
Externe Audit Wet Politiegegevens Koninklijke Marechaussee 2011

12 januari 2012
Referentie: 2011-
0057/

Definitief

Inhoudsopgave

Assurance verklaring	3
Audit rapport	4
1. Samenvatting	5
2. Algemeen	11
2.1. Aanleiding	11
2.2. Doelstelling, aard en scope van de opdracht	11
2.3. Afbakening	12
2.4. Normenkader	12
2.5. Inherente beperkingen voor de privacy audit	12
2.6. Onderzoeksmethoden en werkwijze	12
2.7. Doelgroep van het rapport	13
3. Bevindingen	14
3.1. Inleiding	14
3.2. Overkoepelende bevindingen	14
3.2.1. Centrale regie voor de Wpg implementatie en doorzettingsmacht	14
3.2.2. Bekendheid met de Wpg binnen de organisatie	14
3.3. Bevindingen per artikel	15
3.3.1. Verantwoordelijke/Mandaatbesluit (artikel 1f)	15
3.3.2. Kwaliteitsaspecten van politiegegevens (artikel 3 en 4)	15
3.3.3. Gevoelige gegevens (artikel 5)	16
3.3.4. Autorisatie (artikel 6)	16
3.3.5. Geautomatiseerd Vergelijken (GV)/In Combinatie Met Elkaar Verwerken (ICMEV)(artikel 11)	17
3.3.6. Bewaartermijnen (artikel 14)	18
3.3.7. Ter beschikking stellen (artikel 15)	19
3.3.8. Verstrekken van politiegegevens (artikel 16)	20
3.3.9. Rechten van betrokkenen (artikel 25/28)	20
3.3.10. Protocolplicht (artikel 32)	21
3.3.11. Audits (artikel 33)	22
3.3.12. Privacyfunctionaris (artikel 34)	22
3.3.13. Functionaris Gegevensbescherming (artikel 36)	22
A. Geïnterviewde medewerkers	23
B. Ontvangen documentatie	24
C. KMar in Nederland	25
D. Gehanteerde afkortingen	26

Assurance verklaring

In het jaar 2011 heeft PwC in opdracht van de waarnemend directeur van de Auditdienst van het Ministerie van Defensie namens de minister van Defensie, een privacy audit op grond van de Wet politiegegevens (Wpg) uitgevoerd naar de verwerkingen die in de Wpg zijn beschreven bij de Koninklijke Marechaussee (KMar) in Nederland. Deze privacy audit is in november en december 2011 uitgevoerd bij de KMar te Den Haag en Amsterdam.

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 van politiegegevens bij de KMar in Nederland.

Dit onderzoek is uitgevoerd conform de richtlijn 3600, 'Assurance-opdrachten met betrekking tot de bescherming van persoonsgegevens (privacy audits)' van juni 2006, van 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 de Koninklijke Marechaussee in Nederland, naar de stand van ultimo december 2011 c.q. over 2011, in opzet, bestaan en werking niet 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 de Koninklijke Marechaussee te nemen maatregelen.

Ook is gebleken dat het volledig kunnen voldoen aan de Wpg eisen mede afhankelijk is van besluiten die buiten de KMar dienen te worden genomen. Tekortkomingen op deze vlakken hebben uiteindelijk mede geleid tot het geformuleerde oordeel.

De verantwoordelijke, zijnde de Commandant Koninklijke Marechaussee, is op grond van artikel 4 lid 1 van de Regeling Periodieke Audit Politiegegevens, verplicht binnen drie maanden een verbeterrapport op te stellen waarin de maatregelen worden beschreven die getroffen zijn ter verbetering van de in de privacy audit geconstateerde tekortkomingen. Op grond van artikel 4 lid 3 dient hercontrole plaats te vinden.

Wij adviseren die hercontrole te laten uitvoeren door de interne auditors van de Koninklijke Marechaussee. Het verbeterrapport en de uitgevoerde hercontrole zullen in de navolgende jaren door de privacyauditor worden beoordeeld.

Den Haag, 13 januari 2012

PricewaterhouseCoopers Advisory N.V.

Partner

Audit rapport

Het hierna volgende audit rapport hoort bij de assurance verklaring waarin wij verklaren in welke mate het stelsel van maatregelen en procedures gericht op de bescherming van de politiegegevens, betrekking hebbende op de in de Wpg genoemde artikelen bij de Koninklijke Marechaussee in Nederland, naar de stand van ultimo december 2011 c.q. over 2011, in opzet, bestaan en werking voldoet aan de vereisten zoals genoemd in de Wpg.

De assurance verklaring is een verklaring gericht op het maatschappelijk verkeer. Het audit rapport is vertrouwelijk en niet bestemd voor het maatschappelijk verkeer, maar voor het management van de KMar voor het nemen van beslissingen met betrekking tot verbetermaatregelen.

1. Samenvatting

Deze audit heeft zich gericht op de opzet, het bestaan en waar mogelijk, de werking van de implementatie van de Wet politie gegevens (Wpg) bij de Koninklijke Marechaussee in Nederland. Voor deze audit hebben wij gesteund op de door de afdeling Onderzoeken Interne Beheersing (OIB) uitgevoerde audits en onderzoeken over 2010 en 2011. De werkzaamheden bestaan uit dossier en document reviews van de door OIB uitgevoerde werkzaamheden en aanvullende interviews en documentanalyse.

Wij hebben onze werkzaamheden uitgevoerd in de maanden november en december 2011. Het concept rapport met bevindingen is 2 januari 2012 besproken met ** 10,2,2 LOKB* en op 13 januari 2012 vastgesteld.

De Koninklijke Marechaussee heeft in opzet, op hoofdlijnen, zorggedragen voor een borging van de invoering van de Wet politie gegevens. Door middel van Wijzers, de opleiding Bevoegd functionaris LOCKMar, mandaatbesluit, de benoeming van een privacyfunctionaris en de Helpdesk Wpg van SJZ/Privacyfunctionaris zijn verantwoordelijkheden en bevoegdheden bepaald. Eveneens hebben diverse interne audits plaatsgevonden waarin de status van getroffen maatregelen is bepaald. Op basis van deze status zijn verbeterplannen opgesteld en zijn twee Project Initiatie Documenten (PID's) opgesteld met als doel het verbeteren van het autorisatie beheer en het aanpassen van ICT-systemen.

