Ministerie van Veiligheid en Justitie

Audit Wpg politie Gooi en Vechtstreek

Rapport

Datum	5 december 2011
Status	Definitief

Colofon

Afzendgegevens	**Departementale Auditdienst**
	Kalvermarkt 53 2511 CB Den Haag Postbus 20301 2500 EH Den Haag www.rijksoverheid.nl/venj
Contactpersonen	[redacted] *Senior auditors* T 070 370 65 60 M wpg@minvenj.nl
Projectnaam	Audit Wet Politiegegevens
Ons kenmerk	DDS/5718878/11
Auteurs	[redacted]

Inhoud

Colofon 3

1 Assurance Verklaring 7

2 Samenvatting 9

3 Inleiding 16
3.1 Algemeen 16
3.2 Aanleiding 16
3.3 Doelstelling, aard en scope van de opdracht 16
3.4 Afbakening 17
3.5 Normenkader 17
3.6 Beperkingen voor de privacy audit 18
3.7 Onderzoeksmethoden en werkwijze 18
3.8 Doelgroep van het rapport 18

4 Bevindingen 19
4.1 Inleiding 19
4.2 Verantwoordelijke (artikel 1.f) 20
4.3 Kwaliteitsaspecten van politiegegevens (artikel 3 en 4) 20
4.4 Gevoelige gegevens (artikel 5) 22
4.5 Autorisatie (artikel 6) 23
4.6 Geautomatiseerd Vergelijken/In Combinatie Met Elkaar Verwerken (artikel 11) 24
4.7 Bewaartermijnen (artikel 14) 25
4.8 Ter beschikking stellen (artikel 15) 28
4.9 Verstrekken (artikel 16/24) 29
4.10 Rechten van betrokkenen (artikel 25/28) 30
4.11 Protocolplicht (artikel 32) 31
4.12 Audits (artikel 33) 32
4.13 Privacy functionaris (artikel 34) 32
4.14 Functionaris Gegevensbescherming (artikel 36) 33

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 maanden oktober en november 2011 is een privacy audit uitgevoerd bij het korps Gooi en Vechtstreek.

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 Gooi en Vechtstreek.

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

Den Haag, 5 december 2011

De Directeur van de Departementale Auditdienst

I & III

J.C. van Praat RE RA

2 Samenvatting

Het korps Gooi en Vechtstreek heeft een aantal zaken in opzet goed opgepakt, zoals het werken met een autorisatiematrix gekoppeld aan het personeelssysteem, het opstellen van een actieplan voor het centraal beheren van de convenanten en de samenwerking met korpsen Flevoland en Utrecht met betrekking tot de Wpg. De korpsleiding toont hiermee en met andere initiërende activiteiten haar aandacht voor de Wpg.
Niettemin voldoet het door ons beschouwde stelsel van maatregelen nog niet in opzet, bestaan en werking aan de vereisten van de Wpg.

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

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

Norm	Aspect		Bevinding en oordeel
Art. 1.f, Verantwoordelijke			
1.f	Mandaatbesluit		Er is een Mandaatbesluit Wet politiegegevens politieregio Gooi en Vechtstreek d.d. 14 juni 2010, waarin wordt aangetoond dat het bevoegd gezag (korpsbeheerder), met terugwerkende kracht tot en met 11 maart 2009, zijn mandaat verleent aan de korpschef van het regionaal politiekorps Gooi en Vechtstreek. Hiermee wordt voldaan aan de Wpg.
Art. 3 en 4, Kwaliteitsaspecten van politiegegevens			
8.1 en 9.1	Onderscheid onderzoek Dagelijkse Politietaak (8) versus Bepaald geval (9)		Op het intranet is de Beslisboom Wet Politiegegevens beschikbaar. Hierin kan iedereen nagaan onder welk artikel de politiegegevens verwerkt moeten worden. Hiermee wordt voldaan aan de Wpg.
3.1 t/m 3.3 (8) 4.1 (8)	Noodzakelijkheid (8) Doelbinding Rechtmatigheid Juistheid Volledigheid		Er is niet beschreven op welke wijze de zorg voor het voldoen aan de criteria plaatsvindt. Tevens vindt geen toetsing plaats op de gestelde criteria. Er zijn geen "vuistregels" opgesteld voor Blauw hoe te voldoen aan de Wpg. Hiermee wordt niet 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		Er zijn geen procesbeschrijvingen aangetroffen waaruit blijkt hoe de recherche moet handelen om te voldoen aan de kwaliteitscriteria van de Wpg. Hiermee wordt niet voldaan aan de Wpg.
3.4 (10 en 12)	Noodzakelijkheid (10 en 12)		Bij de CIE en RID zijn de kwaliteitscriteria in verband met de aard van het werk goed ingeregeld.

Norm	Aspect		Bevinding en oordeel
4.1 (10 en 12)	Doelbinding Rechtmatigheid Herkomst en wijze van verkrijging Juistheid Nauwkeurig Volledigheid		Bij de CIE gebeurt dit volgens het landelijk proceshandboek CIE en de toezichthoudende rol van de CIE-OvJ. Bij de RID liggen de kwaliteitscriteria al in het doel van de taak vast. Hiermee wordt voldaan aan de Wpg.
4.3	Beveiliging		BVH, BVO en de mappenstructuur worden beveiligd door middel van autorisaties. In de mappenstructuur is een scheiding aangebracht tussen de verschillende artikelen. De afdelingen RID en CIE zijn fysiek alleen toegankelijk voor medewerkers van deze afdeling. Echter zijn nog niet alle systemen WPG-proof. Een aantal systemen, waaronder BVH, voldoet niet aan de in de Wpg gestelde bewaartermijnen. Hierdoor ontstaat het risico op onrechtmatig gebruik van politiegegevens. Hiermee wordt deels voldaan aan de Wpg.
Art. 5, Gevoelige Gegevens			
• Gevoelige gegevens			Gevoelige gegevens worden niet als kenmerk aan een persoon toegekend, maar als omschrijving bij het incident. Er zijn hier echter geen richtlijnen voor. Er wordt wel volgens de Wpg gehandeld, maar de werkwijze is niet vastgelegd en daardoor misschien niet bij iedereen bekend. Hiermee wordt deels voldaan aan de Wpg.
Art. 6, Autorisatie			
• Korpsautorisatiematrix			Het korps Gooi en Vechtstreek heeft een 'levende' autorisatiematrix die gekoppeld is aan het personeelssysteem Beaufort. Deze autorisatiematrix is door het KMT geaccordeerd. Hiermee wordt voldaan aan de Wpg.
• Aanvraagproces			Er is een procesbeschrijving aanwezig. Autorisatieaanvragen worden via de personeelsmedewerkers doorgevoerd na schriftelijke toestemming van een leidinggevende. Hiermee wordt voldaan aan de Wpg.
• Wijziging en verwijdering			De functioneel beheerders checken dagelijks de mutaties binnen de autorisatiematrix, of er niets verkeerd is gegaan. Daarnaast doen zij steekproefsgewijze controle op autorisaties. De privacyfunctionaris heeft een overzicht van externe autorisaties (andere korpsen) op basis van het autorisatiebesluit. Wanneer een medewerker van functie of afdeling wisselt, dan wordt deze mutatie door de personeelsmedewerker in Beaufort ingevoerd. Hierdoor wordt direct de mutatie doorgevoerd in de autorisatiematrix, waarna geautomatiseerd de autorisaties muteren. Als een medewerker uit dienst gaat worden automatisch alle autorisaties ingetrokken.

