



Ministerie van Veiligheid en Justitie

Audit Wpg politie Rotterdam-Rijnmond Rapport

Datum
Status

16 december 2011
Definitief

Colofon

Afzendgegevens

Departementale Auditdienst

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

Contactpersonen

drs. [REDACTED] RE CISA
drs. ing. [REDACTED] RO CIA
Senior auditors

T 070 370 65 60

Projectnaam

Audit Wet Politiegegevens

Ons kenmerk

DDS 5719717/11

Auteurs

[REDACTED] RE RA

Inhoud

Colofon - 3

1 Assurance verklaring - 7

2 Samenvatting - 9

3 Inleiding - 17

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

4 Bevindingen - 21

- 4.1 Inleiding - 21
 - 4.1.1 Regie en doorzettingsmacht voor de Wpg implementatie - 21
 - 4.1.2 Bekendheid met de Wpg binnen de organisatie - 21
 - 4.1.3 Wpg en de praktijk - 22
- 4.2 Verantwoordelijke (artikel 1.f) - 22
- 4.3 Kwaliteitsaspecten van politiegegevens (artikel 3 en 4) - 23
 - 4.3.1 Norm - 23
 - 4.3.2 Bevindingen - 23
- 4.4 Gevoelige gegevens (artikel 5) - 25
 - 4.4.1 Norm - 25
 - 4.4.2 Bevindingen - 26
- 4.5 Autorisatie (artikel 6) - 26
 - 4.5.1 Norm - 26
 - 4.5.2 Bevindingen - 26
- 4.6 Geautomatiseerd Vergelijken (GV)/In Combinatie Met Elkaar Verwerken (ICMEV)(artikel 11) - 28
 - 4.6.1 Norm - 28
 - 4.6.2 Bevindingen - 28
- 4.7 Bewaartermijnen (artikel 14) - 28
 - 4.7.1 Norm - 28
 - 4.7.2 Bevindingen - 29
- 4.8 Ter beschikking stellen (artikel 15) - 31
 - 4.8.1 Norm - 31
 - 4.8.2 Bevindingen - 31
- 4.9 Voor de impact van artikel 15 Wpg zijn een aantal maatregelen getroffen bij Politie Rotterdam-Rijnmond Verstrekken (artikel 16/24) - 32
 - 4.9.1 Norm - 32
 - 4.9.2 Bevindingen - 32
- 4.10 Rechten van betrokkenen (artikel 25/28) - 34
 - 4.10.1 Norm - 34
 - 4.10.2 Bevindingen - 34
- 4.11 Protocolplicht (artikel 32) - 35
 - 4.11.1 Norm - 35
 - 4.11.2 Bevindingen - 35

- 4.12 Audits (artikel 33) - 36
- 4.12.1 Norm - 36
- 4.12.2 Bevindingen - 36
- 4.13 Privacyfunctionaris (artikel 34) - 37
- 4.13.1 Norm - 37
- 4.13.2 Bevindingen - 37
- 4.14 Functionaris Gegevensbescherming (artikel 36) - 38

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 november 2011 is een privacy audit uitgevoerd bij het korps Rotterdam-Rijnmond.

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 Rotterdam-Rijnmond.

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

Den Haag, d.d. 16 december 2011

De Directeur van de Departementale Auditdienst

A large, stylized handwritten signature in blue ink, consisting of several loops and a long horizontal stroke at the bottom.

J.C. van Praat RE RA

2 Samenvatting

Het korps Rotterdam-Rijnmond heeft een aantal zaken in opzet goed opgepakt, zoals het werken met een autorisatiematrix en het inrichten van een bureau voor het centraal beheren van de convenanten. De korpsleiding toont hiermee en met andere initiërende activiteiten haar aandacht voor de Wpg.

Het korps Rotterdam-Rijnmond is bezig met de operationalisering en borging op de werkvloer, onder andere door het inrichten van interne controle binnen de processen, om aantoonbaar te maken dat ook de werking volledig voldoet aan de Wpg.

In 2011 is een Wpg pre-scan en een gedegen interne audit conform de NOREA-richtlijnen uitgevoerd. Op basis van de rapportage over de pre-scan zijn actiepunten opgedragen aan de proceseigenaren, diensthoofden en districtchefs, en wordt een verbeterprogramma doorlopen voor de implementatie van de Wpg vanaf strategisch management tot aan de werkvloer. De afronding van de actiepunten wordt centraal bewaakt en verloopt conform planning.

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	Kleur	Bevinding en oordeel
Artikel 1.f, Verantwoordelijke			
1.f	Mandaatbesluit		Er is een mandaatbesluit waarin wordt aangetoond dat het bevoegd gezag (korpsbeheerder) zijn mandaat geeft aan de Korpschef. Hiermee wordt voldaan aan de Wpg.
Artikel 3 en 4, Kwaliteitsaspecten van politiegegevens			
8.1 en 9.1	Onderscheid onderzoek Dagelijkse Politietaken (8) versus Bepaald geval (9)		Er is een instructie voor Opsporing en Dienst Regionale Informatie Organisatie (RIO) met het onderscheid tussen artikel 8 en 9 Wpg onderzoeken. Deze is gecommuniceerd aan de bevoegde functionarissen. Hiermee wordt voldaan aan de Wpg.
3.1 t/m 3.3 (8) 4.1 (8)	Noodzakelijkheid (8) Doelbinding Rechtmatigheid Juistheid Volledigheid		Er zijn vuistregels voor Blauw en een werkinstructie. Een aantal Teach-The-Teacher (TTT) sessies heeft plaatsgevonden voor chefs van de Wijkpolitie, de Directe Hulpverlening (DHV) en de Executieve Ondersteuning (EXO), en een vervolg TTT-sessie is voorbereid. De chefs instrueren de medewerkers en koppelen hun voortgang terug aan de hoofden van de DHV, de EXO en de Wijkpolitie.

Norm	Aspect	Kleur	Bevinding en oordeel
			De RIO Gegevensbeheer controleert de Basisvoorziening Handhaving (BVH) met TrueBlue. Binnen RIO worden interne controles uitgevoerd bij de infodesks en gerapporteerd aan het diensthoofd. 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 criteria. De Plan-Do-Check-Act-cyclus sluit via het Openbaar Ministerie en de rechter. Binnen het korps zijn voor artikel 9 werkafspraken vastgelegd waarin de kwaliteitsaspecten naar voren komen. Hiermee wordt voldaan aan de Wpg.
13.4 (10 en 12) 4.1 (10 en 12)	Noodzakelijkheid (10 en 12) Doelbinding Rechtmatigheid Herkomst en wijze van verkrijging Juistheid Nauwkeurig Volledigheid		Bij de Criminele Inlichtingen Eenheid (CIE) en de Regionale Inlichtingen Dienst (RID) zijn de kwaliteitscriteria in verband met de aard van het werk goed ingeregeld. Bij de CIE gebeurt dit volgens het [REDACTED] CIE en de toezichthoudende rol van de CIE-officier van justitie (CIE-OvJ). De CIE-OvJ voert elk halfjaar een zogenaamde registercontrole/audit uit bij de CIE. Bij de RID liggen de kwaliteitscriteria al in het doel van de taak vast. Hiermee wordt voldaan aan de Wpg.
4.3	Beveiliging		Modelleren van Wpg, in kaart brengen van werkprocessen in relatie tot systemen, autorisatiebeheer etc. zijn opgepakt en uitgevoerd of in acceptabele plannen uitgewerkt. Dienst Regionale Informatievoorziening (DRI) heeft de Wpg-aspecten van de regionale informatiesystemen in kaart gebracht en Wpg-manco's vastgesteld. Alle manco's zijn echter nog niet in overleg met de proceseigenaren verwerkt in actieplannen. Daarnaast zijn nog niet alle landelijke systemen Wpg-proof. Hiermee wordt niet voldaan aan de Wpg.
Art. 5, Gevoelige Gegevens			
	• Gevoelige gegevens		Tijdens de interne audit zijn geen niet-toegestane gegevensverzamelingen gebaseerd op gevoelige gegevens aangetroffen binnen het korps. Het korps heeft in werkinstructies, in TTT-sessies en in de vuistregels voor Blauw aandacht voor het omgaan met gevoelige gegevens. Hiermee wordt voldaan aan de Wpg.
Artikel 6, Autorisatie			
	• Korpsautorisatiematrix		De korpsautorisatiematrix is opgesteld samen met de DRI, Personeel & Organisatie (P&O), de proceseigenaren en de diensthoofden. De korpsautorisatiematrix is in het overleg Korpsleiding vastgesteld. Hiermee wordt voldaan aan de Wpg.