Deze plannen hebben echter (nog) niet geleid tot een invulling van het stelsel van maatregelen en procedures gericht op de bescherming van de politiegegevens dat voldoet aan de bepalingen in de Wpg. De invoering van de Wpg is nog niet gedetailleerd genoeg gebeurd en de systemen die gebruikt worden, het autorisatiebeheer en districtonderdelen zijn nog niet zodanig ingericht dat wordt voldaan aan de gestelde eisen.

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 de KMar, in opzet, bestaan en werking niet heeft voldaan aan de vereisten zoals genoemd in de Wpg. Verbetering is noodzakelijk.

Wij adviseren de onderdelen 'do' en 'act' van de plan- do- check- act-management cyclus beter te borgen zodat invulling gegeven wordt aan de gemaakte plannen en opvolging gegeven wordt aan de uitkomsten van audits en controles.

De bevindingen vanuit deze privacy audit zijn hieronder samengevat per artikel/lid 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, maar er is een acceptabel actieplan inclusief planning en staffing.
- Rood = Er wordt niet voldaan aan de norm en er is geen acceptabel actieplan.
- Grijs = Niet van toepassing.

Norm	Aspect	Kleur	Bevinding en oordeel (opzet, bestaan, werking)
Artikel 1.f, Verantwoordelijke			
1.f	Mandaatbesluit		Er is een getekend mandaatbesluit waarin bevoegdheden zijn vastgelegd.

Artikel 3 en 4, Kwaliteitsaspecten van politiegegevens			
8.1 en 9.1	Onderscheid onderzoek Dagelijkse Politietaken (8) versus Bepaald geval (9)		Procedures voor borging van de kwaliteit zijn in opzet op hoofdlijnen vastgelegd in de verstrekkingen en operationele Wpg-wijzer. De aard en diepgang van deze beschrijvingen zijn niet voldoende om eenduidige interpretatie voor een juiste, volledige, rechtmatige en noodzakelijke vastlegging te waarborgen. Het integreren van de Wpg in de procesbeschrijvingen en werkinstructies (invoerafspraken) is (nog) niet gerealiseerd.
3.1 t/m 3.3 (8) 4.1 (8)	Noodzakelijkheid (8) Doelbinding Rechtmatigheid Juistheid Volledigheid		
3.1 t/m 3.4 (9) 4.1 (9)	Noodzakelijkheid (9) Doelbinding Rechtmatigheid Herkomst en wijze van verkrijging Juistheid Nauwkeurig Volledigheid		Binnen de KMar worden zowel door het BIK als het bureau gegevensbeheer van CR&I activiteiten uitgevoerd om de kwaliteit van politiegegevens te controleren en te verbeteren. Activiteiten zijn bijvoorbeeld het opstellen van monitors en het gebruik van de Tool Signalen Gegevensbeheer. Deze worden (nog) niet KMar-breed voor alle verwerkingen ingezet. Ook vindt opvolging van geconstateerde fouten niet altijd plaats.
3.4 (10 en 12) 4.1 (10 en 12)	Noodzakelijkheid (10 en 12) Doelbinding Rechtmatigheid Herkomst en wijze van verkrijging Juistheid Nauwkeurig Volledigheid		
4.3	Beveiliging (isolatie)		Niet alle systemen zijn geaccrediteerd; bevindingen uit accreditaties zijn (nog) niet in alle gevallen opgevolgd. Er zijn bij functioneel beheer (nog) geen eenduidige (schriftelijke) processen opgesteld.
Artikel 5, Gevoelige gegevens			
• Gevoelige gegevens			De norm is opgenomen in de Wpg-wijzer als algemeen uitgangspunt. Hoe de vertaling hiervan in de dagelijkse praktijk dient plaats te vinden, is niet beschreven.
Artikel 6, Autorisatie			
• Autorisatiematrix			Op hoofdlijnen is de norm deels omschreven in de Wpg-wijzer. Er zijn echter geen organisatie specifieke autorisatiematrices, procesbeschrijvingen voor het aanvragen, toekennen, controleren en opschonen van autorisaties. De verantwoordelijkheid hiervoor wordt op verschillende wijze vormgegeven. Aanvragen per e-mail worden bewaard, maar de aansluiting met systemen, rollen, taken en medewerkers is niet (op eenvoudige wijze) te maken. Een PID is (in concept) opgesteld ter verbetering van de autorisaties.
• Aanvraagproces			
• Reconciliatie en schoning			
• Verwijderen			
• Autorisatiebeheer CIE			
32.1.c	Protocollering autorisaties		
32.3 voor 32.1.c	Bewaren protocolgegevens autorisaties		

Artikel 11, Geautomatiseerd vergelijken en in combinatie zoeken			
• Hanteerbare interpretatie			In de Operationele Wpg-wijzer zijn de definities van 'Geautomatiseerd vergelijken' en 'In combinatie verwerken' opgenomen.
• Aangewezen functionarissen			In de Operationele Wpg-wijzer, zijn bij de definities van 'Geautomatiseerd vergelijken' en 'In combinatie verwerken' verantwoordelijke functionarissen en afdelingen aangewezen. Nadere uitwerkingen in werkinstructies over de wijze waarop zij hier invulling aan dienen te geven, zijn niet beschikbaar. Hierdoor kan niet op adequate wijze invulling gegeven worden aan protocollering en bewaarplicht.
11.4	Bevoegd gezag		
32.1.d	Protocollering 11.1, 11.2 en 11.4		
32.3 voor 32.1.d	Bewaren protocolgegevens 11.1, 11.2 en 11.4		
11.5	Andere gegevens		
32.1.h	Protocollering 11.5		Een overzicht van geautomatiseerde vergelijkingen of het in combinatie met elkaar verwerken wordt nog niet bijgehouden door de privacyfunctionaris.
32.3 voor 32.1.h	Bewaren protocolgegevens 11.5		
Artikel 14, Bewaartermijnen			
8.2 en 8.3	(8) van 1 tot 5 jaar		In de operationele Wpg-wijzer is per artikel, dat een doel voor verwerking van politiegegevens formuleert, de levensloop van gegevens aangegeven inclusief een proces voor verwijdering en vernietigen/archiveren beschreven. Hierbij zijn de verantwoordelijkheden weergegeven in het proces. Ook zijn diverse formulieren op intranet beschikbaar.
8.6	(8) verwijderen na 5 jaar		
14.1 (8)	(8) vernietigen na 5 jaar verwijderd		
9.4	(9) verwijderen na onherroepelijk (OH) plus ½ jaar		
14.1 (9)	(9) vernietigen na 5 jaar verwijderd		
10.6	(10) verwijderen na 5 jaar geen subjectwaardige registratie		Met uitzondering van BPS hebben de meeste gebruikte computersystemen niet de functionaliteit om geautomatiseerd gegevens te verwijderen of af te schermen. Binnen BPS worden mutaties na 5 jaar in een archief omgeving gezet, waar de toegang toe beperkt is. Deze 'archivering' houdt geen rekening met het type verwerking.
14.1 (10)	(10) vernietigen na 5 jaar verwijderd		
14.3	Hernieuwde verwerking		Operationele werkinstructies voor vernietigen, schonen, hernieuwd verwerken en protocolleren zijn niet beschikbaar of niet goed bekend.
32.1.e	Protocollering 14.3		
32.3 voor 32.1.e	Bewaren protocolgegevens 14.3		Hernieuwde verwerking komt (nog) niet voor. Wel is een formulier beschikbaar om deze te melden.
12.2	(12) verwijderen na 4 maanden		Artikel 12 gegevens worden niet vernietigd, wel verwijderd.
12.6	(12) controleren en vernietigen		
			Aan handmatige schoning en archivering wordt niet structureel invulling gegeven. Gegevens zijn algemeen toegankelijk binnen de verschillende systemen. Controle op het verwijderen en vernietigen van gegevens wordt niet structureel uitgevoerd.
			Een PID is opgesteld om de applicaties aan de Wpg aan te passen.