Norm	Aspect		Bevinding en oordeel
			Hiermee wordt voldaan aan de Wpg.
• Autorisatiebeheer CIE en RID.			Autorisaties voor medewerkers van de CIE en RID worden toegekend door het hoofd van de CIE respectievelijk RID. De CIE OvJ heeft het autorisatiebeleid goedgekeurd. Hiermee wordt voldaan aan de Wpg.
32.1.c	Protocollering autorisaties		De Privacyfunctionaris heeft zelf een overzicht van de externe autorisaties doordat hij deze zelf toetst en toekent. Daarnaast kan hij een overzicht van de interne autorisaties opvragen bij Functioneel Beheer. Hiermee wordt voldaan aan de Wpg.
32.3 voor 32.1.c	Bewaren protocolgegevens autorisaties		De protocolgegevens worden bewaard. Hiermee wordt voldaan aan de Wpg.
Art. 11, Geautomatiseerd vergelijken en in combinatie zoeken			
• Hanteerbare interpretatie			Definitie ontbreekt op landelijk en op korpsniveau. Hiermee wordt niet voldaan aan de Wpg.
• Aangewezen functionarissen			Aangewezen functionarissen zijn de analisten bij de Infodesk (medewerkers van het RIK/DIK). Hiermee wordt voldaan aan de Wpg.
11.4	Bevoegd gezag		Het RIK betrekt niet zelf het bevoegd gezag (OM), dit gebeurt door de aanvrager (rechercheteam). Het RIK verwijst bij gevonden informatie de aanvrager door naar de eigenaar/bevoegd functionaris. Hiermee wordt voldaan aan de Wpg.
32.1.d en 32.1.h	Protocollering 11.1, 11.2, 11.4 en 11.5		De overzichten van vastleggingen worden bijgehouden door het RIK. De Privacyfunctionaris kan hier op terugvallen. 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 protocolgegevens worden door het RIK vastgelegd in BVO. Hiermee wordt voldaan aan de Wpg.
Art. 14, Bewaartermijnen			
8.2 en 8.3	(8) van 1 tot 5 jaar		Er is in de nieuwe release een schoningsmodule in BVH, maar deze staat op landelijk verzoek van de voorzitter van de stuurgroep nog niet aan. Hiermee wordt niet voldaan aan de Wpg
8.6	(8) verwijderen na 5 jaar		Er vindt nog geen verwijdering van informatie uit BVH plaats, de informatie is nog niet ouder dan 5 jaar. Voorganger BPS wordt wel maandelijks geschoond. Hiermee wordt voldaan aan de Wpg.
14.1 (8)	(8) vernietigen na 5 jaar verwijderd		Er vindt nog geen verwijdering van informatie uit BVH plaats. Voorganger BPS wordt wel maandelijks geschoond. Hiermee wordt voldaan aan de Wpg.
9.4	(9) verwijderen na OH plus ½ jaar		Er wordt niet toegezien op het verwijderen van gegevens als ze niet noodzakelijk zijn. Dit gebeurt alleen als in BVO het onderzoek wordt afgemeld door een TGO. Er komen bijna geen afloopberichten

Norm	Aspect		Bevinding en oordeel
			binnen. Hiermee wordt niet voldaan aan de Wpg.
14.1 (9)	(9) vernietigen na 5 jaar verwijderd		Er vindt nog geen verwijdering van informatie uit BVO plaats, want er staat nog geen informatie langer dan 5 jaar in. De informatie die wel ouder dan 5 jaar is, zit nog in lopende zaken. Hiermee wordt deels voldaan aan de Wpg.
10.6	(10) verwijderen na 5 jaar geen subjectwaardige registratie		Dit wordt door de CIE en RID nageleefd en bij de CIE gecheckt door de CIE-officier. Hiermee wordt voldaan aan de Wpg.
14.1 (10)	(10) vernietigen na 5 jaar verwijderd		Dit wordt door de CIE en RID nageleefd en bij de CIE gecheckt door de CIE-officier. Hiermee wordt voldaan aan de Wpg.
14.3	Hernieuwde verwerking		Er zitten nog geen verwijderde gegevens in BVH. In het protocol van de voorganger BPS is er wel een procesbeschrijving over het aanvragen van een hernieuwde verwerking opgenomen. Hiermee wordt voldaan aan de Wpg.
32.1.e	Protocollering 14.3		De hernieuwde verwerkingen vanuit BPS worden vastgelegd door de privacyfunctionaris en de hernieuwde verwerkingen vanuit BVO worden vastgelegd door middel van het opmaken van een MRO. Hiermee wordt voldaan aan de Wpg.
32.3 voor 32.1.e	Bewaren protocolgegevens 14.3		De protocolgegevens worden bewaard. Hiermee wordt voldaan aan de Wpg.
12.2	(12) verwijderen na 4 maanden		Informatie wordt binnen een termijn van maximaal 4 maanden verwerkt en netto in een andere omgeving gezet. Dit zit vast in de werkwijze van de CIE. Hiermee wordt voldaan aan de Wpg.
12.6	(12) controleren en vernietigen		Informatie wordt binnen de CIE en RID regelmatig gecontroleerd en geschoond. Bij de RID gebeurt dit automatisch elke 5 jaar. Bij de CIE toetst de CIE-OvJ jaarlijks het informantenregister. Hiermee wordt voldaan aan de Wpg.
Art. 15, Ter beschikking stellen			
• Infodesk voor bevraging			De Infodesk benadert de bevoegd functionaris altijd met de vraag of informatie mag worden gebruikt en gedeeld. Dit is opgenomen in de werkinstructies van het RIK. Daarmee wordt voldaan aan de Wpg.
• Codering			Codering wordt alleen gebruikt bij embargo-onderzoeken en CIE, deze hebben richtlijnen hiervoor. Hiermee wordt voldaan aan de Wpg.
• Aanwijzing Bevoegd Functionaris			Er zijn bevoegd functionarissen aangewezen, echter nog niet op alle afdelingen. De bevoegd functionarissen worden aangewezen als zij de opleiding hebben gevolgd.

Norm	Aspect		Bevinding en oordeel
			Hiermee wordt deels voldaan aan de norm, maar er is een acceptabel actieplan.
• Opleiding Bevoegd Functionaris			De bevoegd functionarissen die reeds zijn benoemd hebben een opleiding gevolgd. Hiermee wordt voldaan aan de Wpg.
15.2	Weigeringgronden		De bevoegd functionarissen zijn op de hoogte van de wettelijke weigeringgronden in relatie tot de verplichting van het ter beschikking stellen. Dit is opgenomen in de opleiding voor bevoegd functionarissen. Hiermee wordt voldaan aan de Wpg.
Art. 16 t/m 24, Verstrekking			
• Verstrekkingenwijzer (landelijk)			Er is een landelijke verstrekkingenwijzer, deze is uitgedeeld binnen het korps en is digitaal beschikbaar op intranet. Hierdoor wordt voldaan aan de Wpg.
• Proces voor convenanten			Er is een nieuwe convenantenprocedure opgesteld, waarbij de Privacyfunctionaris de convenanten beheert en mede-parafeert. De getekende convenanten staan op intranet. Binnenkort wordt het besluit genomen dat convenanten die niet op intranet staan niet meer geldig zijn. Hiermee wordt nog niet geheel voldaan aan de norm, maar er is een acceptabel actieplan.
• Proces voor Art. 20 Besluiten			In de convenantenprocedure is het proces voor art. 20 besluiten vormgegeven. Hiermee wordt voldaan aan de Wpg.
• Verstrekkingenschema (regio)			Er wordt verstrekt volgens de landelijke verstrekkingenwijzer. Er is geen verstrekkingenschema specifiek voor het korps Gooi en Vechtstreek aanwezig. De meeste verstrekkingen lopen via de Infodesk, privacyfunctionaris of worden vastgelegd in het I90-formulier. In de convenanten wordt aangegeven welk contactpersoon binnen het korps aan de partner verstrekt. Hiermee wordt deels voldaan aan de Wpg.
• Proces voor geautomatiseerde verstrekking			Er is binnen het korps een procedurebeschrijving voor geautomatiseerde verstrekkingen beschikbaar. Hiermee wordt voldaan aan de Wpg.
7.2	Geheimhouding		In het modelconvenant is een onderdeel geheimhouding opgenomen. Daarin is opgenomen dat er een geheimhoudingsplicht geldt voor alle deelnemers aan het convenant. Deze plicht strekt zich uit tot de geheimhouding van persoonsgegevens, ook indien het convenant niet meer van kracht is. Hiermee wordt voldaan aan de Wpg.
32.1.f	Protocollering verstrekking		Verstrekkingen worden vastgelegd bij de Privacyfunctionaris, via I90-formulieren en bij het RIK. De privacyfunctionaris heeft geen zicht op alle verstrekkingen. Hiermee wordt voldaan aan de Wpg.