~~XXXXXXXXXXXXXXXXXXXX~~

Norm	Aspect	Kleur	Bevinding en oordeel
	• Aanvraagproces		Er is een procedure voor het aanvragen van autorisaties. Het aanvraagproces verloopt via P&O, chefs, security officers, DRI, Verzorgingsgebied Zuid West (VG ZW) en voorziening tot samenwerking Politie Nederland (vtsPN). Over het algemeen is de leidinggevende verantwoordelijk voor het aanvragen van autorisaties. Hiervoor is een speciaal formulier beschikbaar. Hiermee wordt voldaan aan de Wpg.
	• Wijziging en verwijdering		In de zomer van 2011 is een uitdraai gemaakt van alle autorisaties ter voorbereiding op een schoning. Uit het interne auditrapport is gebleken dat er sprake is van vervuiling (onder andere niet tijdige verwijdering). De wijzigingen zijn beoordeeld in de interne audit. Het proces is eenmalig doorlopen en daarmee nog niet geborgd. Er is een acceptabel plan voor een centralisatie van het wijzigings- en schoningproces. Ook de tijdige verwijdering is nog niet geheel geborgd. Er is een acceptabel plan voor centralisatie van het autorisatieproces. Hiermee wordt deels voldaan aan de Wpg.
	• Autorisatiebeheer CIE en RID		De CIE en de RID beheren zelf de autorisaties op de systemen. Hiermee wordt voldaan aan de Wpg.
32.1.c	Protocollering autorisaties		Alle mutaties op autorisaties worden vastgelegd. De privacyfunctionaris kan de autorisaties bij de verschillende beheerders opvragen in het kader van de toezichthoudende of controlerende taak. Hiermee wordt voldaan aan de Wpg.
32.3 voor 32.1.c	Bewaren protocolgegevens autorisaties		De vastlegging van mutaties op autorisaties wordt momenteel onbeperkt bewaard. Hiermee wordt voldaan aan de Wpg.
Artikel 11, Geautomatiseerd vergelijken en in combinatie zoeken			
	• Hanteerbare interpretatie		Op landelijk niveau ontbreekt er een definitie voor geautomatiseerd vergelijken in en in combinatie zoeken (GV en ICMEV). Binnen het korps is hieraan invulling gegeven door de vuistregel: "Artikel 11 Wpg is RIO". Hoe om te gaan met GV/ICMEV is vastgelegd in werkinstructies voor Opsporing en RIO. Hiermee wordt voldaan aan de Wpg.
	• Aangewezen functionarissen		De bevoegde functionarissen en infodesks zijn ingelicht over de vuistregel en hoe daarmee om te gaan. RIO voert hier interne controles op uit. Hiermee wordt voldaan aan de Wpg.
11.4	Bevoegd gezag		Het handboek Infodesk geeft aan dat in bijzondere gevallen gegevens in combinatie met elkaar kunnen worden verwerkt hiervoor is toestemming nodig van het bevoegd gezag (OM). Hiermee wordt voldaan aan de Wpg.

Norm	Aspect	Kleur	Bevinding en oordeel
32.1.d en 32.1 h	Protocollering 11.1, 11.2, 11.4 en 11.5		Opsporing en de infodesks leggen alle aanvragen inclusief de antwoorden voor artikel 11.1 en 11.2 Wpg vast. Tot op heden is binnen het korps nog geen sprake geweest van verwerking van artikel 11.4 Wpg gegevens. Hiermee wordt voldaan aan de Wpg.
32.3 voor 32.1.d en 32.1 h	Bewaren protocolgegevens 11.1, 11.2, 11.4 en 11.5		De vastlegging van aanvragen en antwoorden in het kader van artikel 11.1 en 11.2 Wpg wordt door Opsporing en de infodesks op dit moment onbeperkt bewaard. Tot op heden is binnen het korps nog geen sprake geweest van verwerking van artikel 11.4 Wpg gegevens. Hiermee wordt voldaan aan de Wpg.
Artikel 14, Bewaartermijnen			
8.2 en 8.3	(8) van 1 tot 5 jaar		De nieuwste versie van BVH 1.2.2 is operationeel binnen het korps. Er is een acceptabel actieplan voor het activeren van het mechanisme voor beperkt zoeken in de periode van 1 tot 5 jaar. Dit mechanisme is echter nog niet geactiveerd. Hiermee wordt deels voldaan aan de Wpg.
8.6	(8) verwijderen na 5 jaar		De nieuwste versie van BVH 1.2.2 is operationeel binnen het korps. Er is een acceptabel actieplan voor het activeren van het mechanisme voor verwijdering. Dit mechanisme is echter nog niet geactiveerd. Hiermee wordt deels voldaan aan de Wpg.
14.1 (8)	(8) vernietigen na 5 jaar verwijderd		Er vindt nog geen verwijdering van informatie uit BVH plaats. Landelijk is geadviseerd het mechanisme voor vernietiging in BVH versie 1.2.2 niet te activeren. Het korps onderzoekt nog hoe dit mechanisme moet worden gebruikt en welke invloed het heeft op de werkprocessen. Hiermee wordt niet voldaan aan de Wpg.
9.4	(9) verwijderen na OH plus ½ jaar		Politiegegevens uit artikel 9 Wpg onderzoeken worden na afronden van het onderzoek toegankelijk gemaakt door de autorisaties op nul te zetten. Dit is vaak eerder dan het moment van het onherroepelijke vonnis. Deze werkwijze is verankerd in het werkproces. Hiermee wordt voldaan aan de Wpg. Echter bij artikel 14.1 en 14.3 Wpg treedt hiermee een complicatie op. (Zie hieronder.)
14.1 (9)	(9) vernietigen na 5 jaar verwijderd		Het korps en het OM hebben geen proces ingericht voor het afmelden (onherroepelijk vonnis) van artikel 9 Wpg onderzoeken. Hierdoor is het vernietigmoment niet eenduidig bepaald. Hiermee wordt niet voldaan aan de Wpg.
10.6	(10) verwijderen na 5 jaar geen subjectwaardige registratie		De CIE en de RID hanteren [REDACTED] procedures voor het verwijderen van politiegegevens zijn opgenomen. De CIE-officier van justitie voert halfjaarlijks een registercontrole/audit bij de CIE uit.

—

—

Norm	Aspect	Kleur	Bevinding en oordeel
			De RID staat deels onder toezicht van de AIVD. Uit het interne auditrapport is gebleken dat er geen afwijkingen zijn geconstateerd. Hiermee wordt voldaan aan de Wpg.
14.1 (10)	(10) vernietigen na 5 jaar verwijderd		De CIE en de RID hanteren [REDACTED] procedures voor het verwijderen van politiegegevens zijn opgenomen. De CIE-officier van justitie voert halfjaarlijks een registercontrole/audit bij de CIE uit. De RID staat deels onder toezicht van de AIVD. Uit het interne auditrapport is gebleken dat er geen afwijkingen zijn geconstateerd. Hiermee wordt voldaan aan de Wpg.
14.3	Hernieuwde verwerking		Artikel 8 Wpg gegevens worden nog niet verwijderd. Voor artikel 9 Wpg gegevens is het verwijdermoment nog niet eenduidig ingevoerd. Hierdoor kan nog worden gezocht in artikel 8 en 9 Wpg gegevens die niet meer toegankelijk hadden mogen zijn, zonder dat het bevoegd gezag daartoe toestemming heeft gegeven. Hiermee wordt niet voldaan aan de Wpg.
32.1.e	Protocollering 14.3		Aangezien verwijderen na 5 jaar nog niet eenduidig is ingevoerd, wordt artikel 14.3 Wpg niet nageleefd en vindt er ook geen protocollering plaats. Hiermee wordt niet voldaan aan de Wpg.
32.3 voor 32.1.e	Bewaren protocolgegevens 14.3		Aangezien verwijderen na 5 jaar nog niet eenduidig is ingevoerd, wordt artikel 14.3 niet nageleefd en vindt er ook geen protocollering plaats. Hiermee wordt niet voldaan aan de Wpg.
12.2	(12) verwijderen na 4 maanden		De CIE en de RID hanteren [REDACTED] en [REDACTED] procedures voor het verwijderen van politiegegevens zijn opgenomen. De CIE-officier van justitie voert halfjaarlijks een registercontrole/audit bij de CIE uit. De RID staat deels onder toezicht van de AIVD. Uit het interne auditrapport blijkt dat er geen afwijkingen zijn geconstateerd. Hiermee wordt voldaan aan de Wpg.
12.6	(12) controleren en vernietigen		De CIE en de RID hanteren landelijke [REDACTED] procedures voor het verwijderen van politiegegevens zijn opgenomen. De CIE-officier van justitie voert halfjaarlijks een registercontrole/audit bij de CIE uit. De RID staat deels onder toezicht van de AIVD. Er zijn geen afwijkingen geconstateerd. Hiermee wordt voldaan aan de Wpg.
Artikel 15, Ter beschikking stellen			
• Infodesk voor bevraging			Er is een protocol voor de infodesks over hoe om te gaan met aanvragen vanuit artikel 8 en 9. RIO voert interne controles uit op het volgen van dit protocol. Hiermee wordt voldaan aan de Wpg.
• Codering			Er is een beleid en een werkinstructie voor Opsporing over codering in BVH en Basisvoorziening Opsporing (BVO).

—

—

—

—

—

—

Norm	Aspect	Kleur	Bevinding en oordeel
			Deze zijn beide door de proceseigenaar Opsporing en het Diensthoofd RIO geaccordeerd. Dit onderwerp vormt een onderdeel van de training voor de bevoegde functionaris en de training van de medewerkers van de infodesks. Hiermee wordt voldaan aan de Wpg.
	• Aanwijzing Bevoegd Functionaris		De bevoegde functionarissen zijn aangewezen. Hiermee wordt voldaan aan de Wpg.
	• Opleiding Bevoegd Functionaris		In een aantal TTT-sessies zijn vrijwel alle bevoegde functionarissen getraind in de Wpg. Hiermee wordt voldaan aan de Wpg.
15.2	Weigeringgronden		In een aantal TTT-sessies zijn vrijwel alle bevoegde functionarissen getraind in de Wpg. Hiermee wordt voldaan aan de Wpg.
Artikel 16 t/m 24, Verstrekking			
	• Verstrekkingenwijzer (landelijk)		De verstrekkingenwijzer is gepubliceerd op intranet en wordt behandeld in de TTT-sessies voor chefs. Hiermee wordt voldaan aan de Wpg.
	• Proces voor convenanten		Dienst Beleid en Bestuurszaken (BBZ) heeft een convenantenloket ingericht. Dit loket heeft een model ontworpen voor convenanten, een werkinstructie opgesteld en de bestaande convenanten verzameld. Daarnaast is dit loket ook bezig met schoning en vernieuwing. De actuele conventanten zijn gepubliceerd op intranet. Hiermee wordt voldaan aan de Wpg.
	• Proces voor Artikel 20 Besluiten		Dienst BBZ heeft een model ontworpen voor artikel 20 Wpg besluiten. Hiervoor is een werkinstructie opgesteld en is het loket bezig met het opstellen en laten accorderen van de relevante artikel 20 Wpg besluiten. Dit is een doorlopend proces. Hiermee wordt voldaan aan de Wpg.
	• Verstrekkingenschema (regio)		Het korps heeft een eenduidig beleid hoe met verstrekkingen dient te worden omgegaan, welke functies hiervoor verantwoordelijk zijn en hoe met incidentele verstrekkingen om wordt gegaan. Het verstrekkingenschema is gepubliceerd op intranet. Hiermee wordt voldaan aan de Wpg.
	• Proces voor geautomatiseerde verstrekking		Alle scripts en mechanismen voor geautomatiseerde verstrekkingen zijn geïnventariseerd door de DRI en waar nodig geschoond. Voor het aanvragen van nieuwe geautomatiseerde verstrekkingen is door de DRI en de BBZ een proces ingericht. Hiermee wordt voldaan aan de Wpg.
7.2	Geheimhouding		Bij alle schriftelijke en geautomatiseerde verstrekkingen wordt aangegeven dat de informatieontvanger een geheimhoudingsplicht heeft. Voor mondelinge verstrekkingen gelden de vuistregels voor Blauw, waarin dit is opgenomen. Hiermee wordt voldaan aan de Wpg.
32.1.f	Protocollering verstrekking		Via de vuistregels voor Blauw is protocollering via een I90-formulier in BVH verplicht gesteld.

