220220120000 1

B. de Rooy

Ministerie van Veiligheid en Justitie

Audit Wpg politie KLPD

Rapport

Datum	6 januari 2012
Status	Definitief

Colofon

Afzendgegevens	**Departementale Auditdienst** Kalvermarkt 53 2511 CB Den Haag Postbus 20301 2500 EH Den Haag www.rijksoverheid.nl/venj
Contactpersonen	drs. drs. T M wpg@minvenj.nl
Projectnaam	Audit Wet Politiegegevens
Ons kenmerk	DDS/5719719/11
Auteurs	

Inhoud

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 november en december 2011 is een privacy audit uitgevoerd bij het Korps Landelijke Politiedlensten (KLPD).

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 KLPD.

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

Den Haag, 6 januari 2012

De Directeur van de Departementale Auditdienst

2 Samenvatting

Het KLPD heeft de implementatie van de Wpg serieus opgepakt. Er is een Programma WPG opgestart onder leiding van een projectmanager. Het Programma WPG heeft een risicoanalyse bij de verschillende diensten uitgevoerd om te achterhalen waar zij de focus moesten leggen met betrekking tot de Wpg implementatie. Op basis van de uitkomsten is een Wpg implementatieproject gestart waar alle KLPD diensten aan hebben meegewerkt. Dit heeft er toe geleid dat in december 2011 het merendeel van de processen conform Wpg is opgesteld en het merendeel van de medewerkers is opgeleid.

Niettemin voldoet het door ons beschouwde stelsel van maatregelen nog niet geheel 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
artikel 1.f Verantwoordelijke			
1.f	Mandaatbesluit		De mandatering van de verantwoordelijkheid voor de Wpg is als volgt belegd: • De Minister van BZK heeft de korpsbeheerder van het KLPD gemandateerd; • De korpsbeheerder heeft de korpschef van het KLPD gemandateerd; • De korpschef heeft de diensthoofden, concernhoofden en hoofden van de stafafdelingen gemandateerd. Hiermee wordt voldaan aan de Wpg.
artikel 3 en 4 Kwaliteitsaspecten van politiegegevens			
8.1 en 9.1	Onderscheid onderzoek Dagelijkse Politietaak (8) versus Bepaald geval (9)		De diensten binnen het KLPD zijn gecompartimenteerd en sterk gericht op het voor hen van toepassing zijnde regime (artikel 8, 9 of 10 Wpg). De medewerkers zijn op de hoogte van het regime waarin zij werken en de regels die hierop van toepassing zijn. Hiermee wordt voldaan aan de Wpg.
3.1 t/m 3.3 (8) 4.1 (8)	Noodzakelijkheid (8) Doelbinding Rechtmatigheid Juistheid Volledigheid		Het KLPD heeft in 2009 en 2010, in totaal 350 medewerkers een op maat gesneden Wpg-opleiding laten volgen. Deze medewerkers zijn als kerninstructeur opgeleid om de kennis aan hun medewerkers over te dragen. Tevens hebben de diensten hun werkinstructies of procesbeschrijvingen op de Wpg gecontroleerd en waar nodig aangepast of aangevuld. De infodesk controleert bij aanvragen voor

Norm	Aspect		Bevinding en oordeel
			politiegegevens op het doel en de noodzakelijkheid van de te verstrekken gegevens. Dit wordt in de BVO Infodesk module vastgelegd. Hiermee wordt voldaan aan de Wpg.
3.1 t/m 3.4 (9) 4.1 (9)	Noodzakelijkheid (9) Doelbinding Rechtmatigheid Herkomst en wijze van verkrijging Juistheid Nauwkeurig Volledigheid		Voor artikel 9 verwerkingen zijn de volgende maatregelen getroffen: • Er zijn kerninstructeurs opgeleid; • Procesbeschrijvingen zijn getoetst en aangepast; • De DOS infodesk controleert de aanvragen. Aanvullend hierop zijn door de volgende diensten specifieke maatregelen getroffen: Vanuit de DNR zijn Q-Kringen opgericht die afspraken hebben gemaakt over zaken als kwaliteit en opbouw van een dossier. IPOL borgt in hun artikel 9 onderzoeken de herleidbaar van herkomst en wijze van verkrijging door gegevens uit BVH alleen uit het proces verbaal te extraheren. Een proces verbaal wordt ambtsedig opgemaakt en wordt daardoor als betrouwbaard beschouwd. Hiermee wordt voldaan aan de Wpg.
3.4 (10 en 12) 4.1 (10 en 12)	Noodzakelijkheid (10 en 12) Doelbinding Rechtmatigheid Herkomst en wijze van verkrijging Juistheid Nauwkeurig Volledigheid		De CIE voldeed voor de implementatie van de Wpg al aan veel van de gestelde eisen. De CIE maakt gebruik van het landelijk goedgekeurde en Wpg geverifieerde Handboek CIE. De systemen BVO-bruto en BVO-netto zijn sturend in het werkproces. De Zwacri-criteria zijn algemeen bekend. De CIE-OvJ is nauw betrokken bij de werkzaamheden en komt wekelijks op locatie. Twee keer per jaar worden verschillende toetsen op onder andere kwaliteitscriteria uitgevoerd door het Landelijk Parket. Hiermee wordt voldaan aan de Wpg.
4.3	Beveiliging		Tijdens de Wpg-implementatie heeft het KLPD vastgesteld dat de applicaties die door het KLPD worden gebruikt niet de gewenste ondersteuning geven om aan de Wpg te voldoen. Mede door de hoge kosten en onduidelijkheid over de toekomstige taken is besloten de eigen applicaties niet aan te passen. Als mitigerende maatregel zijn waarborgen in de werkprocessen (AO) van de diensten geïmplementeerd. Het korps is van mening dat men hierdoor slechts een beperkt risico loopt. Het KLPD maakt gebruik van het Nederlandse Politiebeleid voor Beveiliging. Tevens wordt gebruik gemaakt van een rubriceringregeling waarbij regels zijn voorgeschreven hoe men dient om te gaan met bijvoorbeeld staatsgeheimen of met openbare documenten. Hiermee wordt voldaan aan de Wpg.

Norm	Aspect		Bevinding en oordeel
artikel 5, Gevoelige Gegevens			
• Gevoelige gegevens			Het KLPD beschikt niet over procesbeschrijvingen, werkinstructies of beleidstukken waarin staat beschreven hoe medewerkers dienen om te gaan met gevoelige gegevens. Tijdens de audit zijn geen gegevensverzamelingen met gevoelige gegevens aangetroffen die volgens de Wpg niet zijn toegestaan. Voor Zwacri- en terreuronderzoeken kan het relevant zijn om gevoelige gegevens vast te leggen. Hierbij kan worden aangetoond dat deze verwerkingen noodzakelijk zijn voor een doel. Hiermee wordt deels voldaan aan de Wpg.
artikel 6, Autorisatie			
• Korpsautorisatiematrix			Het KLPD heeft een formeel goedgekeurd autorisatiebeleid dat onderdeel is van het informatiebeveiligingsbeleid. Voor de verschillende diensten van het KLPD zijn autorisatiematrices opgesteld waarin is vastgelegd welke applicaties toegankelijk zijn voor bepaalde functies. Er wordt door functioneel beheer nog gewerkt aan het samenvoegen van de losse matrices tot één centrale autorisatiematrix. Het betreft hier een verbeteractie ten opzichte van de huidige situatie die niet noodzakelijk is om te voldoen aan de norm. Hiermee wordt voldaan aan de Wpg.
• Aanvraagproces			Voor het merendeel van de applicaties worden autorisaties middels vaste en gedocumenteerde aanvraagprocessen bij functioneel beheer aangevraagd. Sinds 2011 zijn verschillende decentrale afdelingen functioneel beheer samengevoegd tot één centrale afdeling. Er wordt gewerkt aan een centraal autorisatieproces en het in lijn brengen van de documentatie. Vanwege gemaakte afspraken met de vtsPN kunnen autorisaties die door hen worden uitgegeven alleen via functioneel beheer worden verstrekt. Voor de overige applicaties worden autorisaties door procesvoerders bij externe partijen aangevraagd. Functioneel beheer heeft geen centraal overzicht van de applicaties die onder extern beheer vallen en de wijze waarop de autorisatieprocessen zijn ingericht. Hiermee wordt voldaan aan de Wpg.
• Wijziging en verwijdering			Verwijderingen van autorisaties in beheer bij functioneel beheer worden aan de hand van door P&O geleverde overzichten verwerkt. Een proces voor interne personeelsmutaties is nog niet geïmplementeerd. Functioneel beheer heeft het voornemen om dit proces in 2012 te ontwikkelen. Hiervoor zal nog een plan van aanpak worden

Norm	Aspect		Bevinding en oordeel
			opgesteld. Wijzigingen of verwijdering van autorisaties in beheer bij externe partners worden door de procesvoerder afgehandeld. Het proces van het autoriseren van uitleenpersoneel verloop door middel van een aanvraagformulier bij de privacyfunctionaris. Functioneel beheer is voornemens dit proces beter inzichtelijk te maken door aparte personeelsnummers voor hen aan te maken. Er is een proces in werking dat autorisaties voor bepaalde applicaties worden geblokkeerd indien er gedurende drie maanden niet is ingelogd. Hiermee wordt deels voldaan aan de Wpg.
• Autorisatiebeheer CIE en RID.			Autorisaties binnen het CIE worden op basis van een hiervoor opgesteld model uitgegeven. In dit model staat aangegeven welke rechten de functiegroepen hebben en aan welke eisen dient te worden voldaan voordat de rechten worden verstrekt. De OvJ was betrokken bij het opstellen van dit model. Voor het merendeel van de in gebruik zijnde applicaties wordt het standaard korpsautorisatieproces gevolgd. Voor het kernsysteem BVO-bruto verlopen aanvragen via de NCIE. De toegang tot eigen artikel 10 en 12 Wpg gegevens wordt in opdracht van het hoofd-CIE door de CIE-registerbeheerder uitgevoerd. Om de paar maanden voeren de procescoördinator en registerbeheerder een controle uit op alle verleende autorisaties. Hiermee wordt voldaan aan de Wpg.
32.1.c	Protocollering autorisaties		Het centrale autorisatie-aanvraagproces wordt door functioneel beheer in drie databases (gezamenlijk genaamd IVO) geprotocolleerd. Het decentrale autorisatie proces wordt door de procesvoerders vastgelegd in functionele mailboxen. Door alle procesvoerders binnen een dienst te benaderen kan de privacyfunctionaris inzicht krijgen in de vastlegging van autorisaties. Hiermee wordt voldaan aan de Wpg.
32.3 voor 32.1.c	Bewaren protocolgegevens autorisaties		De databases IVO waarin autorisatieaanvragen en mutatieverzoeken worden geprotocolleerd, worden niet geschoond aangezien het verantwoordingsinformatie bevat. Vastlegging van onderliggende documenten geschiedt per aanvraag. Hiermee worden de protocolgegevens lang genoeg (minimaal 4 jaar) bewaard om te kunnen gebruiken tijdens interne en externe audits. Hiermee wordt voldaan aan de Wpg.

Norm	Aspect		Bevinding en oordeel
artikel 11, Geautomatiseerd vergelijken en in combinatie zoeken			
• Hanteerbare interpretatie			Binnen het KLPD wordt geen eenduidige definitie van de begrippen geautomatiseerd vergelijken en in combinatie verwerken, gehanteerd. In de praktijk worden politiegegevens geraadpleegd op basis van een beperkt aantal KENO[1] sleutels. Volgens de diensten vallen deze raadplegingen niet onder de begrippen geautomatiseerd vergelijken en in combinatie verwerken. De projectgroep Wpg heeft het onderwerp geautomatiseerd vergelijken en in combinatie verwerken als aandachtspunt voor 2012 geïdentificeerd. Hiermee wordt niet voldaan aan Wpg.
• Aangewezen functionarissen			De onderzochte diensten geven aan geen gebruik te maken van geautomatiseerd vergelijken of in combinatie verwerken. Daarom zijn hiervoor geen functionarissen aangewezen. De projectgroep Wpg is van plan om in 2012 de afdelingen te identificeren die deze verwerkingen uitvoeren en functionarissen aan te wijzen. Hiermee wordt niet voldaan aan Wpg.
11.4	Bevoegd gezag		Het proces om toestemming te vragen aan het bevoegd gezag is niet ingericht. Hiermee wordt niet voldaan aan Wpg.
32.1.d en 32.1.h	Protocollering 11.1, 11.2, 11.4 en 11.5		Protocollering voor geautomatiseerd vergelijken en in combinatie verwerken is niet ingericht. Hiermee wordt niet voldaan aan Wpg.
32.3 voor 32.1.d en 32.1.h	Bewaren protocolgegevens 11.1, 11.2, 11.4 en 11.5		Zie protocollering 11.1, 11.2, 11.4 en 11.5 Hiermee wordt niet voldaan aan Wpg.
artikel 14, Bewaartermijnen			
8.2 en 8.3	(8) van 1 tot 5 jaar		BVH 1.2.2. is in november 2011 binnen het KLPD geïmplementeerd. De module voor de schoning van politiegegevens is op advies van de landelijke projectgroep Wpg niet geactiveerd vanwege mogelijke daaraan verbonden risico's. Het KLPD volgt hieromtrent de landelijke ontwikkelingen. Hiermee is schoning van BVH nog niet geïmplementeerd. Gegevensbeheer heeft in samenwerking met de vtsPN units en diensten autorisaties toebedeeld voor het werken met politiegegevens op de G:\schijf: • 0 tot 1 jaar (lezen en schrijven). • 1 t/m 5 jaar (lezen). • 6 t/m 10 jaar (niet toegankelijk voor

[1] Een combinatie van (delen van) identificerende variabelen zoals geboortedatum, geslacht, naam e.d.).

Norm	Aspect		Bevinding en oordeel
			operationeel gebruik). Op basis van het bij de zaak horende BVH-nummer worden politiegegevens opgeslagen. De autorisaties voor de schijven zijn aan deze BVH-nummers gekoppeld. Periodiek zullen lijsten worden uitgeprint en autorisaties handmatig worden aangepast. Het aanpassen van de autorisaties van de mappen zal in de toekomst in een maandelijks terugkerend proces worden opgenomen. Hiermee wordt deels voldaan aan de Wpg.
8.6	(8) verwijderen na 5 jaar		Zie "(8) van 1 tot 5 jaar". Hiermee wordt deels voldaan aan de Wpg.
14.1 (8)	(8) vernietigen na 5 jaar verwijderd		Zie "(8) van 1 tot 5 jaar". Hiermee wordt deels voldaan aan de Wpg.
9.4	(9) verwijderen na OH plus ½ jaar		Voor het verwijderen van artikel 9 politiegegevens is het KLPD afhankelijk van terugkoppelingen van het OM (het landelijk parket en alle arrondissement rechtbanken) over onherroepelijke zaken. Naar schatting ontvangt de DNR slechts in 50% van de gevallen een terugkoppeling van het OM. Als gevolg hiervan is het niet mogelijk om de schoning te garanderen. Als mitigerende maatregel zijn medewerkers getraind om onderzoeken af te sluiten wanneer deze zijn afgerond. Hiermee wordt deels voldaan aan de Wpg.
14.1 (9)	(9) vernietigen na 5 jaar verwijderd		BVO ondersteunt nog niet de automatische vernietiging van verwijderde politiegegevens na vijf jaar. Het KLPD heeft op landelijk niveau samengewerkt om een module te ontwikkelen die hierin voorziet. Als de tests goed verlopen zal de module in januari 2012 in productie worden genomen. Het KLPD heeft in 2011 handmatig een schoning op de onderzoeken uitgevoerd. Alle zaken ouder dan vijf jaar zijn voorgelegd aan de verantwoordelijke bevoegde functionarissen waarbij zij dienden vast te stellen of de gegevens konden worden vernietigd. Wanneer een wettelijke reden aanwezig was om de gegevens niet te vernietigen is hiervan afgezien. Het KLPD zal dit proces jaarlijks herhalen zolang de landelijke applicaties nog niet in de schoning ondersteunen. Binnen de DNR is de G:\ schijf niet effectief te schonen omdat er geen eenduidige namen worden gebruikt en gegevens hiermee niet altijd herleidbaar zijn. Bij de overgang van BVO naar Summ-IT zullen medewerkers een jaar de tijd krijgen om gegevens van de G:\ schijf naar het betreffende onderzoek te verplaatsen. Hierna worden de niet verplaatste gegevens verwijderd dan wel vernietigd. Binnen de DKDB is sprake van grote diversiteit en versnippering van informatie. Hierdoor zou het schonen van bestaande mappen veel tijd in beslag nemen. Daarom is gekozen om te wachten tot

Norm	Aspect		Bevinding en oordeel
		[redacted]	SUMM-IT beschikbaar is. Hiermee wordt deels voldaan aan de Wpg.
10.6	(10) verwijderen na 5 jaar geen subjectwaardige registratie	[redacted]	Tot op heden wordt het automatisch verwijderen van politiegegevens in BVO-netto niet technisch ondersteund. Er wordt een module ontwikkeld die automatische schoning mogelijk moet maken. De politiegegevens in BVO zijn zes jaar oud. Hiermee word deels voldaan aan de Wpg.
14.1 (10)	(10) vernietigen na 5 jaar verwijderd	[redacted]	Zie "(10) verwijderen na 5 jaar geen subjectwaardige registratie". Hiermee word deels voldaan aan de Wpg.
14.3	Hernieuwde verwerking	[redacted]	Er is geen proces voor de vastlegging en afhandeling van hernieuwde verwerkingen. Hiermee wordt niet voldaan aan de Wpg.
32.1.e	Protocollering 14.3	[redacted]	Zie "Hernieuwde verwerking". Hiermee wordt niet voldaan aan de Wpg.
32.3 voor 32.1.e	Bewaren protocolgegevens 14.3	[redacted]	Zie "Hernieuwde verwerking". Hiermee wordt niet voldaan aan de Wpg.
12.2	(12) verwijderen na 4 maanden	[redacted]	Gegevens van informanten worden binnen vier maanden van BVO-bruto naar BVO-netto overgezet. Voordat de gegevens worden overgezet voert de teamchef een controle uit. Zodra de gegevens in BVO-netto zijn opgenomen zijn het artikel 10-gegevens en kunnen ze verder worden verwerkt. Na de overdracht van de gegevens worden deze tegen schrijven beveiligd. Hiermee wordt voldaan aan de Wpg.
12.6	(12) controleren en vernietigen	[redacted]	Artikel 12-gegevens dienen na 10 jaar te worden vernietigd. Hiertoe is een project gestart om de gegevens binnen één systeem samen te voegen en de gegevens inhoudelijk te controleren. Hierbij wordt gecontroleerd of bepaalde informanten niet in meerdere onderzoeken voorkomen en of de gegevens niet ouder zijn dan 10 jaar. Naar verwachting zal het project in januari 2012 worden afgerond. Hiermee word deels voldaan aan de Wpg.
artikel 15, Ter beschikking stellen			
• Infodesk voor bevraging		[redacted]	De infodesk deelt geen artikel 10-politiegegevens. Artikel 9 politiegegevens worden alleen na toestemming van een bevoegd functionaris ter beschikking gesteld. Het document "procesbeschrijving / werkinstructie KIK-infodesk versie 2.0" beschrijft hoe dient te worden omgegaan met "hits" op artikel 10 CIE-onderzoeken. Het document omschrijft niet hoe artikel 9-gegevens worden gedeeld. Hiermee word deels voldaan aan de Wpg.
• Codering		[redacted]	Binnen het KLPD wordt geen codering toegepast. De infodesks van het KLPD nemen altijd eerst contact op met de bevoegd functionaris voordat informatie wordt gedeeld.

