



Ministerie van Veiligheid en Justitie

Audit Wpg politie Noord-Holland Noord

Rapport

Datum	10 januari 2012
Status	Definitief

Colofon

Afzendgegevens

Departementale Auditdienst

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

Contactpersonen

[REDACTED]
[REDACTED]
Senior auditors

T 070 370 65 60
M wpg@minvenj.nl

Projectnaam

Audit Wet Politiegegevens

Ons kenmerk

DDS/5719694/11

Auteurs

[REDACTED]

1. The first part of the document is a list of the names of the persons who were present at the meeting. The names are listed in alphabetical order.

2. The second part of the document is a list of the topics that were discussed at the meeting. The topics are listed in alphabetical order.

Inhoud

Colofon 3

1 Assurance Verklaring 7

2 Management Samenvatting 9

3 Inleiding 20

- 3.1 Algemeen 20
- 3.2 Aanleiding 20
- 3.3 Doelstelling, aard en scope van de opdracht 21
- 3.4 Afbakening 21
- 3.5 Normenkader 22
- 3.6 Beperkingen voor de privacy audit 22
- 3.7 Onderzoeksmethoden en werkwijze 22
- 3.8 Doelgroep van het rapport 23

4 Bevindingen 24

- 4.1 Inleiding 24
- 4.2 Verantwoordelijke (artikel 1.f) 25
- 4.3 Kwaliteitsaspecten van politiegegevens (artikel 3 en 4) 25
- 4.4 Gevoelige gegevens (artikel 5) 28
- 4.5 Autorisatie (artikel 6) 28
- 4.6 Geautomatiseerd Vergelijken (GV)/In Combinatie Met Elkaar Verwerken (ICMEV)(artikel 11) 31
- 4.7 Bewaartermijnen (artikel 14) 32
- 4.8 Ter beschikking stellen (artikel 15) 35
- 4.9 Rechten van betrokkenen (artikel 25/28) 39
- 4.10 Protocolplicht (artikel 32) 39
- 4.11 Audits (artikel 33) 40
- 4.12 Privacyfunctionaris (artikel 34) 41
- 4.13 Functionaris Gegevensbescherming (artikel 36) 41

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 politiekorps Noord-Holland Noord.

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 politiekorps Noord-Holland Noord.

Dit onderzoek is uitgevoerd conform de richtlijn 3600N, 'Assurance-opdrachten met betrekking tot de bescherming van persoonsgegevens (privacy audits)' d.d. 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 politiekorps Noord-Holland Noord, naar de stand van ultimo mei 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 Noord-Holland Noord te nemen maatregelen. Ook is gebleken dat het politiekorps Noord-Holland Noord voor het volledig kunnen voldoen aan de Wpg eisen mede afhankelijk is van besluiten die buiten het politiekorps Noord-Holland Noord 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 Noord-Holland Noord, 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. Wij adviseren die hercontrole te laten uitvoeren door de interne auditfunctie van het korps Noord-Holland Noord. Het verbeterrapport en de uitgevoerde hercontrole zullen in de navolgende jaren door de privacyauditor worden beoordeeld.

Den Haag, 10 januari 2012

De Directeur van de Departementale Auditdienst





2 Management Samenvatting

Het korps Noord-Holland heeft tot eind 2010 aanzienlijke vorderingen gemaakt met de uitrol van de Wpg, mede door de gedreven inzet van de toenmalige privacyfunctionaris. In die tijd is veel aandacht besteed aan het voorlichten van de medewerkers over de breedte van het korps. Na het uitvallen van deze functionaris is de snelheid van uitrol verloren gegaan en is de kennis van de Wpg op de werkvloer niet meer aantoonbaar gestimuleerd.

Met instemming van de kwartiermaker van de regio Noord West Nederland is eind 2011 een breed programma- en projectteam ingericht met onder andere als doel een goede en zorgvuldige implementatie van de Wpg. Op basis van de uitkomsten van de externe privacy audits hebben de korpsen Noord-Holland Noord, Kennemerland en Zaanstreek Waterland besloten tot een gemeenschappelijk verbeterplan voor zowel de Wpg als ook voor informatiebeveiliging. De aansturing is op strategisch niveau verankerd en er zal gewerkt gaan worden aan de hand van door de drie huidige korpsen vastgesteld programma. Door gebruik te maken van aan hen ter beschikking gestelde werkpakketten verwachten de korpsen snel tot resultaten te kunnen komen.

Het door ons beschouwde stelsel van maatregelen voldoet op het moment van onze externe privacy audit in opzet, bestaan en werking nog niet aan de vereisten zoals genoemd in de Wpg.

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

Criteria:

- Groen = Er wordt in hoofdlijnen voldaan aan de norm.
- Geel = 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 of ligt buiten de invloedssfeer van de auditee.

Norm	Aspect		Bevinding en oordeel
Art. 1.f, Verantwoordelijke			
1.f	Mandaatbesluit		Op 7 januari 2008 is een mandaatbesluit door de korpsbeheerder ondertekend ter mandatering van de taken en bevoegdheden gesteld in de Wet politiegegevens en de Wet bescherming persoonsgegevens. 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)		In 2009 hebben zeven leidinggevenden een tweedaagse Wpg-opleiding gevolgd, aangevuld met een op hun taak gerichte opleidingsdag. Deze opleiding was praktisch ingestoken. Vooral doelbinding, autorisaties en de artikelen 8 en 9 WPG kwamen aan bod. De kennis begint echter te vervagen en is niet aantoonbaar onderhouden. Hiermee wordt deels voldaan aan de Wpg.

Norm	Aspect		Bevinding en oordeel
3.1 t/m 3.3 (8) 4.1 (8)	Noodzakelijkheid (8) Doelbinding Rechtmatigheid Juistheid Volledigheid		De borging van deze kwaliteitscriteria is impliciet geïntegreerd in het politieproces. Er is een kwaliteitsbureau ingericht voor kwaliteitscontrole op politiegegevens. De Groep Regionale Invoer en Verwerking (RIV) richt zich zowel op Handhaving als op Opsporing en heeft tot hoofdtaak de data-entry van eindproducten en de kwaliteitscontrole op die producten. Het blijkt echter dat BPZ-medewerkers veel informatie niet invoeren in BVH. Hiermee wordt deels 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 de kwaliteitsaspecten. De PDCA-cyclus sluit via het OM en de rechter. De doelbinding is geborgd. De onderzoeken worden vastgelegd middels MRO's. De integriteit en volledigheid van informatie in BVO wordt bewaakt via controles door de functioneel beheerder. Er wordt echter gebruik gemaakt van zowel 'eigen administraties' als BVO, waarbij de gegevens uit de eigen administratie niet altijd in BVO worden geregistreerd. Hiermee wordt deels voldaan aan de Wpg.
3.4 (10 en 12) 4.1 (10 en 12)	Noodzakelijkheid (10 en 12) Doelbinding Rechtmatigheid Herkomst en wijze van verkrijging Juistheid Nauwkeurig Volledigheid		De CIE-OvJ voert halfjaarlijks een controle uit op: • de rechtmatigheid van de verkrijging en de opslag van de gegevens; • de noodzakelijkheid van de registratie van de gegevens gezien het doel van de gegevensverzameling; • de juistheid van de opgenomen gegevens; • de volledigheid van de gegevens. Hiermee wordt voldaan aan de Wpg.
4.3	Beveiliging		De ondersteuning vanuit de IT schiet te kort om te kunnen voldoen aan het aspect 'beveiliging van politiegegevens'. Er is niet beschreven op welke wijze isolatie is gerealiseerd tussen de regimes 8, 9, 10 en 12 Wpg, tussen onderzoeken en tussen informatieposities. Tevens vindt geen toetsing plaats op het daadwerkelijke functioneren van de 'logische' isolatie. De manco's van de informatiesystemen zijn niet inzichtelijk gemaakt. Hiermee wordt niet voldaan aan Wpg.
Art. 5, Gevoelige Gegevens			
	• Gevoelige gegevens		Het onderwerp gevoelige gegevens is onderdeel van het lesprogramma Wpg en is bekend bij Blauw en Opsporing.

Norm	Aspect	Bevinding en oordeel
		Er zijn geen niet-toegestane gevoelige gegevensverzamelingen aangetroffen bij korps Noord-Holland Noord. Hiermee wordt voldaan aan de Wpg.
Art. 6, Autorisatie		
• Korpsautorisatiematrix		Het korps heeft een autorisatiematrix. De matrix bevat een overzicht van de functies binnen het korps en geeft aan tot welke systemen iedere functie toegang heeft, inclusief de specifieke autorisaties binnen die systemen. Hiermee wordt voldaan aan de Wpg.
• Aanvraagproces		Binnen het korps is het bedrijfsbureau van de afdeling Informatie Management (IM) in samenwerking met de privacyfunctionaris verantwoordelijk voor het autorisatiebeheer. Het toekennen van autorisaties gebeurt aan de hand van de nota "Beleid Autorisaties Politie Noord-Holland Noord" en op basis van de autorisatiematrix. Er is sprake van een centraal autorisatiebeleid waarbij het bedrijfsbureau bijhoudt welke autorisaties zijn uitgegeven. Autorisatieverzoeken komen binnen bij het bedrijfsbureau, waarna aan de hand van de autorisatiematrix wordt gecontroleerd of de autorisaties dienen te worden toegekend of te worden afgewezen. Hiermee wordt voldaan aan de Wpg.
• Wijziging en verwijdering		Het korps heeft veel aandacht besteed aan het beheersbaar maken van het autorisatieproces, het aanvraagproces en het verwijderen bij ontslag. [REDACTED] De volledigheid is echter niet geborgd voor het proces van tijdig intrekken van autorisaties bij mutaties en bij de beëindiging van een tijdelijke inzet. Tevens is de volledigheid van het proces voor reconciliatie en schoning niet geborgd. Wij hebben diverse voorbeelden vernomen van medewerkers met bevoegdheden die al hadden moeten zijn verwijderd. Indien een medewerker van functie wijzigt, dan worden de autorisaties voor de nieuwe functie tegenwoordig pas verstrekt nadat de voormalige chef de autorisaties behorende bij de oude functie heeft ingetrokken.