Norm	Aspect	Kleur	Bevinding en oordeel
			Bij de RIO wordt geprotocolleerd in Outlook of via de BVO Infodesk module. Bij Opsporing wordt geprotocolleerd in BVO of het journaal. Hiermee wordt voldaan aan de Wpg.
32.3 voor 32.1.f	Bewaren protocolgegevens verstrekking		Op dit moment worden alle vastleggingen voor protocollering van verstrekkingen onbeperkt bewaard. Hiermee wordt voldaan aan de Wpg.
• Toezicht door leidinggevend en op verstrekkingen en protocollering			Toezicht op verstrekkingen vormt onderdeel van de TTT-sessies voor chefs binnen het korps. Hiermee wordt voldaan aan de Wpg.
Artikel 25 t/m 31, Rechten van de betrokkene			
25.1	Verzoek om kennisgeving		In maart 2011 is het inzageproces gecentraliseerd en wordt ook centraal bewaakt, inclusief de afhandeling van klachten en bezwaarschriften. Hiermee wordt voldaan aan de Wpg.
28.1 t/m 28.3	Correctie		In maart 2011 is het correctieproces gecentraliseerd en wordt ook centraal bewaakt, inclusief de afhandeling van klachten en bezwaarschriften. Hiermee wordt voldaan aan de Wpg.
Artikel 32, Protocolplicht (32.1.c, d, e, f en h behandeld bij thema's)			
9.2 en 32.1.a	Protocollering doel onderzoek		Onderzoeken die worden vastgelegd in BVO worden via een Melding Recherche Onderzoek (MRO) gemeld in Verwijzingsindex Recherche Onderzoek en Subjecten (VROS). Voor artikel 9 Wpg onderzoeken die worden vastgelegd in BVH is in een procedure opgenomen dat ook een BVO omgeving wordt geopend, met een MRO koppeling naar VROS. Hiermee wordt voldaan aan de Wpg.
32.3 voor 32.1.a	Bewaren protocolgegevens doel onderzoek		VROS kent een eigen schoningsregime. Hiermee wordt voldaan aan de Wpg.
13.4 en 32.1.b	Protocollering artikel 13 gegevensverzameling en		Er is een volledig register voor artikel 13 Wpg gegevens. Voor een aantal protocollen zijn er landelijk modellen beschikbaar gesteld. Er ligt een actieplan om deze protocollen aan te passen aan de regionale situatie en om de nog ontbrekende protocollen op te stellen. Dit is geen vereiste vanuit de Wpg. Hiermee wordt voldaan aan de Wpg.
32.3 voor 32.1.b	Bewaren protocolgegevens artikel 13 gegevensverzameling en		Het artikel 13 register wordt onbeperkt bewaard en waar nodig geactualiseerd. Hiermee wordt voldaan aan de Wpg.
32.1.g	Protocollering onrechtmatige handeling		Onrechtmatig handelen wordt behandeld door Bureau Interne Zaken (BIZ). Hiermee wordt voldaan aan de Wpg.

Norm	Aspect	Kleur	Bevinding en oordeel
32.3 voor 32.1.g	Bewaren protocolgegevens onrechtmatige handeling		Onrechtmatig handelen wordt behandeld door Bureau Interne Zaken (BIZ). Hiermee wordt voldaan aan de Wpg.
32.2	Gemeenschappelijke verwerking		Er is geen gemeenschappelijke verwerkingen aangetroffen.
Artikel 33, Audits			
RPAP 3.1	Interne auditfunctie		De interne auditfunctie bestaat uit 1 fte. Hiermee wordt voldaan aan de Wpg.
RPAP 3.4	Interne auditplan		Het interne auditplan voor 2012 t/m 2014 is beschikbaar en voldoet aan de vaktechnische regels. Hiermee wordt voldaan aan de Wpg.
RPAP 3.6	Interne auditrapport		Er zijn interne auditrapporten beschikbaar en de resultaten zijn gebruikt voor het opstellen van actieplannen. Hiermee wordt voldaan aan de Wpg.
Artikel 34, Privacyfunctionaris			
34.1 en 34.4	Benoemd en gemeld		Er zijn twee privacyfunctionarissen formeel aangesteld en gemeld bij het CBP. In oktober 2011 is een derde privacyfunctionaris aangesteld, die momenteel wordt ingewerkt en zal worden aangemeld bij het CBP. Hiermee wordt voldaan aan de Wpg.
34.2	Overzicht over protocollering		De privacyfunctionarissen zijn op de hoogte waar wordt geprotocolleerd en hebben de mogelijkheid protocolgegevens op te vragen. Op dit moment wordt het opvragen nog uitgevoerd door de interne auditor, in samenspraak met een privacyfunctionaris. Hiermee wordt voldaan aan de Wpg.
34.3	Jaarverslag		De jaarverslagen 2009 en 2010 zijn beschikbaar en voorgelegd aan de korpsleiding. Hiermee wordt voldaan aan de Wpg.
Optioneel Artikel 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 Rotterdam-Rijnmond 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 Rotterdam-Rijnmond in de maand november 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

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 Rotterdam-Rijnmond.

De privacy audit leidt tot een assurance verklaring met een oordeel over de genoemde doelstelling en over de in dit rapport aangegeven thema's. Vanwege het feit dat het een review betreft hebben wij geen verbeterpunten in het rapport opgenomen.

De privacy audit richt zich op de opzet, het bestaan en indien van toepassing de werking, per ultimo november 2011, van maatregelen en procedures, waarmee het korps Rotterdam-Rijnmond 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 Rotterdam-Rijnmond. Dit betekent dat wij geen onderzoek hebben verricht naar door de vtsPN aan het korps Rotterdam-Rijnmond geleverde faciliteiten, voor zover de verantwoordelijkheid daarvoor is belegd bij de vtsPN of bij anderen dan het korps Rotterdam-Rijnmond.

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

In 2011 is een pre-scan en interne audit uitgevoerd. Uit de pre-scan zijn actiepunten geformuleerd en verbeterplannen opgesteld. Het korps is momenteel bezig met het oppakken van de verbeterpunten.

De interne audit is onder leiding van de interne auditor van het korps Rotterdam-Rijnmond uitgevoerd door IT Auditors van een extern bureau. Hierbij zijn de Code of Ethics en richtlijnen van de beroepsorganisatie, de Nederlandse Orde van Register IT Auditors (NOREA) gehanteerd.

Voor de privacy audit hebben wij de interne audit werkzaamheden gereviewd. Tijdens de review hebben wij gesproken met het interne auditteam en hebben deelwaarnemingen gedaan in de relevante documentatie. De werkzaamheden zijn uitgevoerd in november 2011. Vanwege het feit dat het een review betreft hebben wij geen verbeterpunten in het rapport opgenomen.

Het conceptrapport met bevindingen is op 13 december 2011 besproken met de korpschef van het korps Rotterdam-Rijnmond. Op 10 januari 2012 is het rapport in het driehoekoverleg besproken. 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. [REDACTED]
mr. [REDACTED] neemt namens DG Politie deel aan de stuurgroep.
drs. [REDACTED] neemt namens het KBB deel aan de stuurgroep.

De specifieke doelgroep waarvoor het rapport is bestemd bestaat uit:

- Onze opdrachtgever zoals bovengenoemd.
- De korpsbeheerder dhr. Ing. A. Aboutaleb.

[REDACTED]

[REDACTED]
[REDACTED]

- De korpschef drs. F. Paauw.
- De Hoofd Officier van Justitie dhr. Mr. F.K.G. Westerbeke.
- De privacyfunctionarissen dhr. Mr. [REDACTED] en dhr. [REDACTED]
- De voorzitter van het College Bescherming Persoonsgegevens.

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

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

— —



4 Bevindingen

4.1 Inleiding

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

4.1.1 Regie en doorzettingsmacht voor de Wpg implementatie

Het korps Rotterdam-Rijnmond heeft een aantal zaken in opzet goed opgepakt, zoals het werken met een autorisatiematrix en het inrichten van een bureau voor het centraal beheren van de convenanten. De korpsleiding toont hiermee en met andere initiërende activiteiten haar aandacht voor de Wpg.

Het korps Rotterdam-Rijnmond is bezig met de operationalisering en borging op de werkvloer, onder andere door het inrichten van interne controle binnen de processen, om aantoonbaar te maken dat ook de werking volledig voldoet aan de Wpg.

