivende termijnen").

'Afscherming'

Voor het ter beschikking stellen van informatie wordt de afscherming in BVO op niveau 4 gezet. De praktijk heeft echter uitgewezen dat dit in incidentele gevallen tot schade heeft geleid bij zaken waarbij door andere korpsen zonder vooroverleg gebruik is gemaakt van de informatie. Er zijn geluiden dat teamleiders in het land de afscherming naar niveau 5 hebben gebracht. Bij niveau 5 is deze informatie niet bevaagbaar via BlueView en wordt de informatie 'afgeschermd' van andere politieonderdelen. Dat druist tegen het principe van de Wpg in, waarin delen van informatie een uitgangspunt is. Meerdere teamleiders van diverse korpsen zeggen

inmiddels veelal op niveau 5 te verwerken. De kans op lekproblemen wordt aangehaald als reden voor de 'afscherming'.

Over het algemeen staan alle onderzoeken op niveau 4, zodat de Infodesk (makelaar) hun taak kan uitoefenen. Formeel wordt in een enkel geval (mensenhandel en prostitutie in de regio) niveau 5 gehanteerd. Men heeft niet gekozen voor een aanvraag bij het College Bescherming Persoonsgegevens, omdat de procedure voor een embargo-onderzoek als te zwaar wordt ervaren en de gekozen oplossing pragmatisch van aard is. Vanwege de kans op het verbreken van de doelbinding is men gehouden contact op te nemen met de projectleider of de bevoegd functionaris van een onderzoek.

In BVO is inzage tot en met niveau 3 mogelijk in objecten. Inzage van de netto-informatie is voorbehouden aan medewerkers van de Infodesk, die geautoriseerd zijn op niveau 4. Vanuit deze functie treden zij op als makelaar naar de tactische teams.

Aanwijzing bevoegd functionaris

Intern is er een helpdesk voor de Wpg, namelijk de privacyfunctionaris. Op decentraal niveau en met name in het rechte proces zijn de aangewezen bevoegd functionarissen de aangewezen contactpunten. De bevoegd functionarissen zijn op persoon aangewezen en een aanwijzingsbesluit is in hun personeelsdossier opgenomen.

In opvolging van de regelgeving Wpg worden hierna de proceseigenaren genoemd die de (eind) verantwoordelijkheid dragen voor de uitvoering van een proces. Het betreft hier de reeds aangewezen proceseigenaren conform het RBP, aangevuld met proceseigenaren voor specifieke Wpg-processen:

De genoemde functionarissen zijn bij besluit door de Korpschef aangewezen. Een door de Korpschef getekend besluit "aanwijzing proceseigenaren ter uitvoering van de WPG" wordt beheerd door de unit P&O.

De verantwoordelijkheid tot protocolleren van de doelstelling is neergelegd bij de aangewezen bevoegd functionarissen (BF). De protocolverplichting in deze is aangereikt binnen de opleiding BF en in een aanwijzing protocolplicht welke is toegezonden aan alle Bevoegd Functionarissen.

De bevoegd functionarissen leggen de vereiste gegevens vast in de bedrijfsapplicaties BVO en/of BVH. De verplichting tot protocolleren is in de betreffende werkprocessen vastgelegd.

Dossier beheersmaatregelen - Overige waarneming

Vanuit de rol als toezichthouder heeft de privacyfunctionaris vastgesteld dat bevoegd functionarissen binnen de DR en CR consequent rechercheonderzoeken aanmelden in BVO.

Opleiding bevoegd functionaris

Alle bevoegd functionarissen van Zaanstreek-Waterland hebben een Wpg-cursus gehad. De training wordt gegeven door de politieacademie en alle aspecten van de uitoefening van de functie bevoegd functionaris worden hierin meegenomen. Daarnaast zijn een zelfstudie-cursus, modellen en de verstrekkingwijzer op Intranet beschikbaar gesteld.

De teamleiders van de recherche (30 in totaal, inclusief bevoegd functionarissen van andere secties) hebben allen een opleiding bevoegd functionaris genoten (intern gegeven door de politieacademie). De bevoegd functionarissen zijn zich bewust van het gebruik van de Wpg en van de gevolgen van onjuiste toepassing van de wet.