Norm	Aspect		Bevinding en oordeel
			Hiermee wordt deels voldaan aan de Wpg.
	• Autorisatiebeheer CIE en RID		[REDACTED]
			Hiermee wordt voldaan aan de Wpg.
32.1.c	Protocollering autorisaties		Het bedrijfsbureau van IM houdt bij welke autorisaties zijn uitgegeven. In geval van nieuwe autorisaties ontvangt het bedrijfsbureau een kopie van de tickets van vtsPN, bewaakt de voortgang en neemt het resultaat van de acties waar. Hiervan wordt een administratie bijgehouden. Tijdelijke autorisaties worden tegenwoordig door IM in een Excel-bestand bijgehouden. Met behulp van de applicatie [REDACTED] van vtsPN is het mogelijk voor een aantal applicaties de toegekende autorisaties in beeld te brengen. Hiermee worden overzichten gecreëerd van applicaties waarvoor een medewerker is geautoriseerd. Er is echter geen overzicht van alle autorisaties op de groepsschijven. Hiermee wordt deels voldaan aan de Wpg.
32.3 voor 32.1.c	Bewaren protocolgegevens autorisaties		Iedere door het bedrijfsbureau van IM vastgelegde mutatie op de autorisaties wordt bewaard. Hiermee wordt voldaan aan de Wpg.
Art. 11, Geautomatiseerd vergelijken en in combinatie zoeken			
	• Hanteerbare interpretatie		Een definitie van het geautomatiseerd vergelijken is vastgesteld. Het korps heeft echter geen definitie beschreven en vastgelegd van artikel 11.4 Wpg zoekacties. Het geautomatiseerd vergelijken met andere gegevens dan politiegegevens op grond van artikel 11.5 Wpg heeft nog niet plaatsgevonden. Hiermee wordt deels voldaan aan de Wpg.
	• Aangewezen functionarissen		De bevoegd functionarissen zijn aangewezen middel een aanwijzingsbesluit en mogen artikel 11-zoekacties laten verrichten. Hiermee wordt voldaan aan de Wpg.
11.4	Bevoegd gezag		Doordat het in combinatie met elkaar verwerken niet eenduidig is vastgesteld, is het onbekend wanneer het bevoegd gezag moet worden

1871

1872

Norm	Aspect		Bevinding en oordeel
			geraadpleegd.
			Hiermee wordt niet voldaan aan de Wpg.
32.1.d en h	Protocollering 11.1, 11.2, 11.4 en 11.5		Verzoeken gericht aan de Regionale en Districtelijke Informatie Knooppunten (RIK en DIK) worden vastgelegd, evenals de antwoorden.
			Hiermee wordt voldaan aan de Wpg.
32.3 voor 32.1.d en h	Bewaren protocolgegevens 11.1, 11.2, 11.4 en 11.5		Vastleggingen van RIK en DIK over informatieverzoeken worden bewaard.
			Hiermee wordt voldaan aan de Wpg.
Art. 14, Bewaartermijnen			
8.2 en 8.3	(8) van 1 tot 5 jaar		Het korps heeft besloten dat BVH 1.2.2 voorlopig nog niet wordt geïmplementeerd, mede op landelijk advies. Daarmee wordt nog geen invulling gegeven aan de schoning.
			Hiermee wordt niet voldaan aan de Wpg.
8.6	(8) verwijderen na 5 jaar		IM schoont periodiek de gegevens in BVH en BVO. Onlangs heeft IM ook BPS geschoond. Op deze wijze probeert men ervoor te zorgen dat Art. 8 politiegegevens niet langer dan vijf jaar beschikbaar zijn. Dit proces loopt echter wat achter, waardoor ook politiegegevens ouder dan vijf jaar nog zichtbaar zijn.
			Hiermee wordt deels voldaan aan de Wpg.
14.1 (8)	(8) vernietigen na 5 jaar verwijderd		Het korps heeft geen proces voor vernietiging.
			Hiermee wordt niet voldaan aan de Wpg.
9.4	(9) verwijderen na OH plus ½ jaar		Richtlijnen ontbreken bovendien voor wat betreft de bewaartermijn van digitale data en het verwijderen van gegevens na afronding van een rechtsprocedure. Dit is een landelijk onderwerp van discussie. Het korps heeft nog geen besluit genomen over hoe mee om te gaan.
			Hiermee wordt niet voldaan aan de Wpg.
14.1 (9)	(9) vernietigen na 5 jaar verwijderd		De politie is afhankelijk van het OM voor terugkoppeling van zaken. Het verwijderen van art. 9 politiegegevens moet binnen een half jaar geschieden indien ze niet langer noodzakelijk zijn voor het doel van het onderzoek
			Het korps en OM samen hebben geen proces ingericht voor het afmelden van Art. 9 onderzoeken.
			Hiermee wordt niet voldaan aan de Wpg.
10.6	(10) verwijderen na 5 jaar geen		De CIE-OvJ controleert halfjaarlijks de gegevensverwerking van CIE door steekproeven te

Norm	Aspect		Bevinding en oordeel
	subjectwaardige registratie		nemen op de subjectdossiers. Tijdens deze controle wordt aandacht besteed aan: • Het voldoen aan opslagcriteria zoals bedoeld in artikel 10.2 Wpg; • De verwijdering en vernietiging van gegevens, zoals bedoeld in artikel 10.6 Wpg. Hiermee wordt voldaan aan de Wpg.
14.1 (10)	(10) vernietigen na 5 jaar verwijderd		De CIE-OvJ controleert halfjaarlijks de vernietiging van gegevens door steekproeven te nemen op de subjectdossiers van CIE. Hiermee wordt voldaan aan de Wpg.
14.3	Hernieuwde verwerking		Gegevens worden in onvoldoende mate verwijderd. Er is geen proces ingericht voor hernieuwde verwerking in opdracht van het bevoegd gezag. Hiermee wordt niet voldaan aan de Wpg.
32.1.e	Protocollering 14.3		Er is geen proces voor hernieuwde verwerking. Hiermee wordt niet voldaan aan de Wpg.
32.3 voor 32.1.e	Bewaren protocolgegevens 14.3		Er is geen proces voor hernieuwde verwerking. Hiermee wordt niet voldaan aan de Wpg.
12.2	(12) verwerken na 4 maanden		De CIE-OvJ ziet erop toe dat de van een informant afkomstige gegevens binnen vier maanden worden opgenomen in de daarvoor bestemde gegevensverzamelingen. Tevens controleert de CIE-OvJ minstens twee keer per jaar via steekproeven. Hiermee wordt voldaan aan de Wpg.
12.6	(12) controleren en vernietigen		Informatie wordt binnen de CIE regelmatig gecontroleerd en geschoond. De CIE-OvJ toetst halfjaarlijks het informantenregister. Hiermee wordt voldaan aan de Wpg.
Art. 15, Ter beschikking stellen			
• Infodesk voor bevraging			De informatieverzoeken worden gericht aan de informatieknooppunten. Deze vragen naar het doel van het informatieverzoek. Er zijn echter geen criteria vastgelegd waarmee dit doel kan worden getoetst. Er vindt door de Infodesk toetsing plaats op de aspecten zoals gedefinieerd in artikel 3 Wpg. Hiermee wordt deels voldaan aan de Wpg.
• Codering			De CIE maakt gebruik van informatiecoding voor het delen van informatie.

Norm	Aspect		Bevinding en oordeel
			Hiermee wordt voldaan aan de Wpg.
	• Aanwijzing Bevoegd Functionaris		Middels het 'Aanwijzingsbesluit bevoegd functionaris 2009' zijn de rollen van bevoegde functionaris genoemd in de artikelen 9 tot en met 13 Wpg toebedeeld aan functies. Het besluit is op 13 augustus 2009 door de korpsbeheerder ondertekend.
	• Opleiding Bevoegd Functionaris		Hiermee wordt voldaan aan de Wpg. Medewerkers die in eerste instantie als bevoegd functionaris zijn aangewezen zijn in de gelegenheid geweest de opleiding bevoegd functionaris te volgen. Er is echter geen rekening gehouden met opfriscursussen of met medewerkers die op een later tijdstip als bevoegd functionaris zijn aangewezen.
15.2	Weigeringgronden		Hiermee wordt deels voldaan aan de Wpg. In de door het korps ontwikkelde beslissingentabel wordt er verwezen naar de wettelijk toegestane weigeringgronden. Men wordt erop gewezen dat alleen in geval van de (limitatief) opgesomde weigeringgronden de ter beschikkingstelling van gegevens kan worden geweigerd.
Hiermee wordt voldaan aan de Wpg.			
Art. 16 t/m 24, Verstrekking			
	• Verstrekkingenwijzer (landelijk)		Het korps maakt gebruik van de landelijke verstrekkingenwijzer. De verstrekkingen vanuit de informatieknooppunten zijn geprotocolleerd en de verstrekkingen zelf worden geregistreerd.
	• Proces voor convenanten		Hiermee wordt voldaan aan de Wpg. Het korps heeft de convenanten en artikel 20-besluiten geïnventariseerd inclusief verloopdatum. Het korps is bezig een proces in te richten om (nieuwe) convenanten te communiceren naar de medewerkers. Het procesontwerp heeft echter nog de conceptstatus.
	• Proces voor Art. 20 Besluiten		Hiermee wordt deels voldaan aan de Wpg. Het korps is bezig om een proces in te richten om (nieuwe) artikel 20-besluiten te communiceren naar de medewerkers. Het procesontwerp heeft echter nog de conceptstatus.
	• Verstrekkingenschema (regio)		Hiermee wordt deels voldaan aan de Wpg. Het verstrekken van informatie gebeurt aan de hand van een verstrekkingentabel. Dit is een handleiding die per verzoekende instantie de informatie specificeert die mag worden verstrekt.