Norm	Aspect		Bevinding en oordeel
32.3 voor 32.1.f	Bewaren protocolgegevens verstrekking		Protocolgegevens worden bewaard. Hiermee wordt voldaan aan de Wpg.
• Toezicht door leidinggevenden op verstrekkingen en protocollering			Verstrekkingen worden in BVH, BVO of bij de privacyfunctionaris vastgelegd, maar een centraal overzicht ontbreekt. Hiermee wordt niet volledig voldaan aan de Wpg.
Art. 25 t/m 31, Rechten van de betrokkene			
25.1	Verzoek om kennisneming		Het korps Gooi en Vechtstreek heeft een procedure voor rechten van betrokkenen. Alle verzoeken met betrekking tot rechten van betrokken, zoals inzagerecht van burgers, gaan via de privacyfunctionaris. De privacyfunctionaris houdt een overzicht bij van de klachten met betrekking tot inzageverzoeken. Hiermee wordt voldaan aan de Wpg.
28.1 t/m 28.3	Correctie		De privacyfunctionaris houdt een overzicht bij van de correcties met betrekking tot inzageverzoeken. Hiermee wordt voldaan aan de Wpg.
Art. 32, Protocolplicht (32.1.c, d, e, f en h behandeld bij thema's)			
9.2 en 32.1.a	Protocollering doel onderzoek		Doelomschrijving artikel 9 verwerkingen wordt bijgehouden door de privacyfunctionaris. Hiermee wordt voldaan aan de Wpg
32.3 voor 32.1.a	Bewaren protocolgegevens doel onderzoek		Protocolgegevens worden bewaard. Hiermee wordt voldaan aan de Wpg.
13.4 en 32.1.b	Protocollering Art. 13 gegevensverzameling en		Een overzicht van artikel 13 verwerkingen wordt bijgehouden door het RIK. De Privacyfunctionaris kan hier op terugvallen. Hiermee wordt voldaan aan de Wpg
32.3 voor 32.1.b	Bewaren protocolgegevens Art. 13 gegevensverzameling en		Protocolgegevens worden bewaard. Hiermee wordt voldaan aan de Wpg.
32.1.g	Protocollering onrechtmatige handeling		Onrechtmatige handelingen worden binnen het korps niet bijgehouden. Alleen bij een aanleiding wordt Bureau Integriteit ingeschakeld. Hiermee wordt niet voldaan aan de Wpg
32.3 voor 32.1.g	Bewaren protocolgegevens onrechtmatige handeling		Onrechtmatige handelingen worden binnen het korps niet bijgehouden. Alleen bij een aanleiding wordt Bureau Integriteit ingeschakeld. Hiermee wordt niet voldaan aan de Wpg
32.2	Gemeenschappelijke verwerking		Gemeenschappelijke verwerkingen vinden in TGO's plaats. De verantwoordelijkheid ligt bij het korps van de TGO-leider. Voor de andere TGO-leden worden externe autorisaties uitgegeven. Gemeenschappelijke verwerkingen worden niet bij het CBP gemeld omdat de verantwoordelijkheid bij

Norm	Aspect		Bevinding en oordeel
			een korps belegd is. Van een gemeenschappelijke verwerking volgens de Wpg is hiermee geen sprake.
Art. 33, Audits			
RPAP 3.1	Interne audit-functie		Er is bij korps Gooi en Vechtstreek geen interne auditfunctie. Hiermee wordt niet voldaan aan de Wpg.
RPAP 3.4	Interne audit-plan		Er is geen intern auditplan. Hiermee wordt niet voldaan aan de Wpg.
RPAP 3.6	Interne audit-rapport		Er heeft geen interne audit plaatsgevonden. Hiermee wordt niet voldaan aan de Wpg.
Art. 34, Privacyfunctionaris			
34.1 en 34.4	Benoemd en gemeld		De privacyfunctionaris is middels Mandaatbesluit Wet politiegegevens Privacy Functionaris, politieregio Gooi en Vechtstreek d.d. 1 januari 2008 formeel aangewezen door de korpsbeheerder. De eerste privacyfunctionaris is op 10-11-2008 aangemeld bij het CBP en de huidige privacyfunctionaris is op 01-12-2010 aangemeld bij het CBP. Hiermee wordt voldaan aan de Wpg.
34.2	Overzicht over protocollering		De overzichten van protocollering worden niet door de privacyfunctionaris bijgehouden, maar zijn bij het RIK belegd. Overzichten worden dus wel bijgehouden, maar niet door de privacyfunctionaris. Hiermee wordt voldaan aan de Wpg.
34.3	Jaarverslag		Er zijn Privacy jaarverslagen van 2009 en 2010 aanwezig. t ja Hiermee wordt deels voldaan aan de Wpg.
Optioneel Art. 36, Functionaris Gegevensbescherming			
36.1 en 36.2	Benoemd		Er is geen Functionaris Gegevensbescherming benoemd.
Wbp 63.3	Gemeld		Niet van toepassing.
Wbp 64.1 t/m 64.4	Toezichthoudende rol		Niet van toepassing.

3 Inleiding

3.1 Algemeen

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

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 november 2011, van maatregelen en procedures, waarmee het

politiekorps Gooi en Vechtstreek 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 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 Gooi en Vechtstreek. Dit betekent dat wij geen onderzoek hebben verricht naar door de vtsPN aan het korps Gooi en Vechtstreek geleverde faciliteiten, voor zover de verantwoordelijkheid daarvoor is belegd bij de vtsPN of bij anderen dan het korps Gooi en Vechtstreek.

3.5 Normenkader

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

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

3.6 Beperkingen voor de privacy audit

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

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

3.7 Onderzoeksmethoden en werkwijze

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

Het onderzoek is uitgevoerd door het houden van interviews onder medewerkers en leidinggevenden van het politiekorps Gooi en Vechtstreek en het Openbaar Ministerie, deelwaarnemingen in de procesbeschrijvingen en andersoortige documentatie en deelwaarnemingen in informatiesystemen.
Wij hebben onze werkzaamheden uitgevoerd in de periode van 10 oktober 2011 tot en met 17 november 2011.

Het conceptrapport met bevindingen is op 25 november 2011 besproken met de korpschef van het korps Gooi en Vechtstreek en op 30 november met de korpsbeheerder.
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 P.I. Broertjes;
- de korpschef W. Woelders;
- de Hoofd Officier van Justitie mr. H.E. Hoogendijk;
- de Privacy Functionaris ;
- de voorzitter van het College Bescherming Persoonsgegevens.