Artikel 15, Ter beschikking stellen		
• Infodesk voor bevraging		Het proces van ter beschikking stellen en welke partijen daarbij betrokken zijn, is op hoofdlijnen vastgelegd in de operationele wijzer en het handboek BF.
• Aanwijzing Bevoegd Functionaris		Hierin is aangegeven dat gegevens ter beschikking worden gesteld door de Infodesk, met toestemming van de bevoegd functionaris. Bij het ter beschikking stellen van gegevens door de CIE wordt de kwaliteit van de gegevens gecontroleerd. Nadere schriftelijke werkafspraken en instructies van de werkwijze van de Infodesk zijn niet beschikbaar.
• Opleiding Bevoegd Functionaris		In principe zouden in de periode 2008-2011 alle BF en medewerkers BIK de BF een opleiding hebben gevolgd. Een actueel overzicht van alle medewerkers die als BF fungeren en zijn opgeleid is echter niet beschikbaar.
15.2	Weigeringgronden	Een concept document met betrekking tot deze norm is in het Handboek Bevoegde Functionarissen opgenomen, echter dit is nog niet vastgesteld en verspreid.
Artikel 16 t/m 24, Verstrekking		
• Verstrekkingenwijzer, verstrekkingenschema		De verstrekkingenwijzer beschrijft wie binnen de KMar bevoegd is verstrekkingen te doen, aan wie, en onder welke voorwaarden. Eveneens zijn diverse (technische) handleidingen beschikbaar. Actuele procesbeschrijvingen/werkinstructies die zijn toegespitst op verschillende functies zijn niet beschikbaar.
• Convenanten en Artikel 20 Besluiten		Voor structurele verstrekkingen in samenwerkingsverbanden worden convenanten opgesteld. Hiervoor zijn richtlijnen aanwezig. De privacyfunctionaris houdt een centraal overzicht bij. Een overzicht van de actualiteit van de convenanten actueel is niet beschikbaar. Eveneens is de inhoud van de convenanten niet altijd goed bekend bij de betrokkenen.
• Proces voor geautomatiseerde verstrekking		
7.2	Geheimhouding	De geheimhoudingsplicht wordt niet in alle gevallen kenbaar gemaakt aan de ontvangers van gegevens.
32.1.f	Protocollering verstrekking	De verstrekkingenwijzer geeft invulling aan welke gegevens geprotocolleerd moeten worden. In de praktijk worden niet alle verstrekkingen op juiste wijze geprotocolleerd, omdat criteria niet bekend zijn bij de medewerkers. Instructies voor het bewaren van protocolleringen zijn niet aanwezig.
32.3 voor 32.1.f	Bewaren protocolgegevens verstrekking	
• Toezicht door leidinggevend op verstrekkingen en protocollering		Structurele controle op verstrekking en de protocollering daarvan vindt niet plaats.

Artikel 25 t/m 31, Rechten van de betrokkene			
25.1	Verzoek om kennisneming		De Operationele Instructie Rechten betrokkene Wpg (2010) bevat een procesbeschrijving van inzage verzoeken, verantwoordelijkheden en borging. Deze wordt in de praktijk nageleefd.
28.1 t/m 28.3	Correctie		De Operationele Instructie Rechten betrokkene Wpg (2010) bevat een procesbeschrijving van correctie verzoeken en daarbij horende mededelingen. Deze wordt in de praktijk nageleefd.
Artikel 32, Protocolplicht (32.1.c, d, e, f en h behandeld bij thema's)			
9.2 en 32.1.a	Protocollering doel onderzoek		Er zijn Handboeken opsporing - startmutatie en maken MRO. Hierin wordt ingegaan op het vastleggen van het doel van het onderzoek. Op deze wijze wordt invulling gegeven aan de protocollering van het doel van het onderzoek.
32.3 voor 32.1.a	Bewaren protocolgegevens doel onderzoek		Zie bewaartermijnen.
13.4 en 32.1.b	Protocollering Artikel 13 gegevensverzamelingen		(Nog) niet voor alle artikel 13 verwerkingen zijn vastgestelde instellingsprotocollen aanwezig.
32.3 voor 32.1.b	Bewaren protocolgegevens Artikel 13 gegevensverzamelingen		Zie bewaartermijnen.
32.1.g	Protocollering onrechtmatige handeling		Er is een formulier beschikbaar op intranet voor onrechtmatige verwerkingen. Melding aan de privacyfunctionaris vindt niet altijd plaats. Instructies / procedures voor het bewaren zijn niet beschikbaar.
32.3 voor 32.1.g	Bewaren protocolgegevens onrechtmatige handeling		
32.2	Gemeenschappelijke verwerking		In de Wpg-wijzer wordt uiteengezet hoe omgegaan dient te worden met gemeenschappelijke verwerkingen. Voor gemeenschappelijke verwerking is een formulier 'melding gemeenschappelijke verwerking' op intranet beschikbaar gesteld. Aangegeven wordt dat deze in de praktijk niet voor komen.
Artikel 33, Audits			
RPAP 3.1	Interne audit-functie		De afdeling OIB verzorgt periodiek onderzoeken en audits naar de invoering van de Wpg binnen de KMar.
RPAP 3.4	Intern audit-plan		Voorafgaand aan het onderzoek, of de audit wordt een plan opgesteld.
RPAP 3.6	Intern audit-rapport		Op basis van de rapportages worden actieplannen opgesteld, de voortgang wordt periodiek door de afdeling OIB onderzocht.