Norm	Aspect		Bevinding en oordeel
			Tevens wordt de wijze van verstrekking beschreven.
			Hiermee wordt voldaan aan de Wpg.
• Proces voor geautomatiseerde verstrekking			Het korps maakt geen gebruik van geautomatiseerde gegevensverstrekking naar externe partijen. De verstrekkingen vinden altijd plaats via een medewerker.
			Dit onderwerp is niet van toepassing voor het korps Noord-Holland Noord.
7.2	Geheimhouding		Bij het opstarten van BVH wordt de gebruiker gewezen op de plicht tot geheimhouding. Tevens hebben alle medewerkers de politie-eed afgelegd. De convenanten en artikel-20 besluiten bevatten een bepaling waarin de geheimhoudingsplicht conform artikel 7.2 Wpg wordt benadrukt.
			Hiermee wordt voldaan aan de Wpg.
32.1.f	Protocollering verstrekking		Verstrekkingen door de informatieknooppunten worden vastgelegd via de Infodesk module in [REDACTED]. Hierin wordt aangegeven welke bronnen zijn bevraagd, en hoe en aan wie het antwoord op het informatieverzoek is verstrekt. Zowel de zoekvraag als het antwoord worden vastgelegd.
			Hiermee wordt voldaan aan de Wpg.
32.3 voor 32.1.f	Bewaren protocolgegevens verstrekking		In de praktijk worden de verstrekkingen niet altijd geregistreerd. Het blijkt dat het Regionale Informatieknooppunt (RIK) regelmatig telefoontjes en e-mails krijgt over eerder beantwoorde vragen, waarbij blijkt dat er niets is terug te vinden over wie de vraag oorspronkelijk heeft beantwoord en wat er is verstrekt.
			Hiermee wordt niet voldaan aan de Wpg.
• Toezicht door leidinggevenden op verstrekkingen en protocollering			De materiedeskundige, de ploegchef en de informatiemedewerker gaan over de verstrekking van politiegegevens. Verzoeken tot verstrekking worden weleens geweigerd.
			Hiermee wordt voldaan aan de Wpg.
Art. 25 t/m 31, Rechten van de betrokkene			
25.1	Verzoek om kennisneming		De informatieknooppunten krijgen gemiddeld 800 aanvragen per jaar van burgers om inzage in gegevens die de politie verzameld heeft over de aanvrager.
			Als er klachten zijn, komen die binnen bij de privacyfunctionaris voor verdere afhandeling. In 2011 zijn er geen klachten geweest over inzagenverzoeken.

Norm	Aspect		Bevinding en oordeel
			Een inzagenprocedure is echter niet beschikbaar.
			Hiermee wordt deels voldaan aan de Wpg.
28.1 t/m 28.3	Correctie		Het proces voor rechten van betrokkenen wordt goed doorlopen.
			Een procedure voor de afhandeling van correctieverzoeken is echter niet beschikbaar.
			Hiermee wordt deels 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		Bij het starten van een onderzoek wordt een [REDACTED] verstuurd naar de landelijke verwijzindex [REDACTED], onder beheer van KLPD.
			Hiermee wordt voldaan aan de Wpg.
32.3 voor 32.1.a	Bewaren protocolgegevens doel onderzoek		De [REDACTED] wordt bewaard in [REDACTED].
			Hiermee wordt voldaan aan de Wpg.
13.4 en 32.1.b	Protocollering Art. 13 gegevensverzameling en		Het korps maakt gebruik van landelijke artikel 13 gegevensverzamelingen. Daartoe zijn algemene beschrijvingen van de gegevensverzamelingen in het korps zelf uitgezet naar de functioneel beheerders die werken met de desbetreffende gegevensverzamelingen. De functioneel beheerders hebben de couleur locale van het korps toegevoegd aan de beschrijvingen.
			Hiermee wordt voldaan aan de Wpg.
32.3 voor 32.1.b	Bewaren protocolgegevens Art. 13 gegevensverzameling en		De beschrijving van de gegevensverzamelingen onder artikel 13 beschrijft tevens de bewaartermijnen voor de protocollering.
			Hiermee wordt voldaan aan de Wpg.
32.1.g	Protocollering onrechtmatige handeling		Een overzicht van onrechtmatige verwerkingen ontbreekt.
			Hiermee wordt niet voldaan aan de Wpg.
32.3 voor 32.1.g	Bewaren protocolgegevens onrechtmatige handeling		Een overzicht van onrechtmatige verwerkingen ontbreekt.
			Hiermee wordt niet voldaan aan de Wpg.
32.2	Gemeenschappelijke verwerking		Als een van de politiekorpsen Amsterdam-Amstelland, Zaanstreek-Waterland, Noord-Holland-Noord of Kennemerland een persoon screent, worden deze gegevens inzichtelijk gemaakt voor de andere drie korpsen.
			Deze gemeenschappelijke verwerking is conform

1. The first part of the document is a list of the names of the persons who have been appointed to the various offices of the city of New York.

2. The second part of the document is a list of the names of the persons who have been appointed to the various offices of the city of New York.

3. The third part of the document is a list of the names of the persons who have been appointed to the various offices of the city of New York.

Norm	Aspect		Bevinding en oordeel
			artikel 32 lid 2 Wpg aangemeld bij het College Bescherming Persoonsgegevens. Hiermee wordt voldaan aan de Wpg.
Art. 33, Audits			
RPAP 3.1	Interne audit-functie		Een interne Wpg audit-functie is niet ingericht bij korps Noord-Holland Noord. In in januari 2011 heeft een extern bureau een pre-audit uitgevoerd bij het korps Noord-Holland Noord om de status te inventariseren van de al getroffen maatregelen voor de Wpg. De interne Wpg audit-functie is echter niet structureel belegd. Hiermee wordt deels voldaan aan de Wpg.
RPAP 3.4	Interne audit-plan		Er is geen vaktechnisch verantwoord en meerjarig intern Wpg audit-plan. Hiermee wordt niet voldaan aan de Wpg.
RPAP 3.6	Interne audit-rapport		Er is geen intern Wpg audit-rapport. Het rapport dat is opgesteld door het externe bureau betreft een pre-auditrapport. Hiermee wordt niet voldaan aan de Wpg.
Art. 34, Privacyfunctionaris			
34.1 en 34.4	Benoemd en gemeld		De privacyfunctionaris van het korps Noord-Holland Noord is langdurig afwezig. Hierdoor heeft het korps momenteel geen fulltime privacyfunctionaris. De taken worden tijdelijk en parttime waargenomen door de integriteitfunctionaris van het korps Noord-Holland Noord samen met de privacyfunctionaris van het korps Zaanstreek-Waterland. De laatste is zeer capabel, maar heeft te weinig tijd beschikbaar om de afwezige privacyfunctionaris daadwerkelijk te kunnen vervangen. Hiermee wordt niet voldaan aan de Wpg.
34.2	Overzicht over protocollering		Een overzicht van de protocollering kon ten tijde van de audit niet worden overlegd. Hiermee wordt niet voldaan aan de Wpg.
34.3	Jaarverslag		Er is geen jaarverslag over 2020. De integriteitfunctionaris het korps Noord-Holland Noord geeft aan gemiddeld 3 uur per week met de Wpg bezig te zijn. De privacyfunctionaris van het korps Zaanstreek-Waterland heeft slechts een beperkt aantal dagen beschikbaar.

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

3

Inleiding

3.1 Algemeen

In opdracht van de landelijke stuurgroep Wpg, waarin de Directeur-Generaal Politie en het KBB zijn vertegenwoordigd, heeft de DAD van het ministerie van VenJ een privacy audit uitgevoerd bij het korps Noord-Holland Noord 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 Noord-Holland Noord in 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.

Uit vooronderzoek is begin 2011 gebleken dat de implementatie Wpg binnen de diverse korpsen veelal nog in de opstartfase is, waardoor een volledige privacy audit naar de opzet, het bestaan en de werking van de Wpg, conform de Regeling periodieke audit politiegegevens, in 2011 weinig zinvol leek. In overleg met de stuurgroep is toen afgesproken dat wij dit jaar zouden benutten om te inventariseren in hoeverre bij de betrokken politieonderdelen de bepalingen van de Wpg in opzet aanwezig zijn. Daarnaast hebben wij onze aandacht gericht op de aanwezige knelpunten om, daar waar mogelijk, aanbevelingen te doen om de korpsen op weg te helpen bij de implementatie van de Wpg binnen hun organisatie.

Ten tijde van de landelijke Stuurgroep Wpg van 20 juli 2011 stond de tussenrapportage van de acht afgeronde onderzoeken op de agenda. Tijdens deze bijeenkomst is tevens aan de orde gesteld dat het College Bescherming Persoonsgegevens (CBP) van de korpsen vereist dat zij de resultaten van een externe privacy audit aan het CBP doen toekomen.

De stuurgroep heeft aan de DAD gevraagd om, vanuit het beeld dat wij hebben opgebouwd uit de tussenrapportage, na te denken over de vraag hoe wij enerzijds het beste kunnen inspelen op de eis van het CBP met betrekking tot het uitvoeren

van een privacyaudit en anderzijds de behoefte van de politiekorpsen om per korps de stand van zaken met betrekking tot de implementatie Wpg verder in beeld te brengen. Daarop heeft de stuurgroep besloten om de onderzoeken om te vormen tot privacyaudits. 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 politiekorps Noord-Holland Noord.

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 mei 2011, van maatregelen en procedures, waarmee het politiekorps Noord-Holland Noord 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:

- a. Noodzakelijkheid, rechtmatigheid en doelbinding (artikel 3);
- b. Juistheid, volledigheid en beveiliging politiegegevens (artikel 4);
- c. Gevoelige gegevens (artikel 5);
- d. Autorisaties (artikel 6);
- e. Geautomatiseerd vergelijken en in combinatie verwerken (artikel 11);
- f. Bewaartermijnen (artikel 14);
- g. Ter beschikking stellen van politiegegevens (artikel 15);
- h. Verstrekkingen (artikel 16 t/m 24);
- i. Rechten van betrokkenen (artikel 25 t/m 31);
- j. Protocolplicht (artikel 32);
- k. Audits (artikel 33);
- l. Privacyfunctionaris (artikel 34);
- m. 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 politiekorps. Pas wanneer wij, tijdens het uitvoeren van de audit bij een politiekorps, hebben geconstateerd dat de opzet en het bestaan aan de daaraan te stellen eisen voldoen voeren wij aanvullende werkzaamheden uit om de werking vast te stellen.