In 2011 is een Wpg pre-scan en een gedegen interne audit conform de NOREA-richtlijnen uitgevoerd. Op basis van de rapportage over de pre-scan zijn actiepunten opgedragen aan de proceseigenaren, diensthoofden en districtchefs, en wordt een verbeterprogramma doorlopen voor de implementatie van de Wpg vanaf strategisch management tot aan de werkvloer.

4.1.2 Bekendheid met de Wpg binnen de organisatie

Politie Rotterdam-Rijnmond heeft in 2008 tot en met 2010 een reeks opleidingen verzorgd voor beleidsmedewerkers en leidinggevenden. In 2011 zijn Teach The Teacher (TTT) opleidingen verzorgd voor vrijwel alle bevoegde functionarissen en de chefs van de Wijkpolitie, de Directe Hulp Verlening (DHV) en de Executieve Ondersteuning (EXO). Er zijn opleidingssessies geweest voor functioneel beheerders en voor medewerkers van de Dienst Regionale Informatie Organisatie (RIO).

De beleidsmedewerkers, de chefs, de functioneel beheerders en de RIO-medewerkers functioneren als vraagbaak voor de rest van het korps en dienen vanuit hun rol de Wpg uit te dragen.

Voor de medewerkers in Blauw zijn geplastificeerde kaarten gedrukt met de Wpg-vuistregels voor verwerken en verstrekken, welke door de chefs zijn toegelicht tijdens briefings en bijeenkomsten.

Vanuit elk district en elke relevante dienst is in 2009 een Chef Opsporing naar een vierdaagse Wpg-cursus gestuurd. Deze Chefs Opsporing hebben de opdracht meegekregen de door hen opgedane kennis binnen hun onderdeel verder uit te dragen. Deze kennisdeling is niet binnen elk onderdeel succesvol geweest, onder andere door personeelsverloop.

In 2011 is de opleiding uitgebreider opgepakt door een training verplicht te stellen voor alle bevoegde functionarissen. Hiermee is een dekking van vrijwel 100% behaald.

Rechercheurs zijn ingelicht over de Wpg door de centraal opgeleide bevoegde functionarissen, namelijk de Leiders Onderzoek en de Tactische Coördinatoren. Zij brengen hun Wpg-kennis in tijdens de uitvoering van de onderzoeken.

4.1.3 Wpg en de praktijk

Wpg-uitrol in 2008, 2009 en 2010

Bij het ontwerp van de Wpg heeft een van de leidinggevendenden van Rotterdam-Rijnmond geparticipeerd. Daarnaast waren beleidsmedewerkers van het korps betrokken bij het beoordelen van het ontwerp en het geven van feedback. Vanaf het ontwerpstadium is binnen het korps kennis opgebouwd over de Wpg en de interpretatie van deze wet. Deze kennis is van 2008 tot en met 2010 projectmatig overgedragen via cursussen, voorlichtingcampagnes, een quiz, posters etc. In die periode werd de Wpg echter nog niet goed begrepen en als een belemmering gezien voor de doelmatigheid van de politietak. De Wpg werd niet echt omarmd op de werkvloer. In 2011 is de Wpg gemodelleerd als een combinatie van de "I" van Informatie en de "O" van Organisatie, en via een aantal presentaties overgebracht aan de diverse doelgroepen. Dit heeft geleid tot een omslag in de attitude binnen het korps.

Pre-scan

Tezamen met de interne auditor heeft een extern bureau in de periode van januari tot mei 2011 een Wpg pre-scan uitgevoerd. Het rapport is op 31 mei 2011 overhandigd aan de korpsleiding en driehoek. Naar aanleiding van dit rapport zijn in juni 2011 in totaal 101 actiepunten uitgezet bij de Proceseigenaren, Diensthoofden en Districtchefs in de vorm van werkpakketten. De korpschef heeft een persoonlijke brief gestuurd aan deze leidinggevendenden en het belang van adequate actie onderstreept. Een team van consultants heeft de betrokkenen bezocht, voorlichting verzorgd, gerichte adviezen gegeven, alle opgeleverde stukken beoordeeld en waar nodig geadviseerd over verdere verbetering. Op het hoofdbureau is een medewerker aangesteld die de voortgang bewaakt en periodiek voortgangsrapporten over alle werkpakketten oplevert aan de korpsprojectleider, die op periodieke regionale bijeenkomsten met de betrokkenen vanuit de lijn worden besproken. Daarnaast hebben enkele IT-auditors van een extern bureau, in samenwerking met de interne auditor, gerichte reviews uitgevoerd. Deze hebben zich gericht op onder meer de RIO-afdelingen en 8 van de 10 afdelingen van EXO. Daarnaast is bij de Dienst Regionale Informatievoorziening (DRI) een technical audit uitgevoerd op de NAS-tool voor wat betreft autorisatiebeheer. De hieruit volgende bevindingen en adviezen zijn door de lijn opgepakt en verwerkt in actieplannen, waarvan de voortgang centraal wordt bewaakt.

4.2 Verantwoordelijke (artikel 1.f)

Mandaatbesluit

Net als onder de oude Wet Politie registers (Wpolr) is ook onder 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.

De korpsbeheerder Rotterdam-Rijnmond heeft via een mandaatbesluit aan de korpschef Rotterdam-Rijnmond het mandaat gegeven voor het implementeren van maatregelen om te voldoen aan de Wpg.

4.3 Kwaliteitsaspecten van politiegegevens (artikel 3 en 4)

4.3.1 Norm

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

4.3.2 Bevindingen

Kwaliteitsaspecten van Art. 8 politiegegevens

Het korps Rotterdam-Rijnmond staat op het standpunt dat kwaliteit al aandacht moet krijgen bij de bron, namelijk bij de registratie in de Meldkamer of door een medewerker in Blauw. Veel aspecten die in Art. 3 en 4 worden genoemd zijn al onderdeel van de reguliere opleiding en het gangbare werkproces. Niettemin zijn door het korps vuistregels ontwikkeld en een opleidingstraject met Teach The Teacher (TTT) sessies voor chefs ontworpen. Onder leiding van het Plaatsvervangend Diensthoofd Wijkpolitie is van juli tot en met september 2011 een werkgroep van ongeveer 12 personen periodiek bij elkaar geweest om de vuistregels, werkinstructies, TTT-sessies en voorlichtingsmateriaal te ontwikkelen. Daarbij zijn de consequenties van het niet volgen van de vuistregels onder de aandacht gebracht. Tijdens deze sessies is de top van het korps aanwezig geweest om het belang van de uitrol van de Wpg op de werkvloer te benadrukken.

Voor "Blauw" zijn naast de vuistregels ook een werkinstructie "Wpg voor Blauw" uitgereikt aan de chefs ter bespreking met hun medewerkers. Deze is beschikbaar gesteld via intranet en wordt geciteerd tijdens briefings en werkoverleggen.

Artikel 8 Wpg deling via de RIO en de infodesk

Medewerkers van de RIO zijn op basis van hun taken en verantwoordelijkheden opgeleid. Daarnaast hebben zij ter voorbereiding op de Wpg een aantal Wpg casussen behandeld. Medewerkers zullen in de toekomst verder worden opgeleid via twee e-learning modules.

Bij de infodesks vragen de chefs hun medewerkers aandacht te besteden aan de kwaliteit van de artikel 8 Wpg politiegegevens en zoveel mogelijk met de aanvragers van informatie mee te denken. Bij vragen vanuit artikel 8 of 9 Wpg wordt de opgevraagde informatie eerst door de medewerkers van de infodesk beoordeeld of deze noodzakelijk is ter beantwoording, of dat selectie of aanvulling nodig is. Hierbij wordt het gezond verstand gebruikt, en eventueel geëscaleerd naar een hoofdmedewerker of een chef. Indien er twijfels zijn over de kwaliteit, althans voor zover dat kan worden beoordeeld door een medewerker van een infodesk, wordt deze twijfel gemeld aan de aanvrager.

Artikel 8 Wpg gegevensbeheer

Bij de RIO is de afdeling Gegevensbeheer ingericht ter verdere borging van de kwaliteit van de artikel 8 Wpg politiegegevens. Deze afdeling is onder andere verantwoordelijk voor het controleren en beheren van alle politiegegevens welke in Basisvoorziening Handhaving (BVH), Basisvoorziening Opsporing (BVO), HerKenningsdienst Systeem (HKS), Amazone, Foto Confrontatie Module (FCM)

worden ingevoerd. Gegevensbeheer controleert zelfstandig, en in samenwerking met de RIO Real Time Intelligence Center (RTIC).

De RIO Gegevensbeheer gaat niet actief op zoek naar dubbele objecten, maar acteert reactief op binnenkomende signalen.

Kwaliteitsaspecten van artikel 9 Wpg politiegegevens

Vanuit de professie heeft een rechercheur aandacht voor de herkomst, de rechtmatigheid en de nauwkeurigheid van politiegegevens. Voor Opsporing is het belangrijk dat een zaak niet stukloopt op procedurefouten. De eisen uit artikel 3, 4 en 5 Wpg worden daarom streng in de gaten gehouden door de leider van een onderzoek. Voor artikel 9 Wpg zijn binnen het korps werkafspraken vastgelegd waarin de kwaliteitsaspecten zijn opgenomen.

Binnen de werkprocessen is sprake van een gesloten Plan-Do-Check-Act-cyclus. Het onderzoek leidt tot een procesdossier, dat wordt overhandigd aan het Openbaar Ministerie (OM). Tijdens de zitting wordt het procesdossier getoetst door de rechter. Indien deze constateert dat de kwaliteitsaspecten niet voldoen, zal deze de zaak afwijzen. Het OM koppelt dit terug naar Opsporing, waarop de interne werkprocessen worden verbeterd.