Norm	Aspect		Bevinding en oordeel
			Hiermee word voldaan aan de Wpg.
• Aanwijzing Bevoegd Functionaris			Binnen het KLPD zijn voor artikel 9 en 10 bevoegd functionarissen op functie aangesteld. Hun taken en bevoegdheden zijn beschreven. Hiermee wordt voldaan aan de Wpg.
• Opleiding Bevoegd Functionaris			Binnen het KLPD hebben in 2009 en 2010, 231 bevoegd functionarissen een op maat gesneden Wpg-opleiding bij de politieacademie en een extern bureau gevolgd. Er is een handreiking speciaal voor de bevoegd functionarissen opgesteld. Deze is beschikbaar gesteld via intranet. Hiermee wordt voldaan aan de Wpg.
15.2	Weigeringgronden		Tijdens de opleiding zijn de bevoegde functionarissen geïnstrueerd hoe dient te worden omgegaan met de formele weigeringsgronden. De DNR voert onder andere zogenaamde embargo-onderzoeken uit waarbij per definitie geen informatie wordt gedeeld. De embargo-onderzoeken vallen onder de formele weigeringsgronden. Gezien de grote tactische belangen van een aantal (niet embargo) onderzoeken binnen de DNR is gekozen voor een tussenoplossing, de zogenaamde "tussenfase dossiers". Samen met de stuurgroep en het Landelijk Parket wordt dan besloten de informatie op niveau 5 aan te maken, waardoor het niet meer landelijk raadpleegbaar is. Dit kan alleen na een besluit op het hoogste bestuursniveau. Hiermee geeft de DNR uitvoering aan de intentie van de wetgever, zonder de tactische belangen te schaden. Hiermee wordt voldaan aan de Wpg.
artikel 16 t/m 24, Verstrekking			
• Verstrekkingenwijzer (landelijk)			De landelijke verstrekkingenwijzer geeft informatiemakelaars handvatten om gegevens op een rechtmatige manier te verstrekken. De informatieverstrekkende afdelingen die zijn bezocht maken gebruik van de landelijke verstrekkingenwijzer en konden deze fysiek of digitaal benaderen. De verstrekkingenwijzer wordt voornamelijk gebruikt om nieuwe medewerkers te informeren aan welke partijen politiegegevens mogen worden verstrekt. Hiermee wordt voldaan aan de Wpg.
• Proces voor convenanten			Convenanten worden door de privacyfunctionaris in samenwerking met een operationeel expert opgesteld. Hierbij wordt gebruik gemaakt van een template gebaseerd op de landelijke handreikingen. Tijdens het maandelijkse privacyoverleg is het proces voor het opstellen van convenanten met alle privacyfunctionarissen besproken. Alle convenanten zijn beoordeeld. In 95% van de gevallen betrof het alleen een

Norm	Aspect		Bevinding en oordeel
			samenwerkingsverband. Bij de overige 5% is sprake van het verstrekken van politiegegevens. De convenanten waarbij sprake was van verstrekking van politiegegevens zijn conform de Wpg aangepast en opnieuw afgetekend. De projectleider-Wpg bewaart momenteel alle artikel 20-convenanten. Deze worden gepubliceerd op het KLPDweb. Hiermee wordt voldaan aan de Wpg.
• Proces voor artikel 20 Besluiten			Het convenant en artikel 20-besluit zijn in een document geïntegreerd. Zie "Proces voor convenanten". Hiermee wordt voldaan aan de Wpg.
• Verstrekkingenschema (regio)			Het KLPD heeft een inventarisatie gemaakt van alle units die structureel politiegegevens verstrekken aan externe partijen. Per onderzochte unit zijn de wijzen van verstrekken en de aanwezige convenanten inzichtelijk gemaakt. Binnen deze afdelingen zijn de medewerkers op de hoogte van aan welke organisaties zij politiegegevens mogen verstrekken. Op basis van een risicoafweging is geconcludeerd dat door het Wpg conform inrichten van het verstrekkingenproces bij de drie grootste verstrekkende afdelingen invulling is gegeven aan de Wpg. Op dit moment zijn er geen andere structureel verstrekkende afdelingen bij het KLPD bekend. Hiermee wordt voldaan aan de Wpg.
• Proces voor geautomatiseerde verstrekking			Binnen de onderzochte afdelingen van het KLPD worden politiegegevens niet geautomatiseerd verstrekt.
7.2	Geheimhouding		In de template voor het opstellen van nieuwe convenanten worden partijen gewezen op de geheimhoudingsplicht. De DOS infodesk wijst tijdens het verstrekken aan externe partijen niet op de geheimhoudingsplicht. Er wordt uitgegaan van de verantwoordelijkheid van de partners. Hiermee wordt deels voldaan aan de Wpg.
32.1.f	Protocollering verstrekking		Binnen de DOS OIV worden verstrekkingen vanuit BVH middels een I90 (maatschappelijke klasse) vastgelegd. Verstrekkingen of controles van politiegegevens worden ook in de transactiemodule vastgelegd. Als de gegevens per post worden aangeboden wordt dit geprotocolleerd in CORSA. Protocollering van verstrekkingen door de infodesk vindt plaats in BVO onder de registratie "26 infodesk". De DNR protocolleert verstrekkingen van artikel 9-gegevens binnen het onderzoek. Hiermee wordt voldaan aan de Wpg.
32.3 voor 32.1.f	Bewaren protocolgegevens		Geprotocolleerde verstrekkingen worden conform de wettelijke termijn bewaard.

Norm	Aspect		Bevinding en oordeel
	verstrekking		Hiermee wordt voldaan aan de Wpg.
• Toezicht door leidinggevenden op verstrekkingen en protocollering			Bij DOS OIV worden complexe verzoeken tot verstrekking van politiegegevens door de privacyfunctionaris afgehandeld. Deze zelfde privacyfunctionaris dient te toetsen of dit proces goed verloopt. Hierdoor kan er sprake zijn van belangenverstrengeling. Binnen de DOS infodesk hielden in het verleden dagcoördinatoren toezicht op onder andere verstrekkingen en protocollering. Ten tijde van de audit wordt er niet meer actief gestuurd op de inzet van dagcoördinatoren als gevolg van capaciteit problemen. Hierdoor is sprake van beperkt toezicht. Bij de DNR worden verstrekkingen door de bevoegd functionaris uitgevoerd en geprotocolleerd. Hiermee wordt deels voldaan aan de Wpg.
artikel 25 t/m 31, Rechten van de betrokkene			
25.1	Verzoek om kennisneming		De privacyfunctionarissen zijn verantwoordelijk voor het afhandelen van inzage verzoeken. Het merendeel van de verzoeken komt binnen bij de privacyfunctionaris van IPOL. Voor deze processen zijn procesbeschrijvingen opgesteld. Hierin is niet duidelijk aangegeven bij wie de verantwoordelijkheid voor de afhandeling ligt. Conform de "Notitie Borging Programma WPG in de lijn" zal het juridische loket inzage verzoeken in de toekomst gaan afhandelen. Hiermee wordt deels voldaan aan de Wpg.
28.1 t/m 28.3	Correctie		Voor het afhandelen van verzoeken van betrokkene zijn procesbeschrijvingen opgesteld. Hierin wordt niet aangegeven hoe wordt omgegaan met artikel 30. Hiermee wordt deels voldaan aan de Wpg.
artikel 32, Protocolplicht (32.1.c, d, e, f en h behandeld bij thema's)			
9.2 en 32.1.a	Protocollering doel onderzoek		De DKDB meldt na de start van een artikel 9-project het doel van het onderzoek binnen een week bij de privacyfunctionaris. De privacyfunctionaris kan door unieke projectcodes (vanaf 1999) zien welke projecten actief zijn. Binnen de DNR maakt de privacyfunctionaris gebruik van een speciale tool voor de registratie van de lopende onderzoeken. Hierin worden de doelen van onderzoeken bijgehouden. Bevoegde functionarissen vragen een nieuwe BVO-omgeving aan bij functioneel beheer. Hiervoor moeten zij aangegeven wat het doel van het onderzoek is. Dit wordt door functioneel beheer doorgegeven aan de privacyfunctionaris die het vastlegt in de tool. Hiermee wordt voldaan aan de Wpg.
32.3 voor 32.1.a	Bewaren protocolgegevens		Geprotocolleerde verstrekkingen worden conform de wettelijke termijn bewaard.

Norm	Aspect		Bevinding en oordeel
	doel onderzoek		Hiermee wordt voldaan aan de Wpg.
13.4 en 32.1.b	Protocollering artikel 13 gegevensverzameling en		Het KLPD heeft per afdeling geïnventariseerd welke artikel 13-protocollen noodzakelijk zijn. De privacyfunctionarissen hebben gedurende het KLPD privacyfunctionarissenoverleg afspraken gemaakt over het opstellen van artikel 13-protocollen. Hierbij wordt gebruik gemaakt van een template artikel 13 protocol. De projectleider Wpg bewaart momenteel alle artikel 13-protocollen. Deze worden gepubliceerd op het KLPDweb en staan vermeld in het privacyjaarverslag. Hiermee wordt voldaan aan de Wpg.
32.3 voor 32.1.b	Bewaren protocolgegevens artikel 13 gegevensverzameling en		De projectleider Wpg bewaart alle artikel 13-protocollen. Uit het document Overdracht Programma WPG" blijkt dat de opslag in 2012 wordt overgedragen aan de staande organisatie. Hiermee wordt voldaan aan de Wpg.
32.1.g	Protocollering onrechtmatige handeling		Vanuit het korps wordt melding gemaakt van het onrechtmatig verwerken van politiegegevens aan de privacyfunctionarissen. Deze maken hier melding van in het privacyjaarverslag. *Er vindt nog geen actieve monitoring op* onrechtmatige handelingen plaats. Hiermee wordt deels voldaan aan de Wpg.
32.3 voor 32.1.g	Bewaren protocolgegevens onrechtmatige handeling		Protocolgegevens over onrechtmatige verwerkingen worden bewaard voor auditing doeleinden. Op het moment dat de externe audit is afgesloten worden de gegevens verwijderd. De gegevens worden maximaal vijf jaar door de privacyfunctionaris bewaard. Hiermee wordt voldaan aan de Wpg.
32.2	Gemeenschappelijke verwerking		Tijdens de audit zijn geen gemeenschappelijke verwerkingen aangetroffen.
artikel 33, Audits			
RPAP 3.1	Interne audit-functie		Binnen het KLPD zijn interne Wpg auditors opgeleid. Zij vervullen primair de controlerende taak op de Wpg. In 2011 is een interne audit bij een aantal *diensten van het KLPD uitgevoerd.* Hiermee wordt voldaan aan de Wpg.
RPAP 3.4	Interne audit-plan		Voor de interne audit 2011 is een auditplan opgesteld. Hierin is aangegeven welke capaciteit benodigd is maar een planning ontbreekt echter. Er is met de interne audit afdeling afgesproken dat op afroep van Programma WPG capaciteit voor de interne audit wordt ingezet. Voor de interne audit 2011 was 300 uur gereserveerd. Voor 2012 is een zelfde capaciteit gereserveerd. Bij de start van de audit hebben de Wpg auditors een plan van aanpak opgesteld met hierin de verplichte elementen. Hiermee wordt voldaan aan de Wpg.

Norm	Aspect		Bevinding en oordeel
RPAP 3.6	Interne audit-rapport		Van de audit is per te onderzoeken dienst of afdeling een audit rapportage opgesteld. Tijdens de externe audit waren de bevindingen nog niet gevalideerd waardoor de resultaten niet in de externe auditrapportage zijn gebruikt. De rapportages zijn wel gebruikt om aandachtspunten te identificeren voor het onderzoek. Hoewel de interne audit is uitgevoerd en de rapporten grotendeels zijn afgerond hebben wij tijdens de audit geen definitieve versie ontvangen. Het afronden van het auditrapport staat gepland voor eind januari 2012. Hiermee wordt deels voldaan aan de Wpg.
artikel 34, Privacyfunctionaris			
34.1 en 34.4	Benoemd en gemeld		Binnen het KLPD zijn negen privacyfunctionarissen benoemd en op 12 januari 2011 bij het CBP aangemeld. Hiermee wordt voldaan aan de Wpg.
34.2	Overzicht over protocollering		In 2010 en 2011 hadden de privacyfunctionarissen voornamelijk een adviserende rol. Zij ondersteunen bij het opstellen van convenanten en artikel 13 protocollen en zijn momenteel verantwoordelijk voor het beantwoorden van de verzoeken van de betrokkene conform artikel 25. De controle taak was in 2010 en 2011 primair neergelegd bij de interne Wpg auditors. De privacyfunctionarissen geven in het jaarplan voor 2012 aan meer aandacht te zullen geven aan de controle taak. Hiermee wordt deels voldaan aan de Wpg.
34.3	Jaarverslag		Het KLPD heeft een formeel goedgekeurd jaarverslag 2009 en 2010. Het privacyjaarverslag 2011 zal eind maart 2012 worden opgeleverd waarna deze in april, samen met verslag 2010 middels een oplegnotitie, zal worden aangeboden aan de korpsleiding. Hiermee wordt voldaan aan de Wpg.
Optioneel artikel 36, Functionaris Gegevensbescherming			
36.1 en 36.2	Benoemd		Met betrekking tot de invulling van de functionaris Gegevensbescherming wacht het KLPD op de vorming van de nationale politie. Vanuit deze nieuwe organisatie zou de functionaris dienen te worden aangesteld. Dit standpunt staat verwoord in het auditdossier "gebruikersorganisatie". Niet van toepassing.
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 KLPD 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 KLPD in de maanden november en december 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 KLPD.

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 december 2011, van maatregelen en procedures, waarmee het

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

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 KLPD en het Openbaar Ministerie, deelwaarnemingen in de procesbeschrijvingen en andersoortige documentatie en deelwaarnemingen in informatiesystemen.
Wij hebben onze werkzaamheden uitgevoerd in de periode van 28 november 2011 tot en met 30 december 2011.

De korpschef heeft de portefeuillehouder Wpg gemandateerd voor de inhoudelijke afhandeling van alle Wpg gerelateerde zaken. Het conceptrapport met bevindingen is op 4 januari 2012 besproken met de portefeuillehouder Wpg van het KLPD ir. G.F.S.J. Kuijlaars en wordt aan de korpsbeheerder aangeboden.
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.
neemt namens DG Politie deel aan de stuurgroep.
neemt namens het KBB deel aan de stuurgroep.

De specifieke doelgroep waarvoor het rapport is bestemd bestaat uit:
- onze opdrachtgever zoals bovengenoemd;
- de korpsbeheerder van het KLPD Drs. H.W.M. Schoof;
- de waarnemend korpschef van het KLPD Mvr. P.M. Zorko
- de Hoofd Officier van Justitie van het landelijk parket mr. G.W. van der Burg;
- Portefeuillehouder Wpg van het KLPD
- de voorzitter van het College Bescherming Persoonsgegevens Mr. J. Kohnstamm.

Het rapport mag uitsluitend met toestemming van de korpsbeheerder dan wel de korpschef van het KLPD 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*

In 2007 is het KLPD begonnen met het Wpg programma. Het programma bestaat uit drie onderdelen:

1. Korps: hieronder vallen generieke zaken zoals het opstellen van mandaatbesluiten, artikel 13 protocollen en samenwerkingsverbanden, organisatie WPG opleidingen, campagne "Borging & Bewustwording", aanstelling privacyfunctionaris en bevoegd functionarissen etc..
2. Organisatorisch (in 2009/2010): de implementatie van de Wpg binnen de bedrijfsprocessen. De verantwoordelijkheid hiervoor was in eerste instantie bij de verschillende diensthoofden belegd. De diensten hadden echter moeite met het vertalen van de letter van de wet naar de praktijk. Vanaf 2011 heeft het Programma WPG de leiding over de implementatie van de diensthoofden overgenomen. Naar verwachting zal het project eind 2011 niet volledig zijn afgerond, daarom word het project met maximaal een half jaar verlengd. Wel is het de verwachting dat de Wpg per 1 januari 2012 in de lijn zal zijn geborgd (zie notitie Borging WPG).
3. Informatievoorziening (zie § 4.3 onderdeel Beveiliging).

Om de diensten te ondersteunen met de implementatie van de Wpg heeft de stuurgroep WPG ervoor gekozen om te kijken hoe operationele processen momenteel verlopen, dit vast te leggen en te onderzoeken hoe de Wpg hier in past.

DKDB

De DKDB (Dienst Koninklijke en Diplomatieke Beveiliging)is drie jaar geleden begonnen met de implementatie van de Wpg. Aan de hand van een jaarplan, opgesteld door het centrale Wpg project, heeft de DKDB zijn activiteiten ontplooid. Een werkgroep bestaande uit 9 medewerkers heeft de regie gehad bij het implementeren van de Wpg. De focus lag bij het aanpassen van de bedrijfsprocessen het opstellen van een artikel 13 protocol, het zorg dragen voor een opleiding en het creëren van bewustwording bij de medewerkers.

DNR

De DNR (Dienst Nationale Recherche) heeft een projectgroep opgericht om invulling te geven aan het projectplan dat is opgesteld door de centrale projectgroep WPG. De projectgroep heeft er voor gezorgd dat de bedrijfsprocessen zijn geanalyseerd en indien nodig bijgewerkt. Bij dit proces is de werkvloer betrokken.

DOS OIV

De OIV (Operationele Informatie Verwerking) is twee jaar geleden begonnen met de implementatie van de Wpg. De organisatie was in eerste instantie zoekende, omdat er nog te weinig Wpg kennis beschikbaar was. Procesbeschrijvingen zijn opgesteld om medewerkers te instrueren hoe ze Wpg compliant kunnen werken. Deze

beschrijvingen zijn door een senior medewerker gecontroleerd op de Wpg en indien nodig bijgewerkt. De OIV heeft besloten om een gezamenlijke procesgang voor de WOB en de Wpg in te richten. Dit vanwege de overeenkomsten tussen beide wetgevingen.

IPOL, unit Criminaliteit
In 2009 zijn de eerste stappen in het kader van de Wpg gezet. De privacyfunctionaris heeft een standaard format met Wpg normen geschreven. Dit format diende als basis voor gesprekken met de verschillende diensten die uitvoering zouden gaan geven aan de Wpg. Dit heeft geleid tot het beschrijven van alle bedrijfsprocessen en het toetsen hiervan aan de Wpg.

4.1.2 *Bekendheid met de Wpg binnen de organisatie*
Binnen het KLPD hebben in 2009 en 2010, 350 functionarissen een op maat gesneden Wpg opleiding bij de politieacademie en Mazars gevolgd. Er zijn opleidingen geweest voor onder andere: bevoegd functionarissen, informatiemedewerkers, privacyfunctionarissen, Wpg-auditors en leidinggevenden. Doelstelling van de opleidingen was dat de deelnemers als kerninstructeur zouden worden opgeleid om vervolgens de opgedane kennis aan hun medewerkers door te kunnen geven. Vanuit het Programma WPG is niet getoetst of alle kerninstructeurs de kennis hebben overgedragen. Wel zijn ze door de dienstprojectleiders geïnformeerd over de voortgang van de kennisoverdracht.

In het document "opleidingsplan Wet Politiegegevens versie 1.0" staan welke doelgroepen voor de Wpg opleidingen zijn onderkend en welke modules voor deze groepen zijn ontwikkeld. Dit document is gedateerd 29 april 2009.

DKDB
Alle operationele medewerkers binnen de DKDB hebben een Wpg instructie genoten. De instructie is voornamelijk gegeven op basis van casuïstiek. Gedurende een periode van drie maanden zijn deze casussen tijdens briefings behandeld. Tevens hebben medewerkers beschikking gekregen over een e-learning module. Hiervan was de toegevoegde waarde beperkt omdat deze niet goed aansloot bij de werkprocessen van de DKDB.

DNR
Er zijn kennisteams gevormd met daarin teamleiders en dossiervormers. Alle leden van de kennisteams hebben een WPG opleiding gevolgd. De doelstelling van deze kennisteams was om de opgedane kennis over te dragen aan de collega's en hen te coachen in zowel de Wpg aspecten als in de afspraken over de vastlegging in een dossier. Tevens is een handleiding met de Wpg items voor de medewerkers ter beschikking gesteld en een themasite Wpg op het intranet ingericht. Dit heeft er toe geleid dat alle medewerkers van de DNR nu op de hoogte zijn van de Wpg.

DOS OIV
De procesvoerder OIV heeft de training Wpg leidinggevende en bevoegd functionaris gevolgd. Twee senior medewerkers hebben de basis training Wpg gevolgd. De overige medewerkers zijn in december 2011 nog niet Wpg opgeleid. Voor hen is een opleiding geregeld die op 17 of 26 januari 2012 zal worden verzorgd.

DOS Infodesk
De medewerkers infodesk hebben twee jaar geleden een Wpg training gevolgd. Deze cursus is verzorgd door kerninstructeurs. De cursussen sloten aan op het werkveld van de infodesk. Naast deze training worden medewerkers bij indiensttreding door een coach (senior) begeleid, die onder andere toelichting geeft op de Wpg.

IPOL, unit Criminaliteit
De medewerkers van de unit criminaliteit hebben de opleiding Wpg gevolgd. Om het kennisniveau op peil te houden en voor het opleiden van nieuwe medewerkers wordt op dit moment een nieuwe introductiecursus gevormd waar ook de Wpg deel van uit zal maken. De cursus wordt gegeven vanuit het KLPD en zal aan alle medewerkers van de unit criminaliteit worden gegeven.

4.1.3 *Wpg en de praktijk*

De korpsleiding heeft de implementatie van de Wpg op hoofdlijnen aangestuurd. De diensten waren zelf verantwoordelijk voor de implementatie van de Wpg binnen hun eigen dienst.

Binnen het KLPD wordt een rapportage bijgehouden door de dienst Sturing en Ondersteuning. In deze rapportage staat op welke punten al dan niet wordt voldaan aan de Wpg. Ook de verbeterpunten zijn in de rapportage opgenomen, zodat hier monitoring op kan plaatsvinden.

DKDB
De Wpg sluit niet goed aan bij de taakstelling van de DKDB. De wet is hoofdzakelijk gericht op handhaving van de openbare orde en vervolging. Dit sluit niet goed aan bij de taakstelling van de DKDB. Hiertoe heeft de DKDB contact gehad met meerdere juristen die elk een andere visie hadden over hoe de Wpg moest worden aangepakt. Dit heeft er toe geleid dat er maatregelen zijn genomen in het proces waardoor de gegevens grotendeels worden verwekt conform artikel 9.

DNR
Voor de CIE is er weinig veranderd met de komst van de Wpg. De meeste elsen vanuit de Wpg waren reeds verwerkt in de regels en procedures van de CIE die zijn opgenomen in het landelijk goedgekeurde Handboek CIE. Ook de systemen BVO bruto en BVO netto zijn sturend in het werkproces. De criteria of iets binnen de CIE hoort, de Zwacri-criteria, zijn algemeen bekend. De CIE OvJ tekent voor akkoord voor de opname in het Zwacri-register. De CIE OvJ is nauw betrokken bij de werkzaamheden en komt wekelijks op locatie. Twee keer per jaar worden verschillende toetsen uitgevoerd door het Landelijk Parket.

DOS OIV
De dienst was in eerste instantie zoekende omdat er nog te weinig Wpg kennis was. Eind 2011 zijn de werkprocessen conform de Wpg aangepast.

DOS Infodesk
Ten tijde van de implementatie van de Wpg vonden infodesk medewerkers de Wpg op sommige punten onduidelijk. Dit werd mede veroorzaakt door de verschillende interpretaties die experts en professionals gaven over de artikelen van de Wpg. Dit heeft er toe geleid dat binnen de infodesk vragen of onduidelijkheden over de Wpg tijdens briefings of koffiemomenten worden besproken. Dit resulteert in onderlinge kennisoverdracht. Voor aanvullend advies wordt de leidinggevende en indien nodig de privacyfunctionaris benaderd.

IPOL, unit Criminaliteit
De privacyfunctionaris geeft aan dat er wisselende aandacht is voor de Wpg. Het komt als abstract over bij de dienstleiding. De unitleidingen zijn zich over het algemeen goed bewust van de Wpg en wat er moet gebeuren.