3.4 Afbakening

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

De audit is gericht op bovengenoemde objecten en aspecten voor zover onder verantwoordelijkheid van het politiekorps Noord-Holland Noord. Dit betekent dat wij

geen onderzoek hebben verricht naar door de vtsPN aan het korps Noord-Holland Noord geleverde faciliteiten, voor zover de verantwoordelijkheid daarvoor is belegd bij de vtsPN of bij anderen dan het korps Noord-Holland Noord.

3.5 Normenkader

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

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

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

3.6 Beperkingen voor de privacy audit

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

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

3.7 Onderzoeksmethoden en werkwijze

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

Het onderzoek is uitgevoerd door het houden van interviews onder medewerkers en leidinggevendenden van het politiekorps Noord-Holland Noord en het Openbaar Ministerie, deelwaarnemingen in de procesbeschrijvingen en andersoortige documentatie en deelwaarnemingen in informatiesystemen. Wij hebben onze werkzaamheden uitgevoerd in 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 van het korps Noord-Holland Noord;
- de korpschef van het korps Noord-Holland Noord;
- de Hoofd Officier van Justitie voor het korps Noord-Holland Noord;
- de vervangende Privacy Functionarissen;
- de voorzitter van het College Bescherming Persoonsgegevens.

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

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

4.2 Verantwoordelijke (artikel 1.f)

Mandaatbesluit

4.2.1

Norm

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

4.2.2

Bevindingen

Op 7 januari 2008 is een mandaatbesluit door de korpsbeheerder ondertekend. De korpsbeheerder heeft de korpschef daarbij gemandateerd tot het uitoefenen van taken en bevoegdheden ten aanzien van de Wet bescherming persoonsgegevens en de Wet politiegegevens (artikel 2 Mandaatbesluit). In artikel 4 van het besluit wordt de korpschef de mogelijkheid geboden de krachtens artikel 2 opgedragen bevoegdheden te ondermandateren aan medewerkers van het korps.

In het mandaatbesluit heeft de korpschef, bekrachtigd door de korpsbeheerder, de bevoegdheden inzake de Wbp en de Wpg gemandateerd aan de medewerkers van de Infodesk.

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 noodzakelijkheid, rechtmatigheid en doelbinding (artikel 3) en juistheid, volledigheid en beveiliging (artikel 4).

4.3.2 Bevindingen

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

Onderscheid onderzoek Dagelijkse Politietaak (8) versus Bepaald geval (9)

Vanuit de landelijke aanpak is een Wpg-opleiding van vijf dagen aangeboden voor medewerkers uit de regio's. Initieel is voorgesteld 18 medewerkers van het korps te laten opleiden.

De privacyfunctionaris heeft tijdens het directieoverleg op 26 november 2007 voorgesteld zeven medewerkers de Wpg-opleiding te laten volgen. Dit voorstel was gebaseerd op de hoge werkdruk bij de recherche en de tevens in die periode lopende opleidingen voor BVH en BVO. Dit voorstel is opgevolgd. Zeven leidinggevenden hebben een tweedaagse Wpg-opleiding, aangevuld met een opleidingsdag gewijd aan hun professie in samenhang met de Wpg, gevolgd.

Op intranet zijn tien gouden regels beschikbaar gesteld. Deze zijn voorzien van een beslisboom ter ondersteuning van het proces.

In 2009 is een Wpg-opleiding gegeven aan belangrijke spelers binnen de politieorganisatie. Deze opleiding was praktisch ingestoken. Vooral doelbinding, autorisaties en de artikelen 8 en 9 WPG kwamen aan bod:

- BHV (artikel 8 Wpg) informatie over klein werk, meestal van de surveillant op straat. Dit wordt over een periode van 1 jaar bevraagd en wanneer noodzakelijk over een periode van 5 jaar.
- BVO (artikel 9 Wpg) informatie over meer diepgravende onderzoeken van de recherche: dit wordt over een periode van 5 jaar bevraagd. BVO is een

gesegmenteerde database. Dit betekent dat de database afgeschermd is voor anderen dan die noodzakelijkerwijs in dat deel van de database moeten kunnen werken.

De systemen BVH en BVO zijn niet gekoppeld.

Kwaliteit Artikel 8 Wpg

Er is een Kwaliteitsbureau ingericht voor kwaliteitscontrole op politiegegevens. Het Kwaliteitsbureau richt zich op Handhaving en Opsporing en heeft tot taak:

- controle op de kwaliteit van de ingevoerde dossiers;
- coördinatie in BVH;
- screening van de aangiftes;
- monitoren van inzendtermijnen.

In de praktijk betreft dit veelal informatie van Opsporing zoals processen-verbaal die naar Justitie gaan.

De [REDACTED] richt zich op Handhaving en Opsporing en heeft tot hoofdtaak de data-entry van eindproducten en de kwaliteitscontrole op die producten. Neven taken zijn het afhandelen van post en het beheer van het archief, de servicedesk en het monitoren van inzendtermijnen. De groep [REDACTED] is onderverdeeld in [REDACTED] invoer en Centrale Verwerking (CV).

Veel informatie van BPZ-medewerkers blijkt niet in de basisvoorziening BVH te worden opgenomen. De oorzaak hiervan lijkt te liggen in het feit dat veel medewerkers niet tevreden zijn over de werking en functionaliteiten van BVH. Wijkagenten bezitten bijvoorbeeld achtergrondinformatie die nuttig kan zijn bij rechercheonderzoeken. Doordat deze niet wordt ingevoerd in BVH kan hier weinig gebruik van worden gemaakt.

Rechtmatigheid

Tien gouden regels zijn beschikbaar gesteld op intranet. Deze zijn voorzien van een beslisboom ter ondersteuning van het politieproces.

Rechtmatigheid zit al geborgd in het politieproces. Door de interne 'drive' van de politie om criminelen te laten veroordelen en zaken niet te laten seponeren en door de toetsing van een rechter bij een rechtszaak is de rechtmatigheid impliciet geborgd. Tijdens de training is aandacht besteed aan casuïstiek waarbij zaken door het OM werden afgewezen of voor de rechtbank faalden door slordigheid en onzorgvuldigheid.

Kwaliteitsbureau

Het korps maakt gebruik van [REDACTED]. Het Kwaliteitsbureau controleert en herstelt politiegegevens onder andere op basis van de meldingen vanuit TrueBlue. Tevens maken zij de registreerder duidelijk welke fouten zijn gemaakt. Op deze manier is het leerproces geborgd in het korps. Deze afdeling bestaat uit ongeveer 25 medewerkers die zich richten op de kwaliteit in onder andere BVH, [REDACTED], [REDACTED] etc.

Kwaliteit Artikel 9 Wpg

Volledigheid & Juistheid

De digitale recherche maakt images van de harde schijven van verdachten. De toename van het digitale beslag (images) levert archiveringsproblemen op. De Officier van Justitie dient aan te geven of de gegevens mogen worden verwijderd.

1. The first part of the document is a list of the names of the persons who have been appointed to the various positions of the Board of Directors of the Corporation.

2.

3.

4.

5.

Als er geen toestemming tot verwijdering gegeven wordt blijft de data op de server staan. Het image is nodig om de bewijsvoering te kunnen ondersteunen.

De afdelingsrecherche zet alle gegevens in BVH. Daarna wordt het handmatig in BVO gezet. De rechercheurs zijn hiervoor geautoriseerd door de functioneel beheerder BVO.

Binnen de informatieknooppunten in het korps Noord-Holland Noord zijn invoerafspraken vastgelegd voor BVO, conform de landelijke invoerafspraken voor BVO. Door middel van deze afspraken probeert men de kwaliteit van de in te voeren gegevens te borgen.

Binnen het invoerproces voor BVO vinden een aantal controles plaats, waaronder:

- Controle op dienstnummer van de betreffende invoermedewerker;
- Alleen ZAR en het te bevragen object koppelen aan de mutatie;
- Alle ingevoerde personen moeten in het GBA zijn gecontroleerd.

Als de uniformdienst een feit in BVH vastlegt dat voldoende ernstig is, wordt dit later ook in BVO vastgelegd. Deze vastlegging gaat aan de hand van een formulier waarop het informatieregime (artikel 9 of 10 Wpg) moet worden vastgelegd. Dit formulier, dat naar de Servicedesk Noordwest (vtsPN) dient te worden verzonden, bevat zowel de aanvraag voor BVO als voor een Summ-IT registratie. Op dit formulier dient onder andere te worden aangegeven om welke misdaadcategorie het gaat, een beknopte omschrijving van het onderzoek worden ingevuld en het betreffende Wpg-artikel te worden vermeld.

Dit formulier wordt gestuurd aan de functioneel beheerder BVO, die dit controleert op eventuele fouten.

Doelbinding

Doelbinding is geborgd in het werkproces. De onderzoeken worden vastgelegd middels [REDACTED]. Dit gebeurt bij het starten van een onderzoek. Deze zijn ter inzage voor de privacyfunctionaris. Van de onderzoeken wordt een overzicht bijgehouden.

De functioneel beheerder BVO controleert de meldingen. Indien hierbij een fout wordt geconstateerd, wordt de indiener hierover ingelicht.

Artikel 10 en 12 Wpg

Bij de CIE draagt de CIE-OvJ zorg voor een deugdelijke vastlegging van gegevens in de gegevensverzamelingen door middel van het geven van aanwijzingen omtrent, en het uitvoeren van controle op de rechtmatigheid van de verkrijging en verwerking van gegevens. Hierbij wordt tevens gecontroleerd op de juistheid, volledigheid, gebruik en verwijdering van de gegevens. De beheerder van de gegevensverzameling blijft echter verantwoordelijk voor de kwaliteit van de daarin opgenomen gegevens.