Artikel 34, Privacyfunctionaris			
34.1 en 34.4	Benoemd en gemeld		Een privacy functionaris is benoemd en gemeld.
34.2	Overzicht over protocollering		Niet voor alle typen protocolleringen is een overzicht beschikbaar op basis waarvan een controle wordt uitgevoerd.
34.3	Jaarverslag		De privacyfunctionaris heeft een meerjaren verslag opgesteld over de periode 2008 – 2010.
Artikel 36, Functionaris Gegevensbescherming (Optioneel)			
36.1 en 36.2	Benoemd		N.v.t. Er is geen functionaris gegevensbescherming benoemd.
Wbp 63.3	Gemeld		N.v.t. Er is geen functionaris gegevensbescherming benoemd.
Wbp 64.1 t/m 64.4	Toezichthoudende rol		N.v.t. Er is geen functionaris gegevensbescherming benoemd.

2. Algemeen

In opdracht van waarnemend Directeur Auditdienst Defensie (ADD), namens de minister van Defensie, heeft PwC een privacy audit uitgevoerd bij de Koninklijke Marechaussee in Nederland zoals deze, uit hoofde van de Wpg, iedere vier jaar dient te worden uitgevoerd.

De opdracht is beschreven in het document 'Externe Audit Wpg Voorstel voor een externe audit Wpg Koninklijke Marechaussee' d.d. 15-11-2011 met kenmerk 2011-2053

De audit is uitgevoerd bij de Koninklijke Marechaussee te Den Haag en Amsterdam in de maanden november en december 2011.

2.1. Aanleiding

De 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.

PwC is in november 2011 benoemd als de externe auditor voor de audit naar de implementatie van de Wpg voor de Koninklijke Marechaussee in Nederland. In opdracht van de waarnemend Directeur Auditdienst Defensie, namens de minister van Defensie, voert PwC de privacy audit uit bij de Koninklijke Marechaussee in lijn met 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 opgenomen hebben.

2.2. Doelstelling, aard en scope van de opdracht

Deze privacy audit heeft tot doel 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 de Koninklijke Marechaussee.

De privacy audit richt zich op de opzet, het bestaan en indien van toepassing de werking, per ultimo december 2011 c.q. over 2011, van maatregelen en procedures, waarmee de Koninklijke Marechaussee in Nederland 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 bij de Koninklijke Marechaussee in Nederland. Pas wanneer wij, tijdens het uitvoeren van de audit, hebben geconstateerd dat de opzet en het bestaan aan de daaraan te stellen eisen voldoen, hebben wij de werking beoordeeld.

2.3. 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 de verwerking van politiegegevens voor zover deze plaatsvinden bij de Koninklijke Marechaussee in Nederland. In bijlage C is aangegeven wat wij in het kader van dit onderzoek verstaan onder KMar in Nederland.

2.4. Normenkader

Dit normenkader voor de privacy audit is afgeleid uit de navolgende documenten en is afgestemd met de opdrachtgever en de KMar.

- a) Wet politiegegevens, de wet van 21 juli 2007, houdende regels inzake de bescherming van politiegegevens.
- b) Besluit politiegegevens, besluit van 14 december 2007, houdende bepalingen ter uitvoering van de Wet politiegegevens.
- c) 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.

2.5. Inherente 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 op basis van het gehanteerde normenkader.

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.

2.6. Onderzoeksmethoden en werkwijze

De privacy audit is uitgevoerd conform de richtlijnen voor het uitvoeren van IT audits van de Nederlandse Orde van IT Auditors (Norea Richtlijn 3600).

Het onderzoek is uitgevoerd op basis van dossier en document reviews van door de afdeling Onderzoeken Interne Beheersing (OIB) uitgevoerde audits en onderzoeken over 2010 en 2011 en aanvullende interviews en documentanalyse (zie Bijlage).

Wij hebben onze werkzaamheden uitgevoerd in de maanden november en december 2011.

Het conceptrapport met bevindingen is op 2 januari 2012 besproken met de heer R. Daalder en mevrouw K. van Gessel en op 13 januari 2012 vastgesteld.

Het eindrapport is met inachtneming van het ontvangen commentaar vastgesteld.

2.7. Doelgroep van het rapport

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

Wij voeren deze audit uit in opdracht van waarnemend Directeur Auditdienst Defensie, namens de minister van Defensie.

De specifieke doelgroep waarvoor het rapport is bestemd bestaat uit:

- Onze opdrachtgever zoals bovengenoemd.
- De minister van Defensie
- De Secretaris Generaal
- De Commandant KMar
- De privacyfunctionaris van de KMar
- De voorzitter van het College Bescherming Persoonsgegevens.

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

Het rapport mag uitsluitend met toestemming van PwC aan derden ter beschikking worden gesteld.

3. Bevindingen

3.1. 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.

3.2. Overkoepelende bevindingen

3.2.1. Centrale regie voor de Wpg implementatie en doorzettingsmacht

De invoering van de Wpg binnen de KMar is nog een proces in uitvoering, waarbij er meerdere goede stappen zijn genomen, maar er zijn ook nog meerdere acties noodzakelijk om risico's af te dekken. Voornaamste zorgpunten zijn gebruikte systemen en autorisaties en de verdere detaillering in werkprocessen. Voor het aanpassen van systemen en autorisaties zijn inmiddels Project Initiatie Documenten (PID's) opgesteld. Deze zijn echter nog niet goedgekeurd. Eveneens wordt door de projectleider Wpg aangegeven dat de vrijgemaakte (financiële en personele) middelen onvoldoende zijn.

De benoeming van een privacyfunctionaris en het uitvoeren van interne audits zijn belangrijke stappen om aan de Wpg te (gaan) voldoen. De privacyfunctionaris heeft op dit moment vooral een adviserende functie en geeft (nog) geen structurele invulling aan controlerende taken.

Binnen de jaarplannen van de districten is geen structurele aandacht voor doelstelling in relatie tot de Wpg. Centrale regie welke de voortgang op verbeteringen bewaakt en overzicht heeft op de status ontbreekt. Door het ontbreken van een goedgekeurd PID en voldoende middelen en structurele controle wordt de doorzettingsmacht voor het invoeren van de Wpg belemmerd.