Elke nieuwe diender die van de politieschool komt moet langs bij Bureau Interne Onderzoeken, de vertrouwenspersoon en de privacyfunctionaris. Laatstgenoemde wijst de nieuwkomers op het belang van de Wpg.

Weigeringsgronden

De bevoegd functionarissen zijn op de hoogte van de wettelijke weigeringsgronden in relatie tot de verplichting van het ter beschikking stellen. Dit is opgenomen in de opleiding voor bevoegd functionarissen.

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

Verstrekkingswijzer (landelijk)

De wet (en het besluit) voorziet in aan wie verstrekt mag worden. Hiervoor is een zogenaamde verstrekkingswijzer ontwikkeld door het landelijk project. Het korps hanteert de landelijke verstrekkingswijzer.

Verder zijn in elk werkproces van het dossier beheersmaatregelen beschreven, wie wat mag verstrekken etc. Het dossier beheersmaatregelen is een levend dossier. Een voorbeeld is het convenant dat alle regio's hebben getekend aangaande de RIEC's, terwijl de Minister recent hiervoor een Besluit heeft getekend (op basis van artikel 18 Wpg) dat dit convenant overbodig maakt. Wijzigingen worden meegenomen in het dossier beheersmaatregelen.

Proces voor artikel 20 besluiten

Op 1 januari 2010 is korps Zaanstreek-Waterland begonnen met het actualiseren van de artikel 20-besluiten conform de Wpg.

Er is door het Korps Management Team afgekondigd dat alle convenanten die het korps met derden aangaat via de korpsleiding en het convenantenloket moeten lopen. In de praktijk blijkt dat dit goed verloopt.

Het korps heeft een procesbeschrijving opgesteld met betrekking tot het opstellen van convenanten. Dit proces bevat de volgende (beknopt weergegeven) processtappen:

1. De convenanteigenaar (functie van de persoon die het convenant afgesloten heeft) maakt het initiatief tot opstellen van een convenant bekend bij het convenantenloket. Het loket overhandigt de initiatiefnemer de ondersteunende documenten.

2. De convenanteneigenaar geeft de conceptversie van het convenant ter controle af aan het convenantenloket, indien sprake is van gegevensuitwisseling wordt een artikel 20-besluit opgesteld.
3. Het convenant wordt juridisch gecontroleerd door het loket.
4. De convenanteneigenaar past het convenant aan naar de genoemde opmerkingen en/of verbeterpunten.
5. De convenanteneigenaar agendeert in samenspraak met het diensthoofd het convenant.
6. Indien het KMT akkoord gaat met het stuk, wordt het stuk ondertekend door de korpschef.
7. De convenanteneigenaar geeft het door alle partijen getekende convenant met voorlegger af bij ADO en stuurt een kopie naar het convenantenloket.

Daarnaast heeft het korps voor interne en eventueel externe opdrachtgevers een aanspreekpunt in de vorm van een convenantenloket bij Kabinet Korpsleiding met een adviesteam bestaande uit een beleidsadviseur, jurist en privacyfunctionaris. Dit team ondersteunt bij het opstellen en vaststellen van convenanten en artikel 20 Wpg-besluiten door 'convenanteigenaren' in het korps. Het loket heeft ter ondersteuning van dit proces voor opdrachtgevers ook een checklist gemaakt voor het algemeen beoordelen/opstellen van een convenant en een checklist specifiek gericht op de Wpg.

De verantwoordelijkheid voor het opstellen van een convenant ligt bij de korpsinitiatiefnemer (vaak portefeuillehouder) en het betreffende diensthoofd (MT-lid). De beoordeling en de controle van het convenant en het artikel 20 besluit wordt gedaan door de korpsleiding en/of de korpsjurist en worden daarbij door het convenantenloket ondersteund. De interne opdrachtgever adviseert welke politiegegevens zullen worden uitgewisseld.

De tekenbevoegdheid is door de korpsbeheerder gemandateerd aan de (plv.) korpschef. Binnen het korps is dit recht alleen ondergemandateerd aan de korpschef, daarom krijgt hij alle convenanten en artikel 20 besluiten onder ogen.

Overzicht convenanten

Er is een convenantenloket opgesteld. Het convenantenloket is gepositioneerd onder het Kabinet Korpsleiding (KKL). Het convenantenloket is verantwoordelijk voor het bijhouden van de afspraken met het oog op structurele informatie-uitwisseling.