Kwaliteitsaspecten van artikel 10 en 12 Wpg politiegegevens

Gezien de bijzondere aard van de taakstelling van de Criminele Inlichtingen Eenheid (CIE) mogen zij brede gegevensverzamelingen aanhouden. In de Wpg vallen deze verwerkingen onder artikel 10 Wpg. Deze gegevensverzamelingen kunnen een grote impact hebben op de privacy. Daarom wordt binnen de CIE strikt een landelijk handboek gevolgd waarin staat beschreven hoe de CIE dient om te gaan met de gegevensverzamelingen. Zo beschrijft het handboek onder welke voorwaarde gegevens mogen worden vastgelegd (doelbinding) en hoe men de bronvermelding dient te registreren (herkomst). Binnen de CIE heeft het OM (met name de CIE OvJ) een toezichthoudende rol. Dit toezicht zorgt voor de borging van de naleving van het handboek.

De Regionale Inlichtingen Dienst (RID) verwerkt en verstrekt politiegegevens binnen drie regimes voor de informatiestromen, namelijk:

- Politiegegevens voor de inlichtingendienst AIVD onder artikel 24 Wpg;
- Politiegegevens voor het handhaven van de openbare orde onder artikel 10 Wpg;
- Informatie over informanten onder artikel 12 Wpg.

De RID verstrekt rechtstreeks politiegegevens aan de AIVD volgens artikel 24 Wpg. De aanvragen vanuit de AIVD en de beantwoordingen zijn geprotocolleerd. Door deze strikte protocollering is de doelbinding geborgd.

De werkzaamheden voor de openbare orde volgens artikel 10 Wpg richten zich op een aantal interessegebieden, zoals voetbal, hooligans, milieuactivisme, stakingen etc. De gemeente wil voorbereid zijn op een evenement, tijdig voldoende dranghekken neerzetten, voldoende personeel op de juiste plaats hebben klaarstaan, zorgen voor tijdig opruimen van het afval, de verkeersstroom in stand kunnen houden etc. Dit zijn taken van het bevoegd gezag, waarvoor informatie vanuit de RID nodig is. De burgemeester bepaalt in dit geval de doelbinding. De kwaliteit van de gegevens die wordt gebruikt is in veel gevallen afhankelijk van andere afdelingen, aangezien de RID gebruikt maakt van de zoekmogelijkheden in de verschillende systemen. De eigenaar van de bron gegevens is in die gevallen verantwoordelijk voor de kwaliteit. Daarnaast heeft de RID in 2009 een procesbeschrijving opgesteld waarin afspraken staan over de werkwijze en vastlegging van gegevens.

Voorlichten en permanente educatie medewerkers RID

In 2009 is een runner RID aangesloten bij de regionale projectgroep WPG. Deze runner heeft de opleiding Wpg en een herhalingscursus gevolgd. Inmiddels hebben alle medewerkers binnen de RID één of meerdere presentaties bijgewoond over de WPG. Tevens zijn alle medewerkers van de RID medio 2011 via een e-mail door het hoofd RID gewezen op de mogelijkheid van e-learning aangaande het onderwerp WPG.

Artikel 4.3 Wpg Beveiliging

Van oudsher zijn politiesystemen reeds tegen onrechtmatige toegang door personen van buiten de politie beschermd. De standaard beveiliging is een van de taken die het korps reeds heeft ingericht of dient in te richten. Ook binnen de VtsPN en het Verzorgingsgebied Zuid West zijn of moeten acties te worden ondernomen voor de beveiliging tegen indringers.

Naast het voorkomen van onrechtmatige toegang door externe personen dient het korps aandacht te schenken aan het voorkomen van onrechtmatige verwerkingen binnen het korps zelf. Hiertoe dient men de applicaties in samenhang met de werkprocessen te analyseren. Binnen DRI is een selectie gemaakt van 32 applicaties waarmee ongeveer 90% van alle politiegegevens worden verwerkt. Van ieder van deze applicaties is beoordeeld of zij individueel en in samenhang met het werkproces voldoen aan de Wpg. Binnen deze analyse heeft men zich gericht op drie aspecten:

- 1 Isolatie;
- 2 Autorisaties;
- 3 Levensloop van de gegevens.

Zowel in de regionale als in de landelijke applicaties zijn op deze gebieden een aantal manco's geïdentificeerd. Voor de regionale applicaties wordt nu eerst beoordeeld of de applicaties worden uitgefaseerd of in de toekomst worden gecontinueerd.

Ook de landelijke applicaties zijn nog niet in alle gevallen Wpg-proof. Inmiddels is BVH 1.2.2 operationeel met een aantal mechanismen om beperkte toegang na een jaar te faciliteren, evenals het verwijderen en het vernietigen. Alleen passen deze mechanismen nog niet bij de vigerende werkprocessen voor handhaving en opsporing.

Het in kaart brengen van de werkprocessen in relatie tot de informatiesystemen, het vaststellen van de Wpg-vereisten, Wpg-manco's en actieplannen, en het rapporteren hierover is nog niet gereed.

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

Tijdens de interne audit zijn geen niet-toegestane gegevensverzamelingen gebaseerd op gevoelige gegevens aangetroffen binnen het korps. Het korps heeft onder andere in TTT-sessies, in werkinstructies en in de vuistregels voor Blauw aandacht besteed aan het onderwerp gevoelige gegevens.

4.5 Autorisatie (artikel 6)

4.5.1 Norm

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

4.5.2 Bevindingen

Korpsautorisatiematrix

De korpsautorisatiematrix is op 24 oktober 2011 formeel goedgekeurd door het Overleg Korpsleiding (OKL). De korpsautorisatiematrix is gemaakt op basis van een inventarisatie van de huidige autorisaties, een analyse van de werkprocessen en een mapping op de regimes uit de Wpg. Vervolgens is de matrix voorgelegd aan de verschillende processen en diensten. Namens de proceseigenaren en diensthoofden is feedback gegeven en zijn wijzigingsvoorstellen gedaan.

Wijziging en verwijdering

Door de vastgestelde korpsautorisatiematrix is het nu mogelijk geworden om de bestaande autorisatie te schonen. Hiertoe is een nulmeting uitgevoerd op 32 belangrijkste applicaties, waarbij de lijst met de actuele autorisaties is opgevraagd. Uit een vergelijking tussen de korpsautorisatiematrix en de werkelijke autorisaties bleken zowel incidentele als structurele afwijkingen. De DRI heeft een root cause analyses uitgevoerd om onderliggende manco's in processen te identificeren en daarvoor verbeteringen voor te stellen.

Momenteel voert de interne Wpg-auditor een audit uit op de nulmeting en de analyses, ter voorbereiding van een voorstel voor een schoningsactie.

Centraal autorisatieloket

De DRI heeft een actieplan opgesteld voor het ontwikkelen van een business case en een ontwerp voor een centraal autorisatieloket. Hiermee worden de reguliere autorisaties centraal inzichtelijk en wordt het eenvoudiger vervuiling te voorkomen of een schoning uit te voeren.

Er is al een hulpmiddel beschikbaar, genaamd het NASTool, voor het beheer van de schijfruimte van het korps. Dit wordt uitgebreid om tevens het beheer van de autorisaties op de 32 belangrijkste applicaties te ondersteunen.

De interne auditors hebben in oktober en november 2011 een technical audit uitgevoerd op de huidige versie van het NASTool en geconstateerd dat dit hulpmiddel enkele beveiligingsmanco's kent. Binnen het korps kunnen deze manco's met procedurele maatregelen worden gecompenseerd. Een verbetering van het hulpmiddel wordt opgenomen in de op te stellen business case.

Procedures voor het aanvragen en verwijderen van autorisaties

Voor 29 applicaties is door de DRI het autorisatiebeheer in kaart gebracht. Deze analyse is vastgelegd in beschrijvende documenten, welke dienen als input voor de nieuw te ontwikkelen autorisatieprocessen. De documenten geven een beschrijving van de taken en verantwoordelijkheden voor onder andere de uitgifte, mutatie en verwijdering van autorisaties. Over het algemeen is de leidinggevende verantwoordelijk voor het aanvragen van autorisaties. Hiervoor is een speciaal formulier beschikbaar. In bepaalde districten wordt deze taak uitgevoerd door de security officer.

Protocollering van mutaties op autorisaties

Momenteel worden de aanvragen voor autorisaties, afhankelijk van de applicatie, op verschillende wijze opgeslagen. Dit kan zijn in de mailboxen van functioneel beheerders of in een van de applicaties. De privacyfunctionaris kan de autorisaties bij de verschillende beheerders opvragen in het kader van de toezichthoudende of controlerende taak. Deze controle heeft echter nog niet plaatsgevonden.

Autorisatie op mappen

Binnen het korps worden medewerkers door middel van het NASTool geautoriseerd op specifieke schijven. Security officers voeren het beheer over de autorisaties binnen de districten en diensten. Zij hebben zicht op de actuele functies van de medewerkers en brengen autorisaties aan op de benodigde schijven, muteren deze en verwijderen zodra dat nodig blijkt.

Autorisatieproces RID

Het hoofd RID houdt toezicht op de rollen en de autorisaties binnen de RID.

RID: BVO

Het hoofd en plaatsvervangend hoofd van de RID zijn verantwoordelijk en bevoegde om autorisaties te verlenen binnen BVO. Alle autorisaties zijn per functie verleend. Zo hebben de chefs autorisatieniveau 8 en de informantenrunners, informatierechercheurs en administratieve ondersteuning autorisatieniveau 6. Er is een BVO-handboek RID.

RID: Mappenstructuur op de O-schijf

Door het hoofd RID zal worden zorg gedragen voor een mappenstructuur voor de afdeling RID op jaartal. Een korte inventarisatie levert op dat er niet tot nauwelijks gebruik wordt gemaakt van deze mappen.