Verbeterpunten

Wij adviseren de onderdelen 'do' en 'act' van de plan- do- check- act-management cyclus beter te borgen zodat invulling gegeven wordt aan de gemaakte plannen en opvolging gegeven wordt aan de uitkomsten van audits en controles.

Wij adviseren dit onder andere te doen door doelstellingen rondom de Wpg te definiëren en de opgestelde PID's zo spoedig mogelijk te beoordelen en (na de beoordeling) goed te keuren zodat systemen en autorisaties aangepast kunnen worden. Dit moet het werken conform de Wpg voor de operationele medewerkers vergemakkelijken en kan de focus van de privacyfunctionaris verschuiven van advies naar controle.

3.2.2. Bekendheid met de Wpg binnen de organisatie

Bevindingen

Een groot deel van de medewerkers van de Koninklijke Marechaussee is over de Wpg geïnformeerd via opleiding, training of instructie binnen de brigades. Echter, een belangrijk deel van alle medewerkers van de KMar is op dit moment onvoldoende bekend met de gevolgen die dit heeft voor de dagelijkse praktijk of ervaart de Wpg en bijbehorende werkwijze als multi-interpretabel, mede vanwege de geringe ondersteuning vanuit de informatiesystemen.

Verbeterpunten

Verbeter de bekendheid met de Wpg binnen de organisatie verder door de Wpg vast onderdeel van opleiding, communicatie, training en evaluatie te maken.

3.3. Bevindingen per artikel

3.3.1. Verantwoordelijke/Mandaatbesluit (artikel 1f)

Norm

De Commandant KMar heeft de bevoegdheden benodigd voor de verwerking van politiegegevens conform de Wpg doorgemandateerd.

Bevindingen

De Commandant KMar is door de minister van Defensie gemandateerd als verantwoordelijke. De KMar heeft een mandaatbesluit opgesteld waarin de verantwoordelijkheden zijn (door)gemandateerd. Zo is in het mandaatbesluit de verantwoordelijkheid voor het gegevensbeheer, het verstrekken van politiegegevens aan derden en het nemen van beslissingen aangaande het verstrekken van gegevens neergelegd bij de BCR&I. Het beheer van de verstrekkingenwijzer is neergelegd bij SJZ. In het mandaatbesluit worden ook de bevoegde functionarissen aangewezen.

Verbeterpunten

Geen.

3.3.2. Kwaliteitsaspecten van politiegegevens (artikel 3 en 4)

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).

Bevindingen

Bij het starten van een (art 9) onderzoek wordt een Melding Recherche Onderzoek 'MRO' aangemaakt waarin het doel van het onderzoek wordt vastgelegd. Deze werkwijze is opgenomen in Handboeken opsporing - startmutatie en maken MRO. Er bestaat geen duidelijke richtlijn voor het maken van onderscheid tussen artikel 8 of 9 verwerkingen.

Procedures voor borging van de kwaliteit zijn in opzet op hoofdlijnen vastgelegd in de Verstrekkingen- en Operationele Wpg-wijzer. De aard en diepgang van deze beschrijvingen zijn niet voldoende om eenduidige interpretatie voor een juiste, volledige, rechtmatige en noodzakelijke vastlegging te waarborgen. Het integreren van de Wpg in de procesbeschrijvingen en werkinstructies (invoerafspraken) is (nog) niet gerealiseerd.

Binnen de KMar worden zowel door het BIK als het bureau gegevensbeheer van CR&I activiteiten uitgevoerd om de kwaliteit van politiegegevens te controleren en te verbeteren. Activiteiten zijn bijvoorbeeld het opstellen van monitors en het gebruik van de Tool Signalen Gegevensbeheer. Deze worden nog niet voor alle type verwerkingen KMar-breed ingezet. Eveneens vindt opvolging van geconstateerde fouten niet altijd plaats. De verantwoordelijkheden voor gegevenskwaliteit zijn belegd in mandaatbesluit en de wijzers.

De afdeling OIB heeft in 2010 een deelwaarneming uitgevoerd of door BIK uitgevoerde controles goed uitgevoerd werden. Hieruit zijn diverse constatering naar voren gekomen met betrekking tot juistheid en nauwkeurigheid van ingevoerde gegevens. De gegevens bleken in het algemeen ter zake dienend en niet bovenmatig.

* art. 10, 2, c WvB

Het functioneel beheer is ingedeeld in verschillende domeinen. Elk domein is verantwoordelijk voor een aantal van de operationele informatiesystemen. De domeinen voeren de processen naar eigen inzichten uit en werken (nog) niet (altijd) volgens eenduidig beschreven processen.

Binnen de KMar wordt gewerkt op basis van een accreditatieschema met betrekking tot de beveiliging van systemen. Deze worden uitgevoerd op basis van risicoanalyses. De meest gebruikte systemen zijn (onder voorbehoud) geaccrediteerd, echter nog niet alle. Ook zijn (nog) niet alle bevindingen uit de accreditaties opgevolgd. Aangegeven wordt dat deze worden meegenomen in de overdracht van het rekencentrum KMar aan IVENT dat ten tijde van de audit loopt.

Voor de verwerking van politie gegevens maakt KMar gebruik van systemen die (in beheer zijn van) vtsPN. Voor het aanpassen van deze systemen op de Wpg is KMar afhankelijk van andere partijen (politie, vtsPN). Ook deze systemen voldoen (nog) niet aan de daaraan te stellen eisen.

Verbeterpunten

Als verbeterpunten zijn te noemen:

- het vertalen van de wijzers in operationele processen en werkinstructies;
- het (laten) uitvoeren van de accreditaties van systemen en het opvolgen van de bevindingen daaruit;
- het eenduidig inrichten en beschrijven van de processen van functioneel beheer.

3.3.3. Gevoelige gegevens (artikel 5)

Norm

De verwerking van politiegegevens betreffende iemands godsdienst of levensovertuiging, ras, politieke gezindheid, gezondheid, seksuele leven, alsmede van 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.

Bevindingen

De norm is opgenomen in de Wpg-wijzer als algemeen uitgangspunt. Hoe de vertaling hiervan in de dagelijkse praktijk dient plaats te vinden, is niet beschreven.

Over het algemeen worden in de praktijk gevoelige gegevens alleen geregistreerd indien dit nodig is voor de afhandeling van een onderzoek; indien onduidelijkheid bestaat worden de teamleider of bevoegd functionaris om raad gevraagd.