De convenanten worden tevens gepubliceerd op intranet, maar men is van mening dat dit vindbaarder kan. Via een link op intranet worden medewerkers doorgestuurd naar de map waarin de convenanten zijn opgeslagen.

Een andere manier voor medewerkers is om contact op te nemen met KKL om na te gaan of er aan de betreffende verstrekking een artikel-20 besluit ten grondslag ligt. Soms denkt men dat een convenant van kracht is terwijl dit in de praktijk niet het geval blijkt te zijn.

Looptijd

Het convenantenloket heeft een inventarisatielijst met convenanten waarin de doorlooptijden zijn opgenomen. De gehanteerde termijn van de convenanten loopt van één tot maximaal twee jaar, waarvan een aantal automatisch wordt verlengd. De interne opdrachtgever/portefeuillehouder is verantwoordelijk voor het onderhoud. Het convenantenloket kan vanuit een controletaak de betrokken interne opdrachtgever/portefeuillehouder er op wijzen dat het convenant verloopt. Ook

vanuit ADO/DIV kan de opdrachtgever aan het eventueel aflopen van termijnen worden herinnerd.

In de praktijk is het vaak de portefeuillehouder die tijdig het initiatief neemt en dit kenbaar maakt bij het convenantenloket.

Geheimhouding

Een bepaling omtrent de geheimhoudingsplicht staat standaard in de formulieren, daarmee worden de betrokken partijen altijd op deze geheimhouding gewezen. Het korps hanteert een standaard zinsnede bij het ter beschikking stellen van informatie: "informatie is vertrouwelijk, voor meer informatie neem contact op met teamleider X".

Bij elke verstrekking dient aan de ontvanger (schriftelijk of mondeling) meegedeeld te worden dat de ontvanger geheimhoudingsplichtig is en dat de ontvangen gegevens niet verder mogen worden verstrekt. Ook voor incidentele verstrekkingen wordt de disclaimer voor geheimhouding bijgevoegd.

De volgende "vaste" zin wordt gebruikt:

"Ik ben u verplicht mede te delen dat u voor wat betreft bovenstaande informatie geheimhoudingsplichtig bent ex. artikel 7 van de Wet Politiegegevens. U mag deze gegevens alleen voor deze zaak gebruiken en niet doorverstrekken."

Proces voor geautomatiseerde verstrekking

Enkele leden van het Openbaar Ministerie van het parket Haarlem hebben toegang tot BVH (Basis Voorziening Handhaving) en BOSZ (vanaf 5 januari 2012), zijnde de coördinatiemodule van BVH. Hiervoor is een convenant afgesloten. De verantwoordelijke (i.c. de korpsbeheerder) heeft hiervoor zijn goedkeuring gegeven. Tevens zijn de geautoriseerde mensen onderworpen aan een betrouwbaarheidsonderzoek.

Gelet op artikel 16 van de Wpg is verstrekking alleen toegestaan voor zover het OM deze gegevens behoeven voor de in het artikel gestelde doeleinden (noodzaak en doelbinding). Door middel van het verlenen van onbegrensde toegang tot BVH is geenszins geborgd dat de verwerking die het OM verricht op basis van BVH-gegevens gerechtvaardigd is.

Door toekenning van deze structurele toegang is de koppeling van een bevraging met de noodzaak en doelbinding vooraf niet toetsbaar. Een controle op bevragingen vooraf ontbreekt.

Ook artikel 23 (rechtstreekse verstrekking aan leden van het OM) stelt aanvullende eisen met betrekking tot het verstrekken van gegevens aan het Openbaar Ministerie. De verantwoordelijke dient passende technische en organisatorische maatregelen te treffen teneinde te waarborgen dat rechtstreekse verstrekking uitsluitend plaatsvindt voor zover noodzakelijk is op grond van het bepaalde in de eerste twee leden van dit artikel. Door rechtstreekse toegang tot BVH te verschaffen aan leden van het OM ontbreekt ook de controle op bovenstaande punten.

Aangaande deze rechtstreekse verstrekking van politiegegevens heeft men een convenant opgesteld met de bedoeling bovenstaande punten af te dekken.