Het rapport mag uitsluitend met toestemming van de korpsbeheerder dan wel de korpschef van politiekorps Gooi en Vechtstreek 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 Gooi en Vechtstreek heeft de coördinatie omtrent de Wpg voldoende belegd. In het Korps Management Team (KMT) beheert één persoon de portefeuille Wpg voor zowel korps Gooi en Vechtstreek als korps Flevoland. Daarnaast is een gezamenlijk projectteam aangesteld die maandelijks de voortgang van actiepunten uit het PID doorneemt en naast de rapportages van de landelijk projectleider legt. Hierin nemen de portefeuillehouder vanuit het KMT, hoofd Bureau Korpsondersteuning, de projectleider Flevoland/ Gooi en Vechtstreek, de projectcoördinator en de Privacy Functionarissen van korpsen Gooi en Vechtstreek en Flevoland plaats. Het korps kijkt vooruit en zoekt voor implementatie en borging van de Wpg ook de samenwerking met het korps Utrecht.

Algehele aandachtspunten die bij de audit binnen Politie Gooi en Vechtstreek naar voren zijn gekomen zijn:

- Op de werkvloer is behoefte aan protocollering, werkinstructies, stroomschema's etc. waarin de regelgeving van de Wpg concreet en helder wordt beschreven. Dit biedt de functionaris handvatten bij het uitvoeren van zijn dagelijkse werkzaamheden conform de Wpg.
- De informatie die wordt aangehouden op de groepsschijven en persoonlijke schijven die binnen het korps middels de kantoorautomatisering wordt gebruikt voldoet niet aan de Wpg-vereisten. Wij adviseren het korps om de inrichting van de mappenstructuur te herzien conform de Wpg.

4.1.2 *Bekendheid met de Wpg binnen de organisatie*

Politie Gooi en Vechtstreek is samen met korps Flevoland bezig met het opzetten van opleidingen voor Bevoegd Functionarissen, workshops voor de leiding en voorlichtingsbijeenkomsten voor eerst de recherche en daarna de andere dienstonderdelen. De projectcoördinator en Privacy Functionaris dienen als vraagbaak voor de rest van het korps. Vanwege de opleidingsdruk binnen het korps is er (in overleg met de docenten van de Politieacademie) voor gekozen de beoogde bevoegde functionarissen een 1 daagse cursus te geven. Dezelfde cursus wordt als opfriscursus gegeven aan degene die al wel de volledige bevoegd functionaris cursus hebben gevolgd. Hierdoor bestaat het risico dat een deel van het korps onvoldoende kennis heeft van de Wpg. Uit interviews blijkt dat in de initiële politieopleiding te weinig aandacht wordt geschonken aan het onderwerp Wpg. De opleiding voor Bevoegd Functionarissen wordt wel samen met de Politieacademie opgezet.

Het doel van de Wpg, onder voorwaarden verplicht delen van informatie, wordt nog niet algemeen onderschreven in het operationele werkveld binnen het korps. Door zowel top down als bottom up communicatie, het vastleggen van toepassingen van

de Wpg in werkinstructies en het structureel bespreken van vragen c.q. knelpunten van de Wpg tijdens werkoverleggen, zal de bewustwording van de Wpg toenemen.

De Wpg maakt onderdeel uit van het werkproces en wordt deels ook afgedwongen door het werkproces, maar komt niet als zodanig terug in iedere overweging die wordt gemaakt. Casuïstieken en Veelgestelde Vragen zijn beschreven op intranet. De vraag blijft hier wel of agenten daar ook gebruik van maken.

4.1.3 *Wpg en de praktijk*
Doordat momenteel de informatie in verschillende informatiesystemen moet worden geregistreerd en vanwege de geringe ondersteuning vanuit de informatiesystemen, wordt de Wpg binnen het korps ervaren als een toename van de administratieve last.

Schonings- en bewaartermijnen worden soms als knellend ervaren. Functionarissen willen informatie graag langer dan 1 jaar gebruiken. Doordat de informatiesystemen deze informatie na 1 jaar niet achter slot zetten, wordt de informatie in de praktijk ook vaak langer dan 1 jaar gebruikt.

4.2 Verantwoordelijke (artikel 1.f)

Mandaatbesluit

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

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

4.2.2 *Bevindingen*
Er is een Mandaatbesluit Wet politiegegevens politieregio Gooi en Vechtstreek d.d. 14 juni 2010, waarin wordt aangetoond dat het bevoegd gezag (korpsbeheerder), met terugwerkende kracht tot en met 11 maart 2009, zijn mandaat verleent aan de korpschef van het regionaal politiekorps Gooi en Vechtstreek. Daarnaast is er ook een Ondermandaatbesluit Wet politiegegevens politieregio Gooi en Vechtstreek d.d. 1 januari 2008, waarin de korpschef van Gooi en Vechtstreek ondermandaat verleent aan de districts-, divisiechefs dan wel concerndiensthoofden/hoofd bureau korpsondersteuning.

4.3 Kwaliteitsaspecten van politiegegevens (artikel 3 en 4)

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

4.3.2 *Bevindingen*
De bevindingen zullen hieronder worden gecategoriseerd in rechtmatigheid, volledigheid & juistheid en beveiliging.

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

Op het intranet van het korps Gooi en Vechtstreek is de Beslisboom Wet Politiegegevens geplaatst. Door middel van deze beslisboom kan iedereen nagaan onder welk artikel de politiegegevens verwerkt moeten worden. De beslisboom is vanuit het landelijke Wpg-project aan de korpsen beschikbaar gesteld.

Met betrekking tot artikel 8 informatie 'verwerken van politiegegevens ten behoeve van de dagelijkse politiepraktijk, zoals surveilleren, advisering over preventie, afhandelingen van de verkeersproblematiek, eenvoudig recherchewerk, verlenen van hulp en handhaven van wetten en regels' zijn geen procesbeschrijvingen aangetroffen waarin is opgenomen op welke wijze de zorg voor het voldoen aan de criteria voor deze informatie dient plaats te vinden. De volledigheid en juistheid van gegevens wordt enigszins geborgd door de verplichte invulvelden van BVH. Ook vindt er een check plaats op de persoonsgegevens met het GBA-systeem. Uit gesprekken komt naar voren dat informatie ten behoeve van de dagelijkse politiepraktijk opgeslagen wordt in privé- en groepsmappen op de kantoorautomatiseringsomgeving. Dit gebeurt bijvoorbeeld omdat mediabestanden niet in de landelijke systemen, zoals BVH, opgehangen kunnen worden. Het risico is hier dat informatie niet kan worden gedeeld.

In artikel 9 Wpg wordt gesproken over het 'gericht verwerken van politiegegevens ten behoeve van een onderzoek met het oog op de handhaving van de rechtsorde in een bepaald geval'. Hiervoor zijn geen procesbeschrijvingen aangetroffen waarin is opgenomen op welke wijze de zorg voor het voldoen aan de criteria voor deze gegevens dient plaats te vinden. Op dit gebied zijn werkinstructies voor BVO beschikbaar op intranet. Bij onduidelijkheden en vragen wordt de privacy functionaris benaderd. De juistheid en volledigheid van informatie wordt niet automatisch in het systeem gecontroleerd. Het doel van recherche-onderzoeken wordt vastgelegd in de MRO's.

De Infodesk behandelt de aanvragen voor ter beschikking stellen en verstrekkingen. Bij het behandelen van de aanvragen wordt nadrukkelijk naar het doel gevraagd. De aanvragen komen via mail, telefoon of persoonlijk binnen. De informatie wordt ook via mail of persoonlijk verstrekt. Er zijn werkinstructies en afspraken voor de Infodesk beschikbaar.

Bij de informatie verwerkende afdelingen als de CIE en de RID wordt aan deze aspecten vanwege de bijzondere aard van hun taakstelling wel specifiek aandacht besteed. Daarbij is in de opzet het voldoen aan deze criteria zeker bij de CIE vanwege de toezichthoudende rol van het OM (de CIE OvJ) en het landelijk gebruik van het proceshandboek CIE goed verzorgd.