CIE

Autorisaties voor medewerkers van de CIE worden toegekend door het hoofd van de CIE. Het toezicht op de autorisaties is een taak en verantwoordelijkheid van de CIE Officier van Justitie. Deze taak is beschreven in de "Instructie CIE-Officier van Justitie" van het college van PG's.

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 bevoegde functionaris- zijnde de leider van het betreffende onderzoek of zijn plaatsvervanger, voor dat onderzoek verder worden verwerkt. Indien politiegegevens in combinatie met elkaar worden verwerkt, worden van die verwerking nader genoemde gegevens vastgelegd (protocolplicht).

4.6.2 Bevindingen

Interpretatie van artikel 11 Wpg

Het korps Rotterdam-Rijnmond heeft als basisregel ingevoerd: "Artikel 11 Wpg is RIO". Daarbij vallen alle zoekacties ten behoeve van de artikelen 8, 9 en 10 Wpg onder de artikelen 8.3, 11.1 en 11.2 Wpg, en zorgt de RIO voor de vereiste toetsingen, waar nodig voor overleg met de bevoegde functionaris, en voor protocollering.

Voor de implementatie van deze basisregel bij de RIO en Opsporing is door een van de privacyfunctionarissen een protocol opgesteld. Dit protocol is door het Hoofd RIO en de proceseigenaar Opsporing ondertekend. Hiermee is vastgesteld dat alle activiteiten voor de artikelen 8.3, 11.1 en 11.2 Wpg altijd door de RIO moeten worden uitgevoerd.

RIO protocol voor infodesks

In het kader van de gemaakte afspraken over de basisregel heeft de RIO een protocol opgesteld voor de infodesks. In dit protocol zijn de relevante Wpg-vereisten opgenomen zoals toetsing van de doelbinding, vastlegging van de vraag en het antwoord, bewaartermijnen etc. Het protocol is bekrachtigd door het Hoofd RIO en uitgerold.

Interne controle door RIO zelf

De RIO heeft twee chefs infodesk aangewezen, die als een intern controle team onaangekondigd infodesks bezoeken ter verificatie van naleving van de Wpg. In oktober 2011 heeft dit team alle infodesks bezocht en heeft een aantal adviezen opgesteld aan Hoofd RIO. Daarnaast hebben zij voorlichting verzorgd binnen de infodesks waar dat nodig bleek.

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

BVH 1.2.2

De Basis Voorziening Handhaving (BVH) versie 1.2.2 is door vtsPN beschikbaar gesteld om aan de Wpg te voldoen. In deze versie van BVH wordt onderscheid gemaakt in de leeftijd van registraties en zijn drie autorisatieniveaus aangebracht. In de onderstaande tabel van vtsPN is zichtbaar hoe dit zich tot elkaar verhoudt.

BVH 1.2.2	Beoogde groep medewerkers	Inzage- en verwerkingstermijn		
		0 - 1 jaar	1 - 5 jaar 'afgeschermd'	5 - 10 jaar 'bewaard'
breed	RIO, CIE, etc.	✓	✓	✓
standaard	bijna alle medewerkers	✓	✓	-
beperkt	evt. ondersteunend personeel, arrestantenverzorgers	✓	-	-

De tabel bevat door vtsPN beoogde groepen medewerkers om de autorisaties aan te verlenen. De werkelijke inrichting moet door het korps worden bepaald. De autorisaties zijn in BVH toe te kennen per Organisatorische Eenheid (OE), per functie, of per individuele medewerker.

Bewaartermijn: artikel 8 Wpg gegevens van 1 tot 5 jaar

BVH wordt op dit moment voor zowel artikel 8, 9 als 13 Wpg politiegegevens gebruikt, ieder met een eigen bewaartermijn. BVH 1.2.2 geeft de mogelijkheid via het instellen van beslotenheid en het kiezen van de juiste combinaties van autorisaties te voldoen aan de regel van een verhoogde barrière voor de periode van 1 tot en met 5 jaar voor artikel 8 Wpg gegevens.

Het korps Rotterdam-Rijnmond heeft een actieplan opgesteld om de DRI tezamen met de proceseigenaren te laten onderzoeken op welke wijze de faciliteiten van BVH 1.2.2 kunnen worden benut, in samenhang met de daarbij behorende aanpassing van de werkprocessen binnen de regimes van artikel 8, 9 en 13 Wpg.

Bewaartermijn: artikel 8 Wpg gegevens verwijderen na 5 jaar

In BVH 1.2.2 blijft de bestaande methode van beslotenheid van registraties werken tot de gegevens 5 jaar oud zijn. Dan zullen deze voor de WPG worden 'bewaard'. De VtsPN heeft voor verwijderde gegevens de term 'bewaard' gekozen. Controle op de termijnen vindt plaats middels een dagelijkse 'batch'. Registraties die nog niet zijn afgehandeld en gezien door de verantwoordelijke chef zullen niet worden 'afgeschermd' of 'bewaard'.

Hoe met dit mechanisme moet worden omgegaan in de praktijk in relatie tot de werkprocessen wordt eveneens onderzocht door het korps Rotterdam-Rijnmond.

Bewaartermijn: artikel 8 Wpg gegevens vernietigen na 5 jaar verwijderd

In BVH 1.2.2 vernietigt de dagelijkse batch geen gegevens. Dat gaat met een losse tool ('Cleanreg'), die door gegevensbeheer kan worden gebruikt. Na 10 jaar zullen gegevens worden vernietigd, tenzij is aangegeven dat vernietigen niet is gewenst omdat die gegevens niet vernietigd mogen worden.

Voor oudere gegevens kan geen onderscheid worden gemaakt tussen de gegevens vallend onder de regimes van artikelen 8, 9 en 13 Wpg. Op dit moment is er nog geen oplossing hoe hiermee om te gaan.

In dit kader heeft het korps op 2 november 2011 van de landelijk projectleider Wpg het verzoek gekregen om het schoningscript nog niet aan te laten zetten. Het korps Rotterdam-Rijnmond oriënteert zich op een oplossing voor het vernietigingsprobleem, maar moet daarbij mogelijk wachten op een landelijk besluit.

Bewaartermijn: artikel 9 Wpg gegevens verwijderen na OH+1/2 jaar

Er wordt onderscheid gemaakt tussen Art. 8 versus 9 onderzoeken, tussen districtelijke en regionale Opsporing, en tussen opslag in BVH, BVO of schijven.

Vanuit het OM wordt zelden een melding van onherroepelijk vonnis gestuurd naar het korps. Binnen het korps wordt na afloop van het onderzoek de meeste autorisaties verwijderd waardoor wordt getracht politiegegevens in technische zin zo goed mogelijk te verwijderen. Bij deze aanpak ontstaat er echter een complicatie. Het werkelijke verwijdermoment is eerder dan het wettelijk voorgeschreven OH-moment plus een half jaar. Hierdoor is niet eenduidig vast te stellen wanneer niet meer mag worden gezocht in deze technisch gesproken verwijderde gegevens. De zoekacties van de RIO kunnen nu ongemerkt het OH-moment plus een half jaar passeren, waardoor in strijd met artikel 14.3 Wpg wordt gehandeld.

Bewaartermijn: artikel 9 Wpg gegevens vernietigen na 5 jaar verwijderd

Doordat het OH-moment niet bekend is, kan niet worden bepaald wanneer artikel 9 politiegegevens moeten worden vernietigd.

CIE: Artikel 10 en 12 Wpg bewaartermijnen

Binnen de CIE wordt gewerkt volgens het landelijk [REDACTED] CIE. Hierin is opgenomen dat het Hoofd CIE met regelmaat controleert op onder andere de bewaartermijnen. Als gegevens niet meer voldoen aan het doel waarvoor ze werden bewaard, dan worden ze direct verwijderd. Als de gegevens nog wel voldoen, maar er worden binnen vijf jaar geen nieuwe gegevens verwerkt, dan worden de gegevens na vijf jaar verwijderd. De CIE-officier van justitie doet twee maal per jaar een zogenaamde registercontrole/audit bij de CIE. Daarbij worden steekproefsgewijs subjectendossiers gecontroleerd, onder andere op de bewaartermijnen.

Sinds kort is er binnen BVO een schoningsmodule voor de CIE-bewaartermijnen ontworpen, die momenteel proefdraait in enkele regio's en binnenkort voor alle regio's beschikbaar komt.

RID: artikel 10 en 12 Wpg bewaartermijnen

Binnen de RID wordt voor wat betreft haar Openbare Orde taak tweemaal per jaar gekeken naar de Inlichtingenbalans. Bij het bespreken van de Inlichtingenbalans zijn de RID-leidinggeveenden en de strategisch analist van de RID betrokken. Gezamenlijk wordt gekeken naar de informanten en naar de informatie die deze informanten leveren. Daarbij wordt over wel of niet doorgaan met de informant besloten. Indien er niet wordt doorgegaan met de informant wordt deze uitgeschreven en uit het informantenbestand van de RID-openbare orde verwijderd. Op de afdeling is een werkgroep actief die onder andere kijkt naar de bewaartermijnen ingevolge artikel 12 Wpg en waar deze de termijn van 10 jaar heeft overschreden zal dit worden vernietigd.

1

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

Codering

Om het delen van gegevens te bevorderen is artikel 15.1 opgenomen in de Wpg, welke het delen van gegevens in principe verplicht stelt. Het is echter in bepaalde gevallen wenselijk vooraf beperkende voorwaarde vast te stellen voor het delen. Binnen het korps Rotterdam-Rijnmond zijn afspraken gemaakt tussen de bevoegde functionarissen en de infodesks over de codering van de Melding Recherche Onderzoek (MRO) en coderingen binnen BVO.