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.

4.2.2 *Bevindingen*
In het "besluit gemandateerd beheerder KLPD" van 22 januari 2001 mandateert de Minister van BZK, de directeur-generaal Openbare Orde en Veiligheid, in zijn rol als korpsbeheer, tot het nemen van besluiten, en het vaststellen en ondertekenen van stukken namens de Minister van BZK.

In 2008 heeft de directeur-generaal Openbare Orde en Veiligheid deze bevoegdheden doorgemandateerd naar de Korpschef KLPD ("Besluit nr. 2008-0000109981"gedateerd 3 maart 2008).

In het mandaatbesluit "Mandaatregeling Inzake verwerkingen van persoonsgegevens en politiegegevens Korps Landelijke Politiediensten 2008" mandateert de korpschef diensthoofden, concernhoofden en hoofden van de stafafdelingen voor de uitoefening van taken en bevoegdheden ingevolge de WBP en de Wpg.

4.3 Kwaliteitsaspecten van politiegegevens (artikel 3 en 4)

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

4.3.2 *Bevindingen*

Kwaliteitsaspecten
De diensten binnen het KLPD zijn sterk gericht op het voor hen van toepassing zijnde regime. Binnen elke dienst wordt hoofdzakelijk binnen één van de artikelen 8, 9 of 10 Wpg gewerkt. Medewerkers zijn opgeleid hoe er binnen hun afdeling met politiegegevens moet worden omgegaan. Hierdoor is het onderscheid tussen de twee soorten onderzoeken niet van belang, dit in tegenstelling tot bij de politieregio's. De diensten die zich bezighouden met de informatie makelaarsfunctie baseren het regime op basis van de bronsystemen die ze raadplegen.

Binnen verschillende diensten en units van het KLPD zijn verschillende waarborgen ingebouwd voor de kwaliteitsaspecten van de politiegegevens:

DKDB
Operationele medewerkers van de DKDB kunnen niet direct gegevens in de systemen plaatsen. Hiervoor is een formulier aangemaakt wat aan de Dienst Informatie Knooppunt (DIK) wordt gestuurd. Het DIK is verantwoordelijk voor de kwaliteitscontrole en zorgt voor eenduidige vastlegging.

Om een kwaliteitslag op de bestaande gegevens uit te voeren is besloten om de bestaande informatie in de systemen en op de mappen niet over te zetten op het moment dat het nieuwe verwerkingssysteem SUMM-IT is geïmplementeerd. Men zal de bestaande gegevens controleren en op basis van relevantie, leeftijd en betrouwbaarheid gegevens naar het nieuwe systeem exporteren. De overige gegevens dienen te worden verwijderd. Tevens zal gezien het belang van kwaliteit van politiegegevens volgend jaar binnen de DKDB één fte worden vrijgemaakt om gegevensbeheer in te richten.

DNR
Er zijn binnen de DNR Q-Kringen opgericht die afspraken hebben gemaakt over zaken als kwaliteit en opbouw van dossiers en deze hebben hierop een positieve invloed gehad. De afspraken met betrekking tot dossiervorming zijn bindend voor de gehele DNR.

Medewerkers DNR maken gebruik van het handboek "Proces Opsporen Dienst Nationale Recherche, concept versie 1.8, juni 2011" waarin de belangrijkste werkprocessen zijn opgenomen. Dit handboek is Wpg-compliant. In het handboek worden de producten op hoofdlijnen benoemd. In de bijlage handboek "Proces Opsporen Productbeschrijvingen Dienst Nationale Recherche, concept versie 1.8, juni 2011" staat een opsomming van de producten beschreven.

DNR, CIE
De CIE voldeed voor de implementatie van de Wpg al aan veel van de gestelde eisen. Zij maken gebruik van het landelijk goedgekeurde en Wpg geverifieerde Handboek CIE genaamd " Proceshandboek CIE, Handboek Proces Opsporen DNR, versie 1.6, 24-09-2010". De systemen BVO-bruto en BVO-netto zijn sturend in het werkproces. De Zwacri-criteria zijn algemeen bekend. De CIE-OvJ is nauw betrokken bij de werkzaamheden en komt wekelijks op locatie. Twee keer per jaar worden verschillende toetsen op onder andere kwaliteitscriteria uitgevoerd door het Landelijk Parket.

DOS OIV
De OIV werkt met de gegevens uit BVH, maar is niet de eigenaar van deze applicatie. DOS OIV is daarmee niet eindverantwoordelijk voor de kwaliteit van deze politiegegevens.

DOS Infodesk
Volgens de medewerkers van de Infodesk is de kwaliteit van politiegegevens in de basissystemen (BVH / BVO / BlueView) voor verbetering vatbaar. De procesvoerder informeert bij fouten in BVO het kwaliteitsbureau van de Dienst Nationale Recherche (DNR). Het kwaliteitsbureau neemt vervolgens contact op met de medewerkers die de politiegegevens hebben ingevoerd. Voor de andere systemen zijn er geen kwaliteitsbureaus, daar vindt dan ook geen terugkoppeling plaats.

Voor het eigen werkproces wordt bij het inzamelen van informatie per systeem bijgehouden welke informatie is verzameld. Op basis van het verzoek en de expertise van de behandelend medewerker worden systemen geraadpleegd. Hiervoor is het belangrijk dat de aanvrager het doel en de noodzaak van zijn verzoek duidelijk aangeeft. Indien dit onvoldoende duidelijk is, wordt actief contact gezocht met de verzoeker om alsnog het doel en de noodzaak van het verzoek te achterhalen. Het onderscheid tussen de verschillende artikelregimes bij het doorzoeken van informatie wordt gemaakt op basis van de bron waaruit de informatie wordt verzameld.

Binnen het werkproces van de infodesk waren in het verleden dagcoördinatoren (senior informatieverwerkers) werkzaam die de informatieverwerkers ondersteunden en tevens het werk controleerden. Door gebrek aan capaciteit vindt deze controle sinds november 2011 op eigen initiatief plaats, en wordt dit niet meer actief geregeld. De kwaliteit van de producten van de medewerkers is nu voldoende maar door de controle te laten plaatsvinden door de dagcoördinator kan het niveau van een 6 naar een 8 gaan.

IPOL, unit Criminaliteit
De unit criminaliteit heeft een eigen gegevensverzameling welke valt onder artikel 13 Wpg. De preweeg-documenten vallen onder artikel 9 Wpg. De unit heeft een stroomschema opgesteld waarin is opgenomen welke informatie onder welk artikel valt. De medewerkers van de unit maken wel gebruik van informatie uit BVH, maar zelf zetten medewerkers geen informatie weg in BVH of BVO, maar in de eigen artikel 13 gegevensverzameling.

Alles wat medewerkers van de unit criminaliteit vastleggen wordt voorzien van een bronvermelding. De informatie wordt vastgelegd in Ibase. Tevens vindt een bronvermelding plaats in de preweeg-documenten en wordt het registratienummer uit BVH opgenomen. De documenten moeten altijd herleidbaar zijn omdat de unit analyseproducten maakt.

De unit gebruikt voor het werkproces alleen informatie uit processen-verbaal. Indien informatie in BVH wordt aangetroffen die niet is verwerkt in een Proces Verbaal, wordt de medewerker die de informatie heeft ingevoerd verzocht dit alsnog hierin te verwerken. De reden hiervoor is dat een Proces Verbaal ambtsedig wordt opgemaakt en daardoor als betrouwbaar wordt beschouwd. Als een medewerker wordt verzocht om gegevens alsnog in een Proces Verbaal op te nemen, komt het voor dat men aangeeft de informatie niet als dusdanig betrouwbaar te kunnen kwalificeren. Unit criminaliteit gaat er nooit blind vanuit dat informatie in BVH waar is, dit gebeurt alleen wanneer het een Proces Verbaal betreft.

Het Landelijk Parket en Functioneel Parket voeren een kwaliteitstoets uit op de producten van de unit criminaliteit. De stempel van het OM is belangrijk omdat een zaak dan alleen nog kan worden afgekeurd op prioriteit, en niet op kwaliteit. Als het OM een preweeg niet voldoende acht, dan krijgt de afdeling feedback en kan deze de preweeg verbeteren en aanvullen.

Daarnaast vindt controle plaats vanuit de regio. De regio's ontvangen van IPOL maandoverzichten en geven hier een reactie op. Tevens vindt een controle plaats in het werkproces: de informatieregisseur stelt een preweeg-document op, vervolgens toets de coördinator het document en gaat het document naar de OvJ. Wanneer het komt tot een onderzoek wordt het document overgedragen aan de lijn.

Beveiliging
Met betrekking tot de in gebruik zijnde applicaties binnen het KLPD is vastgesteld dat deze niet aan de Wpg voldoen. Er is geïnventariseerd hoeveel applicaties aangepast dienen te worden. Daarbij is een scheiding gemaakt tussen landelijke applicaties en de applicaties van het KLPD. In eerste instantie zijn 110 KLPD applicaties geïnventariseerd die politiegegevens bevatten. Door consolidatie en het uitfaseren van applicaties is dit terug gebracht tot 45 applicaties. Door gebrek aan budget en onduidelijkheid over de toekomstige taken is binnen het KLPD besloten de applicaties niet aan te passen. Doormiddel van mitigerende maatregelen in de bedrijfsprocessen (AO) heeft het KLPD ervoor gezorgd dat Wpg compliant wordt gewerkt.

De update van BVH (versie 1.2.2) is binnen het KLPD geïmplementeerd. De opties waarmee de bewaartermijnen nagekomen kunnen worden, zijn echter nog niet

geactiveerd. Reden hiervoor zijn de mogelijke risico's die tijdens het proefdraaien in de testomgeving zijn ontdekt. Als mitigerende maatregel zijn medewerkers KLPD door Wpg-training opgeleid om te controleren op de leeftijd van politiegegevens en de te hanteren bewaartermijnen.

Het KLPD maakt gebruik van het Nederlandse Politiebeleid voor Beveiliging. Tevens wordt gebruik gemaakt van een rubriceringregeling waarbij regels zijn voorgeschreven hoe men dient om te gaan met bijvoorbeeld staatsgeheimen of met openbare documenten.

DKDB
Momenteel wordt de meeste informatie opgeslagen in VIPER. VIPER is een programma dat door de DKDB is ontwikkeld en op een acces database wordt gedraaid. VIPER wordt gehost door de vtsPN. Daarnaast worden gegevens opgeslagen op de met Datafort beveiligde G:\ schijf. Toegang tot deze G: schijf is afhankelijk van de door de teamleider uitgegeven autorisaties. Medewerkers krijgen hiermee alleen toegang tot de mappen van projecten waar zij bij betrokken zijn.

Het was de bedoeling dat de DKDB haar gegevens zou opslaan in BVO. Deze applicatie is hiervoor slechts beperkt bruikbaar. In de toekomst is de DKDB van plan te gaan werken met SUMM-IT en in dit systeem alle informatie die door de DKDB gebruikt wordt op te slaan. De verwachting is dat het systeem vanaf januari 2012 beschikbaar is.

IPOL, unit Criminaliteit
De unit criminaliteit beschikt niet over een systeem dat haar werkwijze goed ondersteunt. Politiegegevens worden via BVO, op de G:\ schijf en middels de database Ibase opgeslagen. BVO was bedoeld als leidend systeem waarmee politiegegevens aan andere diensten ter beschikking konden worden gesteld. Door de gekozen IPOL-BVO-structuur, blijkt in de praktijk het echter niet mogelijk om aanvragers toegang te geven tot slechts een bepaald onderzoek. Door de gekozen BVO-structuur krijgt men direct toegang tot alle politiegegevens van IPOL. Deze situatie is ongewenst en de dienstleiding heeft inmiddels ingestemd met een herinrichting van BVO-structuur zodat het delen van politiegegevens gecontroleerd kan verlopen.

De informatie op de G:\ schrijf bevindt zich in de rode omgeving waardoor het delen van informatie van de G:\ schijf zeer gecontroleerd mogelijk is.

Bij de introductie van nieuwe medewerkers worden medewerkers wel bewust gemaakt van het vertrouwelijk omgaan met informatie. Drie jaar geleden zijn veel medewerkers getraind door BV&I over hoe medewerkers om horen te gaan met informatie.

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*

Het KLPD beschikt niet over procesbeschrijvingen, werkinstructies of beleidstukken waarin staat beschreven hoe medewerkers dienen om te gaan met gevoelige gegevens.

DKDB

Er zijn geen gevoelige gegevens aangetroffen binnen de DKDB.

DNR

Voor bepaalde Zwacri-onderzoeken kan het relevant zijn om gevoelige gegevens vast te leggen. Het is echter niet gebruikelijk deze per definitie op te nemen. Ook de afdeling terreur heeft soms gevoelige gegevens nodig maar kan aantonen dat de vastlegging van deze gegevens noodzakelijk is. Door de teamafscheiding zijn de gegevens bovendien niet voor iedereen zichtbaar.

Er zijn geen richtlijnen voor het vastleggen van gevoelige gegevens. Wel wordt rekening gehouden met de wettelijke verplichting dat het alleen toegestaan is als dit onvermijdelijk is voor het doel.

DOS OIV

De OIV verwerkt gegevens in HKS op basis van aangeleverde lijsten met persoonsgegevens. Het kan voorkomen dat hierbij ook gevoelige gegevens worden ingevoerd. Hier wordt door de OIV niet op gelet De verantwoordelijkheid hiervoor ligt bij de partijen die de informatie aanleveren.

DOS Infodesk

De infodesk vervult een raadplegende functie waarbij geen specifieke informatieverzamelingen worden bijgehouden.

IPOL, unit Criminaliteit

De unit criminaliteit maakt analyses waarbij gevoelige gegevens niet relevant zijn. In de preweeg-documenten staan alleen subjecten. De keuze is op basis van criteria, zoals het soort delict. De risico-indicatoren zijn geënt op de feiten en niet op gevoelige gegevens.

4.4.3 *Verbeterpunt*

- Zorg dat een beleid en werkinstructies worden opgesteld over het gebruik en de opslag van gevoelige gegevens.

4.5 Autorisatie (artikel 6)

4.5.1 *Norm*

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

4.5.2 *Bevindingen*

Het KLPD is met betrekking tot de Wpg op het gebied van autorisaties begonnen met het autorisatiebeleid. Ten tijde van de implementatie van de Wpg was het autorisatiebeleid en gegevensbeheerbeleid nog niet geformaliseerd. Het projectteam Wpg heeft het beleid aangepast en formeel laten goedkeuren op 7 december 2010. Het autorisatiebeleid maakt onderdeel uit van de planningscyclus van het KLPD en is een integraal onderdeel van het Informatie(beveiligings)beleid.

Binnen het KLPD wordt het grootste deel van de autorisaties beheerd door de afdeling functioneel beheer. De activiteiten van functioneel beheer waren oorspronkelijk ondergebracht bij de verschillende diensten van het KLPD. Sinds dit jaar (2011) is functioneel beheer samengevoegd tot één nieuwe zelfstandige afdeling van ongeveer 80 mensen. De werkzaamheden worden nog door verschillende functioneel beheer teams uitgevoerd. Er loopt een project om in de toekomst alle aanvragen bij de front-office binnen te laten komen, vanwaar gecentraliseerd taken zullen worden belegd. Het project is vertraagd doordat een nieuw systeemregistratie en workflowsysteem wordt ingevoerd, genaamd Expert Desk. Door de aanzienlijke implicaties van de veranderingen voor de medewerkers is veel capaciteit nodig om de veranderingen te realiseren.

Binnen de verschillende diensten en units van het KLPD worden een aantal specifieke applicaties gebruikt die alleen bruikbaar zijn voor specialistische doeleinden. De autorisaties voor deze applicaties worden door de procesvoerders beheerd. De procesvoerders hebben het beste zicht op het gebruik van deze applicaties. Er is geen KLPD overkoepelend overzicht van de applicaties waarvan het autorisatiebeheer door derden wordt verzorgd. Binnen het KLPD is gekozen om dit per dienst inzichtelijk te maken. Elke privacyfunctionaris weet voor de eigen dienst welke applicaties worden gebruikt. Deze lijsten zijn ook per unit vastgelegd in het door het KLPD aangeleverde dossier.

Autorisatiematrix
De afdeling functioneel beheer maakt tijdens de werkzaamheden gebruik van autorisatiematrices. In de autorisatiematrices staat beschreven of een functionaris geautoriseerd mag worden voor een bepaalde applicatie. Tevens wordt voor veel applicaties beschreven voor welk autorisatieniveau functionarissen bevoegd zijn. Het niveau wordt bepaald door landelijke afspraken en de functie en of rol van de medeweker.

Deze matrices zijn in de tijd dat functioneel beheerders nog voor de diensten werkten, opgesteld in opdracht van de diensthoofden. Doordat de matrices zijn opgesteld onder verschillende diensthoofden zijn verschillende formats gebruikt. Dit laatste is geen Wpg issue maar laat ruimte tot verbetering voor de efficiëntie. Er is een proces gestart om alle matrices gelijk te trekken zodat deze kunnen worden samengevoegd tot een overkoepelende matrix. Deze nieuwe matrices zijn nog niet formeel goedgekeurd. Tot 2010 lag de verantwoordelijkheid van (het onderhoud en het gebruik van) de autorisatiematrix bij de Informatie Management Adviseur van de betreffende dienst. De IMA handelde in opdracht van de dienstleiding.

Sinds de vorming van de nieuwe afdeling is functioneel beheer verantwoordelijk voor het doorvoeren van aanpassingen aan de autorisatiematrices. Verzoeken hiertoe kunnen worden ingediend door de gemandateerde. Het beheer van matrices wordt binnen functioneel beheer door twee personen binnen de back-office gedaan. Indien er een aanpassing door de back-office wordt gedaan, wordt de front-office hierover geïnformeerd. De matrices zijn opgeslagen op de gemeenschappelijke schijf van functioneel beheer. De matrices zijn voor alle medewerkers toegankelijk. De lijsten die door de front-office worden gebruikt zijn niet tegen schrijven beveiligd.

Volgens het autorisatiebeleid kunnen er controles op conflicterende autorisaties worden uitgevoerd. Dit dient nog te gebeuren.

Het autorisatie aanvraagproces
Bij indiensttreding van een nieuwe medewerker informeert de afdeling P&O functioneel beheer en de afdeling waar de medewerker zal worden ingezet, over de indiensttreding en de te vervullen functie. Functioneel beheer maakt vervolgens een account voor Windows aan, inclusief toegang tot de gemeenschappelijke schrijven.

Het diensthoofd van de afdeling waar de nieuwe medewerker is aangesteld, of een door hem gemandateerde vraagt vervolgens de benodigde autorisaties aan. Per dienst is een overzicht met gemandateerden opgesteld, over het algemeen zijn dit operationele chefs of unithoofden. Regelmatig (maandelijks) voert functioneel beheer controles uit op de actualiteit van de gemandateerde lijst door deze te vergelijken met door P&O aangeleverde lijsten. Leidinggevenden kunnen voor het aanvragen van autorisaties gebruik maken van de autorisatiematrix waarin onder andere is vastgelegd welke applicaties toegankelijk dienen te zijn voor bepaalde functies. Op basis van rollen kan dat worden uitgebreid door de gemandateerde.

Na ontvangst van een autorisatie aanvraag controleert functioneel beheer de aanvraag. De identiteit van de aanvrager wordt in principe gecontroleerd aan de hand van de mail. Een uitgangspunt is dat aanvragen alleen via de mail mogen worden gedaan. De controle door functioneel beheer gebeurt aan de hand van de autorisatiematrix. Indien de aangevraagde autorisatie niet overeenkomt met de matrix wordt contact opgenomen met de gemandateerde die de aanvraag heeft gedaan. Voor sommige applicaties zijn opleidingseisen. In deze gevallen controleert functioneel beheer of de medewerkers de benodigde opleidingen gevolgd hebben.

In het verleden was het voor medewerkers van het KLPD mogelijk om rechtstreeks contact op te nemen met de vtsPN om autorisaties aan te vragen. In 2011 heeft de afdeling functioneel beheer afspraken gemaakt met de vtsPN waardoor alleen autorisaties verzoeken van functioneel beheer door de vtsPN worden uitgevoerd.

Aanvragen voor externe medewerkers die niet in dienst zijn van het KLPD worden door het diensthoofd aangevraagd. De privacyfunctionaris heeft hierbij een controlerende functie. Externen krijgen tijdelijke accounts waarvan de afloopdatum handmatig wordt ingesteld. Tijdelijke accounts zijn te herkennen aan het 'dienstnummer' welke afwijkt van het standaard account. Tijdelijke accounts worden maximaal voor één jaar uitgegeven, waarna ze eventueel kunnen worden verlengd. De privacyfunctionaris houdt een overzicht bij van alle aanvragen voor tijdelijke autorisatie door externe medewerkers. Functioneel beheer controleert periodiek of de accounts op korte termijn verlopen. Is dit het geval dan sturen zij de aanvrager hiervan een melding. Deze is dan in de gelegenheid om het account te verlengen.

Als gevolg van de consolidatie van verschillende functionele afdelingen tot één centrale afdeling dienen een aantal procedurebeschrijvingen, werkafspraken en richtlijnen voor autorisatiebeheer nog op elkaar te worden afgesteld. De gewenste uniformiteit moet leiden tot een efficiënter autorisatiebeheer. Deze efficiëntieslag is echter niet noodzakelijk om aan de Wpg te voldoen.

DKDB
Binnen de DKDB maken de leidinggevenden gebruik van het korpsbrede autorisatieproces. Daarnaast wordt toegang gegeven tot specifieke systemen door de lokale functioneel beheerder. Externen krijgen geen toegang tot de gegevens van de DKDB. De functioneel beheerder is tevens privacyfunctionaris en heeft daamee een dubbelrol. Hierdoor heeft privacyfunctionaris overzichten welke medewerkers geautoriseerd zijn tot welke systemen binnen de DKDB. Dit kan op den duur tot

problemen met onafhankelijkheid leiden als de privacyfunctionaris toezicht moet houden over het eigen autorisatieproces.