- Echter, door rechtstreekse toegang tot het systeem ontbreekt – ondanks het contractueel af dichten – de controle *vooraf*. Alleen controle *achteraf* is hierdoor nog mogelijk.
- Bovendien is er door de privacyfunctionaris geconstateerd dat logging – een van de maatregelen in het opgestelde document – als instrument nauwelijks is ontwikkeld, zodat controle op de correcte toepassing van toegekende autorisaties niet goed mogelijk is.

Vestrekkingsschema regio

Politiegegevens kunnen verstrekt worden aan anderen dan de politie en de Koninklijke Marechaussee. Bepaalde verstrekkingen mogen rechtstreeks worden gedaan. Alle verstrekkingen moeten, ongeacht of deze rechtstreeks worden gedaan, schriftelijk worden vastgelegd.

Ten behoeve van handhaving van de openbare orde vindt veelvuldig contact met de burgemeester plaats. De afstemmingen vinden veelal informeel plaats. Het korps overweegt om incidentele verstrekking van artikel 8 Wpg gegevens door de infocoördinator te laten verzorgen (protocolleren per mutatie) en de overige verstrekkingen via de Infodesk (met procedure).

Wanneer in samenwerkingsverbanden (keten) informatie moet worden verstrekt dan wordt de privacyfunctionaris gevraagd of de informatie wel of niet mag worden verstrekt. De privacyfunctionaris gaat dan na of er met de vragende partij een convenant is afgesloten.

Verstrekken RID

Wanneer informatie wordt verstrekt aan het unithoofd van het betreffende gebied, dan verloopt de verstrekking via een verstrekkingrapport op papier.

- Wanneer het informatie betreft buiten de regio, dan verloopt het via de afdeling RID van het betreffende korps, middels hetzelfde verstrekkingrapport. Volgens de Coördinator Regionale Inlichtingen is informatie nog nooit door middel van een proces-verbaal verstrekt. Volgens de coördinator is de hele afdeling in staat om informatie verstrekken, het unithoofd moet hier echter altijd voor tekenen. In het systeem BVO is zichtbaar aan wie de informatie verstrekt zou moeten worden (in bijzonderheden regel).
- Tussen de burgemeester en de korpschef is regelmatig contact, echter wanneer de burgemeester informatie wenst over bepaalde gebieden verloopt dit nog niet volgens een informatiebehoefteplan. Het is voor de informatierechercheurs niet altijd duidelijk in welke richting zij moeten gaan runnen.

In Excel wordt er een nummerlijst van verstrekkingrapporten bijgehouden.

Verstrekken CIE

De CIE-rechercheur controleert de status van de informant ingeval het een verstrekking betreft die niet direct na het registreren van de informatie van de informant plaatsvindt. De CIE-rechercheur overlegt met de CIE-chef over een eventuele verstrekking van het proces-verbaal.

De CIE OvJ is bij elke verstrekking betrokken. Het uitgangspunt is overleg. Dat komt niet zo zeer vanuit de Wpg, maar eerder vanuit de CIE-regeling. De OvJ is zeer nadrukkelijk aanwezig wat betreft bevoegdheden en controle.

De CIE-chef overlegt met de CIE-OvJ in geval van:

- Verstrekking PV aan de AIVD.

- Verstrekking PV buitenland.

De CIE-chef tekent voor verstrekking het betreffende proces-verbaal. De administratief medewerker CIE registreert wanneer en aan wie het proces-verbaal is verstrekt. De administratief medewerker maakt een "Resultaat meldingformulier" en archiveert een kopie van het proces-verbaal.

Vervolgens wordt het betreffende proces-verbaal verstrekt. Een verstrekking vindt plaats:

- Op eigen initiatief van de CIE.
- Op verzoek van een externe CIE, naar aanleiding van een eerder verstrekte ZIR.
- Op verzoek van een teamleider van een opsporingsonderzoek.

De CIE-chef draagt ervoor zorg dat de NCIE in kennis wordt gesteld van de verstrekking van een proces-verbaal Buitenland. In het geval van een meervoudige verstrekking van een proces-verbaal, zorgt de CIE-chef dat alle afnemers in kennis worden gesteld van het feit dat er meervoudige verstrekking heeft plaatsgevonden.

De CIE-rechercheur monitort wat met het procesverbaal wordt gedaan. Indien het procesverbaal niet wordt gebruikt, dan dient de afnemer die te retourneren. De CIE-rechercheur monitort het "Resultaat meldingsformulier". Dit formulier is van belang bij een eventuele aanvraag voor tip- of toongeld.