Het korps heeft als uitgangspunt gekozen om de MRO voor de landelijke verwijsindex VROS voor artikel 9 Wpg onderzoeken in beginsel met '01' te coderen. Deze codering geeft aan dat de gegevens pas operationeel mogen worden gebruikt na expliciete goedkeuring door de bevoegde functionaris. De regels zijn opgenomen in de 'Handreiking bevoegde functionaris' en uitgevaardigd door de proceseigenaar Opsporing, met instemming van het Diensthoofd RIO.

Er is een landelijk probleem met het ontsluitingsinstrument BlueView. Als in BVO een mutatie is gecodeerd met '01', wordt deze op eenzelfde wijze geëxporteerd naar BlueView als politiegegevens die met '11' zijn gecodeerd.

Vanwege het gebrek aan onderscheid tussen '11' en '01' in BlueView, heeft het korps Rotterdam-Rijnmond tevens als uitgangspunt gekozen dat waar artikel 9 Wpg politiegegevens een tactisch belang hebben, deze in BVO met '00' worden gecodeerd. Dankzij de MRO met '01' weet een infodesk dan dat het onderzoek bestaat, en kan bij een vraag verwijzen naar de juiste bevoegde functionaris. Een andere mogelijkheid is de MRO geheel af te schermen door deze met '00' te coderen. Dit is vergelijkbaar met het vooraf weigeren om gegevens te delen. Het betreffende onderzoek kan dan niet door de infodesks en andere onderzoeksleiders worden gevonden in VROS.

De wetgever heeft voor het weigeren van het delen van informatie een limitatieve lijst opgesteld met weigeringsgronden. Alle bevoegde functionarissen zijn op de hoogte gebracht, door middel van de werkinstructie en gedurende de opleiding dat een MRO alleen op '00' mag worden gecodeerd als er sprake is van een van de wettelijke weigeringsgronden.

Rechtvaardiging van het beleid voor codering

Bij het opstellen van de afspraken over het coderingsbeleid binnen het korps zijn de afdelingen DRI, RIO, BBZ, en Opsporing betrokken. Bij het opstellen van het beleid is geconstateerd dat IT-applicaties, in dit geval Blue View, nog niet WPG-proof zijn. Dat levert in de praktijk spanning op tussen twee Wpg-principes, namelijk enerzijds informatiedeling en anderzijds instemming van de bevoegde functionaris voor verdere verwerking van artikel 9 Wpg politiegegevens ten behoeve van een ander doel.

Ondanks deze onduidelijkheid is besloten om de gegevens in principe te delen middels BlueView door de MRO met '01' te coderen. Door de projectleider Wpg van het korps is aangegeven dat deze onduidelijkheid is gecommuniceerd naar de landelijk projectleider.

Medewerkers van de RIO, overkoepelend aan de infodesks, zijn betrokken bij het opstellen van het beleid. Alle medewerkers van de infodesks van het korps Rotterdam-Rijnmond zijn op de hoogte gebracht door een training en het verstrekken van een protocol voor de infodesk.

Aanwijzing en opleiding bevoegde functionaris

In het document 'Besluit Aanwijzing bevoegde functionaris' uit 2009 zijn onder andere alle leiders van een onderzoek en hun vervangers aangewezen als bevoegde functionaris. Hierdoor is slecht beperkt onderhoud van dit document noodzakelijk. Indien een nieuwe persoon wordt aangewezen tot leider onderzoek of vervanger is deze meteen bevoegde functionaris. Om te zorgen dat de bevoegde functionaris de in de Wet beschreven taak effectief kan uitvoeren heeft het korps Rotterdam-Rijnmond een opleiding (TTT-sessies) specifiek voor deze doelgroep ontwikkeld. Deze opleiding is op 12 mei 2011 gegeven. Binnen Opsporing wil men zorgen voor een periodiek terugkerende opleiding voor nieuwe aan te stellen bevoegde functionarissen.

Om de werkafspraken toegankelijk te maken voor de bevoegde functionarissen en hun teamleden zijn deze kort en bondig op papier gezet. De documenten zijn toegankelijk via het intranet (PIT). Op PIT is ook een format PV voor het intern ter beschikking stellen van politiegegevens geplaatst. Door het format PV te gebruiken worden politiegegevens alleen op een gestructureerde wijze gedeeld en houdt de bevoegde functionaris grip op de Wpg-aspecten van de politiegegevens.

4.9 Voor de impact van artikel 15 Wpg zijn een aantal maatregelen getroffen bij Politie Rotterdam-Rijnmond 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

Convenanten en artikel 20 Wpg besluiten

De dienst Bestuurs en Beleids Zaken (BBZ) heeft in 2010 alle convenanten opgevraagd bij de beleidsmedewerkers binnen de districten. Deze zijn centraal gecontroleerd, waar nodig geactualiseerd en waar mogelijk gecentraliseerd. Op intranet is een convenantenloket geopend, waarop, naast toelichtingen, de landelijke Verstrekkingenwijzer is geplaatst, plus de centraal goedgekeurde convenanten. In 2011 heeft de BBZ opnieuw de beleidsmedewerkers bij alle districten laten controleren of er nog lokale conventanten bestaan. De BBZ heeft centraal een procesbeschrijving, een model convenant, een werkinstructie voor het invullen en afhandelen, een model artikel 20 besluit, eveneens met een werkinstructie, en voorlichtende teksten opgesteld. De Wpg-relevante convenanten en artikel 20 Wpg besluiten zijn op het intranet geplaatst.

De BBZ heeft een regionaal Verstrekkingenschema opgesteld met een kapstokartikel, dat op 7 november 2011 is geaccordeerd door het Overleg Korpsleiding (OKL).

Artikel 8 Wpg verstrekkingen

Het korps heeft vuistregels voor Blauw ontwikkeld en een opleidingstraject met TTT-sessies voor chefs ontworpen. Onder leiding van het Plaatsvervangend Diensthoofd Wijkpolitie is van juli tot en met september 2011 een werkgroep van ongeveer 12 personen periodiek bij elkaar geweest om de vuistregels, werkinstructie, TTT-sessies en voorlichtingsmateriaal te ontwikkelen.

Protocolplicht voor artikel 8 Wpg verstrekkingen

Er is een werkinstructie "Wpg voor Blauw" opgesteld. Deze verwijst naar de "Verstrekkingwijzer WPG" voor wat betreft aan wie en door wie welke gegevens kunnen of mogen worden verstrekt. De werkinstructie benadrukt dat bij elke verstrekking een kwaliteitscontrole dient plaats te vinden op juistheid, volledigheid, rechtmatigheid. Binnen de politie is hiervoor elke medewerker, gezien zijn taakveld, zelf verantwoordelijk. De ontvangende partij wordt altijd gewezen op de geheimhoudingsverklaring (artikel 7, lid 2 en 3 WPG en artikel 4:8 BPG).

Zowel de vuistregels als de werkinstructie wijzen op de protocolplicht voor externe verstrekking. Elke mondelinge of schriftelijke verstrekking dient te worden vastgelegd volgens de I-90-procedure, welke terug te vinden is op intranet.

Aangewezen functionaris voor verstrekken artikel 8 Wpg politiegegevens

Als er een verzoek binnenkomt voor het verstrekken van politiegegevens, dient dit verzoek te worden doorverwezen naar de door de korpsleiding aangewezen functionaris.

Artikel 9 Wpg verstrekkingen

Verstrekkingen vanuit artikel 9 Wpg onderzoeken lopen altijd via de bevoegde functionaris. Om te zorgen dat politiegegevens alleen met instemming van de bevoegde functionaris worden verstrekt, geschiedt de verstrekking door middel van een proces-verbaal. Binnen het korps is een format verstrekking artikel 9 Wpg proces-verbaal ontwikkeld, welke door de bevoegde functionaris kan worden ingevuld. Deze is via het intranet beschikbaar gesteld.

Protocollering van artikel 9 verstrekkingen

Externe verstrekkingen moeten worden geprotocolleerd. Als het onderzoek in BVH loopt, wordt dit via de I90-functie verzorgd. Echter indien een artikel 9 Wpg onderzoek in BVH wordt uitgevoerd is het niet wenselijk een eventuele verstrekking in een I-90 vast te leggen in BVH, omdat deze vastlegging zelf niet is afgeschermd. Een andere methode hiervoor is het journaal of de BVO Infodesk-module te benutten.

Er is geen eenduidige procedure voor het vastleggen van de verstrekking van artikel 9 Wpg politiegegevens. Hierdoor is het problematisch om centraal een overzicht te verkrijgen omdat hiervoor een groot aantal decentrale vastleggingen moet worden doorgespit. Door de landelijke aanpak met protocollering via I90 in BVH, via de Infodesk-module in BVO en via het journaal bij onderzoeken is centralisatie van de protocolleringsgegevens onmogelijk.

Geautomatiseerde verstrekkingen

Alle scripts en mechanismen voor geautomatiseerde verstrekkingen zijn geïnteriseerd door de DRI en waar nodig geschoond.

Voor het aanvragen van nieuwe geautomatiseerde verstrekkingen is door de DRI en de BBZ een proces ingericht.

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

Artikel 25 Wpg Inzage

Het korps Rotterdam-Rijnmond kent de volgende twee procedures voor artikel 25 Wpg:

- "Procedure betreft inzagenverzoeken van derden / Gemeente Archief Rotterdam". Hierin staat vermeld hoe het korps omgaat met inzagenverzoeken. Deze procedure is ondertekend door het Plaatsvervangend Hoofd BBZ;
- "Post procedure van afdeling DIV" van de Dienst Informatie Voorziening (DIV).

Bij de BBZ vindt de registratie plaats alsmede de organisatie van de inning van de verschuldigde 'leges'. Vanuit de BBZ worden de inzageverzoeken ter behandeling verdeeld naar de betreffende onderdelen en decentrale beleidsmedewerkers.