DNR
Teamleiders zijn verantwoordelijk voor het aanvragen van autorisaties en zijn hiervoor officieel gemandateerd. De rol van een medewerker binnen een team is bepalend voor de autorisatie die wordt aangevraagd. Omdat de teamleider voornamelijk bezig dient te zijn met zijn dossier en onderzoek en niet met allerlei formulieren en overige procedures, wordt er gestreefd naar het vereenvoudigen van de autorisatieprocedure. Een mail door de teamleiders naar het kwaliteitsbureau en functioneel beheer is voldoende om een autorisatie aan te vragen. Omdat het proces overzichtelijk en inzichtelijk moet zijn is er een autorisatiematrix gemaakt met rollen en bijbehorende autorisaties.

Binnen de DNR wordt van verschillende applicaties gebruik gemaakt. De verantwoordelijkheid voor de applicaties is divers. Voor het autorisatieproces van de DNR is beschreven hoe aanvragen voor autorisaties van het NIS account van het KLPD en specifieke applicaties zoals BVO, Summ-IT de G:\ schrijf, I-base, KVK, Blue View, NSIS, Kadaster, HKS, BVO Bruto/netto, EIS, RDW, AVR, VROS, D&B kunnen worden aangevraagd. Dit handboek is conform de Wpg geschreven.

DOS OIV
De operationele chef is verantwoordelijk voor het aanvragen van autorisaties. Via een digitaal formulier worden de autorisaties via functioneel Beheer aangevraagd. Via vastgestelde profielen worden autorisaties toegewezen. Dit proces verloopt nog niet gestroomlijnd. Zo duurt het in sommige gevallen lang voordat autorisaties worden toegewezen. Dit wordt veroorzaakt door de strakke procedures die nu worden aangehouden. Dit is de succesfactor voor het goed bijhouden van het autorisatieoverzicht maar zorgt in de praktijk soms voor irritatie omdat het volgen van de procedures tijd kost.

Het is mogelijk om tijdelijke krachten te autoriseren. Dit verloopt via standaardprocedures en de tijdelijke krachten krijgen een beperkte autorisatie.

DOS Infodesk
Binnen de infodesk heeft de procesvoerder de taak opgedragen gekregen (van betreffend unithoofd) autorisaties voor de infodesk medewerkers te regelen per 2011. De autorisaties worden bij functioneel beheer en andere plaatsen (Kadaster, KvK, voetbal volgsysteem, het RIK NIK portal) aangevraagd. Hiervoor is een lijst met autorisaties waarvoor medewerkers moeten worden aangemeld.

IPOL, unit Criminaliteit
Bij binnenkomst van een nieuwe medewerker moet een leidinggevende aan de voorkant aankruisen wat er geregeld moet worden zoals de werkplek, de tools die de medewerker nodig heeft, de handelingen die de medewerker mag uitvoeren en de mappen en bronnen waar de medewerker toegang toe moet hebben. Er is een standaard pakket met tools per functionaris en niveau van autorisatie. Dit maakt het aanvinken praktischer. Als een medewerker de unit verlaat of van functie verandert moet de leidinggevende dit doorgegeven.

Voor autorisatieaanvragen is een digitaal aanvraagformulier opgesteld. Het formulier staat op de G:/ schijf. Alleen de gemandateerde kan een aanvraag voor autorisaties indienen. Van de aanvragen wordt een kopie in de personeelsmap op de G:/ schijf bewaard. De bewaartermijn hiervan valt niet onder de verantwoordelijkheid van de leidinggevende.

Voor bijzondere of tijdelijke autorisaties wordt een tijdelijke autorisatie afgegeven. Wanneer een project is afgerond kan een medewerker niet meer bij de mappen van de andere afdeling.

Voor BlueView en BVO geldt dat na een bepaalde termijn van inactiviteit accounts worden geblokkeerd. Medewerkers moeten dan opnieuw een opleiding volgen om weer toegang te krijgen tot de applicatie.

Wijziging en verwijdering
P&O levert periodiek een lijst met medewerkers welke uit dienst zijn getreden. Aan de hand van deze overzichten worden autorisaties ingetrokken. Het proces voor interne personeelsmutaties is nog niet geïmplementeerd. Functioneel beheer heeft het voornemen om dit proces in 2012 te ontwikkelen. Hiervoor zal nog een plan van aanpak worden opgesteld. Het streven is het doorvoeren van wijzigingen op autorisaties van medewerkers op basis van door P&O aangeleverde overzichten. Hoewel nog niet alle interne personeelsmutaties automatisch worden verwerkt, is er een proces in werking dat de autorisaties voor bepaalde applicaties automatisch blokkeert indien er gedurende drie maanden niet is ingelogd. Dit is niet voor alle applicaties ingericht.

Het proces van het autoriseren van uitleen- en tijdelijk personeel verloop via een aanvraagformulier bij de privacyfunctionaris. Functioneel beheer is voornemens dit proces beter inzichtelijk te maken door aparte personeelsnummers voor hen aan te maken.

De procesvoerder handelt wijzigingen of verwijdering van autorisaties in beheer bij externe partners af. Tot op heden is er vanuit het KLPD nog geen controle of audit geweest op het schoningsproces van autorisaties. Er worden nog plannen ontwikkeld om de privacyfunctionarissen een rol te geven bij de controle van het autorisatieproces.

DKDB
Bij uitdiensttreding of verandering van functie wordt dit door de leidinggevenden gemeld. Er geldt een uitzondering wanneer de medewerker ergens anders binnen het korps aan de slag gaat.

Regelmatig wordt gecontroleerd of de door de DKDB zelf uitgegeven autorisaties nog correct zijn of dat er zich mutaties hebben voorgedaan. Dit wordt onder andere gedaan vanwege licentiekosten. Na twee of drie maanden van inactiviteit worden bepaalde applicaties, zoals VIPER, automatisch afgesloten.

DNR
De Teamleiders zijn primair verantwoordelijk voor het verwijderen van autorisaties. Zij hebben een overzicht van welke personen er binnen een onderzoek zijn geautoriseerd. Er zijn afspraken gemaakt over hoe men na een onderzoek een autorisatie van een persoon moet verwijderen. Bij vertrek worden autorisaties op 0 gezet. De autorisaties worden niet verwijderd omdat dan niet meer kan worden aangetoond welke personen binnen een onderzoek werkzaam zijn geweest. Controle op de juiste en tijdige verwijdering van autorisaties is een samenspel tussen de verantwoordelijke teamleider en het kwaliteitsbureau. In de praktijk kan het door de hectiek voorkomen dat autorisaties niet tijdig worden verwijderd. Vooral doordat rechercheurs tijdelijk worden ingeleend of doordat medewerkers vanuit de regio worden toegevoegd.

Langzaam maar zeker groeit het bewustzijn en de professionaliteit op de werkvloer met betrekking tot onder andere het afsluiten van onderzoeken en het verwijderen van autorisaties. Twee keer per jaar worden alle onderzoeken doorgelopen met de teamleiders om te kijken welke onderzoeken nog openstaan en waarbij de autorisaties moeten worden verwijderd.

DOS OIV
Bij functiewijziging of op het moment dat een medewerker de organisatie verlaat informeert de operationeel chef de functioneel beheerders. De operationeel chef van de OIV gaat ervan uit dat functioneel beheer vervolgens de autorisaties verwijdert.

DOS Infodesk
Als medewerkers van functie veranderen of de organisatie verlaten wordt hij of zij per email afgemeld. Of autorisaties altijd netjes worden verwijderd is onbekend. Incidenteel komen er autorisatielijsten binnen en wordt dit gecontroleerd.

IPOL, unit Criminaliteit
Medewerkers van personeelszaken en gegevensbeheer dienen de opdrachten voor het toewijzen of verwijderen van autorisaties af te handelen. De leidinggevende heeft hier verder geen toezicht op. Leidinggevenden ontvangen geen lijsten met overzichten van autorisaties ten behoeve van controle.

De geïnterviewden geven aan dat medewerkers van gegevensbeheer wel alert zijn op de autorisaties. Ze houden overzichten bij wie waarvoor is geautoriseerd en of dit nog actueel is. De privacyfunctionaris voert geen steekproef uit op de autorisaties.

CIE
Voor de uitgifte van autorisaties binnen de CIE is een model opgesteld. Hierin is aangegeven welke medewerkers welke rechten krijgen. Daarnaast zijn hierin de eisen vastgelegd zoals screening. De OvJ was betrokken bij het opstellen van het model. De OvJ wordt niet bij elke nieuwe aanstelling geconsulteerd. Alle medewerkers die in dienst komen bij de CIE krijgen van de CIE-procescoördinator of de registerbeheerder een training hoe de systemen werken en op welke wijze de systemen moeten worden toegepast. Hierbij is aandacht voor de WPG en subjectenbeheer.

Het autorisatieproces van de CIE is tweeledig. Voor de standaard applicaties vragen leidinggevenden bij functioneel beheer autorisaties aan. Dit proces is vergelijkbaar met dat van de andere diensten van het KLPD. Echter voor het kernsysteem BVO Bruto is een ander proces opgesteld. De technische autorisaties voor toegang tot de systemen worden door de Nationale CIE (NCIE) uitgegeven. De registerbeheerder van het KLPD autoriseert de nieuwe medewerker tot de lokale gegevensverzamelingen in opdracht van het hoofd CIE. Om de paar maanden wordt door de procescoördinator en de registerbeheerder een controle op alle verleende autorisaties uitgevoerd.

Protocolleren autorisaties
Autorisatieaanvragen die bij functioneel beheer worden gedaan, worden in verschillende databases vastgelegd. Deze databases worden IVO genoemd. IVO wordt niet geschoond gezien het verantwoordingsinformatie betreft. Vastlegging van onderliggende documenten geschiedt per aanvraag, niet op naam. Er worden met name onderliggende documenten vastgelegd indien het verzoek afwijkt van de autorisatiematrix. Hierbij kan men denken aan de mail uitwisseling die heeft plaatsgevonden tussen de gemandateerde aanvrager en de functioneel beheerder.

In principe worden alleen aanvragen via de mail afgehandeld. In bepaalde gevallen wordt hiervoor een uitzondering gemaakt. Hierbij kan men denken aan een geblokkeerde autorisatie van het mobiele systeem in een dienst auto. De gebruiker komt hier pas achter als deze in de dienstauto plaats neemt. Dit soort aanvragen worden gecontroleerd via een terugbel procedure. Het gaat hier echter alleen om het vernieuwen van een geblokkeerd account en niet het uitgeven van een nieuw account.

Voor aanvragen worden functionele (gemeenschappelijke) mailboxen gebruikt. Aanvragers die zich rechtstreeks wenden tot een medewerker worden doorverwezen.

Het decentrale autorisatieproces wordt door de procesvoerders vastgelegd in functionele mailboxen. Door alle procesvoerders binnen een dienst te benaderen kan de privacyfunctionaris inzicht krijgen in de vastlegging van autorisaties. Dit proces is erg arbeidsintensief maar voldoet wel aan de Wpg.

4.5.3 *Verbeterpunt*

- Als verbeterpunten zijn te noemen:
- Zorg voor algemene bekendheid van het autorisatiebeleid.
- Personeelsmutaties worden in veelvoorkomende gevallen niet verwerkt. Zorg voor een proces dat personeelsmutaties door P&O inzichtelijk worden gemaakt en dat functioneel beheer hierover wordt geïnformeerd. Functioneel beheer kan vervolgens de autorisaties aanpassen.
- Zorg voor toezicht op de protocollering van het decentrale autorisatie proces.

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*

Er is geen eenduidige definitie van de begrippen geautomatiseerd vergelijken en in combinatie met elkaar verwerken. Binnen het KLPD zoekt naar schatting 90% van de medewerkers op basis van KENO-sleutels naar politiegegevens. Deze zoekmethode valt volgens het KLPD niet onder geautomatiseerd gelijken en in combinatie met elkaar verwerken, maar valt volgens het KLPD onder raadplegen.

Er zijn (formeel) nog geen verantwoordelijke functionarissen voor het geautomatiseerd vergelijken aangewezen. Echter, zoals artikel 11 voorschrijft mag slechts een kleine groep functionarissen/medewerkers met artikel 11 werken en dat is bij het KLPD het geval, namelijk de DNR: T-HTC.

Bij complexe zoekacties wordt in veel gevallen de Officier van Justitie betrokken. Dit is nog niet geformaliseerd of herleidbaar in een proces. Momenteel wordt vanuit het

Wpg-programma een risicostudie uitgevoerd om de risico's en mogelijkheden te analyseren

4.6.3 *Verbeterpunten*

- Als verbeterpunten zijn te noemen:
- Op landelijk niveau: Stel een definitie op van geautomatiseerd vergelijken en in combinatie met elkaar verwerken. Geef daarbij de grenzen aan van geautomatiseerd vergelijken en in combinatie met elkaar verwerken en ontwikkel casuïstiek aan de hand waarvan geautomatiseerd vergelijken en in combinatie met elkaar verwerken kan worden besproken.
- Op korps niveau: Draag deze definitie uit en bespreek de casuïstiek met medewerkers die te maken hebben met geautomatiseerd vergelijken en in combinatie met elkaar verwerken.
- Stel schriftelijke afspraken op over hoe bevoegd functionarissen alleen in combinatie mogen verwerken nadat hier schriftelijke toestemming voor is gegeven door het bevoegd gezag. Denk hierbij aan de melding aan de privacyfunctionaris in relatie tot de protocolplicht.

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 aanlelding 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*

Tijdens een eerste risico inventarisatie door het projectteam WPG is vastgesteld dat voor grijze diensten (artikel 9) het verwijderen van politiegegevens goed is geregeld. Bij de recherche wordt dezelfde werkwijze gehanteerd als tijdens de Wet Politieregisters. De "blauwe" afdelingen (artikel 8) worden wel als risico gebied aangewezen gelet op de bewaartermijnen.

Het projectteam WPG heeft beschreven hoe het KLPD de schoning van politiegegevens gaat inrichten. Hierbij is er rekening mee gehouden dat applicaties zoals BVH en BVO niet de opslag van onder andere beeldmateriaal zoals foto's ondersteunen. Deze bestanden worden daarom op de G:\ schijf opgeslagen.

Artikel 8

De politiegegevens die onder artikel 8 vallen worden voornamelijk in BVH en op de G:\schrijf opgeslagen. Hieronder staat per methode van opslag hoe de bewaartermijnen zijn ingeregeld:

- In BVH is nog geen mogelijkheid tot het automatisch verwijderen van politiegegevens. Momenteel wordt de update BVH 1.2.2 van de vtsPN getest die automatische verwijdering mogelijk moet maken. In verband met de risico's van het activeren van de schoningsmodule wordt de update op landelijk niveau getoetst. Het KLPD wacht de uitslagen van deze en haar eigen testen af voordat de schoningsmodule wordt geactiveerd.
- De politiegegevens opgeslagen op de G:\ schrijf werden in het verleden niet of nauwelijks geschoond. De invoering van de Wpg heeft er voor gezorgd dat het

Programma WPG een systematiek heeft ontwikkeld om de mappen conform de Wpg in te richten. Vooralsnog zijn bij de Dienst Verkeerspolitie en de Dienst Spoorwegpolitie acht instructiesessies gehouden voor operationele chefs door het Programma WPG om de nieuwe werkwijze toe te lichten. De opzet is dat de operationele chefs deze instructie onder hun medewerkers verspreiden. Tevens zijn werkinstructies voor medewerkers en functioneel beheer opgesteld waarin de procedures voor schoning zijn opgenomen.

Binnen de nieuwe systematiek heeft de afdeling gegevensbeheer in samenwerking met de vtsPN aan units en diensten autorisaties toebedeeld voor het werken met politiegegevens op de G:\schijf:

- 0 tot 1 jaar (lezen en schrijven).
- 1 t/m 5 jaar (lezen).
- 6 t/m 10 jaar (niet toegankelijk voor operationeel gebruik).

De politiegegevens worden opgeslagen in de mappenstructuur op basis van het bij de zaak horende BVH-nummer. De autorisaties voor de mappen in de mappenstructuur zijn aan deze BVH-nummers gekoppeld. Periodiek zullen lijsten worden uitgeprint en de autorisaties handmatig worden aangepast. Het aanpassen van de autorisaties van de mappen wordt in de toekomst opgenomen in een maandelijks terugkerend proces.

Vooralsnog is de nieuwe werkwijze voor de mappenstructuur ingeregeld voor de Diensten Spoorwegpolitie en Verkeerspolitie. Door kinderziektes en problemen met de autorisaties is het niet mogelijk dit proces in één keer voor alle afdelingen in te voeren. Vanaf 2012 zal dit autorisatieproces bij de overige "blauwe" diensten worden geïmplementeerd.

DOS Infodesk
Volgens het Intern audit rapport worden alle gegevensverzamelingen (afgezien van BVO) binnen de infodesk na één jaar achter een schot geplaatst. Gegevens achter het schot worden na vier jaar vernietigd. De infodesk heeft een map "Verwijderd" in Outlook opgenomen. Hierin wordt alle email correspondentie opgeslagen. Deze vastlegging wordt van Outlook naar de G:\ schrijf getransporteerd. Op de G:\ schrijf worden de gegevens vervolgens vier à vijf jaar bewaard voor verantwoording. Er wordt gezorgd dat na één jaar de gegevens alleen nog voor de beheerder toegankelijk zijn. Hierdoor zijn de gegevens niet langer voor operationele doeleinden beschikbaar.

DOS OIV
De OIV is een doorgeefluik van politiegegevens. Zij voelen zich daarom niet verantwoordelijk voor de bewaartermijnen van deze gegevens. Het toezien op de termijnen voor het verwijderen en vernietigen van gegevens wordt door de OIV gezien als een taak van functioneel beheer. In de praktijk bewaart de OIV meestal een kopie van alles voor een periode van 14 dagen, hierna is het proces afgelopen en worden de gegevens vernietigd.

Artikel 9
Het basispolitiesysteem BVO (artikel 9) maakt het mogelijk om door middel van het intrekken van autorisaties politiegegevens te verwijderen. Het moment van afsluiten is afhankelijk van het moment waarop een zaak onherroepelijk is geworden of wanneer het OM besluit de zaak niet verder te vervolgen. De teamleider is verantwoordelijk om de gegevens ontoegankelijk te maken als een onderzoek wordt afgesloten. Dit wordt gedaan door een autorisatie op niveau 0 te zetten. Daarnaast is het de taak van de teamleider om het af te sluiten dossier bij functioneel beheer aan te melden om het dossier ontoegankelijk te laten maken. De teamleider stuurt

tot slot een Proces Verbaal naar de Privacyfunctionaris met de datum van afsluiting van het onderzoek. De privacyfunctionaris voert vervolgens een controle uit om te kijken of alles is geregeld. De privacyfunctionaris controleert regelmatig of er nog zaken open staan op basis van een overzicht van aangevraagde, afgesloten en openstaande onderzoeken.

Het proces om artikel 9 gegevens efficiënt te kunnen verwijderen is afhankelijk van de terugkoppeling van het OM. Het OM dient het KLPD te voorzien van afloopberichten voor onder andere onherroepelijke zaken. De OIV heeft in 2011 namens de Korpschef van het KLPD een brief naar alle hoofdofficieren van justitie gestuurd met de mededeling dat alle gerechtelijke uitspraken naar de OIV dienen te worden gestuurd. Dit heeft er toe geleidt dat nu ongeveer 50% van de arrondissementsrechtbanken een terugkoppeling naar de OIV stuurt. De overige 50% stuurt geen terugkoppeling of stuurt deze naar de opsporingseenheden die de betreffende zaak hebben behandeld. Als gevolg hiervan kan de OIV niet conform de gerechtelijke uitspraak de status van personen aanpassen. Het monitoren van zaken die onherroepelijk zijn geworden is niet handmatig door teamleiders uit te voeren omdat zaken soms jaren lopen.

Binnen de huidige functionaliteit van BVO is het niet mogelijk om gegevens automatisch te laten vernietigen na het verstrijken van de termijn. Op korte termijn (december 2011) wordt een module geïnstalleerd die dit mogelijk moet maken. Tot dat de systemen het vernietigen ondersteunen heeft het KLPD een handmatig proces ingericht. In 2011 zijn alle zaken ouder dan vijf jaar, door de privacyfunctionaris, voorgelegd aan de verantwoordelijke bevoegd functionarissen waarbij zij dienden vast te stellen of de gegevens konden worden vernietigd. Alleen op basis van wettelijke gronden is hiervan afgeweken.

DKDB
Door de grote diversiteit en de versnippering van informatie is het zeer arbeidsintensief om de bestaande mappen op de G:\ schrijf te schonen. Daarom is gekozen om te wachten met schonen tot SUMM-IT beschikbaar is. Als dit het geval is wordt de mappenstructuur op alleen lezen gezet en worden mappen geschoond als er een bepaalde tijd niet meer in wordt gekeken.

Schoning van de DKDB systemen VIPER en PAPER gebeurt maandelijks door middel van een script. Dit levert een lijst met gegevens op van registraties, die de afgelopen 5 jaar niet zijn gemuteerd. Deze lijst wordt door de DIK gevalideerd, waarna functioneel beheer de gegevens verwijdert. Als gegevens uit de systemen worden verwijderd, verplaatst functioneel beheer de gegevens naar een ontoegankelijke locatie behoudens functioneel beheer zelf. Tot op heden zijn politiegegevens nog niet vernietigd omdat de periode van 10 jaar nog niet is verstreken.

DNR
Het globale proces voor het bewaren van artikel 9 onderzoeken is beschreven. Hierin zijn de Wpg relevante artikelen opgenomen. Tevens is een template proces verbaal opgesteld waarmee een medewerker dient te verklaren dat alle benodigde stappen zijn genomen om een onderzoek af te sluiten. Daarnaast is een gedetailleerde beschrijving opgesteld die stap voor stap beschrijft hoe een onderzoek dient te worden afgesloten. Deze beschrijving is opgesteld door het Kwaliteitsbureau van de DNR.