De administratief medewerker CIE controleert regelmatig het uitstaande "Resultaat meldingsformulier".

RI Processtappen

De functionaris RI verzamelt gevraagd en ongevraagd (heimelijk) informatie. De functionaris RI verstrekt en stelt de informatie gevraagd en ongevraagd ter beschikking aan het gezag, aan andere inlichtingendiensten, c.q. aan diensten of afdelingen binnen de eigen organisatie. Verstrekking van persoonsgegevens aan derden (instanties, personen en bestuursorganen) kan alleen op verzoek van bevoegde/aangewezen instanties.

Protocollering verstrekkingen

De protocolplicht alsmede de uitvoering daarvan wordt opgenomen in alle werkprocessen waarbij politiegegevens verstrekt worden. Voor verstrekkingen uit BVH en het vastleggen daarvan moet een verstrekkingprocedure in de applicatie zelf worden gevolgd.

De verstrekkingen van informatie worden in een proces-verbaal in BVH geregistreerd. Uit de interviews is gebleken dat het 'Blauw' wel bewust is van de vereisten van de Wpg. De Infodesk protocollert in Outlook, BVH of via de BVO Infodesk module.

Voor verstrekkingen uit BVO is de bevoegde functionaris verantwoordelijk. Er is een schriftelijke aanwijzing aan de bevoegde functionarissen uitgereikt waarin de (praktische) uitvoering van de protocolplicht ten aanzien van deze verstrekkingen wordt aangereikt.

De verstrekkingen vinden plaats via zowel convenanten als conform de wet. Men wordt zich steeds bewuster dat men er anders mee moet omgaan. De wijkagent krijgt en verstrekt dermate veel informatie dat niet alles wordt vastgelegd. Voor dergelijke situaties hanteert het korps vastlegging via een samengesteld mutatieverslag van de hele dag.

De privacyfunctionaris controleert steekproefsgewijs of zijn medewerkers de vastleggingen in BVH op een adequate wijze verrichten. De privacyfunctionaris constateert in zijn jaarverslag dat er een positieve kentering zichtbaar is en het aantal vastleggingen steeds groter wordt.

Procedure voor het vastleggen van incidentele en structurele verstrekkingen

- De registraties worden gemaakt gebruikmakende van de I90 in BVH.
- Als sprake is van een incidentele verstrekking met toestemming van de OvJ (strafrechtelijk) of burgemeester (openbare orde), dan wordt als referentie 'WPG ART19' vermeld.
- Als de verstrekking plaatsvindt op basis van een structureel uitwisselingsbesluit (convenant), dan wordt vermeld bij de referentie artikel 20 en de naam van het convenant.

Bewaren protocollering

Zowel de Infodesk als alle overige medewerkers die verstrekkingen (kunnen) doen binnen het korps leggen de verstrekkingen vast in BVH of BVO, hier is ook nadrukkelijk binnen het korps bekendheid aan gegeven.

Conform wettelijke eisen dienen de vastleggingen bewaard te worden tot een volgende audit en eventuele heraudit heeft plaatsgevonden. De hiervoor gestelde termijn bij Zaanstreek-Waterland is vijf jaar.

4.9.3 *Verbeterpunten*

- Een aandachtspunt voor het korps is om het structureel gebruik van de I90-formulieren in alle korpsonderdelen verder te stimuleren.

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*

Verzoek om kennisneming en correctie

De kennisnemingsverzoeken worden door de privacyfunctionaris en diens administratief medewerker in behandeling genomen. De verzoeken worden ingeschreven in postsysteem Corsa, welke een rappel functie heeft. Daarnaast houdt de administratief medewerker een eigen protocol bij van verzoeken. In de praktijk worden nagenoeg alle verzoeken binnen zes weken afgehandeld.

Indien een verzoek niet wordt ingewilligd worden de redenen hiervoor bijgehouden in een overzicht welke door de privacyfunctionaris wordt bijgehouden.

De privacyfunctionaris geeft aan *het proces* niet op papier te hebben uitgeschreven daar de wet hierin duidelijk genoeg is.