Volledigheid
In BVH vindt een automatische check plaats op de volledigheid van de invoer van de velden. Wanneer het niet volledig is krijgt invoerder een signaal van de beheerder terug. Bij het niet aanpassen volgt er weer een signaal en na 3 signalen gaat er een melding naar de leidinggevende.

Er kunnen statistieken uitgedraaid worden voor een overzicht van het aantal keer aanpassen, doorlooptijd aanpassen etc. Dit gebeurt echter alleen op aanvraag en komt eigenlijk nooit voor. Door middel van de campagne Informatie Gestuurde Politie (IGP) probeert het korps de agenten bewust te maken van het nut van informatie delen en dat het niet in de blauwe boekjes moet blijven staan. Er staat een eenmalige schoning van de kantoorautomatisering gepland, voor afronding van het project implementatie Wpg in het voorjaar 2012.

Juistheid
Na de registratie gaat het complete verbaal naar het RIK of KWABU voor een inhoudelijke check. BVH heeft een directe link met GBA om de juistheid van de persoonsgegevens te controleren.

Beveiliging
BVH, BVO en de mappenstructuur worden beveiligd door middel van autorisaties. In de mappenstructuur is een scheiding aangebracht tussen de verschillende artikelen. De afdelingen RID en CIE zijn fysiek alleen toegankelijk voor medewerkers van deze afdeling. Echter zijn nog niet alle systemen WPG-proof. Een aantal systemen, waaronder BVH, voldoet niet aan de in de Wpg gestelde bewaartermijnen. Hierdoor ontstaat het risico op onrechtmatig gebruik van politiegegevens.

4.3.3 *Verbeterpunten*
Als verbeterpunten zijn te noemen:
- Bied praktische handreikingen aan om de politiegegevens bij binnenkomst van de politie organisatie te toetsen op de in artikel 3 en 4 genoemde kwaliteitscriteria.
- Organiseer de toezichtstaak op de kwaliteitscriteria van politiegegevens.
- Beperk de vastleggingen van politiegegevens in de kantoorautomatisering.

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.

4.4.2 *Bevindingen*
In een interview is aangegeven dat gevoelige gegevens niet als kenmerk bij een persoon worden opgeslagen, maar als kenmerk bij het incident. Er zijn binnen het korps Gooi en Vechtstreek geen richtlijnen hiervoor opgesteld. Op het intranet staat de term gevoelige gegevens wel toegelicht in de Wpg-begrippenlijst. Er heeft landelijk een discussie gespeeld over het verwerken van gevoelige gegevens. Daar kwam uit dat het wel nodig is om deze gegevens te verwerken, ook als input voor het Discriminatie Platform en om trends voor onder andere het OM te genereren. De gegevens worden daarom nu aan het incident gekoppeld. Binnen HKS worden wel gevoelige gegevens aan de persoon gekoppeld, mits in relatie tot het incident. Dit betreft met name gezondheidsgegevens, in verband met gevarenclassificatie.

4.4.3 *Verbeterpunt*
- Stel richtlijnen op voor het verwerken van gevoelige gegevens, zodat iedereen weet hoe hiermee om te gaan.

4.5 Autorisatie (artikel 6)

4.5.1 *Norm*

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

4.5.2 *Bevindingen*

Autorisatieproces

Het korps Gooi en Vechtstreek beschikt over een 'levende' autorisatiematrix die gekoppeld is aan het personeelssysteem Beaufort. In deze matrix zijn standaard relaties vastgelegd tussen enerzijds functies, organisatieonderdelen en taakaccenten en anderzijds gebruikersrollen of autorisatieniveaus op applicatie en gegevensbronnen. Dit betekent dat wanneer een medewerker van functie of afdeling wisselt, de autorisaties ook meteen worden aangepast. Zo kan een medewerker dan niet meer bij de mappen op de oude afdelingsschijf. Als een medewerker uit dienst gaat worden automatisch alle autorisaties ingetrokken.

Wijzigingen in autorisaties worden via de personeelsadviseurs doorgevoerd na schriftelijke toestemming van een leidinggevende. Elke nacht wordt Beaufort geupdate en worden mutaties doorgezet naar de autorisatiematrix en daarmee naar de applicaties. De functioneel beheerders checken dagelijks of de mutaties goed zijn doorgevoerd. Daarnaast voert functioneel beheer steekproefsgewijze controles uit op autorisaties.

De privacy functionaris houdt een overzicht bij van de externe autorisaties (andere korpsen) op basis van autorisatiebesluit. De privacyfunctionaris screent de aanvragen voor de externe autorisaties en heeft zo een volledig overzicht van alle mutaties. De mutaties op de interne autorisaties controleert de privacyfunctionaris niet. Dit gebeurt door Functioneel Beheer. Wanneer er iets niet klopt met de interne autorisaties gaat er vanuit Functioneel Beheer een signaal naar de privacyfunctionaris die het dan verder op pakt.

Proces Handhaving

De autorisaties voor BVH worden toegekend op de manier, zoals hierboven beschreven. Alle politieambtenaren op autorisatieniveau 3 en 4 kunnen de onderzoeken in BVH raadplegen. Leidinggevenden kunnen echter in BVH zaken op besloten zetten. Dan is de zaak voor buitenstaanders niet in te zien en is de informatie niet terug te vinden in Blueview. De contactpersoon van de zaak wordt wel weergegeven, zodat daar contact mee opgenomen kan worden voor meer informatie.

Logging BVH staat aan, maar is niet gebruiksvriendelijk om in te zien. BVH wordt nog niet als optimaal ondersteunend gezien, daarom wordt er nog in de KA-omgeving gewerkt. Binnen de KA-omgeving zijn er groepsschijven, afdelingsschijven en persoonlijke schijven. Deze worden niet gecheckt op het bevatten van politieinformatie. Voor onderzoeken worden groepsmappen aangemaakt. De informatie wordt daarna overgezet in BVO. Het is niet bekend of de groepsmappen daarna geschoond worden.

BPS is de voorloper van BVH en wordt momenteel uitgefaseerd tot 1 januari 2012. BPS wordt iedere maand geschoond door functioneel beheer. Alleen functioneel beheer en de privacyfunctionaris kunnen achter het schot in BPS.

Proces Opsporing
Als een onderzoek wordt gestart ten gevolge van een strafbaar feit, krijgt functioneel beheer het verzoek om een stuk database in BVO te reserveren. In deze onderzoeksaanvraag staan de namen van degenen die geautoriseerd moeten worden. Functioneel beheer zorgt ervoor dat dit gebeurt. In BVO worden per onderzoek medewerkers geautoriseerd. De medewerkers die belast worden met de dagelijkse leiding van het onderzoek, ook wel registratiebeheerder genoemd, krijgen na de onderzoeksaanvraag een autorisatie tot niveau 6 en zijn dan zelf belast voor het verder autoriseren van de andere medewerkers die tot het team behoren. Dit betekent dat de registratiebeheerder het autorisatieniveau van de medewerkers bepaalt. De andere medewerkers krijgen autorisatie tot niveau 4 voor het onderzoek. Wanneer de onderzoeken zijn afgelopen blijven medewerkers de autorisatie houden.

CIE
Autorisaties voor medewerkers van de CIE worden toegekend door het hoofd van de CIE. De CIE-officier keurt het autorisatiebeleid goed.

RID
Autorisaties voor medewerkers van de RID worden toegekend door het hoofd van de RID. [redacted]

Hiermee voldoet het autorisatiesysteem aan de vereisten van zorgvuldigheid en evenredigheid.

4.5.3 *Verbeterpunt*
Als verbeterpunt is te noemen:
- Het realiseren van een zicht op autorisaties in de KA omgeving.