In de praktijk zal na terugkoppeling van het OM dat een zaak onherroepelijk is, de teamleider het onderzoek afsluiten en de gegevens laten verwijderen door

functioneel beheer. De privacyfunctionaris voert een controle uit op de afsluiting van onderzoeken.

BVO ondersteunt niet de opslag van bewijsmateriaal zoals bijvoorbeeld foto´s. Dit soort documenten worden op de G:\ schijf opgeslagen. Omdat op de G:\ schijf gedegen controle op bewaartermijnen en het effectief delen en doorzoeken van informatie niet mogelijk is, heeft de DNR de intentie om de G:\ schijf niet langer te gebruiken voor operationele gegevens. Hiervoor in de plaats zal de DNR gebruik maken van SUMM-IT die de opslag van onder andere beeld en geluidsmateriaal in het programma zelf mogelijk maakt.

In het document "0 3 Projectplan G_schrijf Summ-IT" staat beschreven hoe bij de overgang van BVO naar Summ-IT de medewerkers een jaar de tijd zullen krijgen om gegevens van de G:\ schijf naar het betreffende onderzoek te verplaatsen. Hierna worden de niet verplaatste gegevens op de G:\ schijf verwijderd dan wel vernietigd.

IPOL, unit Criminaliteit
Voor Fluïde Netwerken Aanpak (FNA) geldt dat voor artikel 9 de preweeg wordt bewaard in een archief in de mappenstructuur op de G:\ schijf. De informatie wordt na één jaar vernietigd. Coördinatoren zijn verantwoordelijk voor de schoning van de G:\ schrijf. De analyses en preweeg documenten blijven een jaar raadpleegbaar en worden daarna vernietigd door een coördinator van de afdeling.

Artikel 10
Volgens de Wpg moet artikel 10 informatie uiterlijk vijf jaar na de datum van de laatste verwerking van gegevens die blijk geeft van de noodzaak tot het verwerken van politiegegevens van betrokkene op grond van het doel. Tot op heden wordt het automatisch verwijderen van politiegegevens in BVO netto technisch niet ondersteund. In de praktijk is het vooral voor de systemen lastig te bepalen welke informatie subjectwaardig is. Daarom heeft het KLPD samengewerkt op landelijk niveau om een module te ontwikkelen die hierin voorziet. De nieuwe module wordt momenteel in de testomgeving getest. Als de tests goed verlopen zal de module in januari 2012 in productie worden genomen. Na oplevering zal de CIE een inhaalslag maken en de gegevens schonen.

Artikel 12
Artikel 12 gegevens dienen na 10 jaar te worden vernietigd. Tot voor kort werden deze gegevens in verschillende systemen en op verschillende locaties opgeslagen. Dit werd veroorzaakt door verschillende werkwijzen per team. Er is een project gestart om de gegevens in één systeem samen te voegen. De technische samenvoeging is afgerond en de gegevens staan nu in BVO bruto. Het tweede deel van het project bestaat uit een inhoudelijke controle van de gegevens. Hierbij wordt gecontroleerd of bepaalde informanten niet in meerdere onderzoeken voorkomen en of de gegevens niet ouder zijn dan 10 jaar. Dit deel van het project zal naar verwachting in januari 2012 worden afgerond.

De schoningswerkzaamheden ten behoeve van de bewaartermijn van artikel 12 vergen in het algemeen niet veel tijd. Bij de back office van de CIE is een lijst van alle ICS-coderingen met bijbehorende inschrijf- en afmelddata. Daaruit is eenvoudig af te leiden of gegevens moeten worden verwijderd. Na overleg met de teamleider en de CIE-OvJ kunnen de gegevens vrij eenvoudig uit BVO-bruto worden verwijderd. Een schriftelijke procedure hiervoor wordt in het huidige project beschreven.

Binnen de CIE wordt rekening gehouden met de halfjaarlijkse controle op de bewaartermijnen van artikel 10 en 12. De halfjaarlijkse controle is opgenomen in de

instructie voor de CIE officieren. De periodieke controle door de officier is aanvullend op de doorlopende controle van de gegevens door de CIE zelf. De back office van de CIE handelt alle netto-verslagen administratief af. Deze worden gekoppeld, beoordeeld op opnamecriteria en zo nodig juridisch verantwoord middels subjectregistraties. De registerbeheerder brengt maandelijks een verslag uit over de geconstateerde kwaliteit van de administratie en controleert of de verbeteringen worden doorgevoerd. De CIE-procescoördinator presenteert daarnaast per kwartaal een overzicht van zowel de bruto als de netto productie, inclusief de administratieve mutaties.

Gegevens van informanten worden binnen vier maanden van BVO bruto naar BVO netto overgezet. Voordat de gegevens worden overgezet voert de teamchef een controle uit. Zodra de gegevens in BVO netto zijn opgenomen zijn het artikel 10 gegevens en kunnen ze verder worden verwerkt. Na de overdracht van de gegevens worden deze tegen schrijven beveiligd.

Artikel 13
Het schonen van artikel 13 gebeurt door een coördinator van IPOL. Informatie ouder dan één jaar wordt als verouderd beschouwd en is daarom niet meer nuttig.

Het systeem Landelijk Overvallen Registratie Systeem (LORS) wordt gebruikt voor de opslag van informatie over overvallen en daders. De opgeslagen gegevens in dit systeem worden na 20 jaar geschoond. Dit is een landelijke afspraak. Omdat de informatie in LORS nog geen 20 jaar oud is heeft er nog geen schoning van gegevens plaatsgevonden.

Hernieuwde verwerking
Er is nog geen formeel proces voor de vastlegging en afhandeling van hernieuwde verwerkingen. Hiermee is de protocollering voor de privacyfunctionaris ook nog niet georganiseerd. Hernieuwde verwerkingen is een onderwerp dat in 2012 door het KLPD zal worden onderzocht.

DKDB
Het is binnen de DKDB nog niet voorgekomen dat verwijderde gegevens terug dienden te worden gehaald voor operationele doeleinden. Het kan wel voorkomen dat vanuit de politiek om verantwoording wordt gevraagd voor uitgevoerde activiteiten door de DKDB. Zo zou men bijvoorbeeld kunnen vragen welke activiteiten de DKDB heeft uitgevoerd op Koninginnedag.

Functioneel beheer
Indien gegevens afgeschermd zouden worden door middel van autorisaties, is het van belang dat de functioneel beheerders op de hoogte zijn van de regels omtrent hernieuwde verwerkingen. Tijdens de audit is aangegeven dat hernieuwde verwerkingen slechts na toestemming van de Officier van Justitie mogen worden uitgevoerd. Dit wordt op de afdeling als algemeen bekend beschouwd.

DOS infodesk
De regeling voor hernieuwde verwerkingen is bij de procesvoerder bekend. Voor zover bekend zijn bij de infodesk hernieuwde verwerkingen nog niet voorgekomen. Relevante 'te' oude informatie wordt ondanks dat het relevant is, niet verstrekt. Daar waar het om artikel 9 onderzoeken gaat is er in veel gevallen nog geen uitspraak en is het dus nog mogelijk om de informatie te gebruiken.

4.7.3 *Verbeterpunten*

- Houd beheersmaatregelen voor verwijdering en vernietiging in de systemen BVH en BVO landelijk op de agenda.
- Stel procedures op voor de aanvragen en vastlegging van hernieuwde verwerkingen. Denk hierbij aan de melding aan de privacyfunctionaris in relatie tot de protocolplicht.
- Implementeer de reeds ontwikkelde mappenstructuur voor alle relevante "blauwe" diensten.
- Blijf betrokken bij de landelijke aanpassingen op de basisvoorzieninngen.
- Zorg dat het onderwerp afloopberichten van het OM op de landelijke agenda komt met hoge prioriteit.

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*

Volgens het "het opleidingsplan Wet Politiegegevens versie 1.0" zijn tussen het tweede kwartaal 2009 en het tweede kwartaal 2010, 120 bevoegd functionarissen opsporing en 80 bevoegd functionarissen informatieverwerking opgeleid. In voorafgaande fases waren reeds 31 bevoegd functionarissen opgeleid. De opleiding "bevoegd functionaris opsporing" bestaat uit twee dagdelen en de opleidlng "bevoegd functionaris informatie" bestaat uit vier dagdelen.

Binnen het KLPD zijn voor artikel 9 en 10 bevoegd functionarissen op functie aangesteld. De taken van de bevoegd functionaris inzake artikel 9 staan beschreven in het document "Werksetting bevoegd functionaris in het kader van artikel 9 WPG". Hieronder zijn de taken opgenomen:

1. Meldt tijdig het doel van een verwerking aan, als bedoeld in artikel 9, tweede lid WPG.
2. Ziet er op toe dat binnen zijn/haar onderzoek de herkomst en de wijze van verkrijgen van de gegevens wordt geregistreerd (artikel 3, vierde lid WPG).
3. Autoriseert de personen voor de verwerking van politiegegevens die door zijn team worden uitgevoerd ten behoeve van onderzoeken, zoals bedoeld in artikel 9 WPG.
4. Toets het voorgenomen doelafwijkend gebruik van politiegegevens aan de regels van de WPG (Zowel pro-actief als re-actief), als bedoeld in artikel 9 WPG.
5. Beoordeelt en geeft al dan niet instemming tot verdere verwerking van politiegegevens van zijn/haar onderzoek, als bedoeld in artikel 9, derde lid, artikel 11, eerste lid, vierde lid, artikel 12, derde lid WPG.
6. Meldt het afgeronde artikel 9 onderzoek af en schoont de gegevens of biedt deze ter archivering aan, als bedoeld in artikel 14 WPG.

In het kader van artikel 10 Wpg zijn de volgende bevoegd functionarissen aangewezen:

1. Hoofd Criminele Inlichtingen Eenheid en diens plaatsvervanger (DNR).
2. Hoofd van de eenheid die zich bezig houdt met het verwerken van gegevens met het ook op het verkrijgen van betrokkenheid van personen bij handelingen die kunnen wijzen op het beramen of plegen van terroristische misdrijven, mensenhandel of mensensmokkel en diens plaatsvervanger (DNR).
3. Hoofd van de Inlichtingendienst en diens plaatsvervanger (DOS).

De taken van de bevoegd functionaris inzake artikel 10 staan beschreven in het document "Werksetting bevoegd functionaris in het kader van artikel 10 WPG". Hieronder zijn de taken opgenomen:

1. Ziet er op toe dat binnen zijn/haar onderzoek de herkomst en de wijze van verkrijgen van de gegevens wordt geregistreerd (artikel 3, vierde lid Wpg);
2. Autoriseert de personen voor de verwerking van politiegegevens die door zijn team worden uitgevoerd ten behoeve van de verwerking, zoals bedoeld in artikel 10 WPG;
3. Toets het voorgenomen doelafwijkend gebruik van politiegegevens aan de regels van de WPG (Zowel pro-actief als re-actief), als bedoeld in artikel 9 WPG.

DKDB

Als de DKDB politiegegevens met een andere politiedienst deelt, verloopt dit altijd via het DIK. Het DIK heeft vier specialist informatieverwerkers en het hoofd DIK als bevoegd functionaris aangewezen. Elke specialist is gekoppeld aan een "robuuste eenheid" van 130 man. De specialist fungeert als aanspreekpunt voor deze medewerkers.

De DKDB is verantwoordelijk voor het beveiligen van hoogwaardigheidsbekleders. Vanwege onder andere het reisgedrag van de te beveiligen personen, heeft de DKDB regelmatig contact met de politieregio's om informatie in te winnen. Het komt ook voor dat het reisschema of de planning aan een politieregio kenbaar wordt gemaakt. Hierbij wordt de ontvangende politieregio middels een disclaimer erop gewezen dat zij de gedeelde gegevens niet binnen het opsporings- of handhavingsproces mogen gebruiken.

De disclaimer luidt als volgt:
"Gelet op artikel 7, tweede lid, van de Wet politiegegevens is de persoon dan wel instantie aan wie politiegegevens zijn verstrekt verplicht tot geheimhouding van politiegegevens, behoudens voor zover een bij of krachtens de wet gegeven voorschrift tot verstrekking verplicht of zijn taak daartoe noodzaakt. Deze geheimhoudingsplicht staat in de weg aan doorverstrekking van gegevens, tenzij een wettelijk voorschrift die mogelijkheid wel biedt. In die gevallen geldt de geheimhoudingsplicht dan tevens voor volgende ontvangers, die de gegevens doorverstrekt hebben gekregen".

Tijdens de audit is geconstateerd dat de door de DKDB in e-mails gebruikte disclaimer de ontvangende korpsen niet waarschuwt dat de gegevens niet mogen worden gebruikt bij het opsporings- en handhavingproces.

DNR

De DNR voert onder andere zogenaamde embargo-onderzoeken uit waarbij per definitie geen informatie wordt gedeeld. De embargo onderzoeken vallen onder de formele weigeringsgronden.
Gezien de grote tactische belangen van een aantal (niet embargo) onderzoeken binnen de DNR is er gekozen voor een tussenoplossing, het zogenaamde 'tussenfase dossiers'. Samen met de stuurgroep en het Landelijk Parket wordt dan besloten de

informatie op niveau 5 aan te maken, waardoor het niet meer landelijk raadpleegbaar is. Dit kan alleen na een besluit op het hoogste besturingsniveau. Hiermee geeft de DNR uitvoering aan de intentie van de wetgever zonder de tactische belangen te schaden.

Indien informatie beschikbaar wordt gesteld voor een ander onderzoek zal de teamleider een proces-verbaal opstellen van de verstrekte informatie.

IPOL, unit Criminaliteit
De unit criminaliteit stelt maandelijks de RIK's via het maandbericht (artikel 13) op de hoogte van de lopende onderzoeken. De unit criminaliteit vervaardigd tevens preweegdocumenten (artikel 9) en stelt deze, na goedkeuring van de stuurgroep aan een onderzoeksteam ter beschikking. Het onderzoeksteam zal op basis van deze documentatie een onderzoek starten. De overdracht vindt zowel digitaal via de politiemail als in hardcopy plaats. In de meeste gevallen vindt een persoonlijke overdracht plaats naar het team dat het onderzoek zal uitvoeren. Medewerkers van de unit criminaliteit informeren dan het onderzoeksteam persoonlijk hoe ze tot bepaalde conclusies zijn gekomen.

Binnen de unit criminaliteit zijn bevoegd functionarissen aangewezen. In het document "Overzicht functietyperingen – Bevoegd functionarissen artikel 9 def" is per dienst aangegeven welke functies als bevoegd functionaris zijn benoemd.

IPOL, unit Criminaliteit
Binnen de unit criminaliteit zijn bevoegd functionarissen aangewezen. Dit zijn over het algemeen de teamleiders en een aantal coördinatoren. Allen hebben een cursus tot bevoegd functionaris gevolgd. Tevens hebben de bevoegd functionarissen toegang tot de handreiking voor bevoegd functionaris die via het intranet beschikbaar is gesteld.

Infodesk
Om artikel 9 informatie goed te kunnen beheren is het van belang dat de infodesken die vergaande zoekmogelijkheden tot hun beschikking hebben, goed samenwerken met de bevoegd functionarissen.

De bezochte DOS infodesk verzamelt operationele gegevens door bronnen die eigendom zijn van anderen te raadplegen. De DOS infodesk heeft geen eigen gegevensverzamelingen en heeft daarom geen bevoegd functionarissen aangesteld. Wanneer de infodesk artikel 9 of 10 politiegegevens nodig heeft, vragen ze hiervoor toestemming aan de bevoegd functionaris van het betreffende onderzoek. Nadat de bevoegd functionaris heeft besloten de politiegegevens al dan niet te delen, neemt hij contact op met de aanvrager of vraagt dit aan de infodesk. Na dat de infodesk alle bronnen heeft doorzocht en alle mogelijke informatie heeft ontvangen wordt deze gegroepeerd en ter beschikking gesteld aan de aanvrager. De ter beschikking stelling wordt vastgelegd in een eigen registratie van de infodesk in BVO, genaamd "26 infodesk". Het document "procesbeschrijving / werkinstructie KIK-infodesk versie 2.0" beschrijft hoe dient te worden omgegaan met hits op artikel 10 CIE onderzoeken. Het document omschrijft echter niet hoe artikel 9 gegevens worden gedeeld.

Het KLPD maakt nog geen gebruik van de mogelijkheden om artikel 9 onderzoeken vooraf te coderen, waarmee van te voren kan worden bepaald of informatie van een bepaald onderzoek ter beschikking gesteld mag worden.

4.8.3 *Verbeterpunten*

- De DKDB dient aanvullende maatregelen te nemen om te borgen dat politiegegevens die ter beschikking zijn gesteld niet voor andere doeleinden worden gebruikt;
- Beschrijf in het document "procesbeschrijving / werkinstructie KIK-infodesk versie 2.0" hoe de infodesk met het delen van artikel 9 gegevens dient om te gaan.

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*

Het KLPD heeft een inventarisatie gemaakt van alle units die structureel politiegegevens verstrekken aan externen. Binnen het KLPD zijn de volgende afdelingen verantwoordelijk voor het merendeel van de verstrekkingen:

- De Spoorwegpolitie.
- De Waterpolitie.
- DOS OIV (verkeer).
- DOS infodesk.
- IPOL.

Deze afdelingen hebben bij de Wpg implementatie extra aandacht gekregen. Per onderzochte afdeling zijn de wijze van verstrekken en de aanwezige convenanten inzichtelijk gemaakt. Binnen deze afdelingen zijn de medewerkers op de hoogte van aan welke organisaties zij politiegegevens mogen verstrekken. Hiervoor maken zij onder andere gebruik van de landelijke verstrekkingenwijzer. De door ons bezochte informatie verstrekkende afdelingen die gebruik maken van de landelijke verstrekkingenwijzer, konden deze fysiek of digitaal benaderen. De Verstrekkingenwijzer wordt voornamelijk gebruikt om nieuwe medewerkers te informeren aan welke partijen politiegegevens mogen worden verstrekt.

Op basis van een risicoafweging is geconcludeerd dat door het Wpg conform inrichten van het verstrekkingenproces bij de drie grootste verstrekkende afdelingen invulling is gegeven aan de Wpg. Op dit moment zijn er geen andere structureel verstrekkende afdelingen bij het KLPD bekend.

Convenanten

Tijdens een maandelijks privacyoverleg is het proces voor het opstellen van convenanten en artikel 20 besluiten afgestemd. Dit is overeengekomen met alle privacyfunctionarissen van het KLPD. Er is een template convenant ontwikkeld waar het artikel 20 besluit onderdeel van uit maakt. Voor het opstellen van convenanten zijn de volgende punten van belang:

1. Convenanten worden door een privacyfunctionaris in samenwerking met een operationeel expert opgesteld.
2. Bij het opstellen van convenanten wordt gebruik gemaakt van een template gebaseerd op de landelijke handreikingen.
3. Momenteel bewaart de projectleider Wpg alle convenanten; deze zijn/worden gepubliceerd via het intranet.

4. In het ondermandaat en de hierbij behorende documenten staat beschreven wie formeel een convenant mag goedkeuren.
5. De meeste verstrekkingen lopen via IPOL en de intake functie van OIV.
6. Het NIC verstrekt informatie maar dit is voornamelijk geaggregeerde data.

Binnen het KLPD zijn in 2011 alle bestaande convenanten op onder andere de Wpg gecontroleerd. In 95% van de gevallen betrof het alleen werkafspraken en was er geen sprake van het uitwisselen of verstrekking van politiegegevens. Bij de overige 5% was dit wel het geval. De convenanten waarbij politiegegevens worden verstrekt zijn conform Wpg aangepast en vervolgens afgetekend. De projectleider Wpg bewaard momenteel alle artikel 20 convenanten. Deze worden gepubliceerd op het KLPDweb/intranet.

De DNR maakt ook gebruik van convenanten. Deze zijn echter niet volgens een eenduidige template opgesteld. Hierin zijn wel onder andere de volgende aspecten opgenomen: het onderwerp en doel, welke informatie wordt uitgewisseld, contactpersonen, geheimhouding en beveiliging.

DNR

Binnen de DNR zijn mondelinge beleidsafspraken gemaakt over hoe medewerkers met verstrekkingen om moeten gaan. Een voorbeeld van deze afspraken is dat de teamleider verstrekt in overleg met de betrokken officier. De teamleider is bevoegd functionaris en mag informatie delen. In de praktijk wordt weinig informatie uit artikel 9 onderzoeken gedeeld, mede omdat de Wpg daar weinig ruimte voor biedt. Elke verstrekking vanuit een artikel 9 onderzoek wordt vastgelegd in een mutatie in BVO.

De DNR verstrekt gegevens voor een groot deel op basis van convenanten. Tijdens de interviews is aangegeven dat echter een besluit nodig blijft voordat gegevens daadwerkelijk worden verstrekt, ook al ligt er een convenant aan ten grondslag. Op basis van convenanten worden politiegegeven verstrekt aan gemeenten, de belastingdienst en de IND. Tevens verstrekt de DNR politiegegevens aan het buitenland, hierbij borgt de bestaande regelgeving de juiste afhandeling. Medewerkers van de DNR beoordelen of het ontvangende land voldoende waarborgen treft om de privacy te waarborgen.

DOS OIV

De OIV verstrekt politiegegevens aan burgers. Het betreft hier hoofdzakelijk foto's van snelheidsovertredingen en informatie over verkeersongevallen waar de politie een registratie van heeft gemaakt in BVH.