Aantallen

In 2010 zijn er 413 verzoeken (van externen) om informatie geweest. In 2011 ligt het aantal tot en met 12 december 2011 op 582 verzoeken. Over 2010 waren er 32 daadwerkelijke inzageverzoeken, waarvan er 20 zijn gehonoreerd na overleg met de verzoeker(s).

Klachten

Er zijn de afgelopen jaren twee klachten geregistreerd bij Zaanstreek-Waterland, welke beide door de Nationale Ombudsman zijn behandeld. In één geval ging het om niet tijdig verwijderen van gegevens, welke is gehonoreerd. In het andere geval betrof het een klacht dat de betrokkene *zelf* niet de over hem opgeslagen informatie mocht lezen. Deze klacht is niet gehonoreerd, omdat artikel 25 het recht op *kennisneming* vastlegt en geen recht op inzage.

De correctieverzoeken worden tevens door de privacyfunctionaris in behandeling genomen conform de Wpg.

4.11 Protocolplicht (artikel 32)

4.11.1 Norm

De verantwoordelijke draagt zorg voor de schriftelijke vastlegging van:

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

Protocollering doel onderzoek

Voor het aanmaken van onderzoeken geldt het volgende proces:

- In BVO is een onderdeel voor het aanmaken van onderzoeken. De start van een onderzoek verloopt grotendeels via de meldkamer (het gemeenschappelijk meldkamersysteem), naar BVH en vervolgens BVO.
- Indien wordt besloten door de recherche dat een onderzoek wordt gestart, dan wordt een formulier ingevuld. Via vtsPN komt er via Intranet een melding bij de functioneel beheerder.
- Op basis van de melding wordt een registratie voor een onderzoek (MRO) aangemaakt in BVO. In beginsel moet elk onderzoek binnen vijf dagen na de start worden aangemeld. Als in BVO een mutatie wordt aangemaakt, dan moet er een MRO (melding recherche onderzoek) worden opgesteld. De melding wordt in het landelijke VROS systeem verwerkt (staat bij KLPD). De KLPD onderzoekt of er matches zijn in het land. Het doel van het onderzoek conform artikel 9 maakt geen onderdeel uit van de MRO.
- Een afschrift van het geopende onderzoek gaat naar de privacyfunctionaris. In een BVO-registratie, een soort digitale kaartenbak, kan informatie worden opgeslagen door de bevoegd functionaris en zijn medewerkers.

Kleine onderzoeken worden niet altijd gemeld, hoewel dat wettelijk gezien wél moet. Voor de grotere onderzoeken geldt dat zij standaard worden gemeld. Een registratie in BVO is noodzakelijk om bijvoorbeeld tapgesprekken te importeren, uit te werken

of te vertalen. Over de omvang van niet gemelde onderzoeken is geen kennis aanwezig.

Uit de interviews is gebleken dat de mate waarin protocollering plaatsvindt een stijgende lijn vertoont, maar de zorgvuldigheid nog aandacht vergt. Het is nu niet mogelijk alle zoekslagen vast te leggen, aangezien de systemen dit niet ondersteunen. De privacyfunctionaris kan dit nu niet controleren.

In de praktijk blijkt dat bij het protocolleren van artikel 9 verwerkingen in BVO regelmatig een wel héél korte doelomschrijving is gebruikt. Dit feit is geconstateerd door de privacyfunctionaris. Dergelijke omschrijvingen zijn te summier en voldoen daarom niet aan de wettelijke eisen.

Bewaren protocolgegevens doel onderzoek

De privacyfunctionaris houdt een overzicht bij van alle (aangemelde) lopende verwerkingen (en de doelen daartoe) die worden geopend voor artikel 9. De applicatie VROS kent een eigen schoningsregime.

Procollering artikel 13 gegevensverzamelingen

Het korps Zaanstreek-Waterland heeft een inventarisatie verricht met betrekking tot artikel 13 gegevensverzamelingen. Uit de documentatie blijkt dat voor een aantal specifieke diensten, per sub-proces is aangegeven of het een artikel 13 gegevensverzameling betreft. Voorbeelden hiervan zijn:

- Beheren en autoriseren met betrekking tot vreemdelingen.
- Werkproces kort verblijfregistratie.
- De hardcopy processen-verbaal aangehouden door ADO.