De interne auditor heeft over 2010 een overzicht van de BBZ ontvangen waarin de WOB-verzoeken en de Wpg inzagenverzoeken staan vermeld. Dit proces verliep in het verleden via de decentrale beleidsmedewerkers. Sinds april 2011 vindt de registratie centraal plaats.

Artikel 28 Wpg Vernietigen

Alle medewerkers op de afdeling RIO Gegevensbeheer kunnen registraties vernietigen zoals dubbele registraties, of op verzoek van een lijnchef de foutieve registraties. De Coördinator Gegevensbeheer heeft de bevoegdheid tot het vernietigen van gegevens, zoals bijvoorbeeld uit hoofde van artikel 28 Wpg. Hiervoor is een procedure opgesteld.

4.11 Protocolplicht (artikel 32)

4.11.1 Norm

De verantwoordelijke draagt zorg voor de schriftelijke vastlegging van:

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

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

4.11.2 Bevindingen

Artikel 32.1.a Wpg Doel onderzoek

Een onderzoek conform artikel 9 Wpg wordt verwerkt in BVO, BVH of de mappenstructuur van de Regionale Recherche Dienst (RRD).

Bij het starten van een onderzoek in BVO of door RRD wordt een Melding Recherche Onderzoek (MRO) verstuurd naar de landelijke verwijsindex VROS, onder beheer van KLPD. Het doel van het onderzoek conform artikel 9 Wpg maakt geen onderdeel uit van de MRO. De Dienst Regionale Informatieverwerking (DRI) heeft met het proces Opsporing afgesproken dat in de startmutatie van ieder nieuw onderzoek in BVO melding wordt gemaakt van het bedoelde doel. Er is een format gemaakt in de tekst van de startmutatie in BVO.

Het proces Opsporing heeft de richtlijn uitgevaardigd dat als een onderzoek conform artikel 9 Wpg in BVH wordt verwerkt, er tevens een BVO-omgeving wordt geopend ter verzending van een MRO naar VROS.

Het KwaliteitsBureau Opsporing (KBO) is bezig met de ontwikkeling van een overzicht van deze artikel 9 Wpg meldingen. Het is de bedoeling dat een dergelijk overzicht op aanvraag beschikbaar wordt gesteld aan bijvoorbeeld de privacyfunctionaris.

Artikel 32.1.b Wpg Artikel 13 register

Het korps beschikt over een artikel 13 Wpg register, waarin staat beschreven het specifieke doel van verwerking (artikel 13.4.a Wpg), de categorieën van personen en de soorten van gegevens (artikel 13.4.b Wpg) en de beëindigingstermijn van verwerking (artikel 13.4.c Wpg).

Landelijk zijn door de Expertgroep Politiegegevens & Privacy protocollen opgeleverd voor 9 artikel 13 Wpg systemen.

Het beschikbaar hebben van een protocol is geen eis vanuit de Wpg. Binnen het korps Rotterdam-Rijnmond bestaat het standpunt dat voor alle artikel 13 Wpg systemen protocollen beschikbaar moeten komen. De privacyfunctionaris heeft een actieplan opgesteld om dit te realiseren.

Artikel 32.1.g Wpg BIZ: Onbevoegde of onrechtmatige verwerkingen

Bureau Interne Zaken (BIZ) verricht onderzoeken naar mogelijke integriteitschendingen van politieambtenaren van het korps Rotterdam-Rijnmond. Het bureau heeft tevens een preventieve taak en houdt zich bezig met informatieoverdracht en het geven van feedback.

Het BIZ houdt een overzicht bij van de wijze waarop het BIZ zaken registreert en administreert. In het aan de interne auditor overhandigde overzicht staat een categoriale indeling van alle BIZ-onderzoeken uit 2010 en 2011 tot op heden. Dit overzicht is vertrouwelijk, maar staat ter beschikking van de interne auditor en de privacyfunctionaris. Het korps communiceert via intranet aan de medewerkers wat wel of niet is toegestaan bij het gebruik van politiegegevens voor privédoeleinden.

Gemeenschappelijke verwerking

Uit het interne auditrapport blijkt dat het korps Rotterdam-Rijnmond geen gemeenschappelijke verwerkingen doet. Er zijn wel informatiesystemen en verzamelingen van politiegegevens, waartoe medewerkers van andere korpsen zijn geautoriseerd.

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

In oktober 2010 is een interne Wpg auditor benoemd als een fulltime functie. De interne auditor loopt mee met de activiteiten in het kader van het Wpg-verbetertraject. De interne auditor koppelt dringende zaken rechtstreeks door aan de korpsprojectleider, namelijk het Diensthoofd Controlling, en aan de privacyfunctionaris.

Interne audit plan

Ook de komende jaren is er in het korps Rotterdam-Rijnmond een fulltime interne auditor beschikbaar. De interne auditor heeft een meerjarenopzet gemaakt voor het interne Wpg-auditplan.

In genoemd auditplan is opgenomen dat het korps Rotterdam-Rijnmond interne audits uitvoert met het doel om lerend vermogen op specifieke Wpg gebied te organiseren, het korps te laten voldoen aan het gestelde in de Wpg en gerelateerde wetgeving en bij te dragen aan de functie van de externe auditor.

Verder is in het auditplan aangegeven dat andere onderwerpen voort kunnen vloeien uit de verbeterpakketten van de verschillende proceseigenaren en diensthoofden en de rapportage van de externe auditor naar aanleiding van de externe privacy audit in november 2011.

De opgenomen onderwerpen zijn derhalve niet limitatief en kunnen in overleg met het diensthoofd Controlling worden gewijzigd of aangevuld.

Interne audit rapport

Het korps Rotterdam-Rijnmond voert interne Wpg-audits uit met het doel om lerend vermogen op dit specifieke gebied te organiseren, het korps te laten voldoen aan het gestelde in de Wpg en gerelateerde wetgeving en bij te dragen aan de functie van de externe auditor.

In januari 2011 heeft het korps Rotterdam-Rijnmond een extern bureau ingeschakeld voor de Wpg. Dit bureau heeft in samenwerking met de interne auditor in 2011 een Wpg pre-scan en interne audit uitgevoerd. Op basis van de rapportage over de pre-scan zijn 101 actiepunten benoemd en opgedragen aan de proceseigenaren, diensthoofden en districtchefs.

4.13 Privacyfunctionaris (artikel 34)

4.13.1 Norm

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

4.13.2 Bevindingen

Benoemd en gemeld (artikel 34.1 en 34.4)

In 2008 is de Werkgroep Implementatie Wpg in het leven geroepen. Op aanraden van de Werkgroep zijn er in 2009 2 fte privacyjuristen tot privacyfunctionaris benoemd en gemeld bij CBP. Zij hebben in 2009 en 2010 prioriteit gegeven aan advisering en voorlichting over de Wpg en hebben geparticipeerd bij de implementatie van de Wpg. In 2011 hebben zij de gedachtegang over de Wpg gereconstrueerd. Dit heeft geleid tot het piramidemodel voor werkprocessen en de informatiehuishouding van Rotterdam-Rijnmond. Tevens is deze reconstructie benut voor het ontwikkelen van TTT-opleidings- en trainingsmateriaal.

Door de betrokkenheid bij de uitrol en het verzorgen van voorlichting, hebben de toezichthoudende en controlerende taken van de privacy functionarissen minimale aandacht gehad. Daarom heeft het korps Rotterdam-Rijnmond op 1 oktober 2011 een derde privacyfunctionaris aangesteld, die zich meer richt op deze laatstgenoemde taken. Zij wordt gemeld bij het CBP.

Jaarverslag (artikel 34.3)

De activiteiten en adviezen van de twee zittende privacyfunctionarissen zijn vastgelegd in hun Jaarverslag 2009 en Jaarverslag 2010. Deze verslagen zijn overlegd aan de korpsleiding.

Voor de planning voor 2012 is doorgebouwd op het Jaarverslag 2010. Een aantal aandachtspunten uit dit verslag is tijdens het Wpg-verbetertraject al opgepakt en de geassocieerde risico's zijn al gemitigeerd. Aan de hand van gesprekken met de privacyjuristen en een risicoanalyse zijn er controleactiviteiten vastgesteld die aansluiten op de speerpunten van het Korps.

De privacyfunctionaris stelt een overkoepelend jaarverslag 2012 op ten behoeve van de Korpschef. Hierin zullen de bevindingen van de tussenrapportages integraal worden opgenomen.

Overzicht over protocollering (artikel 34.2)

In paragraaf 4.11.2 in dit auditrapport is beschreven hoe het korps Rotterdam-Rijnmond de protocollering conform Art. 32.1 heeft ingericht. Alle plaatsen van vastleggingen zijn door de interne auditor in kaart gebracht. De vastleggingen zijn toegankelijk voor de privacyfunctionaris. In 2012 zullen door de privacyfunctionaris steekproeven worden genomen ter beoordeling van de werking van het stelsel van vastgestelde maatregelen.

Wpg-loket

Het korps Rotterdam-Rijnmond beschikt centraal over vier medewerkers die daadwerkelijk adviseren over de Wpg. Tevens zijn er een aantal decentrale medewerkers die op districtsniveau Wpg-aspecten toelichten. Daarnaast is binnen Rotterdam-Rijnmond een groep van vier medewerkers, inclusief de twee zittende privacyfunctionarissen, die een informeel kenniscentrum vormen voor kennisontwikkeling en kennisdeling betreffende de Wpg. Dit is in feite het Wpg-loket van het korps. Zij hebben de initiële voorlichtingen en opleidingen verzorgd en zijn betrokken bij de communicatie over de Wpg.

4.14 Functionaris Gegevensbescherming (artikel 36)

De optionele functie van Functionaris Gegevensbescherming bestaat niet bij het korps Rotterdam-Rijnmond.