Aanvragen voor politiegegevens worden hoofdzakelijk schriftelijk ingediend, in uitzonderingen gebeurt dit telefonisch. In eerste instantie wilde de OIV politiegegevens niet telefonisch verstrekken, omdat dan de identiteit van de aanvrager niet met zekerheid is vast te stellen. Echter de nationale ombudsman heeft bepaald dat een verstrekking ook telefonisch dient te geschieden. In het geval van een telefonisch verzoek dient een aanvrager zich met behulp van het burgerservicenummer te identificeren. Dit nummer wordt via het GBA gecontroleerd waarna de aanvrager een aantal standaard vragen over zijn of haar personalia (geboortedatum en -plaats) dient te beantwoorden. Bij een juiste beantwoording gaat de OIV over tot verstrekking van de politiegegevens.

Verstrekkingen van politiegegevens worden in de transactiemodule vastgelegd. Verstrekkingen vanuit BVH worden middels een I90 (maatschappelijke klasse) vastgelegd. Alle uitgaande poststukken worden in CORSA vastgelegd. In het geval van opsporingsverzoeken wordt de aanvrager doorverwezen naar de infodesk.

DOS Infodesk
Het KLPD beleid is dat de DOS infodesk alleen intern informatie deelt en geen informatie verstrekt aan externe partijen. Tijdens de audit is echter gebleken dat ook aan externe partijen informatie wordt verstrekt. De infodesk verstrekt informatie aan bijvoorbeeld FIOD-ECD, AID, SIOD,BIBOB en VROM.

De infodesk controleert voor een verstrekking van politiegegevens het doel en de noodzakelijkheid van de verstrekking. De infodesk controleert niet of de redenen van de aanvrager juist zijn. Op basis van de aanvraag selecteren de medewerkers de te raadplegen bronnen. Artikel 9 politiegegevens worden verstrekt na toestemming van de bevoegd functionaris. Soms geeft de bevoegd functionaris aan zelf contact op te nemen met de aanvrager. De infodesk verstrekt geen artikel 10 politiegegevens. Verstrekkingen worden vastgelegd in de infodeskmodule van BVO. Hierbij worden vastgelegd: de identiteit van de aanvrager, het onderzoek waarvoor de gegevens worden verstrekt, het doel van de aanvraag en per bron welke informatie al dan niet is gevonden en verstrekt. De infodesk wijst de ontvangende partij niet op de geheimhoudingsplicht.

Als een nieuwe medewerker bij de infodesk in dienst treedt, wordt de landelijke verstrekkingenwijzer gebruikt om aan te geven aan welke partijen politiegegevens mogen worden verstrekt. Bij informatieaanvragen die afwijken van de verstrekkingenwijzer wordt de dagcoördinator of de procesvoerder benaderd.

IPOL, unit Criminaliteit
De unit criminaliteit verstrekt in principe geen politiegegevens aan externe partijen. Alleen voor wetenschappelijk onderzoek en statistieken worden gegevens verstrekt, maar deze zijn niet herleidbaar tot een subject. Het gaat bijvoorbeeld om statische gegevens voor de criminaliteitskaart, onderzoeken van wetenschappers of studenten en informatie voor de branche.

4.9.3 Verbeterpunten

- Formaliseer het proces van opstellen, accorderen en beheren van convenanten en draag het over vanuit het project naar de staande organisatie.
- Zorg dat alle partijen bij externe verstrekkingen worden gewezen op de geheimhoudingsplicht.
- Zorg voor toezicht op juiste verstrekkingen door leidinggevenden binnen de afdelingen die structureel verstrekken, zoals de infodesk.

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 merendeel van de informatieverzoeken voor het KLPD komt binnen bij IPOL. Over het algemeen worden de verzoeken door de privacyfunctionarissen van de betreffende diensten afgehandeld. Het ontbreekt nog aan een centraal overzicht waar alle verzoeken worden afgehandeld, maar in de praktijk wordt alles binnen de wettelijke termijnen afgehandeld. Om dit proces in de toekomst inzichtelijker te maken, zal het juridische loket deze verzoeken in de toekomst gaan afhandelen.

Per dienst zijn verschillende procesbeschrijvingen voor het afhandelen van verzoeken van rechten betrokkene. Deze procedures beschrijven de juridische kaders waarin de verzoeken dienen te worden afgehandeld. Wie verantwoordelijk is

voor de afhandeling staat niet beschreven. Daarnaast is niet beschreven hoe wordt voldaan aan de verplichtingen conform artikel 30.

Het proces voor rechten betrokkenen is globaal als volgt opgezet: Allereerst wordt door de verschillende KLPD afdelingen gecontroleerd welke informatie over de aanvrager beschikbaar is. Deze informatie wordt aan de behandeld privacyfunctionaris beschikbaar gesteld waarna deze controleert welke informatie kan worden verstrekt. Het verstrekken van de informatie vindt schriftelijk plaats.

Wij hebben drie documenten ontvangen hoe de verzoeken van betrokkene worden afgehandeld. Dit zijn "procedure Rechten betrokkene. Aantekening Korps concept ", "Proces rechten betrokkenen ex artikel 25 Wpg. Aantekening DNR" en "format input I&F project B&C, deelproject juridische zaken. Aantekening IPOL.

DOS OIV
Wanneer een inzage- of kennisnemingverzoek voor de politiegegevens wordt ingediend wordt deze doorgestuurd naar de privacyfunctionaris. Tevens behandelt de privacyfunctionaris de complexe informatieverzoeken. Bij een verzoek voor rechten van de betrokkene wordt eerst gecontroleerd door de verschillende KLPD afdelingen welke informatie over de aanvrager beschikbaar is, vervolgens beoordeelt de privacyfunctionaris welke informatie kan worden verstrekt. Dit gebeurt schriftelijk.

Tot op heden is er één verzoek tot wijziging van politiegegevens ontvangen. Dit had betrekking op de personenserver. Dit verzoek is bij de beheerder uitgezet en de aanvrager is hiervan op de hoogte gesteld.

In een zeer beperkt aantal gevallen wordt de voorgeschreven afhandelingtermijn uit de Wpg niet gehaald. Dit wordt veroorzaakt door het te laat aanleveren van informatie door andere diensten.

4.10.3 *Verbeterpunt*
- Richt een juridisch loket in zoals reeds beschreven in "Notitie Borging Programma WPG in de lijn". Zorg voor een eenduidige procesbeschrijving. Draag de afhandeling van de verzoeken van de betrokkene (art 25 t/m 31) over aan dit loket.
- Pas de procesbeschrijving aan zodat hieruit blijkt hoe partners worden geïnformeerd over wijzigingen in verstrekte 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*

Protocolleren doelen van onderzoeken

Binnen het KLPD is elke unit die artikel 9 verwerkingen uitvoert verantwoordelijk voor het melden van het doel voor de privacyfunctionaris:

DNR

Binnen de DNR maakt de privacyfunctionaris gebruik van een speciale tool voor de registratie van de lopende onderzoeken. Hierin worden de doelen van onderzoeken bijgehouden. Bevoegd functionarissen vragen een nieuwe BVO omgeving aan bij functioneel beheer. Hiervoor moeten zij aangegeven wat het doel van het onderzoek is. Dit wordt door functioneel beheer doorgegeven aan de privacyfunctionaris die het vastlegt in de tool.

DKDB

De DKDB voldoet aan de eisen van aanmelding. De doelen zijn inzichtelijk omdat deze overeenkomen met de kerntaken van de afdeling. Alle projecten worden direct door de planningsafdeling in BVCM voorzien van een unieke projectcode. De privacyfunctionaris kan op deze wijze zien welke projecten actief zijn. In archiefbestanden van functioneel beheer kan men alle projectcodes vanaf 1999 inzien.

Gegevensverzamelingen op grond van Artikel 13

Het KLPD heeft per afdeling geïnventariseerd welke artikel 13 verwerkingen aanwezig zijn. Op basis hiervan zijn de bijbehorende artikel 13 protocollen opgesteld. Het vervaardigen van deze protocollen is een gecombineerde taak van de betreffende procesvoerder en de privacyfunctionaris. De privacyfunctionarissen hebben tijdens het KLPD privacyfunctionarissen-overleg afspraken gemaakt over het opstellen van artikel 13 protocollen. Hierbij wordt gebruik gemaakt van een template artikel 13 protocol. Nadat de protocollen zijn vastgesteld worden deze aan de projectleider Wpg aangeboden die ze op het intranet van de KLPD plaatst. Aangezien de Wpg projectleidersfunctie van nature van tijdelijke aard is, wordt de taak van het opslag en beheer in 2012 overgedragen aan lijnorganisatie.

Onrechtmatige verwerking

Vanuit de verschillende diensten wordt bij constatering van onrechtmatige verwerkingen melding gemaakt aan de privacyfunctionarissen. De privacyfunctionarissen gebruiken deze meldingen bij het opstellen van het privacyjaarverslag. Er vindt nog geen proactieve monitoring op onrechtmatige verwerkingen plaats.

Protocolgegevens over onrechtmatige verwerkingen worden bewaard voor auditing doeleinden. Op het moment dat de externe audit is afgesloten, worden de gegevens verwijderd. De gegevens worden maximaal vijf jaar door de privacyfunctionaris bewaard.

4.11.3 *Verbeterpunten*

- Documenteer het proces voor het vervaardigen goedkeuren en beheren van de artikel 13 protocollen.
- Zorg dat privacyfunctionarissen in 2012 proactief gaan monitoren op onrechtmatige verwerkingen.

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*

In 2011 is binnen het KLPD een interne audit op de Wpg doorgevoerd. De scope van deze audit was beperkt tot het onderzoeken in hoeverre de Wpg binnen een zestal diensten is geïmplementeerd.

Ter voorbereiding is een auditplan "Concept plan Quickscan KLPD 2011"opgesteld en 300 uur audit-capaciteit gereserveerd. In dit plan is onder andere opgenomen de aanleiding, doelstelling, reikwijdte en scope, normenkader, aanpak en werkwijze, planning en capaciteit.

De bevindingen van het onderzoek zijn per dienst in een auditrapportage opgenomen. Deze rapportages zijn begin december 2011 nog niet door de auditee geverifieerd, dit zal naar verwachting begin 2012 plaatsvinden waarna ze definitief worden gemaakt. Daar de interne auditrapporten ten tijde van de externe audit nog niet definitief waren zijn de bevindingen niet in het externe auditrapport opgenomen.

In 2012 staat een volgende interne audit ingepland. Er is reeds 300 uur audit-capaciteit gereserveerd. Voor deze audit dient nog een auditplan te worden opgesteld.

4.12.3 *Verbeterpunten*

- Zorg dat de interne auditrapportages met de auditees worden afgestemd en vervolgens definitief worden gemaakt.
- Ga na in hoeverre aandachtspunten uit de rapportages gebruikt kunnen worden voor het KLPD Wpg implementatie traject.
- Stel voor de audit gepland in 2012 een auditplan op.

4.13 Privacyfunctionaris (artikel 34)

4.13.1 *Norm*

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

4.13.2 *Bevindingen*

Binnen het KLPD zijn er negen privacyfunctionarissen benoemd en op 12 januari 2011 bij het CBP aangemeld ("Aanmelden privacyfunctionarissen KLPD, kenmerk 2011/01076"). Per dienst is minimaal een privacyfunctionaris aangesteld. Drie privacyfunctionarissen vervullende de rol full-time, de overige functionarissen hebben naast de rol van privacy functionaris een neven rol. De privacyfunctionarissen hebben tot eind 2011 voornamelijk een adviserende rol gehad. Zij ondersteunen bij het opstellen van convenanten en artikel 13 protocollen en zijn verantwoordelijk voor het beantwoorden van de verzoeken van betrokkenen (artikel 25). In 2011 is weinig aandacht besteed aan de toezichthoudende rol. Deze controle taak is in 2010/2011 primair neergelegd bij de interne Wpg auditors. Voor 2012 is een Jaarplan Privacy (zie jaarplan 2011) opgesteld, waarin is opgenomen

dat de toezichthoudende rol in 2012 door de privacyfunctionarissen zal worden uitgevoerd.

In 2009 en 2010 zijn privacyjaarverslagen opgesteld en goedgekeurd. Het privacyjaarverslag 2011 zal eind maart 2012 worden opgeleverd waarna deze in april, samen met verslag 2010 middels een oplegnotitie, zal worden aangeboden aan de korpsleiding.

IPOL, unit Criminaliteit
De privacyfunctionaris heeft geen toegang tot systemen maar kan op verzoek meekijken met de betreffende functionaris. De privacyfunctionaris voert geen controles op autorisaties uit omdat de functie niet goed is ingebed in de organisatie. De privacyfunctionaris geeft aan op dit moment voor 90% van de tijd bezig te zijn met het behandelen van verzoeken om kennisneming. Hierdoor heeft de privacyfunctionaris geen tijd voor de toezichthoudende rol.

DKDB
De privacyfunctionaris is functioneel beheerder en heeft als neventaak de functie privacyfunctionaris. Hierdoor heeft hij toegang tot alle overzichten. Hij voert wekelijks steekproeven uit op de door de DKDB uitgegeven autorisaties. De privacyfunctionaris voert geen steekproeven uit op de uitgegeven autorisaties van landelijke of korpsbrede systemen. Dit is een verantwoordelijkheid van centraal functioneel beheer.

De privacyfunctionaris is in de afgelopen periode primair bezig geweest met het adviseren en helpen implementeren van de Wpg binnen de DKDB en het Korps.

DOS OIV
De privacyfunctionaris is hoofdzakelijk belast met een adviserende rol. De privacyfunctionaris heeft nog geen tijd om de voorgeschreven toezichthoudende rol van de Wpg uit te voeren. Tevens is de Wpg nog niet volledig geïmplementeerd waardoor het uitvoeren van controles nog geen zin heeft. Bij vragen of verzoeken uit de lijn onderneemt de privacyfunctionaris actie.

4.13.3 *Aanbevelingen*

- Zorg dat in 2012 de toezichthoudende rol zoals staat voorgeschreven in de Wpg binnen het KLPD wordt uitgevoerd.
- Zorg voor adequate functiescheiding tussen de operationele en controlerende werkzaamheden.

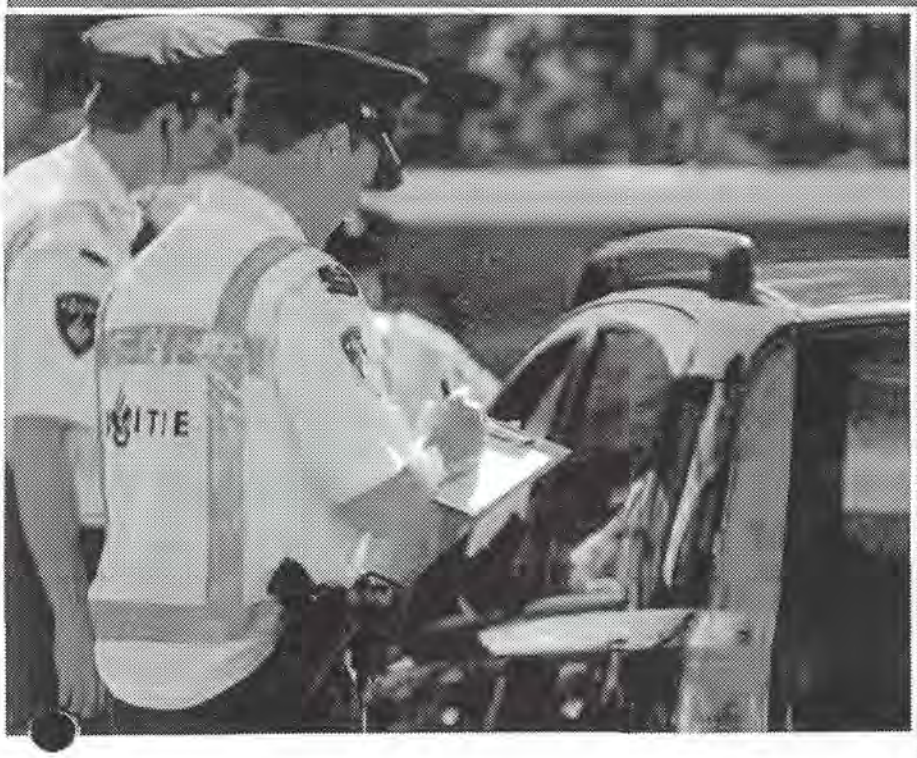
4.14 Functionaris Gegevensbescherming (artikel 36)

Met betrekking tot de invulling van de functionaris Gegevensbescherming wacht het KLPD op de vorming van de nationale politie. Vanuit deze nieuwe organisatie zou de functionaris gegevensbescherming moeten worden aangesteld. Dit standpunt staat verwoord in het auditdossier "gebruikersorganisatie".

2011

Auditrapportage

Interne audit WPG 2011
KLPD



Auditing
Dienst Sturingsondersteuning
December 2011

220220120028

Projectcode	2
Versie	
Datum	
Blad	

Opsteller(s) Drs .

Onderwerp Audit WPG KLPD

Versiebeheer

Versie 0.1		20-12-2011
Versie 0.2	Auditing,	12-01-2012
Versie 1.0	Afstemming met	17-01-2012

Inhoudsopgave

1. Managementsamenvatting

In dit document wordt gerapporteerd over de uitkomsten van de in 2011 gehouden interne audit WPG. Wij hebben vanwege de complexiteit en omvang van de organisatie het KLPD, de focus aangebracht op enkele belangrijke processen van een aantal diensten:

- Bureau Veiligheid en Integriteit (BV&I)
  - proces Interne onderzoeken;
- Dienst Speciale Recherche Toepassingen (DSRT)
  - ULI
  - TIVRI;
- Dienst IPOL (IPOL)
  - Proces Vertalingen en Publiceren, Kenmerken en Opsporingsberichten.
- Dienst Nationale Recherche (DNR)
  - FIET, CIE en Tactiek
- Dienst Koninklijke en Diplomatieke beveiliging (DKDB)
- Dienst Operationele Samenwerking (DOS)
  - Korps Informatie Centrum (KIC)

Hiebij hebben we ons gericht op de opzet van de ingerichte beheersingsmaatregelen.
Van elk dienstonderdeel hebben we een rapport met bevindingen opgesteld, welke zijn weergegeven als bijlage bij dit rapport.
De voorliggende rapportage gaat in essentie over de algehele conclusie die resulteert uit de afzonderlijke dienstrapportages.
De algehele conclusie staat hieronder in tabelvorm weergegeven. Voor uitgebreidere toelichting wordt verwezen naar hoofdstuk 7. Bevindingen en aanbevelingen

	WPG aspect	Bevinding
7.1	Mandaatregeling	+
7.2	Procesbeschrijvingen	+
7.3	Risicoanalyse	0
7.4	Functionele documentatie	n.v.t.
7.5	Aanwijzing Bevoegd functionaris	0
7.6	Samenwerkingverbanden	+
7.7	Protocollen	0
7.8	Opleidingen	+
7.9	Noodzakelijkheid, rechtmatigheid & doelbinding	0
7.10	Juistheid, volledigheid & beveiliging politiegegevens	0
7.11	Autorisatie	0
7.12	Geautomatiseerd vergelijken	0
7.13	In combinatie verwerken	0
7.14	Bewaartermijnen & vernietiging	0
7.15	Gegevensbeheer	0
7.16	Ter beschikking stellen	0
7.17	Verstrekken	0
7.18	Recht van betrokkenen	0

7.19	Privacyfunctionaris	0
7.20	Privacyjaarverslag	+
	(voldoet in beperkte mate aan de eisen van de WPG) **Eindconclusie:**	**0**

Legenda bevindingen:	
+	*voldoet aan de WPG*
o	*voldoet in beperkte mate aan de WPG*
-	*voldoet onvoldoende aan de WPG*
n.v.t.	*WPG aspect niet van toepassing*

In de zomer van 2012 zal een follow-up interne audit plaatsvinden naar de opvolging van de verbeteracties die resulteren uit de gehouden interne en externe audit.

2. Inleiding

Sinds 1 januari 2008 is de Wet politiegegevens (WPG) van kracht. Deze betreft het verwerken van de politiegegevens door de regionale politiekorpsen, het KLPD, de Rijksrecherche en de Koninklijke Marechaussee in het kader van haar politietaken als bedoeld in artikel 2 en artikel 6 van de Politiewet 1993. Van de politie wordt een doelmatige een doeltreffende hulpverlening en handhaving van de rechtsorde verwacht. Voor de ondersteuning van die taken biedt de WPG de ruimte voor het verzamelen en verder verwerken van de benodigde politiegegevens. De WPG zorgt daarbij voor een evenwicht tussen de belangen die met de politietaak gemoeid zijn en de bescherming van de privacy van de burger.

Voor het beheersen van dit evenwicht voor de WPG is er een systeem van auditing op het door de korpsen te onderhouden stelsel van beheersmaatregelen. In dat kader zijn de verantwoordelijken gehouden om de verwerkingsprocessen van politiegegevens door middel van een WPG audit te laten controleren / beoordelen.

In de Regeling periodieke audit politiegegevens (RPAP) zijn de nadere regels beschreven ten aanzien van het toezicht op de naleving van de WPG. Eenmaal in de vier jaar wordt de WPG audit in opdracht van de verantwoordelijke (de Korpsbeheerder) door een externe auditor uitgevoerd. Tevens dient de verantwoordelijke zorg te dragen dat tenminste jaarlijks een interne audit plaatsvindt op één dan wel een aantal onderdelen van de WPG. Deze heeft tot doel op systematische wijze te toetsen of aan de bepalingen van de wet op adequate wijze uitvoering is gegeven. Indien uit de controleresultaten van de interne audit blijkt dat niet wordt voldaan aan het bij of krachtens deze wet bepaalde laat de verantwoordelijke binnen een jaar een hercontrole uitvoeren op die onderdelen die niet voldoen aan de gestelde voorwaarden (artikel 33 WPG).

In deze rapportage vindt u de bevindingen, risico's en aanbevelingen n.a.v. de uitgevoerde interne audit in 2011 bij het KLPD.

3. Doelstelling

Voor de interne audit in het kader van de jaarlijkse WPG audit zijn de volgende doelstellingen geformuleerd:

- Het opstellen van een KLPD specifiek normenkader voor de interne audit van de WPG;
- Het geven van een indicatie over de kwaliteit van de beheersmaatregelen rondom de opzet van de WPG uit het normenkader van een geselecteerd aantal diensten.