Verbeterpunten

Als verbeterpunten zijn te noemen:

- het maken van een richtlijn waarin de norm wordt verhelderd zodat handvatten worden geboden in welke omstandigheden wel en wanneer deze gegevens niet worden geregistreerd, zodat de afweging om de gegevens te registreren op eenduidige wijze wordt gemaakt;
- het controleren op naleving van de norm.

3.3.4. Autorisatie (artikel 6)

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).

Bevindingen

Op dit moment zijn er geen KMar specifieke autorisatiematrices of procesbeschrijvingen voor het aanvragen, toekennen, controleren en opschonen van autorisaties. Op hoofdlijnen is de norm deels omschreven in de Wpg-wijzer. Hierin is het autorisatiemodel per type verwerking beschreven. Deze biedt geen gedetailleerde werkinstructie op basis waarvan zekerheid verkregen kan worden dat alleen die mensen toegang wordt verleend tot applicaties en onderzoeken, die toegang nodig hebben voor de uitvoering van hun taak.

Een (nog niet volledig) overzicht van alle bij de KMar in gebruik zijnde informatiesystemen waarbinnen politiegegevens worden verwerkt is opgesteld. Dit overzicht is (nog) niet gekoppeld aan verwerkingsregimes, taken, rollen en functies. Een eenduidig overzicht van wie op basis van zijn functie en rol toegang heeft tot welke applicaties is niet beschikbaar. Alle binnengekomen e-mails met aanvragen voor autorisaties worden bewaard, maar deze zijn (vrijwel) niet te koppelen aan de autorisaties zoals vastgelegd in systemen.

Een opgesteld Project Initiatie document (PID), waarin voorzien wordt met betrekking tot autorisaties te gaan voldoen aan de Wpg, is nog niet goedgekeurd.

Verbeterpunten

Als verbeterpunten zijn te noemen:

- het aanmaken van autorisatiematrices;
- het gedetailleerd beschrijven van de autorisatie processen (aanvragen, toekennen, controleren en opschonen);
- het refereren naar de procesbeschrijving in de Wpg-wijzer;
- het uitvoeren van controles op het autorisatieproces en de toegekende autorisaties.

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

Norm

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

Indien politiegegevens in combinatie met elkaar worden verwerkt, worden van die verwerking nader genoemde gegevens vastgelegd (protocolplicht).

Bevindingen

In de Operationele Wpg-wijzer zijn bij de definities van 'Geautomatiseerd vergelijken' en 'In combinatie verwerken' verantwoordelijke afdelingen aangewezen. Dit wordt uitgevoerd door de infodesk (KIK, DIK of BIK). Deze werkwijze is eveneens in het (nog niet vastgestelde) handboek FB opgenomen.

De definitie en werkwijze zijn niet nader uitgewerkt in formele protocollen en werkinstructies voor de infodesk, waarin aangegeven is wie verantwoordelijk is. Wel is op intranet een formulier melding Geautomatiseerd vergelijken/ in combinatie met elkaar verwerken beschikbaar.

Toestemming voor het geautomatiseerd vergelijken of in combinatie met elkaar verwerken wordt gegeven door de BF of de OvJ.

Om geautomatiseerd gegevens te vergelijken of deze in combinatie met elkaar te verwerken moeten gegevens uit verschillende systemen gehaald worden.

Deze worden ingelezen in I-Base. De aanvragen bij de infodesk worden vastgelegd in een Infodesk module. Hiervan is een uitdraai te maken. Controle door de privacyfunctionaris op basis van een dergelijk overzicht vindt niet plaats.

In de praktijk wordt niet op adequate wijze invulling gegeven aan protocolplicht en bewaarplicht.

Verbeterpunten

Als verbeterpunten zijn te noemen:

- het uitbreiden van de omschrijvingen in de Wpg-wijzer of het aanmaken van werkinstructies of procesbeschrijvingen die meer verduidelijking bieden;
- het vaststellen van het handboek BF;
- binnen de organisatie duidelijk maken wanneer sprake is van in combinatie met elkaar verwerken en geautomatiseerd vergelijken en de maatregelen die hiervoor gelden.

3.3.6. Bewaartermijnen (artikel 14)

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 verwijderd.

Bevindingen

In de operationele Wpg-wijzer is per artikel dat een doel voor verwerking van politiegegevens formuleert, de levensloop van gegevens aangegeven. Tevens is een proces voor verwijdering en vernietigen/archiveren beschreven. Hierbij zijn de verantwoordelijkheden weergegeven in het proces.

Met uitzondering van BPS hebben de meeste gebruikte computersystemen niet de functionaliteit om geautomatiseerd gegevens te verwijderen of af te schermen. Binnen BPS worden mutaties na 5 jaar in een archief omgeving gezet, waar de toegang toe beperkt is. Deze 'archivering' houdt geen rekening met het type verwerking.

RBS kent een archief omgeving. Om gegevens naar deze omgeving over te zetten is de ontvangst van sepot en afloop berichten nodig. De volledigheid van ontvangst van sepots en afloopberichten vanuit het OM is echter niet gewaarborgd en vormt daarmee een complicerende factor.

Voor gegevens opgeslagen op andere gegevensdragers (buiten de applicaties) is niet inzichtelijk op welke gegevensdragers deze zijn opgeslagen en tot wanneer die mogen worden bewaard.

Aan handmatige schoning en archivering wordt niet structureel invulling gegeven. Oude gegevens zijn algemeen toegankelijk binnen de verschillende systemen.

Artikel 12 gegevens worden niet vernietigd, wel verwijderd. Reden hiervoor is dat in de visie van de KMar de gegevens nodig zijn voor de bescherming van informanten, ook als de bewaartermijn verstreken is.

Hernieuwde verwerking komt in de praktijk (nog) niet voor. Wel is op intranet een formulier beschikbaar voor het aanvragen van hernieuwde verwerking.

In de loop van 2011 zijn analyses op verschillende applicaties uitgevoerd om vast te stellen welke aangepast dienen te worden zodat beter voldaan wordt aan de Wpg. Besloten is om applicaties gedurende de komende jaren 1 voor 1 aan te pakken. Hiervoor is een PID opgesteld. Deze is echter nog niet geformaliseerd.

Eveneens is aangegeven dat de budgettaire ruimte onvoldoende is. Voor diverse systemen bestaat een afhankelijkheid van andere partijen.