De CIE-OvJ geeft toestemming voor inschrijving van een voorlopig geregistreerde informant als geregistreerde informant onder toetsing van de kwaliteit van de informatie, voor vaststelling van de duur en voor een eventuele verlenging van de informant.

De CIE-Officier van Justitie voert halfjaarlijks een steekproefgewijze controle uit op:

- de rechtmatigheid van de verkrijging en de opslag van de gegevens;
- de noodzakelijkheid van de registratie van de gegevens gezien het doel van de gegevensverzameling;
- de juistheid van de opgenomen gegevens;
- de volledigheid van de gegevens.

De taken en bevoegdheden van de CIE-OvJ staan beschreven in de 'Instructie voor de CIE-Officier van Justitie'.

Beveiliging

Elke afdeling heeft een afdelingsmap waar alle medewerkers toe zijn geautoriseerd. Deze afdelingsmap wordt door vtsPN gefaciliteerd. Indien een medewerker tijdelijk of langdurig bij meerdere afdelingen werkzaam is, worden waar nodig passende rechten aangemaakt op de afdelingsmappen. Geconstateerd is dat de bewaking of dergelijke rechten tijdig worden verwijderd bij het aflopen van de betreffende betrokkenheid in onvoldoende mate wordt gefaciliteerd door de gebruikte techniek.

De rechercheurs van Noord-Holland Noord werken ook in een digitale mappenstructuur die de landelijke standaard is van de recherche in Nederland. Deze mappen bevatten MS Word- en Excel-documenten. De teamleiders recherche geven aan dat de informatie in deze mappen niet Wpg-proof is. Er staan op de gezamenlijke schijfruimte directory's uit het jaar 1997. Deze zijn tevens toegankelijk voor de Regionale Recherche.

De Infodesk heeft geen automatisch toegang tot deze mappen.

4.4 Gevoelige gegevens (artikel 5)

4.4.1 Norm

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

4.4.2

Bevindingen

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

Het korps heeft procedurele regels voor de omgang met gevoelige gegevens op intranet staan. Hierin is vastgelegd dat medewerkers van het korps Noord-Holland Noord gevoelige gegevens alleen mogen vastleggen als dat onvermijdelijk is voor het uitvoeren van de politietaak. Dit is tevens zo gepresenteerd tijdens de opleidingen en geïntegreerd in het werkproces. Hiermee wordt voldaan aan artikel 5 van de Wpg.

4.5 Autorisatie (artikel 6)

4.5.1 Norm

Volgens artikel 6 Wpg is de verantwoordelijke onder meer belast met het voeren van een systeem van autorisaties dat voldoet aan de vereisten van zorgvuldigheid

en evenredigheid en wordt zorg gedragen voor een schriftelijke vastlegging van de toekenning van autorisaties (protocolplicht).

4.5.2 Bevindingen

Autorisatiematrix

Een medewerker ondersteuning heeft als taak alle autorisaties te registreren en door te voeren voor functionarissen en (nieuwe) medewerkers. Hierbij wordt gebruik gemaakt van een autorisatietool, waarin een autorisatiematrix is opgenomen.

Het korps heeft een autorisatiematrix. De matrix bevat een overzicht van de functies binnen het korps en geeft aan tot welke systemen iedere functie toegang heeft, inclusief de specifieke autorisaties binnen die systemen.

Het korps heeft een autorisatiebeleid opgesteld, waarin de uitgangspunten van het autorisatieproces zijn beschreven, inclusief de uitgangspunten voor de diverse mappen in de KA-omgeving.

Autorisatieprocedure

Binnen het korps Noord-Holland Noord is het bedrijfsbureau van de afdeling Informatie Management (IM) in samenwerking met de privacyfunctionaris verantwoordelijk voor het autorisatiebeheer. Het toekennen van autorisaties gebeurt aan de hand van de nota "Beleid Autorisaties Politie Noord-Holland Noord" en op basis van de autorisatiematrix.

In de toekomst wil het samenwerkingsverband Noord West Drie het autorisatiebeleid vereenvoudigen.

Werkproces Autorisatiebeheer

De autorisatiematrix vormt de brug van functies naar toe te kennen bevoegdheden binnen applicaties.

Er is sprake van een centraal autorisatiebeleid waarbij het bedrijfsbureau bijhoudt welke autorisaties zijn uitgegeven. Autorisatieverzoeken komen binnen bij het bedrijfsbureau, waarna aan de hand van de autorisatiematrix wordt gecontroleerd of de autorisaties dienen te worden toegekend of afgewezen. Er zijn vier globale autorisatiepaden.

Nieuwe medewerker

Indien een nieuwe medewerker wordt aangesteld, stuurt Human Resource Management (HRM) een standaard formulier aan het bedrijfsbureau met de relevante informatie. Het bedrijfsbureau bepaalt de vereiste autorisaties via de intern ontwikkelde applicatie "NHN inside", conform de autorisatiematrix. De applicatie genereert een ingevulde template met de specifieke autorisaties voor de nieuwe medewerker.

De ingevulde template wordt naar vtsPN verstuurd, die de gegevens in een werkformulier opneemt en het naar de betreffende IT-beheerafdelingen stuurt. Daar worden de autorisaties in de applicaties aangebracht.

Het bedrijfsbureau ontvangt een kopie van de tickets van vtsPN en kan zo de voortgang bewaken en het resultaat van de acties waarnemen. Hiervan wordt een administratie bijgehouden.

Aanvullende autorisatie

Indien nodig kan een aanvullende autorisatie voor een applicatie of folder middels een daarvoor bestemd formulier op intranet worden aangevraagd. Hiervoor dient een goede motivatie te worden gegeven.

Het ingevulde formulier wordt naar vtsPN gestuurd en IM ontvangt een kopie. vtsPN maakt melding van het verzoek in Expertdesk. Het bedrijfsbureau beoordeelt zo een verzoek. Hierbij wordt gekeken of het verzoek past bij de functie. Dit kan bij HRM worden gecontroleerd. IM geeft haar oordeel door aan de Servicedesk van vtsPN. Indien de aanvraag een autorisatie tot een projectmap betreft, vraagt de Servicedesk aan de mapeigenaar of de aanvrager toegang mag krijgen. De Servicedesk koppelt de uitkomst terug aan de aanvrager en IM. Indien de mapeigenaar instemt, geeft de Servicedesk opdracht de autorisaties toe te kennen.

Tijdelijke autorisaties worden door IM in een Excel-bestand bijgehouden. Periodiek wordt gecontroleerd of aanvullende autorisaties dienen te worden geannuleerd. Indien een wijkagent zelfstandig om een aanvullende autorisatie verzoekt, wordt bij hun leidinggevende nagevraagd of het verzoek functioneel verantwoord is. Een tweede controle vindt plaats bij de functioneel beheerder die de autorisatie toekent. In het geval van twijfel wordt de aanvraag niet gehonoreerd.

Functiewijziging

Als binnen het korps een medewerker van functie wisselt, kan een zelfde formulier als het aanvraagformulier van autorisaties worden gebruikt. Nieuwe autorisaties worden toegekend en autorisaties die niet langer bij de nieuwe functie horen worden handmatig door IM gemarkeerd voor verwijdering door vtsPN.

Indien een medewerker van functie wijzigt, dan worden de autorisaties voor de nieuwe functie pas verstrekt indien de voormalige chef de autorisaties passende bij de oude functie heeft ingetrokken.

Uitdiensttreding

Uitdiensttreding van een medewerker wordt in het systeem genoteerd, waarna vervolgens de rechten en het account worden verwijderd.

In het Personeelssysteem 'Beaufort' blijven mensen in het bestand staan, totdat de P-medewerker het 'vinkje' weghaalt. Bij het verlaten van het korps wordt een melding van Beaufort gehanteerd voor de intrekking van de autorisaties.

Overzicht van autorisaties

Met behulp van de applicatie OBV van vtsPN is het mogelijk de toegekende autorisaties in beeld te brengen. Hiermee worden overzichten gecreëerd van applicaties waarvoor een medewerker is geautoriseerd. Tijdens een beperkte waarneming viel het op dat BlueView niet op dit overzicht verschijnt. Het bedrijfsbureau houdt wel een Excel-bestand bij van de medewerkers die zijn geautoriseerd tot BlueView.

Overige applicaties

De analist ordent de vergaarde informatie door middel van de applicatie Analist Notebook (beschikbaar gesteld door VtsPN) en Excel. In deze twee applicaties kunnen NAW-gegevens staan. De informatie in Analist Notebook en Excel worden op een groepsschijf bewaard. Hierdoor ontstaan gegevensverzamelingen waar centraal geen invloed op wordt uitgeoefend met betrekking tot bewaartermijnen. De betreffende afdeling is hier zelf verantwoordelijk voor. Deze groepsdata bestanden

Aanvullende autorisatie

Indien nodig kan een aanvullende autorisatie voor een applicatie of folder middels een daarvoor bestemd formulier op intranet worden aangevraagd. Hiervoor dient een goede motivatie te worden gegeven.

Het ingevulde formulier wordt naar vtsPN gestuurd en IM ontvangt een kopie. vtsPN maakt melding van het verzoek in Expertdesk. Het bedrijfsbureau beoordeelt zo een verzoek. Hierbij wordt gekeken of het verzoek past bij de functie. Dit kan bij HRM worden gecontroleerd. IM geeft haar oordeel door aan de Servicedesk van vtsPN. Indien de aanvraag een autorisatie tot een projectmap betreft, vraagt de Servicedesk aan de mapeigenaar of de aanvrager toegang mag krijgen. De Servicedesk koppelt de uitkomst terug aan de aanvrager en IM. Indien de mapeigenaar instemt, geeft de Servicedesk opdracht de autorisaties toe te kennen.