Voor de interne audit zijn de volgende kwaliteitsaspecten relevant:

Exclusiviteit: Uitsluitend bevoegde personen hebben toegang tot en kunnen gebruik maken van persoonsgegevens;

Integriteit: De persoonsgegevens moeten in overeenstemming zijn met het afgebeelde deel van de werkelijkheid: dit betreft de juistheid, rechtmatigheid, volledigheid en tijdigheid van de gegevens. Niets mag ten onrechte worden achtergehouden of tijdens de (verdere) verwerking zijn verdwenen;

Continuïteit: De persoonsgegevens en de daarvan afgeleide informatie moeten zonder belemmering beschikbaar zijn overeenkomstig daarover gemaakte afspraken en wettelijke voorschriften. Continuïteit wordt gedefinieerd als de ongestoorde voortgang van de gegevensverwerking;

Controleerbaarheid: De controleerbaarheid is de mate waarin het mogelijk is kennis te verkrijgen over de structurering (documentatie) en de werking van een object. Tevens omvat het kwaliteitsaspect controleerbaarheid de mate waarin het mogelijk is vast te stellen dat de verwerking van persoonsgegevens in overeenstemming met de eisen ten aanzien van de hiervoor genoemde kwaliteitsaspecten is uitgevoerd.

4. Reikwijdte en scope

De interne audit richt zich op het stelsel van maatregelen en procedures waarmee het KLPD beoogt te voldoen aan de beheersdoelstellingen die bij en krachtens de Wet politiegegevens voor het KLPD gelden ten aanzien van de verwerkingen van politiegegevens:

1. met het oog op de uitvoering van de dagelijkse politietaak (artikel 8 WPG);
2. ten behoeve van onderzoeken met het oog op de handhaving van de rechtsorde in een bepaald geval (artikel 9 WPG);
3. met het oog op het verkrijgen van inzicht in de betrokkenheid van personen bij bepaalde ernstige bedreigingen van de rechtsorde (artikel 10 WPG);
4. met het oog op de controle op, het beheer van en de kwaliteit van de informatievoorziening rondom informanten, infiltranten en beschermde getuigen (artikel 12 WPG);
5. ten behoeve van de ondersteuning van de politietaak (artikel 13 WPG), zijnde verwerkingen voor zover zij relevant zijn voor:
    a. het vaststellen van eerdere verwerkingen ten aanzien van eenzelfde persoon of zaak, onder meer ter bepaling van eerdere betrokkenheid bij strafbare feiten;
    b. het ophelderen van strafbare feiten die nog niet herleid konden worden tot een verdachte;
    c. de identificatie van personen of zaken;
    d. het onder de aandacht brengen van personen of zaken met het oog op het uitvoeren van een gevraagde handeling danwel met het oog op een juiste bejegening van personen ;
    e. het verkrijgen van landelijk inzicht in specialistische onderwerpen;

f. geautomatiseerde vergelijking met het oog op de melding van verschillende verwerkingen jegens eenzelfde persoon, daarvoor ter beschikking gesteld en verder verwerkt;
g. het uitvoeren van taken ten dienste van de justitie;
h. bij het Meldpunt Ongebruikelijke Transacties.[1] (6:6.1 BPG).

De interne audit richt zich tevens op het stelsel van maatregelen en procedures waarmee de korpschef van het KLPD beoogt te voldoen aan de beheersdoelstellingen die bij en krachtens de Wet politiegegevens gelden ten aanzien van:

- rechten van betrokkenen (artikel 25 t/m 31 WPG);
- de Privacy functionaris (artikel 34 WPG).

Deze interne audit is uitgevoerd bij hieronder gespecificeerde diensten van het Klpd waarop de WPG van toepassing is.
Voor deze interne audit zijn de volgende diensten en afdelingen onderzocht:

- Bureau Veiligheid en Integriteit (BV&I) proces Interne onderzoeken;
- Dienst Speciale Recherche Toepassingen (DSRT) ULI en TIVRI;
- Dienst IPOL (IPOL) proces Vertalingen en Publiceren, Kenmerken en Opsporingsberichten.
- Dienst Nationale Recherche (DNR) proces FIET, CIE en Tactiek
- Dienst Koninklijke en Diplomatieke beveiliging (DKDB)
- Dienst Operationele Samenwerking (DOS) Korps Informatie Centrum (KIC)

Verder zijn er gesprekken geweest voor de korpsbrede items, zoals encryptie en systeembeveiliging.

Deze interne audit heeft mede tot doel om een zo breed mogelijke nulmeting uit te voeren in de organisatie en tevens een indicatie te leveren over de voortgang van de implementatie van de WPG. De interne audit zal als input dienen voor de Departementale Audit Dienst (DAD) die in december 2011 een onderzoek heeft ingesteld naar de implementatie van de WPG bij het KLPD. Deze interne audit is uitgevoerd in de periode van mei t/m december 2011.

[1] Op 1 januari 2008 is de Wet ter voorkoming van witwassen en financieren van terrorisme (WWFT) in werking getreden. Met de WWFT is de Europese regelgeving in de nationale regelgeving verwerkt en zijn de Wet identificatie bij dienstverlening (Wid) en de Wet melding ongebruikelijke transactie (Wet MOT) samengevoegd. Beheersmatig is het MOT vanaf 2006 ondergebracht bij de Financial Intelligence Unit (FIU) van de Dient IPOL van het Korps Landelijke Politiediensten (KLPD).[1]

5. Gehanteerde normen

Het generieke normenkader voor de interne audit is vastgelegd in de navolgende documenten:

- Wet politiegegevens, de wet van 21 juli 2007, Staatsblad 300, 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 politiegegegevens, 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 gegevens voorschriften;
- De Handreiking Normering Wet politiegegevens, vastgesteld door de Raad van Korpschefs, op 8/9 december 2009;
- De Handreiking Auditing Wet politiegegevens, vastgesteld door de Raad van Korpschefs op 30 september 2009;
- De Handreiking Mandaat, vastgesteld door de Raad van Korpschef op 30 september 2009;
- KLPD specifiek normenkader (2010) en de vragenlijst gebaseerd op dit normenkader;
- Pre-audit matrix van het programma implementatie WPG bij het KLPD;

Bijlage X bevat een tabel waarin de auditobjecten in samenhang met het normenkader overzichtelijk worden gepresenteerd.

hebben tot doel om in een aantal logische stappen systematisch de afhankelijkheden en kwetsbaarheden van een informatiesysteem in beeld te brengen teneinde tot een verantwoord niveau van informatiebeveiliging te komen. Hierbij dient het belang van ieder afzonderlijk proces bepaald te worden en de afhankelijkheden tussen de processen onderling. Tevens zijn niet alleen de geautomatiseerde informatiesystemen van belang maar ook naar de niet geautomatiseerde informatiesystemen.

A&K analyses
Voor slechts een beperkt aantal systemen zijn A&K analyses uitgevoerd. De technische maatregelen uit het BBNP zijn in het algemeen geïmplementeerd; de organisatorische maatregelen slechts ten dele. Indien geen A&K analyse is uitgevoerd is niet bekend wat de afhankelijkheden en kwetsbaarheden zijn van de processen en de systemen die deze processen ondersteunen en kan geen inschatting worden gemaakt van het restrisico na het treffen van de maatregelen. Voor zover maatregelen zijn getroffen op het niveau van het BBNP is niet bekend of het niveau van de getroffen maatregelen voldoet. Het is mogelijk dat er, op basis van de risico's in de processen en systemen, uitgegaan dient te worden van een hoger beveiligingsniveau en dat er aanvullende maatregelen getroffen dienen te worden die uitstijgen boven het niveau van het BBNP.

In verband met de vaststelling van het passende beveiligingsniveau (art. 4.3) is tevens aan de diensten gevraagd of (het management van) de dienst een risico-analyse heeft uitgevoerd, de risico-analyse door documenten kon worden onderbouwd en door het management van de dienst is vastgesteld. Het belang van deze vraag is extra groot aangezien in slechts een beperkt aantal gevallen A&K-analyses zijn uitgevoerd.

Wij hebben niet in alle gevallen een risico-analyse aangetroffen. Hierdoor bestaat de mogelijkheid dat er onvoldoende zicht is op de aanwezige risico's en op de getroffen maatregelen om deze risico's te mitigeren. Hierdoor kan onvoldoende gestuurd worden op het terugdringen van deze risico's.
Voorzover er bij diensten wel een risico-analyse hebben uitgevoerd is deze niet in alle gevallen door het managementteam vastgesteld.

De naleving van de WPG is, ten aanzien van het aspect risico-analyse door de diensten, in opzet in beperkte mate gewaarborgd.

Aanbevelingen
Wij adviseren:
- rekening houdend met de uitgevoerde A&K analyses, een KLPD-brede risico-analyse uit te doen voeren gespecificeerd per proces, systeem en dienst en deze door het management te laten vaststellen.
- de uitvoering van deze risico-analyse centraal te begeleiden, te monitoren en op te nemen in de P&C cyclus.
- op basis van deze risico-analyse samenhangende maatregelen in de administratieve organisatie en in de systemen te treffen met als doel de risico's in de processen te mitigeren.

- de maatregelen die zijn getroffen naar aanleiding van de risico-analyse periodiek te evalueren en te beoordelen of de gesignaleerde risico's nog bestaan en of de getroffen maatregelen efficiënt en effectief zijn uitgevoerd
- de risico-analyse periodiek te beoordelen en aan te passen aan wijzigingen in de processen.

7.4 Functionele documentatie

Bevinding

Functionele documentatie beschrijft de wijze waarop een bedrijfsapplicatie voorziet in de behoeften die de gebruikers - ter ondersteuning van processen - aan de applicatie stellen. Functionele documentatie dient aan te sluiten op de processtappen in het proces en beschrijft de beheersmaatregelen in de applicatie ter ondersteuning van de juiste werking van het proces. Wij hebben tijdens de uitvoering van de audit niet in alle gevallen van alle applicaties functionele documentatie aangetroffen. Het betreft veelal applicaties die in eigen beheer zijn ontwikkeld.
De aanwezigheid van functionele documentatie van applicaties is geen verplichting vanuit de WPG en is niet direct van invloed op de mate waarin aan de WPG wordt voldaan.

Indirect is het ontbreken van functionele documentatie wel van invloed op de naleving van de WPG aangezien in dat geval niet kan worden beoordeeld welke beheersmaatregelen in opzet in de applicaties zijn getroffen. Deze beheersmaatregelen - in de vorm van ingebouwde en geprogrammeerde controles - betreffen o.a. de aspecten juistheid, volledigheid en beveiliging van politiegegevens. E.e.a. is is nader toegelicht in paragraaf 7.10 van deze rapportage. Tevens kan, door het ontbreken van functionele documentatie, niet worden ingeschat of de applicaties in opzet voldoende aansluiten op de processen. Dit veroorzaakt ook risico's voor de naleving van de WPG.

7.5 Aanwijzing bevoegd functionaris (art. 6.7)

Bevinding

Op grond van art. 6.7 WPG dient de verantwoordelijke een bevoegd functionaris aan te wijzen. De bevoegd functionaris heeft een aantal taken op het gebied van de naleving van de WPG. T.a.v. art. 9 verwerkingen betreft dit bijv. het aanmelden van het doel van een verwerking, het uitoefenen van toezicht op de herkomst en wijze van verkrijging van de gegevens, de autorisatie van personen voor de verwerking van politiegegevens, het toetsen van voorgenomen doelafwijkend gebruik, het beoordelen van verzoeken tot verdere verwerking en het afmieden van afgeronde art. 9 onderzoeken.

De wetgever is niet duidelijk over de vraag wie een bevoegd functionaris dient aan te wijzen indien bij een onderzoek als onderdeel van een proces in de strafrechtketen meerdere partijen (binnen en buiten het KLPD) zijn betrokken.

De diensten staan op het standpunt dat de aanwijzing van bevoegd functionarissen slechts noodzakelijk is indien een dienst opdrachtgever is voor een onderzoek. In het geval een dienst een onderzoek uitvoert voor een andere opdrachtgever vonden de diensten de aanwijzing van een bevoegd functionaris niet noodzakelijk. Deze opdrachtgever kan een andere dienst van het KLPD zijn, een regiokorps, (de OvJ van) het OM of een Bijzondere Opsporingsdienst (bijv. FIOD, ECD, MIVD of AIVD). De onderzoeksleider buiten het KLPD dient in dat geval als bevoegd functionaris te zijn aangewezen. Wij hebben dit niet nader vastgesteld.

De naleving van de WPG is, ten aanzien van het aspect aanwijzing bevoegd functionaris, bij ketenprocessen in opzet in beperkte mate gewaarborgd.

Aanbevelingen
Wij adviseren de aanwijzing van de bevoegd functionaris voor ketenprocessen nader door de wetgever te doen toelichten.

Wij adviseren daarbij tevens aandacht te doen schenken aan het integraal toezicht binnen op de verwerkingen in ketenprocessen inclusief de verwerking die buiten de eigen organisatie plaatsvinden.

Wij adviseren de besluiten tot aanwijzing van bevoegd functionarissen vast te stellen.

7.6 Samenwerkingsverbanden (art. 20)

Bevinding

De verantwoordelijke kan, voor zover noodzakelijk, ten behoeve van een samenwerkingsverband beslissen tot het verstrekken van politiegegevens aan die personen en instanties voor de volgende doeleinden:

- het voorkomen en opsporen van strafbare feiten;
- het handhaven van de openbare orde;
- het verlenen van hulp aan hen die deze behoeven;
- het uitoefenen van toezicht op het naleven van regelgeving.

In de beslissing wordt vastgelegd waarom de verstrekking noodzakelijk is, aan welk samenwerkingsverband de politiegegevens worden verstrekt, voor welk doel dit samenwerkingsverband is opgericht, welke gegevens worden verstrekt, de voorwaarden onder welke de gegevens worden verstrekt en aan welke personen of instanties de gegevens worden verstrekt.

Bij één van de onderzochte diensten, DNR, is het aspect samenwerkingsverbanden van toepassing. De naleving van de WPG is, ten aanzien van het aspect samenwerkingsverbanden in deze dienst, in opzet voldoende gewaarborgd.

Aanbevelingen
Wij adviseren de ingeslagen weg te continueren en de inhoud van de convenanten periodiek te toetsen aan de wetgeving en, bij het ontstaan van nieuwe samenwerkingsverbanden, de convenanten op volledigheid te beoordelen.

7.7 Protocollen

Bevinding

De verantwoordelijke draagt o.a. zorg voor de schriftelijke vastlegging van:
- de doelen van de onderzoeken (art. 9.2);
- de gegevens die worden vastgelegd (art. 13.4);
- de toekenning van de autorisaties (art.6);
- de geautomatiseerde vergelijking of het in combinatie met elkaar verwerken van politiegegevens (art. 8.3 en art. 11);
- de hernieuwde verwerking van politiegegevens (art. 9, 10 en 14));
- de verstrekking van politiegegevens;

Voor art. 9 verwerkingen (onderzoeken met het oog op de handhaving van de rechtsorde in een bepaald geval) dient het doel van het onderzoek (onderwerp) en het deel van de politietaak waarop het onderzoek is gericht wordt binnen één week nadat begonnen is met de verwerking schriftelijk te worden vastgelegd en gemeld bij de privacyfunctionaris.

Over de landelijke registers en specialistische onderwerpen (art. 13 WPG) wordt tevoren schriftelijk vastgelegd (protocolplicht):
- ten behoeve van welk specifiek doel de gegevens verder worden verwerkt;
- de categorieën van personen over wie gegevens verder worden verwerkt en de soorten van de over hen op te nemen gegevens;
- de termijn waarbinnen de gegevens verder wordt verwerkt resp. wordt beëindigd;
- de frequentie waarmee de beëindiging van de verwerking wordt gecontroleerd;
- de verantwoordelijke of verantwoordelijken die de gegevens verder verwerken;
- de bewerker.

Wij hebben, op basis van interviews en bestudering van documentatie, vastgesteld dat er in een aantal gevallen protocollen zijn uitgewerkt; deze bleken niet in alle gevallen vastgesteld te zijn. Het bestaan van deze protocollen was niet bij iedere relevante functionaris die met de WPG werkt bekend. Wij hebben niet vastgesteld of er voor alle op grond van de WPG geprotocolleerde verwerkingen ook protocollen zijn opgesteld.

De naleving van de protocolplicht uit de WPG is in opzet in beperkte mate gewaarborgd.

Aanbevelingen
Wij adviseren:

- alle op grond van de WPG te protocolleren verwerkingen van (de diensten van) het KLPD te inventariseren;
- alle bestaande protocollen te inventariseren en te toetsen aan WPG en waar nodig aan te passen;
- de status van deze protocollen te beoordelen en protocollen waar nodig vast te stellen;
- de volledigheid van de protocollen te beoordelen en de ontbrekende protocollen alsnog te doen opstellen en deze vast te stellen;
- (het onderhoud en de communicatie van) de protocollen binnen de organisatie te borgen

7.8 Opleidingen

Bevinding

De Politieacademie heeft een WPG opleidingen verzorgd ('train the trainers') aan leden van de kernteams van de diensten. Deze opleidingen waren gedifferentieerd naar doelgroep. Deze kernteams hebben alle overige medewerkers, voorzover zij met de WPG werken, opgeleid. Wij hebben dit vastgesteld door middel van interviews en bestudering van documentatie. De leiding van de diensten van het KLPD heeft de deelname aan de WPG-opleiding verplicht gesteld en daar actief op gestuurd. De WPG maakt tegenwoordig onderdeel uit van de basis opleiding van de Politie Academie.
De leden van de kernteams en privacyfunctionarissen beantwoorden in de voorkomende gevallen vragen van medewerkers.

Wij hebben een centraal opleidingsplan aangetroffen; bij de diensten hebben we dit niet in alle gevallen aangetroffen. In deze gevallen zijn de medewerkers die met de WPG werken worden direct "on the job" opgeleid.

De programmamanager implementatie WPG heeft de ontwikkelingen rondom de implementatie van de WPG bijgehouden en gedeeld met de privacyfunctionarissen en de projectleider van de diensten. De privacyfunctionarissen, leden van de kernteams, procesvoerders of medewerkers van het interne kwaliteitsbureau zorgen voor de verdere verspreiding van de kennis en ontwikkelingen over de WPG. Er wordt regelmatig aandacht gevraagd voor de WPG; hierdoor is de bewustwording bij de medewerkers geborgd. Medewerkers kunnen, voor het onderhouden van hun kennis over de WPG, gebruik maken van E-learning op KLPD-web. Functioneel Beheer volgt de wijzigingen in de landelijke systemen.

De naleving van de WPG is, ten aanzien van het aspect opleidingen, in opzet voldoende gewaarborgd.

Aanbevelingen
Wij adviseren
- de planning en controlecyclus rondom de opleiding van medewerkers te beschrijven, vast te stellen, te implementeren en binnen de organisatie te borgen;
- de taken van de programmamanager implementatie WPG over te dragen aan de staande organisatie;
- de medewerkers jaarlijks te testen op hun kennis van de WPG via E-learning.

7.9 Noodzakelijkheid, rechtmatigheid en doelbinding (art. 3)

Bevinding	

Politiegegevens worden slechts verwerkt voor zover
- dit noodzakelijk is;
- zij rechtmatig zijn verkregen en
- gelet op de doeleinden waarvoor zij worden verwerkt, toereikend, terzake dienend en niet bovenmatig zijn.

Politiegegevens worden uitsluitend voor een ander doel verwerkt dan waarvoor zij zijn verkregen voor zover deze wet daar uitdrukkelijk in voorziet.

Wij hebben, op basis van interviews en bestudering van documentatie, vastgesteld dat de begrippen noodzakelijkheid, rechtmatigheid en doelbinding bekend zijn. De WPG verandert, ten opzichte van WpolR, niets aan de wijze waarop met de gegevens wordt omgegaan. Wij hebben niet in alle gevallen procesbeschrijvingen aangetroffen die de noodzakelijkheid, rechtmatigheid en doelbinding van de verwerking van politiegegevens waarborgen.

Voorzover wordt samengewerkt binnen een keten wordt er veelal van uitgegaan dat de ketenpartner de informatie rechtmatig heeft verkregen; wij hebben niet vastgesteld of hier in alle gevallen terecht van kan wordt uitgegaan.

Eén van de diensten heeft een disclaimer opgenomen om de noodzakelijkheid en rechtmatigheid af te dekken door in de disclaimer het doel van de verzameling van informatie te beperken tot één proces en daarmee het gebruik van informatie voor een ander doel uit te sluiten.

De naleving van de WPG is, ten aanzien van de aspecten noodzakelijkheid, rechtmatigheid en doelbinding, in opzet in beperkte mate gewaarborgd.

Aanbevelingen
Wij adviseren de procesbeschrijvingen en werkinstructies nader uit te werken, vast te stellen en te borgen met als doel de noodzakelijkheid, rechtmatigheid en doelbinding van de verwerking van politiegegevens te waarborgen.

Wij adviseren daarbij met name specifieke aandacht te hebben voor de rechtmatigheid van de informatie die door ketenpartners wordt aangeleverd.

7.10 Juistheid, volledigheid en beveiliging politiegegevens (Art 4)

Bevinding

De verantwoordelijke treft o.a. maatregelen

- opdat politiegegevens, gelet op de doeleinden waarvoor zij worden verwerkt, juist en nauwkeurig zijn;
- opdat politiegegevens worden verwijderd of vernietigd zodra zij niet langer noodzakelijk zijn voor het doel waarvoor ze zijn verwerkt;
- om de politiegegevens op een passende wijze te beveiligen tegen verlies of enige vorm van onrechtmatige verwerking; de verantwoordelijke heeft toegang tot de politiegegevens die onder zijn beheer worden verwerkt ten behoeve van het toezicht op de naleving van het bij of krachtens deze wet bepaalde
- De verantwoordelijke verleent degenen die belast zijn met de controle, toezicht en het verrichten van technische werkzaamheden voorzover nodig toegang tot de politiegegevens die onder zijn beheer worden verwerkt.