Controle op het verwijderen en vernietigen van gegevens wordt nog niet structureel uitgevoerd. Dit betreft zowel geautomatiseerde systemen als hardcopy files.

Verbeterpunten

Als verbeterpunten zijn te noemen:

- waar mogelijk het (laten) aanpassen van de informatiesystemen op de Wpg normen;
- het uitbreiden van de procesdocumentatie en onderlinge afspraken;
- het inrichten van een centraal punt dat zicht houdt op het verkrijgen van sepots en afloopberichten;
- het schonen van huidige archieven;
- de controle op de naleving van de verwijderings- en vernietigingstermijnen.

3.3.7. Ter beschikking stellen (artikel 15)

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.

Bevindingen

Het proces van ter beschikking stellen en welke partijen daarbij betrokken zijn, is op hoofdlijnen vastgelegd in de operationele wijzer. Ook is een hoofdstuk ter beschikking stellen opgenomen in het handboek bevoegd functionaris.

Gegevens worden in geval van artikel 9 en 10 verwerkingen ter beschikking gesteld door de Infodesk met toestemming van de bevoegd functionaris.

Naast BPS, kan onder andere door middel van VROS en BlueView of een verzoek bij de Infodesk gezocht worden. KMar-medewerkers die toegang hebben tot BPS kunnen via BPS zoeken. Politiedeskmedewerkers die informatie uit BPS KMar willen hebben, moeten dit aanvragen via de Infodesk.

De werkwijze van de Infodesk is vastgelegd, maar is niet up to date, niet alle gemaakte werkafspraken komen hierin terug.

Op basis van een deelwaarneming van 7 ter beschikking stellingen heeft de AOIB vastgesteld dat deze rechtmatig zijn geschied. De vastlegging van de terbeschikkingstelling kan wel verbeterd worden. Niet in alle gevallen werd alle vast te leggen informatie ook daadwerkelijk vastgelegd.

In principe zouden in de periode 2008-2011 alle BF en medewerkers BIK de BF een opleiding hebben gevolgd. Een actueel overzicht van alle medewerkers die als BF fungeren en zijn opgeleid is echter niet beschikbaar, waardoor de volledigheid niet is vast te stellen. De opleidingen zijn nu opgenomen in het STOP programma waarna na afronding van de opleiding de realisatie wordt geregistreerd in Peoplesoft.

Een concept document met betrekking tot weigeringsgronden is in het Handboek Bevoegde Functionarissen opgenomen, echter is dit nog niet vastgesteld of verspreid.

Verbeterpunten

Als verbeterpunten zijn te noemen:

- het vastleggen van interne afspraken in procedures met betrekking tot ter beschikking stellen;
- de controle op naleving en vastlegging vorm te geven.

3.3.8. Verstrekken van politiegegevens (artikel 16)

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.

Bevindingen

De Wpg verstrekkingenwijzer beschrijft wie binnen de KMar bevoegd is om een verstrekking te doen, aan wie de bevoegde mag verstrekken en onder welke voorwaarden. In de wijzer wordt ingegaan op protocol gegevens en vaststelling identiteit van de aanvrager. Deze wijzer heeft de status van operationele instructie. Naast de verstrekkingenwijzer zijn diverse (technische) handleidingen beschikbaar voor VST_I en RBS. Deze zijn niet up- to-date en laten ruimte voor meerdere interpretaties. Eveneens hebben medewerkers van BIK, DIK of KIK onderlinge interne afspraken gemaakt over de vastlegging in VST_I. Deze zijn niet schriftelijk vastgelegd.

In de praktijk worden verstrekkingen niet altijd op de juiste manier geprotocolleerd. Niet alle medewerkers zijn op de hoogte van alle beoordelingscriteria en kwaliteitsaspecten die gelden voor het verstrekken van gegevens. Wel wordt bij twijfel de verstrekkingenwijzer geraadpleegd. Instructies voor het bewaren van protocolleringen zijn niet aanwezig. Ook wordt niet in alle gevallen de geheimhoudingsplicht kenbaar gemaakt aan de ontvanger van de gegevens.

Voor structurele verstrekkingen in samenwerkingsverbanden worden convenanten opgesteld. In opzet zijn de richtlijnen en verantwoordelijkheden met betrekking tot het vastleggen van samenwerkingsverbanden aanwezig. De Privacy functionaris houdt een overzicht bij van de convenanten die de KMar heeft gesloten. Diverse convenanten moeten worden geactualiseerd. De bekendheid met de inhoud van convenanten is niet altijd aanwezig bij de medewerkers die op basis daarvan verstrekkingen doen.

Controles op verstrekkingen door het KIK vinden niet structureel plaats, maar op ad hoc basis en op verzoek.

Verbeterpunten

Als verbeterpunten zijn te noemen:

- het nader uitwerken van de procedures in procesbeschrijvingen/werkinstructies;
- het zorg dragen voor de kennisname van de procesbeschrijvingen onder de werknemers;
- het controleren op de naleving van de normen;
- het actualiseren van convenanten.

3.3.9. Rechten van betrokkenen (artikel 25/28)

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.

Bevindingen

De Operationele Instructie Rechten betrokkene Wpg (2010) bevat een procesbeschrijving van correctie verzoeken en daarbij horende mededelingen, inzage verzoeken, verantwoordelijkheden en borging. Aan dit proces wordt invulling gegeven door de privacyfunctionaris (PF). Hij houdt in een Excel overzicht bij aan wie wanneer wat is verstrekt. Dit is afgelopen periode diverse malen gebeurd.

Verbeterpunten

Geen.

3.3.10. Protocolplicht (artikel 32)

Norm

De verantwoordelijke draagt zorg voor de schriftelijke vastlegging van:

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

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

Bevindingen

Voor wat betreft de vastlegging van doelen van onderzoek wordt dit op basis van MRO-formulieren bijgehouden in een Excel-overzicht. Deze werkwijze is opgenomen in Handboeken opsporing - startmutatie en maken MRO.

Aan de protocollering van toekenning van autorisaties kan alleen op handmatige wijze voldaan worden. Zie tevens 3.3.4 Autorisatie (artikel 6).

Niet voor alle artikel 13 verwerkingen zijn vastgestelde instellingsprotocollen aanwezig. Er zijn wel concept protocollen aanwezig.

Voor gemeenschappelijke verwerking is een formulier 'melding gemeenschappelijke verwerking' op intranet beschikbaar gesteld. In de praktijk zijn geen gemeenschappelijke verwerkingen geïdentificeerd.