Tijdelijke autorisaties worden door IM in een Excel-bestand bijgehouden. Periodiek wordt gecontroleerd of aanvullende autorisaties dienen te worden geannuleerd. Indien een wijkagent zelfstandig om een aanvullende autorisatie verzoekt, wordt bij hun leidinggevende nagevraagd of het verzoek functioneel verantwoord is. Een tweede controle vindt plaats bij de functioneel beheerder die de autorisatie toekent. In het geval van twijfel wordt de aanvraag niet gehonoreerd.

Functiewijziging

Als binnen het korps een medewerker van functie wisselt, kan een zelfde formulier als het aanvraagformulier van autorisaties worden gebruikt. Nieuwe autorisaties worden toegekend en autorisaties die niet langer bij de nieuwe functie horen worden handmatig door IM gemarkeerd voor verwijdering door vtsPN.

Indien een medewerker van functie wijzigt, dan worden de autorisaties voor de nieuwe functie pas verstrekt indien de voormalige chef de autorisaties passende bij de oude functie heeft ingetrokken.

Uitdiensttreding

Uitdiensttreding van een medewerker wordt in het systeem genoteerd, waarna vervolgens de rechten en het account worden verwijderd.

In het Personeelssysteem 'Beaufort' blijven mensen in het bestand staan, totdat de P-medewerker het 'vinkje' weghaalt. Bij het verlaten van het korps wordt een melding van Beaufort gehanteerd voor de intrekking van de autorisaties.

Overzicht van autorisaties

Met behulp van de applicatie OBV van vtsPN is het mogelijk de toegekende autorisaties in beeld te brengen. Hiermee worden overzichten gecreëerd van applicaties waarvoor een medewerker is geautoriseerd. Tijdens een beperkte waarneming viel het op dat BlueView niet op dit overzicht verschijnt. Het bedrijfsbureau houdt wel een Excel-bestand bij van de medewerkers die zijn geautoriseerd tot BlueView.

Overige applicaties

De analist ordent de vergaarde informatie door middel van de applicatie Analist Notebook (beschikbaar gesteld door VtsPN) en Excel. In deze twee applicaties kunnen NAW-gegevens staan. De informatie in Analist Notebook en Excel worden op een groepsschijf bewaard. Hierdoor ontstaan gegevensverzamelingen waar centraal geen invloed op wordt uitgeoefend met betrekking tot bewaartermijnen. De betreffende afdeling is hier zelf verantwoordelijk voor. Deze groepsdata bestanden

die de analist maakt in Excel en Analist Notepad worden niet geschoond. Ook worden geen bewaartermijnen vastgelegd van de groepsdata.

De autorisaties tot de groepsschijf waarop analyse informatie wordt bewaard valt hiermee ook onder de verantwoordelijkheid van de afdeling. Hierbij wordt aangetekend dat de toegang tot deze schijf is gelimiteerd tot de afdeling/ groep. Een informatieknooppunt heeft geen toegang tot de informatie van de misdaadanalisten.

Bij de digitale recherche worden geen uitwijkfaciliteiten aangehouden. De server met digitale dataopslag is de enige server die de digitale data van de digitale recherche bevat.



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

Het gecombineerd zoeken geschiedt middels BlueView. Analisten van de informatieknooppunten krijgen pas toegang tot BlueView indien zij een cursus hiervoor hebben afgerond. De informatieverzoeken en de resultaten van de informatieverzoeken worden vastgelegd in de Infodesk module in BVO. Er worden geen artikel 11 verwerkingen buiten de informatieknooppunten uitgevoerd.

Beschrijving geautomatiseerd vergelijken

Het geautomatiseerd vergelijken is beperkter dan het verwerken van politiegegevens. Het geautomatiseerd vergelijken is erop gericht vast te stellen of bepaalde gegevens uit de ene verzameling ook voorkomt in de andere verzameling van gegevens. Bij de hier aan de orde zijnde zoekmogelijkheid geldt dat voor de geautomatiseerde vergelijking alleen gegevens worden gebruikt die voor het doel waarvoor de vergelijking wordt uitgevoerd al zijn verkregen.

De instemmingbevoegdheid van de bevoegde functionaris in het kader van de geautomatiseerde vergelijking is tweemaal. Degene die de vergelijking heeft uitgevoerd ziet als resultaat daarvan alleen de overeenkomende gegevens. Degene die de vergelijking uitvoerde mag de voor hem of haar zichtbaar geworden gegevens vervolgens pas gaan gebruiken nadat de bevoegde functionaris heeft ingestemd met verdere verwerking van die gegevens.



Artikel 11.4 Wpg

Het gecombineerd verwerken op grond van artikel 11.4 Wpg is binnen de RIO zowel bij analysewerkzaamheden als voor de informatieknooppunten is niet beschreven. Voor verdere verwerking van artikel 11.4-gegevens wordt de Officier van Justitie geraadpleegd.

Artikel 11.5 Wpg

Het geautomatiseerd vergelijken met andere gegevens dan politiegegevens op grond van artikel 11.5 Wpg heeft nog niet plaatsgevonden.

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

IM zorgt niet dat politiegegevens na één jaar achter een schotje worden geplaatst. Binnen het korps Noord-Holland Noord hanteert men naast de landelijke applicaties BVH en BVO ook shares voor politiegegevens.

Hier worden politiegegevens opgeslagen die niet kunnen worden opgeslagen in de landelijke basisvoorzieningen. Deze shares staan op lokale schijven of worden gefaciliteerd door vtsPN.

Artikel 8 Wpg

Het korps heeft besloten dat BVH 1.2.2 voorlopig nog niet wordt geïmplementeerd, mede op landelijk advies. Daarmee wordt nog geen invulling gegeven aan de schoning. Het korps wacht af tot een goed werkend schoningsscript is gemaakt, om de uitvoering van de politietaak niet verder te belasten en frustreren.

IM schoont periodiek de registers van BVH en BVO. Onlangs heeft IM ook BPS geschoond. Op deze wijze probeert men ervoor te zorgen dat Art. 8 politiegegevens niet langer dan vijf jaar beschikbaar zijn. Dit proces loopt wat achter, waardoor politiegegevens langer dan vijf jaar terug nog zichtbaar zijn.

De wijkteamchef geeft aan dat schoning van BVH de verantwoordelijkheid is van en uitgevoerd wordt door de functioneel beheerder BVH van het korps.

Artikel 9 Wpg

In BVO kunnen geen MS Word documenten, foto's, video en audio worden opgeslagen. Er is een eigen mappenstructuur gecreëerd om deze bestanden op te slaan. Binnen het korps wordt verondersteld dat deze structuur waarschijnlijk niet Wpg compliant is.

Richtlijnen ontbreken voor wat betreft de bewaartermijn van digitale data en het verwijderen van data na een rechtsprocedure. Dit is een landelijk onderwerp van discussie. Hierover is nog geen besluit genomen.

RID

Binnen het RID wordt onderscheid gemaakt tussen artikel 8 en artikel 9 registraties. Informatie die onder het artikel 8 regime valt wordt 1 jaar bewaard, terwijl artikel 9 informatie 5 jaar wordt bewaard. Door de gesegmenteerde structuur van de BVO database kunnen sommige delen worden afgeschermd.

Bij het RID wordt rekening gehouden met de bewaartermijn van 5 jaar van gegevens in BVO. Het RID geeft aan dat de bewaartermijn van 5 jaar aan hen is meegedeeld.

De RID computerserver en de applicatie RIDS zullen worden uitgefaseerd, maar wordt nu nog gebruikt voor het raadplegen van gegevens. Dit omdat BVO niet de functionaliteit biedt om onderliggende stukken zoals krantenknipsels en foto's op te bergen. RID maakt ook gebruik van mappen op de operationele schijven, waar alleen RID medewerkers toegang toe hebben.

De oudste informatie is van vijf jaar geleden.

Autorisaties voor RIDS verloopt via vtsPN. De desbetreffende afdelingschef geeft hiervoor toestemming. Vervolgens checkt vtsPN of de functie van de aanvrager strookt met de toegang tot de mappen. Enkel en alleen medewerkers van de RID zijn geautoriseerd voor de mappen op de KA-omgeving van RID.

Schoning

RIDS wordt halfjaarlijks door een speciaal daarvoor ontwikkeld programma geschoond. De maanden januari en juli zijn hiervoor aangewezen.



De afdeling Functioneel Beheer krijgt per email verzoeken van teamleiders om gegevens die volgens de Wpg verwijderd moeten worden daadwerkelijk te verwijderen. BVO bevat zelf geen geprogrammeerde controles ter ondersteuning van het handhaven van de bewaartermijnen, zoals vermeld in de Wpg.

De rechercheurs van het korps Noord-Holland Noord werken ook in een digitale mappenstructuur die de landelijke standaard is van de recherche in Nederland. Deze mappen bevatten MS Word en Excel documenten. De teamleiders recherche geven aan dat de informatie in deze mappen niet Wpg-proof is. Er staan op de gezamenlijke schijfruimte directory's uit het jaar 1997.

Het korps heeft de hardcopy archieven, met uitzondering van lopende zaken, centraal gearhiveerd. Er is recentelijk een audit uitgevoerd op het centrale archief van het korps.

Andere applicaties

Bij de digitale recherche worden images gemaakt van de harde schijven van de verdachten. De toename van het digitale beslag (images) levert archiveringsproblemen op. De Officier van Justitie dient aan te geven of de data mag worden verwijderd. Als er geen toestemming tot verwijdering wordt gegeven blijft de data op de server staan.



Tevens wordt bij het korps Noord-Holland Noord in een zaakregistratiesysteem per zaak bijgehouden welke data waar is opgeslagen (datum, nummer, kennisgeving van in beslagname (proces-verbaal)) en een beschrijving van een onderzoeksvraag voor de betreffende zaak. Een half jaar na een veroordeling door de rechtbank wordt de data van de server verwijderd.