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

4.6.1 *Norm*
Voor het onderzoek kunnen politiegegevens die voor dat onderzoek zijn verwerkt, geautomatiseerd worden vergeleken met andere politiegegevens die worden verwerkt op grond van artikel 8 of 9 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*
De inhoud van de activiteiten geautomatiseerd vergelijken (GV) en in combinatie met elkaar verwerken (ICMEV) is niet bij veel medewerkers binnen het korps bekend. Waar bekendheid met deze begrippen uit de Wpg wel aanwezig is, komt direct de vraag aan de orde waar de grenzen van GV en ICMEV liggen en op welke

wijze daarmee in de praktijk moet worden omgegaan. Het korps heeft geen definitie voor de begrippen vastgesteld en uitgedragen. Dit hangt samen met de discussie die momenteel op landelijk niveau gevoerd wordt over deze twee begrippen. Er is landelijk nog geen definitie vastgesteld. Wanneer dit gebeurt zal het korps Gooi en Vechtstreek deze uitdragen.

Het daadwerkelijk uitvoeren van geautomatiseerd vergelijken en in combinatie met elkaar verwerken gebeurt door algemene analisten bij de Infodesk (medewerkers van het RIK/DIK). Bij het in combinatie met elkaar verwerken wordt door het RIK niet het bevoegd gezag betrokken. De toestemming moet op voorhand al gerregeld zijn door de aanvrager, of het RIK verwijst bij gevonden informatie de aanvrager door naar de eigenaar/bevoegd functionaris. Het RIK houdt een overzicht bij van de geautomatiseerde vergelijking of het in combinatie met elkaar verwerken van politiegegevens, door middel van vastlegging van verstrekkingen en ter beschikking stellingen in BVO. Schoning van deze protocolgegevens gebeurt in de systemen, niet door het RIK.

Zoekvragen worden door leden van het korps per mail aan het RIK gesteld. Het korps hanteert daartoe geen vastgesteld format, maar er wordt door de Infodesk wel nadrukkelijk naar het doel gevraagd. Informatie wordt daarna opgehaald en in de regel per mail teruggemeld naar de aanvrager. De Infodesk is daartoe ook buiten kantooruren oproepbaar. Wanneer de tijd dringt, wordt ook wel afgeweken van bovenstaande procedure. Het komt dan ook bijvoorbeeld voor dat vragen in behandeling worden genomen die op een andere manier zijn gesteld (bijvoorbeeld ook telefonisch gestelde vragen).

De privacyfunctionaris heeft geen inzage in de vastleggingen van geautomatiseerd vergelijken en in combinatie met elkaar verwerken en voert daarop ook geen steekproef uit.

4.6.3 *Verbeterpunten*

Als verbeterpunten zijn te noemen:

- Stel procesbeschrijvingen op waarin is aangegeven hoe bij geautomatiseerd vergelijken en in combinatie met elkaar verwerken moet worden gehandeld. Geef daarbij nadrukkelijk de grenzen aan van geautomatiseerd vergelijken en in combinatie met elkaar verwerken.
- Ontwikkel casuïstiek aan de hand waarvan geautomatiseerd vergelijken en in combinatie met elkaar verwerken kan worden besproken.

4.7 Bewaartermijnen (artikel 14)

4.7.1 *Norm*

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

4.7.2 *Bevindingen*

Er wordt niet strikt op het naleven van bewaartermijnen gestuurd, mensen gebruiken informatie naar eigen inzicht. Er is geen procedure om te borgen dat dossiers in BVH, BVO en kantoorautomatisering voldoen aan de bewaartermijnen zoals gesteld in de artikelen 8 en 9 Wpg. Het risico is dat de dossiers inzichtelijk blijven voor zoekvragen, zelfs na de gestelde termijnen voor artikel 8 en artikel 9. Het afmelden van onderzoeken is niet procedureel vastgelegd. De bewaartermijn hangt af het onherroepelijk moment, maar dit wordt niet altijd door het OM teruggekoppeld. Hierdoor is het mogelijk dat de informatie langer wordt bewaard dan volgens de Wpg is toegestaan, namelijk dat het dossier nog open staat bij de politie, terwijl het bij het OM reeds is afgehandeld. Dit is niet conform artikel 9 Wpg.

Proces Handhaving

In november 2011 is de nieuwe release van BVH geïmplementeerd welke over een schoningsmodule beschikt. De schoningstermijnen zijn nog niet aangezet, hiervoor wordt op landelijk akkoord van de stuurgroep gewacht (planning 30 november 2011). Het systeem zorgt er dan voor dat informatie volgens de Wpg-richtlijnen wordt geschoond en vernietigd. Dan zal ook de poortwachtersfunctie worden aangesteld. Korps Gooi en Vechtstreek heeft BVH nu 2,5 jaar in gebruik. De vernietigingstermijn van vijf jaar is hierdoor nog niet overschreden.
BVH levert elke maand een overzichtslijst met openstaande zaken aan de leidinggevende, die checkt of de onderzoeken inderdaad nog lopen. Zo niet, worden de zaken gesloten. Functioneel beheer heeft een signaalfunctie hierin. Als onderzoeken in BVH te lang open staan en er geen mutaties meer plaatsvinden, dan krijgt eigenaar de vraag of het onderzoek afgesloten kan worden.
BPS, de voorganger van BVH, wordt iedere maand handmatig door Functioneel Beheer geschoond.

Er zitten nog geen verwijderde gegevens in BVH. In het protocol "BPS Archief Politie Gooi en Vechtstreek" is wel een procesbeschrijving over het aanvragen van een hernieuwde verwerking opgenomen. Voor een hernieuwde verwerking moet schriftelijk toestemming worden gevraagd aan het bevoegd gezag. Hernieuwde verwerkingen worden door de privacyfunctionaris en vaak ook Functioneel Beheer vastgelegd. Door de uitfasering van BPS wordt er op dit moment een nieuw protocol voor BVH gemaakt waarin de procedure rondom hernieuwde verwerking wordt beschreven. Dit zal conform het huidige protocol zijn.

Het Gemeenschappelijk Meldkamer Systeem (GMS) wordt geschoond. De informatie verdwijnt na 1 jaar achter een schot waar alleen de beheerder bij kan en wordt na 5 jaar vernietigd.

Proces Opsporing

Korps Gooi en Vechtstreek heeft sinds oktober BVO versie 2010A. De volgende versie, 2010B is Wpg-proof, maar onbekend wanneer deze bij Gooi en Vechtstreek wordt uitgerold. In BVO staan een aantal oudere zaken die overgezet zijn vanuit RBS. Dit zijn nog lopende zaken en hebben hierdoor de vernietigingstermijn nog niet overschreden.
Artikel 9 gegevens die niet langer noodzakelijk zijn voor het doel van het onderzoek worden in BVO alleen verwijderd als de zaak wordt afgemeld. Dit gebeurt echter bijna niet omdat afloopberichten maar sporadisch via het TGO binnenkomen. Dit probleem is voor het korps een attentiepunt waarmee ze aan de slag willen gaan.

Voor hernieuwde verwerkingen in BVO wordt een MRO opgemaakt. Hierdoor worden de hernieuwde verwerkingen in BVO vastgelegd.

Kantooromgeving
Mailboxen worden handmatig geschoond. Dit gebeurt niet afhankelijk van de bewaartermijnen, maar als de mailbox vol zit.

Er worden onderzoeksgegevens opgeslagen in de mappenstructuur. Er is op dit moment geen procedure om te borgen dat de informatie op de persoonlijke schijven voldoet aan de bewaartermijnen zoals gesteld in artikel 8 en artikel 9 Wpg. Op dit moment vindt er geen schoning plaats. Er zijn plannen om de KA-omgeving te schonen, naar voorbeeld van korps Zuid-Holland-Zuid. Dit houdt in dat alle bestanden in de mappenstructuur op een vooraf aangekondigd moment worden verwijderd. Dan worden ook de mailboxen meegenomen. Vervolgens wordt de mappenstructuur heringericht waardoor een scheiding ontstaat tussen de KA omgeving mét politiegegevens en de KA omgeving welke alleen bedrijfsgegevens bevat. Hierdoor kan de schoning van politiegegevens volgens de Wpg-richtlijnen gemakkelijker kan worden uitgevoerd.