De documentatie bevat een beschrijving van het specifieke doel van de verwerking (artikel 13.4.a), de categorieën van personen en de soorten van gegevens (artikel 13.4.b). Per werkproces is aangegeven of (aanvullende) protocollering verplicht is en zijn bewaartermijnen vastgesteld. De documenten bevatten verwijzingen naar artikel 13 en 32 van de Wpg.

Er zijn zeven artikel 13 protocollen opgesteld en getekend door de gemandateerde korpschef. Dit zijn de landelijk uniform opgestelde reglementen. In 2012 worden de overige reglementen aangeleverd en eveneens vastgesteld.

Bewaren protocollering artikel 13 gegevensverzamelingen

Per werkproces is aangegeven of (aanvullende) protocollering verplicht is en zijn bewaartermijnen vastgelegd. De documenten bevatten verwijzingen naar artikel 13 en 32 van de Wpg.

De bewaartermijnen zijn per 1 november 2011 vastgesteld en nog niet middels een steekproef gecontroleerd.

Procollering onrechtmatige handelingen

De verwerkingen ten aanzien waarvan aanwijzingen bestaan dat zij door onbevoegden of anderszins onrechtmatig zijn verricht, moeten worden vastgelegd. Als voorbeeld voor onrechtmatige handelingen wordt gesteld: politiegegevens die worden verwerkt door personen die daartoe niet geautoriseerd zijn.

Uit de documentatie blijkt dat voor de verschillende gebruikte applicaties tevens verantwoordelijken zijn aangewezen. Deze zijn verantwoordelijk voor correcte autorisatie en melding van vermoedelijke onrechtmatige handelingen aan de privacyfunctionaris.

De privacyfunctionaris registreert de aangedragen of bekend geworden onrechtmatige verwerkingen. De protocollering van de onrechtmatige handelingen wordt opgeslagen in een specifiek daarvoor bestemde map binnen de kantoorautomatiseringsomgeving.

Bewaren protocolgegevens onrechtmatige handelingen

Er zijn geen onrechtmatige verwerkingen door de privacyfunctionaris geconstateerd. De privacyfunctionaris houdt indien van toepassing hiervan een overzicht bij, zo blijkt uit het overzicht van de privacyfunctionaris in het jaarverslag.

Gemeenschappelijke verwerking

In het dossier beheersmaatregelen is een schriftelijke aanwijzing opgenomen en aan de bevoegd functionarissen uitgereikt. Deze geeft aanwijzingen voor de (praktische) uitvoering van de protocollering ten aanzien van gemeenschappelijke verwerkingen.

De bevoegde functionaris is verantwoordelijk voor het inlichten van het CBP en de privacyfunctionaris. Er zijn overigens geen gemeenschappelijke verwerkingen geconstateerd.

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

De interne Wpg audit-functie is niet structureel belegd. De coördinator integrale kwaliteitszorg is onderdeel van het kabinet korpsleiding (KKL), de stafafdeling van het korps. Als korpsauditor (INK audits) ondersteunt hij vanaf 1999 de beleidsvoering van het korps bij de uitvoering van audits op de processen. Daarnaast voert hij interne audits uit voor het gehele korps. Voor de uitvoering van Wpg audits steunt hij op externe expertise.

Uit het jaarverslag privacy 2009 blijkt dat in 2009 de privacyfunctionaris de auditor-opleiding heeft gevolgd. Het korps is zich bewust van de wettelijke noodzaak tot het verrichten van interne audits. In 2009 was nog geen interne auditor benoemd.

Het besluit tot het aanwijzen van een interne auditor is nog niet geformaliseerd en deze persoon heeft bovendien ook (nog) geen auditor-opleiding genoten.

Interne audit plan

Er zijn Wpg-checklijsten voor de korpsleiding, unithoofden en (wijk)teamchefs. Tevens heeft de privacyfunctionaris een zogenaamde toezichtkalender ontwikkeld. Naar aanleiding van die toezichtkalender rapporteert de privacyfunctionaris aan de stuurgroep en de diensthoofden. Een formeel audit-plan is echter niet aanwezig.

Interne audit rapport

Er is (nog) geen intern auditrapport. Wel is er een student Management Economie en Recht ingezet om in een periode van zes maanden te onderzoeken in welke mate

Overzicht protocollering

Formeel mag de privacyfunctionaris in zijn hoedanigheid als toezichthouder inzage verkrijgen in de systemen voor controle op compliance aan de Wpg, ook artikel 12 informatie. Bezien vanuit de vertrouwelijke aard van de informatie bekijkt de privacyfunctionaris niet de informatie van CIE en RID, zonder aanwezigheid van de desbetreffende chef CIE of chef RID.