De politiegegevens worden naast de landelijke applicaties zoals BVH en BVO verwerkt in Microsoft Office applicaties, waardoor de bewaartermijnen zoals gesteld in de Wpg niet worden gewaarborgd. Hierbij moet worden aangetekend dat het gebruik van Microsoft Office applicaties onvermijdelijk is voor de uitvoering van de dagelijkse politietaken. De verzameling aan gegevens die hierdoor ontstaat dient aan procedures te zijn onderworpen.

Verwijderen en vernietiging artikel 10

De taken en verantwoordelijkheden van de CIE-OvJ zijn vastgelegd in de 'Instructie voor de CIE-Officier van Justitie' welke in werking is getreden op 01-02-2002.

In de instructie is de taak voor de CIE-OvJ om de gegevensverwerking van de criminele inlichtingen eenheid minimaal tweemaal per jaar te controleren. Deze controleverplichting voor de OvJ geldt zowel voor artikel 10 Wpg verwerkingen als artikel 12 verwerkingen. De controle van de OvJ laat de taak en verantwoordelijkheid van de beheerder onverlet.

Met betrekking tot artikel 10 Wpg is bepaald dat de OvJ tijdens de controle van de subjectdossiers aandacht besteedt aan:

- Het voldoen aan opslagcriteria zoals bedoeld in artikel 10, tweede lid, van de Wpg
- De verwijdering en vernietiging van gegevens, zoals bedoeld in artikel 10, zesde lid van de Wpg.

De te onderzoeken dossiers wordt door de CIE-OvJ steekproefsgewijs gekozen.

Informantenregister (artikel 12 Wpg) controleren en vernietigen

[REDACTED] Alleen medewerkers van de RID hebben toegang tot deze informatie. De informanten komen gecodeerd voor in systemen zoals BVH en BVO. [REDACTED]

Bij de CIE ziet de CIE-OvJ erop toe dat de informant onder opgave van redenen uit het informantenregister wordt uitgeschreven, indien hij;

- geen relevante informatie meer verschaft;
- zich niet langer aan de afspraken houdt;
- welbewust onjuiste informatie verschaft;
- als informant bekend is geworden.

Verwerken na 4 maanden (artikel 12 Wpg)

De taken en verantwoordelijkheden van de CIE-OvJ zijn vastgelegd in de 'Instructie voor de CIE-Officier van Justitie' welke in werking is getreden op 01-02-2002.

De CIE-OvJ ziet erop toe dat de van een informatie afkomstige informatie binnen vier maanden wordt opgenomen in de daarvoor bestemde registers. Tevens controleert de CIE-OvJ de registers minstens twee keer per jaar onder overlegging van onder andere de financiële administratie.

1. The first part of the document is a title page. It contains the title of the document, the author's name, and the date of the document. The title is "The First Part of the Document". The author's name is "John Doe". The date is "1/1/2020".

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

Bevoegd Functionarissen

Middels het 'Aanwijzingsbesluit bevoegd functionaris 2009' zijn de rollen van bevoegde functionaris genoemd in artikel 9 tot en met 13 Wpg toebedeeld aan functies. De volgende functies zijn aangewezen als bevoegde functionaris:

- 1 De afdelingshoofden RIO, Recherche Ondersteuning, Regionale Recherche, BPZ, Vreemdelingenpolitie en Milieu en Bijzondere Wetten;
- 2 Het plaatsvervangend afdelingshoofd Regionale Recherche;
- 3 De senior teamleider Regionale Recherche;
- 4 De teamleiders Regionale Recherche;
- 5 De groepschefs Inwinning, RIO, RIK, Misdaadanalyse, Forensische Opsporing, Regionale Recherche, Zeden, Afdelingsrecherche en Vreemdelingenpolitie;
- 6 De senior medewerker Milieu;
- 7 De chef afdeling Integriteit en de onderzoekers integriteit B.

Het besluit is op 13 augustus 2009 door de korpsbeheerder ondertekend.

Opleiding bevoegde functionaris

Medewerkers die in eerste instantie als bevoegd functionaris zijn aangewezen zijn in de gelegenheid geweest om de opleiding bevoegd functionaris te volgen. Er is echter geen rekening gehouden met opfriscursussen of met medewerkers die op een later tijdstip als bevoegd functionaris zijn aangewezen. Deze laatste groep heeft dan niet de voorgeschreven training als bevoegd functionaris gehad.

RID

De informatie die de RID beschikbaar stelt middels BVO is informatie die na verzamelen, duiden, veredelen en analyseren tot stand is gekomen. De informatie c.q. operationele informatie wordt dan beschikbaar gesteld aan blauw.

Infodesk

Met de inwerkingtreding van de Wet politiegegevens heeft korps Noord-Holland Noord de werkzaamheden als gevolg van het verstrekken van politiegegevens regionaal belegd bij een centraal loket, het regionale informatieknooppunt.

Het informatieknooppunt neemt alle verzoeken om inzage en om verstrekking van politiegegevens in behandeling. Zo nodig wordt door hen advies ingewonnen bij de privacyfunctionaris. In het geval dat de verzoeken binnenkomen bij andere korpsonderdelen, dienen deze ontvanger het verzoek zo spoedig mogelijk ter behandeling door te sturen aan het informatieknooppunt.

In het mandaatbesluit heeft de korpschef – bekrachtigd door de korpsbeheerder – de bevoegdheden inzake de Wbp en de Wpg aan de medewerkers van het informatieknooppunt gemandateerd.

Het Decentrale informatieknooppunt (DIK) in Hoorn verwerkt informatieverzoeken. In het gehouden interview wordt gesteld dat de reden van het informatieverzoek wordt gevraagd aan de aanvrager. Vanuit de jarenlange ervaring wordt de afweging gemaakt of in het kader van de Wpg antwoord kan worden gegeven op het verzoek.

Bij de Infodesk wordt tevens de doelbinding gecontroleerd bij informatieverzoeken, met name bij artikel 9 informatie. De Infodesk kijkt daarbij ook naar de gecodeerde informatie. Alle informatieverzoeken gaan naar de knooppunten.

Bij informatieverzoeken wordt informatie van de CIE via de Infodesk verstrekt, na toestemming van de BF.

Informatie delen

De informatieverzoeken komen binnen bij respectievelijk het Nationaal Informatieknooppunt (NIK), het Regionaal Informatieknooppunt (RIK) of het Districtelijk Informatieknooppunt (DIK). Het komt ook voor dat informatie onderling wordt doorgezet. Binnen het korps Noord-Holland Noord werken het RIK en het DIK aan de hand van "handleiding besluit Poortwachter" waarin het bevoegd functionaris principe wordt gehanteerd.

Een beperking bij het delen vormt de lokale opslag in de mappenstructuur. De informatieknooppunten hebben geen automatische toegang tot de mappenstructuur.

Bij de RID wordt aangegeven dat er geen landelijke aansturing is voor het delen van informatie en dat door de regionale opzet van de politie er weinig collegiale samenwerking is. De RID van het korps Noord-Holland Noord stelt informatie wel beschikbaar aan andere korpsen. Deze uitgifte van informatie verloopt via een uit BVO komend verstrekkingformulier. Alle informatie die op basis van dit formulier beschikbaar wordt gesteld komt uit BVO.

Codering

De CIE maakt gebruik van informatiecodering voor het delen van informatie. De volgende codes worden gehanteerd:



Weigeringgronden

In de door het korps ontwikkelde beslissingentabel wordt er verwezen naar de wettelijk toegestane weigeringgronden. Men wordt erop gewezen dat alleen in geval van de (limitatief) opgesomde weigeringgronden de ter beschikking stelling van de gegevens kunnen worden geweigerd.

Verstrekken (artikel 16/24)

4.8.3 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. Art. 20 regelt de omstandigheden en voorwaarden voor de verstrekkingen aan derden structureel voor samenwerkingsverbanden.

1. The first part of the document is a list of names and addresses of the members of the committee. The names are written in a cursive hand, and the addresses are written in a printed hand. The list is organized in two columns, with names on the left and addresses on the right. The names are: John A. Smith, James B. Jones, William C. Brown, and Thomas D. White. The addresses are: 123 Main Street, New York, N.Y.; 456 Elm Street, Boston, Mass.; 789 Oak Street, Philadelphia, Pa.; and 101 Pine Street, Washington, D.C.

4.8.4 Bevindingen

Verstrekkingswijzer (landelijk)

De landelijke verstrekkingswijzer wordt gehanteerd als onderliggende documentatie om deels invulling te geven aan artikel 16 t/m 24. De centraal opgestelde procesbeschrijving geeft weer welke informatie aan welke partijen mag worden verstrekt.

Het verstrekken van informatie gebeurt aan de hand van een verstrekkentabel. Deze tabel is een handleiding waarbij per verzoekende instantie is aangegeven welke informatie wel en welke informatie niet mag worden verstrekt en tevens op welke wijze dit mag worden verstrekt.

Deze tabel is op het Intranet geplaatst. Daarnaast is een beslissingentabel voorhanden waarin De beslissingentabel bevat afwegingen voor toetsing van verzoeken, waarop aanvragen worden gehonoreerd dan wel afgewezen.

Artikel 19-verstrekkings

Het veiligheidshuis heeft zelf ten aanzien van privacywetgeving een aantal regels opgesteld. Met de samenwerkingspartners is een privacyconvenant afgesloten. Dit convenant wil de partners wijzen op bewustwording dat zij bij het uitwisselen van informatie zich dienen te houden aan privacywet- en regelgeving en hun eventueel beroepsgeheim. De partners dienen zich te realiseren dat gezocht moet worden tussen het belang van informatie-uitwisseling en het belang van betrokkene bij zijn of haar persoonlijke omstandigheden.

De RID Noord-Holland Noord verstrekt (bij dringende zaken) gegevens aan het bevoegde gezag (i.c. burgemeester) en aan de AIVD op basis van de Wiv (Wet op de inlichtingen- en veiligheidsdiensten 2002). Om deze verstrekking vast te leggen is het 'Verstrekkingsrapport openbare orde' ontwikkeld. Op dit formulier dient de naam van de verzoeker en de verstrekker te worden vastgelegd evenals de datum waarop er verstrekt is.