Informantenregister
Informanten worden met een unieke code in het informantenregister geregistreerd. Deze code wordt gecheckt met de database van alle informanten, om te voorkomen dat een andere dienst met dezelfde informant praat. De registratie is landelijk bij het NCIE belegd. Na tien jaar, of als het niet langer noodzakelijk is voor het doel van de verwerking, worden de politiegegevens van de CIE vernietigd.

. De CIE-officier gaat tijdens een jaarlijkse controle alle bronnen langs. Hij gaat dan na of de informant genoeg informatie heeft geleverd of dat de bron is opgedroogd. Hoewel het Informantenregister periodiek wordt gecontroleerd is de schoning van het register nog niet in het systeem ingebouwd. Het gebeurt dat informanten geen contact meer opnemen of niet reageren als de politie contact met hen opneemt. Als dat het geval is, worden ze ook uit het systeem gehaald.

Informatie wordt door de CIE binnen een termijn van maximaal 4 maanden verwerkt en netto in een andere omgeving gezet. Dit zit vast in de werkwijze van de CIE.

te

RI ie, na 5 jaar wordt het vernietigd. Sommige zaken worden al eerder geschoond als het niet noodzakelijk is om de informatie te bewaren. De schoning van de mailbox gebeurt handmatig. Informatie waarvan men denkt dat die nog relevant kan zijn, laten ze staan voor een periode van maximaal 5 jaar.

4.7.3 *Verbeterpunten*

- Voer controle uit op de gegevens in de kantoorautomatisering.
- Houd beheersmaatregelen voor verwijdering en vernietiging in de systemen BVH en BVO landelijk op de agenda.

4.8 Ter beschikking stellen (artikel 15)

4.8.1 *Norm*

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

4.8.2 *Bevindingen*

Algemeen kan worden gesteld dat binnen het korps informatie tussen collega's mondeling en/of telefonisch ter beschikking wordt gesteld. Deze informatie staat vaak ook in BVH of BVO en het ter beschikking stellen wordt in deze systemen ook vastgelegd.

Het korps heeft een aantal (11) bevoegd functionarissen aangesteld. Hierbij is ervoor gekozen om slechts die personeelsleden te benoemen die ook daadwerkelijk de cursus bevoegd functionaris hebben gevolgd. De medewerkers van het RIK hebben als eerste een tweedaagse-cursus gehad. In het najaar volgen weer cursussen voor nieuwe bevoegd functionarissen. In deze cursus komen ook de wettelijke weigeringsgronden aan de orde. Er staat een praktische richtlijn voor Bevoegd Functionarissen op het intranet.

Hiernaast zijn een aantal waarborgen om het ter beschikking stellen goed te laten verlopen:

- Soms wordt het RIK ingeschakeld bij het breder verkrijgen en gebruiken van informatie. Dit gebeurt als informatie niet zonder meer beschikbaar is (bijvoorbeeld in de te raadplegen systemen). Medewerkers van de RIK leggen dan standaard contact met de bevoegd functionarissen.
- Bij het ter beschikking stellen van artikel 9 en artikel 10 informatie verwijzen de medewerkers van het RIK de aanvrager door naar de eigenaar of bevoegd functionaris. Zij delen niet zelf de informatie met de aanvrager.
- De CIE stelt slechts gegevens ter beschikking via een procesverbaal. Hiervoor is toestemming van CIE-OvJ vereist. De CIE-OvJ checkt daarom dergelijke verstrekkingen: 20% vooraf en 80% achteraf (afhankelijk van het risico). De CIE-OvJ krijgt hiertoe wekelijks een overzicht van interne ter beschikking gestelde informatie.

Binnen de Opsporingsonderdelen zijn geen algemene regels opgesteld over de coderingen van onderzoeken in verband met de mogelijkheid tot het doorzoeken van onderzoeksinformatie. Op intranet wordt het begrip codering toegelicht in de Wpg-begrippenlijst. Codering is een zwaar middel en wordt eigenlijk alleen binnen embargo-onderzoeken en de CIE gebruikt. Voor deze twee zijn wel richtlijnen opgesteld en binnen dit regime vindt ook systeem controle door het OM plaats. De CIE werkt met bruto-informatie die beperkt (binnen de CIE) raadpleegbaar is en netto-informatie die breder, ook buiten de CIE ter beschikking wordt gesteld.

4.8.3 *Verbeterpunt*

- Zorg voor voldoende opgeleide bevoegd functionarissen, verspreid over de verschillende districten en afdelingen.

4.9 Verstrekken (artikel 16/24)

4.9.1 *Norm*

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

4.9.2 *Bevindingen*

De laatste jaren heeft de informatieverstrekking vanuit het korps aan partijen buiten de politie een sterke vlucht genomen. Het aantal informatieaanvragen is sterk gegroeid.

Sommige verstrekkingen worden binnen het korps centraal verricht. Zo verlopen verstrekkingen aan het Veiligheidshuis via een vaste medewerker van het RIK. Ook wordt de privacyfunctionaris vaak betrokken. Doordat mensen de privacyfunctionaris inmiddels weten te vinden als het om dit onderwerp gaat, is deze het grootste deel van zijn tijd kwijt aan verstrekkingverzoeken. Dit gebeurt in de regel als er vragen rond het doen van verstrekkingen ontstaan. Het komt daarbij regelmatig voor dat de privacyfunctionaris het verstrekken zelf overneemt. Hij verstrekt dan in principe gegevens die in de systemen zijn opgenomen, maar soms is informatie nodig (bijvoorbeeld van wijkagenten). Deze wordt dan separaat ingewonnen.

Om de verstrekkingen te standaardiseren wordt bij verstrekkingen de landelijke verstrekkingenwijzer gehanteerd. Deze meldt welke stukken aan welk soort organisatie verstrekt mogen worden. De verstrekkingenwijzer is uitgedeeld binnen het korps en digitaal beschikbaar op intranet. In de afgesloten convenanten is opgenomen welke informatie door welke contactpersonen aan de partner verstrekt mag worden. Deze convenanten staan ook op intranet. De landelijke verstrekkingenwijzer is niet regiospecifiek gemaakt. Dit kan bijvoorbeeld door de contactpersonen binnen korps Gooi en Vechtstreek per verstrekking aan de tabel toe te voegen.

Op verschillende plaatsen binnen het korps worden overzichten bijgehouden van gedane verstrekkingen. Verstrekkingen uit BVH en uit BVO worden binnen het korps geregistreerd in hiertoe bestemde velden in deze systemen. Daarmee ontstaat overzicht van wat er uit deze systemen is verstrekt. Deze registratie is echter niet volledig. Binnen het korps wordt ook gebruik gemaakt van I90-formulieren om verstrekkingen in BVH vast te leggen en wordt gebruik gemaakt van vastleggingen in werkjournalen bij verstrekkingen afkomstig uit BVO of andere politie systemen. Andere verstrekkingen (per beveiligde mail) worden in een gezamenlijke (Outlook)bak centraal bewaard. De privacyfunctionaris houdt een overzicht bij van door hem gedane verstrekkingen. Er is geen overzicht van alle verstrekkingen. Op dit moment is er een inventarisatie van de convenanten gaande en gaat het merendeel van de verstrekkingen via het I90-formulier. Er wordt momenteel door het project Implementatie Wpg van het korps een voorlichtingsronde langs de wijkteams gemaakt om het gebruik van I90-formulieren na mondelinge verstrekking te stimuleren.