De privacyfunctionaris van Zaanstreek-Waterland is over het algemeen op de hoogte waar wordt geprotocolleerd en heeft de mogelijkheid protocolgegevens op te vragen en in te zien. De privacyfunctionaris heeft bovendien toegang tot de systemen voor controle op Wpg-compliance. Enkele cijfers uit het jaarverslag van 2010 met betrekking tot de protocollering:

- De vraagstellingen van artikel 11-zoekacties (vergelijkingen en combinatie zoekslagen) worden wel vastgelegd in de BVO-Infodeskmodule. De privacyfunctionaris heeft weliswaar geen zelfstandige toegang, doch indien noodzakelijk wordt hem door de Infodesk of functioneel beheerder inzage verleend.
- Gebleken is dat politiemedewerkers die frequent politiegegevens buiten het politiedomein verstrekken, deze verstrekkingen niet of onvoldoende schriftelijk vastleggen op de voorgeschreven manier in de BVH. In 2010 zijn er 275 verstrekkingen in BVH vastgelegd.
- De bevoegde functionarissen melden de doelen van onderzoeken conform de wettelijke bepalingen. In 2010 werden 154 van dit soort meldingen gedaan en 95 verwerkingen zijn in 2010 afgemeld.

Jaarverslag

De privacyfunctionaris heeft een jaarverslag privacy 2008, 2009 en 2010 opgesteld. De privacyfunctionaris rapporteert bovendien regelmatig aan de stuurgroep. De verslagen van de stuurgroep zijn opgenomen in het dossier beheermaatregelen.

Uit de gehouden interviews blijkt dat men bij vragen over de Wpg de weg naar de privacyfunctionaris weet te vinden.

4.14 Functionaris Gegevensbescherming (artikel 36)

De functionaris gegevensbescherming bestaat niet als functie bij het korps Zaanstreek Waterland.

het korps Zaanstreek-Waterland voldoet aan de eisen van de Wpg. Dit gebeurt middels interviews en is tevens zijn afstudeeropdracht.

4.12.3

Verbeterpunten

- Zorg voor een structurele borging van de interne auditfunctie. Borg hierbij ook de vaktechnische kennis, bijvoorbeeld door het aanbieden van een interne audit opleiding.
- Beleg structureel de auditfunctie ten aanzien van de Wpg.
- Richt een vaktechnisch verantwoorde en meerjarig gerichte auditplanning in.

4.13 Privacy functionaris (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 invulling privacyfunctionaris

De privacyfunctionaris is benoemd. Hij vervult deze rol naast het takenpakket vanuit het oogpunt van informatiebeveiliging.

De implementatie van de Wpg is in het korps Zaanstreek-Waterland in 2009 echt op gang gekomen. De privacyfunctionaris geeft invulling aan diverse rollen. In het begin lag de focus veelal op implementatie door voorlichting over de Wpg in het korps en door het ondersteunen van de projectleider met werkdocumenten. Nu ligt het accent meer op de toezichtsrol en op advisering van het korps en de korpsleiding.

Toezichthouder

Inmiddels is een toezichtkalender gemaakt. Memo's worden aan de stuurgroep voorgelegd. De stuurgroep staat onder leiding van een lid van het Management Team en verder nemen bijna alle leden van het MT (inclusief de plaatsvervangende korpschef) daaraan deel. De memo's gaan ook naar diensthoofden toe, zodat zij weten wat er op de werkvloer leeft.

Uit hoofde van de rol als toezichthouder prikt de privacyfunctionaris af en toe in BVH, loopt bij de Infodesk binnen om waar te nemen hoe het met de Wpg gaat en verneemt of er nog praktische knelpunten zijn.

De privacyfunctionaris geeft advies over de hele breedte van het korps, van de korpschef tot aan de agent op straat. Ook geeft de privacyfunctionaris ongevraagd advies. Alle werkprocessen zijn beschreven, waarbij een 'vertaling' is gemaakt van de Wpg en de juridische uitgangspunten naar de praktische invulling.

Uit het functieprofiel blijkt dat de taken vanuit de Wpg zijn geadresseerd.