Geformaliseerde procesbeschrijvingen, die ingaan op geautomatiseerde vergelijking of in combinatie met elkaar verwerken, zijn niet beschikbaar. Protocollering van geautomatiseerd vergelijken of in combinatie met elkaar vergelijken vindt niet op structurele wijze plaats.

Er is een formulier beschikbaar op intranet voor onrechtmatige verwerkingen. De privacyfunctionaris geeft in zijn jaarverslag aan dat tot en met 2010 geen enkele melding via die weg is binnengekomen. In periode 2011 is 1 melding ontvangen, terwijl in de controle tool 'Signalen' 30 onrechtmatige verwerkingen zijn genoteerd. Deze zijn niet aan de privacyfunctionaris gemeld.

De bewaartermijnen van protocolgegevens zijn onvoldoende vastgelegd. Het is onduidelijk of de protocolgegevens worden bewaard tenminste tot de datum waarop de laatste controle is verricht. Controle op protocollering vindt ad hoc en niet structureel plaats.

Niet aan alle protocolverplichtingen (en daarop gebaseerde controles) wordt voldaan of kan voldaan worden.

Verbeterpunten

Als verbeterpunten zijn te noemen:

- het aanmaken van procesbeschrijvingen/werkinstructies met betrekking tot het protocolleren en de bewaartermijnen van protocolgegevens;
- het melden van onrechtmatige verwerkingen aan de privacyfunctionaris;

- het uitvoeren van controles op naleving van de norm en onrechtmatige verwerkingen;
- waar mogelijk aanpassen van applicaties zodat de protocolplicht wordt gefaciliteerd door de gebruikte systemen.

3.3.11. Audits (artikel 33)

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.

Bevindingen

De afdeling OIB heeft gedurende 2010 en 2011 vijf onderzoeken uitgevoerd naar de invoering en bekendheid van de Wpg en de opvolging van daaruit voorgekomen acties. Eind 2011 heeft de externe audit plaatsgevonden.

Verbeterpunten

Geen.

3.3.12. Privacyfunctionaris (artikel 34)

Norm

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

Bevindingen

De KMar heeft een PF voor 1 FTE. De functie is verdeeld over twee personen. De PF functioneert voornamelijk als vraagbaak en adviseur. Naast de PF zijn er binnen de KMar eveneens twee aanspreekpunten. De PF geeft geen structurele invulling aan controle. Eveneens is geen structureel overzicht van de verschillende protocolleringen aanwezig.

Over de jaren 2008 – 2010 heeft de PF een jaarverslag opgesteld. Dit zal ook over 2011 worden opgesteld.

Verbeterpunten

Analyseer het takenpakket van de PF en beoordeel of taken elders moeten worden belegd of dat meer capaciteit vrijgemaakt moet worden zodat de controle functie van de PF meer aandacht krijgt.

3.3.13. Functionaris Gegevensbescherming (artikel 36)

De FGB bestaat niet als functie bij de Koninklijke Marechaussee. Dit is geen verplichting vanuit de Wpg.

A. Geïnterviewde medewerkers

02 Tijdens de uitvoering van deze audit zijn de volgende medewerkers geïnterviewd

Naam	Functie
act. 10, 2, e WOS	Senior Onderzoeker AOIB
	Privacyfunctionaris
	Senior beleidsmedewerker / Projectleider Wpg
	Wpg Scanteam District West
	Wpg Scanteam District West

B. Ontvangen documentatie

03 Tijdens de uitvoering van deze audit is gebruikgemaakt van de volgende documentatie

Naam	Versie
Interne Audit Wpg, Rapportage Verstrekkingen en onderliggend dossier	Versie 1.0, 22 november 2011, Definitief
Interne audit Wpg, Tussenrapportage 2010, en onderliggend dossier	Versie 1.0, 30 september 2010, Definitief
Interne audit Wpg, Rapportage bevindingen Enquête 2010, en onderliggend dossier	Versie 1.0, 29 december 2010, Definitief
Interne audit Wpg, Rapportage Status update, inclusief onderliggend dossier en verbeterplannen.	Versie 1.0 Definitief
Operationele Wpg-wijzer	Versie 1.0, mei 2010
Verstrekkingen wijzer	November 2009
Projectinitiatiedocument, verbetering proces autorisatiebeheer	Versie 0.2, 30 augustus 2011, Concept voor stuurgroep van 5 september 2011
Projectinitiatiedocument WPG-ICT	Versie 1.0 Datum 08-09-2011 Status Definitief

C. KMar in Nederland

Voor de uitvoering van deze audit zijn de volgende onderdelen van de KMar meegenomen in het onderzoek:

District West	District Noord-Oost	District Zuid	District Schiphol	District landelijke en buitenlandse eenheden
• Brigade Den Haag Beveiliging • Brigade Noord-Holland • Brigade Zuid-Holland • Brigade Utrecht • Brigade Recherche & Informatie • Brigade ondersteuning	• Brigade Waddengebied • Brigade Oostgrens-Noord • Brigade Oostgrens-Midden • Brigade Veluwe • Brigade Drenthe-IJsselstreek • Brigade Recherche & Informatie • Brigade ondersteuning	• Brigade Scheldestromen • Brigade Brabant Zuid • Brigade Brabant Noord / Limburg Noord • Brigade Limburg Zuid • Brigade Recherche & Informatie • Brigade Ondersteuning	• Brigade Grensbewaking • Brigade Politie & Beveiliging • Brigade Vreemdelingenzak en • Brigade Operationele Ondersteuning District • Brigade Recherche & Informatie • Afdeling Handhaving & Toezicht	• Brigade Centrale Recherche & Informatie • Brigade Krijgsmacht en Operationele Ondersteuning • Brigade Speciale Beveiligingsopdrachten • Korps Militaire Controleurs Gevaarlijke Stoffen • Brigade Ondersteuning

D. Gehanteerde afkortingen

AOIB	afdeling Onderzoeken Interne Beheersing
BF	Bevoegd Functionaris
BIK	Brigade Informatie Knooppunt
BPS	Applicatie Bedrijfs Processen Systeem
DIK	District Informatie Knooppunt
KIK	KMar Informatie Knooppunt
KMar	Koninklijke Marechaussee
OIB	afdeling Onderzoeken Interne Beheersing
PID	Project Initiatie Document
RBS	Applicatie: Recherchebasissysteem
STOP	Opleidingsprogramma
VROS	Applicatie: Verwijsindex recherche- onderzoeken en subjecten
Wpg	Wet politiegegevens