De vastleggingen van de verstrekkingen worden conform de Archiefwet bewaard. Dit kan spanning geven met de Wpg. Het is binnen het korps echter niet duidelijk welke wet voorrang heeft.

Convenanten
Binnen het korps is een nieuwe convenantenprocedure opgesteld. Deze regelt ten aanzien van het doen van verstrekkingen welke toets convenanten moeten doorlopen. Voor het traceren van bestaande convenanten is binnen het korps een oproep gedaan aan de districtschefs om deze aan te leveren aan de privacyfunctionaris. De convenanten die zijn aangeleverd, zijn getoetst op de Wpg en waar nodig aangepast en op intranet geplaatst. Binnenkort volgt het besluit dat alleen convenanten die op intranet staan, geldig zijn. De rest geldt niet meer en moet opnieuw worden afgesloten. De privacyfunctionaris toetst en mede-parafeert de convenanten en houdt zo een actueel overzicht bij.
De Procedurebeschrijving convenantenprocedure d.d. juni 2011 bevat een checklist aan de hand waarvan een convenant kan worden opgesteld die voldoet aan de Wpg. Daarnaast bevat de Procedurebeschrijving convenantenprocedure ook een modelconvenant waarbij de plicht tot geheimhouding een onderdeel is.

4.9.3 *Verbeterpunten*

- Zorg voor beheersmaatregelen die gericht zijn op een volledige registratie van verstrekkingen door middel van I90 formulieren uit BVH en andere vastleggingen in BVO.
- Zorg voor toezicht op alle vastleggingen van de verstrekkingen.
- Maak de landelijke verstrekkingenwijzer regiospecifiek, door bijvoorbeeld een extra tabel met de contactpersonen binnen korps Gooi en Vechtstreek toe te voegen.

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*
Het korps Gooi en Vechtstreek heeft een procedure voor rechten van betrokkenen. Alle verzoeken met betrekking tot rechten van betrokken, zoals inzagerecht van burgers, gaan via de privacyfunctionaris.

De privacyfunctionaris heeft een overzicht van het aantal ontvangen klachten over de inzageverzoeken. In 2011 ging dat om één klacht. De privacyfunctionaris heeft ook een overzicht van het aantal correcties van gegevens in 2010 en 2011. In 2010 waren er 115 correcties en in 2011 tot nu toe 84 correcties. Naast de eigen overzichten, krijgt de privacyfunctionaris ook een aantal gegevens aangeleverd door Functioneel Beheer.

4.10.3 *Verbeterpunt*

- Zie toe op en rapporteer over verbetering, aanvulling en verwijdering van politiegegevens.

4.11 Protocolplicht (artikel 32)

4.11.1 *Norm*

De verantwoordelijke draagt zorg voor de schriftelijke vastlegging van:

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

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

4.11.2 *Bevindingen*

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

De privacyfunctionaris houdt een overzicht bij van de artikel 9 doelen. In 2010 is door de privacyfunctionaris verschillende malen gewezen op de noodzaak om verbeteringen door te voeren in de beschrijving van artikel 9 doelen. Met name het aanmelden van de doelen en het afmelden van afgesloten artikel 9 verwerkingen liet sterk te wensen over. Dit functioneert nog steeds niet optimaal.

De privacyfunctionaris houdt geen overzicht bij van artikel 13 verwerkingen. Binnen het korps wordt dit gedaan door het RIK. De privacyfunctionaris kan hierop terugvallen.

De privacyfunctionaris houdt eveneens geen overzicht bij van onrechtmatige verwerkingen. Hij toetst wel aanvragen voor externe autorisaties en stuurt deze terug naar de lijnchef als ze niet kloppen. Onrechtmatigheid wordt daarmee voor een deel aan de voorkant van werkprocessen ondervangen.

Bureau Integriteit houdt geen overzicht bij van verwerkingen waarvan aanwijzingen bestaan dat zij door onbevoegden of anderszins onrechtmatig zijn verricht. Er wordt alleen op een aanleiding geacteerd. Om te voorkomen dat agenten zelf in systemen informatie over buren of iets dergelijks gaan opvragen is er preventief een formulier ontwikkeld waarmee de agenten een aanvraag bij Bureau Integriteit kunnen doen. Dit is een preventieve code Blauw- actie (integriteitsbeleid) die door het korps zelf is opgesteld. Bureau Integriteit toetst, soms in overleg met de privacyfunctionaris, de aanvragen.

Gemeenschappelijke verwerkingen gebeuren binnen het korps in korps-overstijgende TGO's. Wanneer in een TGO meerdere korpsen samenwerken is het korps van de TGO-leider verantwoordelijk. De andere TGO-leden krijgen daar externe autorisaties die door de privacyfunctionaris worden getoetst. Deze verwerkingen worden niet aangemeld bij het CBP omdat de eindverantwoordelijkheid bij een korps belegd is.

4.11.3 *Verbeterpunt*

- Zorg ervoor dat de privacyfunctionaris toegang tot alle overzichten van alle verwerkingen heeft.

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*

Binnen het korps Gooi en Vechtstreek heeft er geen interne audit plaats gevonden. Wel hebben een aantal medewerkers in het verleden een audit-cursus gevolgd.

4.12.3 *Verbeterpunten*

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

4.13 Privacy functionaris (artikel 34)

4.13.1 *Norm*

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

4.13.2 *Bevindingen*

De privacyfunctionaris is middels Mandaatbesluit Wet politiegegevens Privacy Functionaris, politieregio Gooi en Vechtstreek d.d. 1 januari 2008 formeel aangewezen door de korpsbeheerder. De eerste privacyfunctionaris is op 10-11-2008 aangemeld bij het CBP en de huidige privacyfunctionaris is op 01-12-2010 aangemeld bij het CBP.

De functie van privacyfunctionaris is binnen korps Gooi en Vechtstreek een stapelfunctie. Dit betekent dat de privacyfunctionaris niet specifiek voor deze functie is vrij gemaakt. Daardoor kan de privacyfunctionaris de taak conform de wettelijke regels voor advies en toezicht niet uitvoeren. Er is onvoldoende tijd voor controle en advies.

De privacyfunctionaris voert de volgende taken uit:

- Overzicht bijhouden van artikel 9 doelen, zowel digitaal als fysiek;
- Voor artikel 9 het toetsen van de volledigheid van de aanvraag, wat er verder in staat wordt door de bevoegd functionaris gedaan;
- Het maken van het privacy jaarverslag;
- Het maken van een overzicht van artikel 6 (externe autorisaties);
- Het bijhouden van het overzicht artikel 9 verwerkingen. Registratiebeheerder staat aan het hoofd van een onderzoek en doet de aanvraag bij FB BVO, welke vervolgens de registratie aanmaakt;

- Het controleren van de ingediende autorisaties op het doel, welke mensen van welke gremia toegang hebben tot de module en of er toestemming van de verantwoordelijke is;
- Verstrekkingsverzoeken, hier is de privacyfunctionaris de meeste tijd mee kwijt;
- Bijhouden van verstrekkingen aan derden (paragraaf 3);
- Een overzicht bijhouden van de gegevens krachtens artikel 25 Wpg in verband met artikel 4 BPG (= recht van betrokkenen).

De volgende taken worden niet door de privacyfunctionaris uitgevoerd:

- Overzicht artikel 13(4) wordt niet door de privacyfunctionaris bijgehouden, maar door het RIK;
- Overzicht van artikel 11 wordt ook door het RIK gedaan, niet door de privacyfunctionaris.

4.13.3 Aanbevelingen

- Borg de toezichthoudende taak van de privacyfunctionaris, zoals in de Wpg benoemd.

4.14 Functionaris Gegevensbescherming (artikel 36)

De Functionaris Gegevensbescherming bestaat niet als functie bij het korps Gooi en Vechtstreek.