De verzoeken worden afgehandeld via de verstrekkingswijzer. De verstrekkingen worden vastgelegd door middel van I-90-formulieren.

Soms, bijvoorbeeld in het geval van dringende zaken, verstrekt de RID ook rechtstreeks informatie aan het bevoegd gezag. Verstrekken van informatie/gegevens de officier van justitie vindt niet plaats.

Informatieverzoeken worden opgeslagen in BVO in de Infodesk module. Hierdoor blijft inzichtelijk wat aan wie verstrekt is. Na 5 jaar is deze informatie niet meer toegankelijk. Dit wordt als problematisch ervaren bij sommige zaken waarbij dit soort informatie relevant is. Om deze reden wordt ook gebruik gemaakt van MS Outlook om deze informatieverzoeken en verstrekkingen op te slaan.

Proces voor artikel 20-besluiten

Het korps heeft in november 2011 een concept convenanten werkproces opgesteld gebaseerd op het werkproces van korps Kennemerland. Het proces is mist nog de nodige processtappen om als volledig te kunnen worden bestempeld, het korps heeft aangegeven hier in januari 2012 op terug te komen. Tot die tijd zal de concept als een leidraad dienen.

Tevens heeft er een inventarisatie plaatsgevonden van de lopende convenanten binnen Noord-Holland Noord. Alle afdelingshoofden hebben tot 27 oktober 2011 de gelegenheid gehad om door te geven of zij nog convenanten hebben liggen die nog niet zijn gearchiveerd. Afdeling Post & Archief heeft ook in de systemen PRS en CORSA naar convenanten gezocht.

Er zijn in totaal 27 convenanten geïnventariseerd. Een aantal convenanten is gepubliceerd op Werkwijzer zodat de medewerkers deze kunnen raadplegen. Uit het overzicht blijkt dat de check op het Wpg-proof zijn nog niet heeft plaatsgevonden.

Verstrekkingschema (regionaal)

De Infodesk verstrekt de informatie aan de hand van een verstrekkentabel (matrix). Deze tabel is een handleiding waaruit per verzoekende instantie (bijv. FIOD, Gemeente, Jeugdzorg etc.) is aangegeven welke informatie aan wie verstrekt mag worden en op welke wijze.

Proces voor geautomatiseerde verstrekking

Het korps maakt geen gebruik van geautomatiseerde gegevensverstrekking. De verstrekkingen vinden altijd plaats met tussenkomst van een medewerker. De afweging hiervoor is dat het korps dit niet wenselijk acht dat derden zondermeer toegang hebben op politiesystemen.

Geheimhouding verstrekking informatie

Bij het opstarten van BVH wordt de gebruiker gewezen op de plicht tot geheimhouding. Tevens hebben alle medewerkers de politie-eed afgelegd. De convenanten en artikel-20 besluiten bevatten een bepaling waarin de geheimhoudingsplicht conform artikel 7.2 Wpg wordt benadrukt.

Protocollering verstrekking

Binnen Noord-Holland Noord wordt protocollering in de registratie '10infodesk' aangehouden. Hierin worden alle informatievragen en de antwoorden daarop vastgelegd.

Verstrekkingen door de Infodesk worden geprotocolleerd in BVO. Hierin wordt weergegeven welke bronnen zijn bevraagd, hoe het antwoord op het informatieverzoek verstrekt is en aan wie het antwoord is verstrekt. Zowel de zoekvraag als het antwoord worden vastgelegd.

RID

Het korps heeft een template voor verstrekkingen RID. Deze wordt gebruikt voor de vastlegging van verstrekkingen. Het verstrekkingenrapport openbare orde bevat de wettelijke noodzakelijke elementen als de naam verzoeker, naam verstrekker, de data en verstrekkingcode.

Iedere twee maanden krijgt het hoofd RID via vtsPN ter controle een overzicht van de geregistreerde gebruikers in deze database.

Informatie wordt verstrekt wanneer de vraag legitiem wordt bevonden.

Bewaren protocolgegevens verstrekking

Alle verstrekkingen worden vastgelegd in BVO via de Infodesk module. De vragen van particulieren, verzekeringsmaatschappijen en bijvoorbeeld woningbouwverenigingen worden in het postregistratiesysteem vastgelegd.

In de praktijk worden de verstrekkingen niet altijd geregistreerd. Het blijkt dat het Regionale Informatieknooppunt (RIK) regelmatig telefoontjes en e-mails krijgt over eerder beantwoorde vragen, waarbij blijkt dat er niets is terug te vinden over wie de vraag oorspronkelijk heeft beantwoord en wat er is verstrekt.

Toezicht leidinggevenden op verstrekkingen en protocollering

De materiedeskundige, de ploegchef en de informatiemedewerker gaan over de verstrekkingen van politiegegevens. Informatieverstrekking wordt weleens geweigerd.

4.9 Rechten van betrokkenen (artikel 25/28)

4.9.1 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.

4.9.2 Bevindingen

Inzagerecht

De Infodesk krijgt gemiddeld 800 aanvragen per jaar van burgers om inzage in gegevens die de politie verzameld heeft over de aanvrager.

Als er klachten zijn, komen die binnen bij de privacyfunctionaris voor verdere afhandeling. In 2011 zijn er geen klachten geweest over inzagenverzoeken.

Een inzagenprocedure is echter niet beschikbaar.

Recht op correctie

Het proces voor rechten van betrokkenen wordt goed doorlopen.

Een procedure voor de afhandeling van correctieverzoeken is echter niet beschikbaar.

4.10 Protocolplicht (artikel 32)

4.10.1 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.

4.10.2 Bevindingen

De protocolplicht zit verweven in meerdere artikelen van de Wpg, bijvoorbeeld autorisaties en verstrekkingen. Zie daarvoor de bevindingen bij de eerder genoemde artikelen.

Artikel 32.1.a

Een onderzoek conform Art. 9 wordt verwerkt in BVO, BVH of de mappenstructuur. Bij het starten van een onderzoek wordt een [REDACTED] verstuurd naar de landelijke verwijsindex VROS, onder beheer van KLPD. Een overzicht van de meldingen is toegankelijk voor de privacyfunctionaris.

Protocollering artikel 13 gegevensverzameling

Het korps maakt gebruik van landelijke artikel 13 gegevensverzamelingen. Daartoe zijn algemene beschrijvingen van de gegevensverzamelingen in het korps zelf uitgezet naar de functioneel beheerders die werken met de desbetreffende gegevensverzamelingen. De functioneel beheerders hebben de couleur locale van het korps toegevoegd aan de beschrijvingen.

Het korps heeft een bespreking gepland voor het vaststellen van de aangepaste procedures voor afhandeling van artikel 13 gegevensverzamelingen.

Bewaren protocolgegevens artikel 13 gegevensverzameling

De beschrijvingen van de artikel 13 gegevensverzamelingen bevatten tevens bewaartermijnen voor de protocollering.

Protocollering onrechtmatige handeling

Een overzicht van onrechtmatige verwerkingen ontbreekt.

Gemeenschappelijke verwerking

Er is een gemeenschappelijk verwerking op het vlak van de screening voor mensen die bij bedrijven werken. Als een van de politiekorpsen Amsterdam-Amstelland, Zaanstreek-Waterland, Noord-Holland-Noord of Kennemerland personen screent, dan worden deze gegevens inzichtelijk gemaakt voor de drie andere korpsen.

Deze gemeenschappelijke verwerking is conform artikel 32 lid 2 Wpg aangemeld bij het College Bescherming Persoonsgegevens.

4.11 Audits (artikel 33)

4.11.1 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.

4.11.2 Bevindingen

Interne audit functie

Een bijzondere jaarlijkse interne controle, die regelmatig in het jaar de toegekende autorisaties controleert, is niet gepland. Een internet auditfunctie is niet ingericht bij

korps Noord-Holland Noord. In in januari 2011 heeft een extern bureau een pre-audit uitgevoerd bij Politie Noord-Holland Noord om de status te inventariseren van de al getroffen maatregelen voor de Wpg.

De interne Wpg auditfunctie is echter niet structureel belegd.

Interne audit-plan

Een bijzondere jaarlijkse interne controle, die regelmatig in het jaar het voldoen aan de Wpg controleert, is niet gepland.

Interne audit rapport

Er is geen intern Wpg audit-rapport. Het rapport dat is opgesteld door het externe bureau betreft een pre-auditrapport.

4.12 Privacyfunctionaris (artikel 34)

4.12.1 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.

4.12.2 Bevindingen

In korps Noord-Holland Noord is in 2007 een privacyfunctionaris aangesteld. Deze functionaris vervulde tevens de rol van Projectleider Wpg, Informatiebeveiliging en was van plan de rol van Interne Auditor te vervullen. Aan het einde van 2010 is hij door ziekte voor langere tijd uitgevallen. Momenteel vervult de integriteitsfunctionaris tijdelijk de functie van Projectleider Wpg.

Het korps heeft momenteel geen eigen privacyfunctionaris. De taken worden tijdelijk waargenomen door de integriteitsfunctionaris met de privacyfunctionaris uit het korps Zaanstreek-Waterland als achtervang.

De privacyfunctionaris van het korps Noord-Holland Noord had 8 sleutelfiguren als bevoegde functionaris opgeleid. Deze hebben ook tot taak de Wpg kennis verder te verspreiden. De integriteitsfunctionaris geeft aan gemiddeld 3 uur per week met de Wpg bezig te zijn.

Overzicht protocollering

De toezichthoudende taak is voor verbetering vatbaar. Een overzicht van de protocollering kon ten tijde van de audit niet worden overlegd. Op basis hiervan kan niet aannemelijk worden gemaakt dat de privacyfunctionaris een overzicht bijhoudt conform artikel 31 Wpg.

4.13 Functionaris Gegevensbescherming (artikel 36)

De Functionaris Gegevensbescherming bestaat niet als functie bij korps Noord-Holland Noord.