De betrouwbaarheid (juistheid, volledigheid en beveiliging) van politiegegevens is afhankelijk van de kwaliteit van de beheersmaatregelen in de organisatie, processen en in de systemen die deze processen ondersteunen. De landelijke systemen zijn over het algemeen goed gedocumenteerd. Daarnaast wordt veel gebruikt gemaakt van applicaties die in eigen beheer zijn gebouwd. Niet in alle gevallen is er van deze systemen functionele documentatie beschikbaar; in deze gevallen kan geen inzicht worden verkregen in de kwaliteit van de beheersmaatregelen in het systeem. De betrouwbaarheid van de politiegegevens is in deze gevallen voor een belangrijk deel afhankelijk van de beheersmaatregelen in de processen (zoals de administratieve organisatie en de interne controle). Deze hebben, ten opzichte van de maatregelen in de systemen, het nadeel dat deze niet kunnen worden afgedwongen.

De diensten van het KLPD die onderdeel uitmaken van een keten gebruiken informatie van derden. Bij de primaire registratie vindt, voorzover mogelijk op basis van diverse bronnen een uitgebreide kwaliteitscontrole plaats op de ontvangen gegevens. Ontbrekende gegevens worden waar mogelijk aangevuld; onjuiste gegevens worden verbeterd. Het is niet in alle gevallen mogelijk de betrouwbaarheid van deze gegevens te controleren met andere bronnen. In deze gevallen wordt er van uitgegaan dat de aangeleverde informatie betrouwbaar is. Wij hebben niet vastgesteld in hoeverre dit uitgangpunt in alle gevallen juist is.

Op de gegevens die intern worden verwerkt wordt collegiale toetsing toegepast om de betrouwbaarheid van verwerkte gegevens te waarborgen. Wij hebben niet vast kunnen stellen of de maatregelen die worden getroffen ten behoeve van de betrouwbaarheid van de politiegegevens in samenhang zijn getroffen en welke restrisico's er bestaan. In de procesbeschrijvingen zijn de aspecten juistheid, volledigheid en beveiliging van politiegegevens niet in alle gevallen voldoende uitgewerkt.

De naleving van de WPG is, ten aanzien van de aspecten juistheid, volledigheid en beveiliging, in opzet in beperkte mate gewaarborgd.

Aanbevelingen
Wij adviseren

- voor zover de functionele documentatie - voor zover deze ontbreekt - uit te werken, vast te stellen en te borgen en daarbij specifieke aandacht te hebben voor de beschrijving van de ingebouwde en geprogrammeerde controles in de applicatie;
- de procesbeschrijvingen - voor zover nodig – nader te detailleren uit te werken, vast te stellen en te borgen en daarbij specifieke aandacht te hebben voor de beheersmaatregelen in de processen op basis van een risico-analyse, waar nodig aanvullende beheersmaatregelen te treffen in de processen en de applicaties (zie de toelichting in paragraaf 7.2).

7.11 Autorisatie (art. 6)

Bevinding

De verantwoordelijke onderhoudt een systeem van autorisaties dat voldoet aan de vereisten van zorgvuldigheid en evenredigheid. Politiegegevens worden slechts verwerkt door ambtenaren van politie die daartoe door de verantwoordelijke zijn geautoriseerd en voor zover de autorisatie strekt. De verantwoordelijke autoriseert de ambtenaren van politie die onder zijn beheer vallen voor de verwerking van politiegegevens. De autorisatie bevat een duidelijke omschrijving van de verwerkingen waartoe de betreffende ambtenaar wordt geautoriseerd.

In november 2010 heeft de Korpsleiding van het KLPD het autorisatiebeleid vastgesteld. Dit beleid geeft de contouren aan van het autorisatiebeheer door het beschrijven van leidende principes m.b.t. het autorisatiebeleid, een beschrijving van het proces autorisatiebeheer op hoofdlijnen en de benoeming van de rollen (functionarissen) die verantwoordelijk en aansprakelijk zijn voor het autoriseren van de verwerkingen van politiegegevens.

Op basis van dit beleid zijn per proces autorisatiemodellen opgesteld; deze vormde het uitgangspunt voor de autorisatiematrices.

In deze rapportage wordt nader ingegaan op het proces opsporing. Voor de registratie van opsporingsinformatie wordt gebruik gemaakt van BVO; de toekenning van de autorisaties in BVO vindt plaats op basis van het landelijke model BVO 2007. In dit model is onderscheid gemaakt naar verschillende rollen en functies waarbij taken en autorisaties elkaar volgen. Per onderzoek wordt vastgesteld welke medewerkers geautoriseerd dienen te worden en welke autorisaties zij dienen te krijgen. Het diensthoofd kent de autorisaties toe; functioneel beheer is belast met de uitvoering. De toegekende autorisaties worden periodiek gecontroleerd. Nieuwe medewerkers worden conform hun rol geautoriseerd. Wij hebben geen beleid aangetroffen ten aanzien van het intrekken van bevoegdheden van niet actieve gebruikers in BVO.

Het huidige autorisatiemodel kent de volgende beperkingen:
- het autorisatiemodel is niet WPG proof;
- het autorisatiemodel sluit niet goed aan op de (specialistische) functies van het KLPD;
- het autorisatiemodel maakt onderscheid tussen 4 categorieën opsporingsgegevens die als uitgangspunt worden genomen voor de toekenning van autorisaties en het delen van opsporingsinformatie. In de praktijk blijken deze categorieën niet te voldoen omdat bij het classificeren van opsporingsinformatie diverse interpretaties mogelijk zijn.

Dit vormde de aanleiding voor het uitwerken van:
- Nationaal Intelligence Model (2008): in dit model zijn de niveaus van sturing op (veiligheids)informatie beschreven. In dit model is de classificatie van opsporingsinformatie nader uitgewerkt;
- het "Autorisatiemodel Uitvoeren Opsporing en Intelligence" (concept; maart 2010): dit model voldoet in opzet aan de eisen die daar, vanuit de WPG, het Nationaal Intelligence Model (NIM) en de werkprocessen van het KLPD aan worden gesteld. Het model ligt vanaf 2010 ter goedkeuring bij de RKC board opsporing maar is tot op heden nog niet vastgesteld.

Naast de landelijke systemen wordt gebruik gemaakt van overige applicaties die de bedrijfsprocessen ondersteunen. Wij hebben voor deze applicatie autorisatiematrices aangetroffen maar de kwaliteit van het toegepaste autorisatiebeleid en beheer niet vastgesteld.

Tevens wordt gebruik gemaakt van de G:/schijf beveiligd voor de registratie van informatie uit de bedrijfsprocessen. Voor het beheer van de mappenstructuur op de G/:schijf beveiligd ontbreekt nog KLPD breed beleid; wij hebben wel beleid per dienst en autorisatiematrices aangetroffen. Niet in alle gevallen hebben de diensten daarbij het principe van controletechnische functiescheiding toegepast. De direct leidinggevende kent - namens het diensthoofd - de autorisaties toe; functioneel beheer is belast met de uitvoering en het beheer van de autorisaties.
De naleving van de WPG is, ten aanzien van het aspect autorisaties, in opzet in beperkte mate gewaarborgd.

Autorisaties
De criteria voor de toekenning van autorisaties in de applicaties en de G:/schijf zijn niet inzichtelijk. Hierdoor bestaat het risico dat ruimere bevoegdheden worden toegekend dan op grond van de functie nodig en dat controletechnische functiescheidingen worden doorbroken. Hierdoor ontstaan risico's voor de betrouwbaarheid van de informatievoorziening t.a.v. de aspecten exclusiviteit, integriteit, beschikbaarheid, controleerbaarheid en compliance.
Het kwaliteitsaspect exclusiviteit - uitsluitend de daartoe geautoriseerde medewerkers krijgen toegang tot de gegevens – geen nadere toeliching. Ten aanzie van kwaliteitsaspect integriteit kan worden toegelicht dat medewerkers elkaar - door de toepassing van functiescheiding - vanuit een tegengesteld belang zullen controleren. Dit zal de integriteit van de informatie bevorderen.

Wij hebben niet in alle gevallen controletechnische functiescheidingen aangetroffen op basis van goedgekeurd autorisatiebeleid uitgewerkt in een autorisatiematrix. Het risico wordt beperkt doordat de afdelingen uit een beperkt aantal medewerkers bestaan.

Ten aanzien van het proces opsporing dient vermeld te worden dat de toekenning van bevoegdheden in BVO - op basis van het huidige landelijke model BVO 2007 - aan medewerkers, door de beperkingen van het huidige autorisatiemodel, in opzet en bestaan niet voldoet aan de eisen die daar op grond van de functie, rol en competenties aan worden gesteld. Bij te ruime bevoegdheden is de exclusiviteit van de informatievoorziening onvoldoende gewaarborgd en wordt de onderzoeksinformatie met teveel medewerkers gedeeld; bij te beperkte bevoegdheden bestaat het risico dat de medewerker zijn functie niet op de juiste wijze kan vervullen omdat onderzoeksinformatie niet met betreffende medewerker wordt gedeeld.

Er wordt in beperkte mate voldaan aan dit aspect van de WPG.

Aanbevelingen
Wij adviseren het KLPD autorisatiebeleid - o.a. voor de bedrijfsapplicaties en de G-schijf - nader uit te werken, vast te stellen en te borgen en de autorisatiematrices op basis van dit beleid in te richten en daarbij uit te gaan van het principe van controletechnische functiescheiding.

Alsmede adviseren wij
- het "Autorisatiemodel Uitvoeren Opsporing en Intelligence te doen vaststellen, implementeren en binnen de organisatie te borgen;
- de criteria voor de toekenning van superregistraties nader te doen uitwerken en implementeren binnen de organisatie.

7.12 Geautomatiseerd vergelijken (Art 11)

Bevinding

Voor zover dat noodzakelijk is voor een onderzoek kunnen politiegegevens die voor dat onderzoek zijn verwerkt, geautomatiseerd worden vergeleken met andere politiegegevens teneinde vast te stellen of er verbanden bestaan tussen de betreffende gegevens.
Wij hebben, op basis van interviews, vastgesteld dat één afdeling binnen het KLPD geautomatiseerde vergelijking toepast. Bij de overige onderzochte diensten is dit aspect niet van toepassing geweest. De naleving van de WPG is, ten aanzien van het aspect geautomatiseerde vergelijking, in opzet in beperkte mate gewaarborgd.

Aanbevelingen
Wij adviseren het proces geautomatiseerd vergelijken uit te werken, vast te stellen, te implementeren en binnen de organisatie te borgen.

7.13 In combinatie verwerken (Art 11)

Bevinding

Bij het KLPD verwerkt de CIE in combinatie op basis van hit/no hit in opdracht van de OvJ. Bij de overige onderzochte diensten is dit aspect van de WPG niet van toepassing geweest. Het betreft 'zachte' informatie waarvoor onvolledige sleutels uit diverse bronnen wordt gebruikt. Door de combinatie van deze gegevens ontstaat nieuwe informatie op basis waarvan personen als verdachte kunnen worden aangemerkt. Dit is een gevoelig proces aangezien personen, op basis van het gebruik van deze onvolledige sleutels, ten onrechte als verdacht kunnen worden aangemerkt. De gecombineerde informatie wordt tot één document gemaakt te behoeve van art 9 en art 10 verwerkingen. Wij hebben geen beschrijving van dit proces aangetroffen.

De naleving van de WPG is, ten aanzien van het aspect in combinatie verwerken, in opzet in beperkte mate gewaarborgd.

Aanbevelingen
Wij adviseren het proces in combinatie verwerken uit te werken, waarbij aandacht wordt gegevens aan toestemming van bevoegd gezag, vast te stellen, te implementeren en binnen de organisatie te borgen.

7.14 Bewaartermijnen en vernietiging (art. 14)

Bevinding

Voor de artikelen 8,9 en 10 is een vaste bewaartermijn vastgesteld in de WPG. Deze vastgelegde bewaartermijnen zijn vastgesteld om politiegegevens na de bewaartermijn na de laatste verwerking niet meer toegankelijk te laten zijn voor alle medewerkers. Ook politiegegevens die niet langer noodzakelijk zijn voor het doel van het onderzoek worden achter een "schot" geplaatst zodat de gegevens niet meer toegankelijk zijn. Het doel is om oude niet meer relevante gegevens op termijn uit het systeem te wissen.

Wij hebben, op basis van interviews en bestudering van de documentatie, vastgesteld dat geen enkele landelijke of KLPD specifieke applicatie de bewaartermijnen automatisch bijhoud of dat de applicatie een signaalfunctie heeft die het de KLPD medewerkers mogelijk maakt om de bewaartermijnen te bewaken. De landelijke applicaties voorzien niet in een dergelijke functionaliteit. Dit betekent dat de organisatie organisatorische maatregelen heeft moet nemen om de bewaartermijn te bewaken.
Wij hebben bij een aantal diensten beleid aangetroffen omtrent de vernietiging van informatie. Het KLPD is veel gevallen niet de eigenaar van de informatie aangezien het KLPD vaak zich in veel gevallen richt op het verzamelen van informatie. Het vernietigen van de informatie vindt dan plaats op bevel van de OvJ, de bevoegd functionaris van de betreffende zaak of op

basis van een afloopbericht. Het achter een schot plaatsen van informatie vindt in bijna alle gevallen periodiek plaats. De periodiciteit waarmee diensten deze handeling en controle verrichten is niet eenduidig; deze varieert van maandelijks tot (half)jaarlijks.

In sommige gevallen wordt informatie bewaard als studie object. Voor deze art 13 informatie dient een protocol geschreven worden. Wij hebben - ten aanzien van de informatie die voor studie doeleinden wordt - geen protocollen aangetroffen.

Het OM stuurt niet in alle gevallen tijdig afloopberichten naar het KLPD. Voorzover het OM afloopberichten verstuurt kunnen deze niet in alle gevallen aan de onderzoeksdossiers worden gekoppeld doordat de gebruikte nummering bij de onderzoeken verschilt van de nummering bij het OM. Handmatige schoning vindt om deze reden slechts fragmentarisch plaats of blijft achterwege.

Het proces bewaartermijnen en vernietiging is nog niet automatisch ingeregeld. De procesvoerder, de privacyfunctionaris of functioneel beheer draagt zorg voor de verwijdering van de betreffende gegevens na 1 jaar. De verwijdering wordt niet ondersteund door het systeem en vindt handmatig plaats. De informatie in outlook en op de G/:schijf wordt ook na 1 jaar verwijderd (achter een schot geplaatst); de vernietiging van deze informatie vindt na 1+4 jaar plaats. Voorzover informatie als te vernietigen wordt aangemerkt vindt te allen tijde afstemming plaats met de bevoegd functionaris uit het proces. Gegevens ouder dan 5 jaar worden niet meer opnieuw gebruikt. Wij hebben niet in alle gevallen procesbeschrijvingen aangetroffen inzake het proces bewaartermijnen en vernietiging.

Wij hebben tijdens de uitvoering van de audit vastgesteld dat de diensten veel behoefte hebben aan een systeem dat voorziet in functionaliteiten voor de ondersteuning van het beheer van informatie, schoning e.d. In dit verband een aantal keren het systeem SUMM-IT genoemd. Het KLPD maakt nog geen gebruik van SUMM-IT; het bevindt zich nog in de pilotfase. Wij hebben niet vastgesteld in welke mate SUMM-IT in deze behoefte voorziet.

In het onderzoek is gebleken dat er, ten aanzien van de informatieuitwisseling met externe partijen die voor de keten werken afspraken zijn gemaakt door middel van aanbesteding. In dit verband zijn echter geen afspraken gemaakt over de opslag en vernietiging van gegevens buiten het KLPD.

De diensten van het KLPD ontvangen de afloopberichten van het OM niet in alle gevallen tijdig. Voorzover het KLPD wel tijdig afloopberichten ontvangt kan geen relatie worden gelegd met het KLPD zaaknummer.

De naleving van de WPG is, ten aanzien van het aspect bewaartermijnen, in opzet in beperkte mate gewaarborgd.

Aanbeveling
Wij adviseren - voorzover nog niet vastgesteld - alsnog de bewaartermijnen of vernietigingsprocedures vast te stellen en de bewaartermijnen en de vernietiging te implementeren.

Wij adviseren u de controle op de handhaving van de bewaartermijnen en vernietiging periodiek uit te voeren en het proces te dit vast te leggen.

Wij adviseren SUMM-IT op korte termijn te implementeren aangezien dit systeem beschikt over de mogelijkheid om de naleving van de bewaartermijnen te ondersteunen door de ingebouwde functionaliteit op het gebied van beheer van informatie, schoning e.d.

Wij adviseren met externe partijen die samenwerken met het KLPD en in dit verband informatie uitwisselen met het KLPD afspraken te maken over:
- de wijze van opslag van gegevens;
- de maximale bewaartermijnen;
- de wijze vernietiging van gegevens.

Wij adviseren toe te zien op de naleving van deze afspraken.

7.15 Gegevens beheer

Bevinding

Gegevensbeheer is niet expliciet een item van uit de WPG. In de punten autorisatie, vernietiging van gegevens, volledigheid, juistheid en bewaartermijnen wordt dieper ingegaan op voor de WPG belangrijke aspecten. Bij gegevens beheer hebben wij vooral gekeken naar andere manieren van het beheer van politiegegevens.

We hebben op basis van interviews en bestudering van documentatie, vastgesteld dat het gegevensbeheer buiten de landelijke systemen niet geheel voldoet aan de WPG.
De diensten van het KLPD maken, voor de registratie rondom al dan niet kritische bedrijfsprocessen, veel gebruik van applicaties op basis van MS-Office. Zij zijn voor een belangrijk deel afhankelijk van de informatie in deze applicaties. Deze applicaties zijn aangekocht of in eigen beheer ontwikkeld. Deze applicaties zijn in de meeste gevallen niet gedocumenteerd en is het beheer niet goed geregeld. MS-Office toepassingen zijn primair geschikt voor single-user toepassingen en voorzien niet standaard in aanvullende beheersmaatregelen om de betrouwbaarheid van de informatievoorziening bij multi-user toepassing voldoende te waarborgen. Hierbij kan gedacht worden aan beheersmaatregelen zoals validaties, ingebouwde en geprogrammeerde controles; deze betreffen o.a. de aspecten juistheid, volledigheid en beveiliging van politiegegevens. Uit oogpunt van beveiliging en betrouwbaarheid van de informatievoorziening voldoen deze applicaties niet aan de daaraan te stellen eisen. Tevens is de naleving van de bewaartermijnen hierdoor onvoldoende gewaarborgd; dit veroorzaakt tevens risico's voor de naleving van de WPG.

Omdat de applicaties vaak maar op één kleine afdeling wordt gebruikt beheert de afdeling zelf de gegevens.Er is geen centrale regie op het beheer van data voor deze applicaties.

Op bevel, op grond van afloopberichten of een andere trigger worden gegevens vernietigd. Wij hebben bij diverse diensten geconstateerd dat er niet in alle gevallen afloopberichten

worden ontvangen of dat de ontvangen afloopberichten niet aan een onderzoek te relateren zijn.

Buiten systemen vonden wij ook dossiers en mappen met politiegegevens. Veelal worden niet digitaal aangeleverde dossiers en documenten gedigitaliseerd. Dossiers worden, voorzover zij niet langer bewaard hoeven te worden, in een shredder vernietigd en via het grijze containercircuit afgevoerd. De overige papieren dossiers worden in het algemeen in kluizen, of in afgesloten kasten en ruimten bewaard. Deze kluizen en ruimte zijn slechts toegankelijk voor een beperkt aantal medewerkers.

Omdat informatie naar externe partners via het openbare internet, niet encrypted, wordt verstuurd bestaat het risico dat documenten onderschept en/of gemanipuleerd worden.

De diensten van het KLPD maken veelvuldig gebruik van de G:/schijf voor de opslag van informatie die niet in de landelijke systemen kan worden opgeslagen. Het beheer vindt handmatig plaats zonder toepassing van logging.

Aanbeveling
Wij adviseren:

- bij het gegevensbeheer niet alleen te steunen op informatie uit de systemen maar tevens te steunen op de primaire registratie in het dossier buiten het systeem en de uitgevoerde controles in dat dossier zichtbaar te maken.

- het proces bewaartermijnen te implementeren en in dit verband nadere afspraken met het OM te maken omtrent de verstrekking van afloopberichten met als doel de betrouwbaarheid van het gegevensbeheer te waarborgen.

- de procedure rondom de opslag van dossiers in kluizen, kasten ed te beschrijven,vast te stellen, te implementeren en in de organisatie te borgen.

- om de uitwisseling van gegevens met externe organisaties vertaalbureaus uitsluitend via een beveiligde lijn te laten plaatsvinden of voor dat doel een beveiligde omgeving te creëren.

- SUMM-IT te implementeren en, op basis van een risico-analyse, aanvullende beheersmaatregelen in de processen te treffen om de betrouwbaarheid van de informatievoorziening te waarborgen.

7.16 Ter beschikking stellen van politiegegevens (Art 15)

Bevinding

Op grond van artikel 15 stelt de verantwoordelijke politiegegevens ter beschikking aan functionarissen binnen het politiedomein (incl. het OM en de Kmar). Dit zijn politieambtenaren voor zover deze voor de uitoefening van de taak nodig zijn.

In uitzonderlijke gevallen kan het ter beschikking stellen worden geweigerd dan wel kunnen er beperkende voorwaarden worden gesteld aan het ter beschikking stellen van politiegegevens Deze beperkingen worden in een algemene maatregel van bestuur vastgelegd.

Wij hebben, op basis van interviews en bestudering van de documentatie, vastgesteld dat de ter beschikking stelling op verschillende manieren gedaan. Niet in alle gevallen wordt daarbij aan de daaraan te stellen eisen voldaan. Wij hebben vastgesteld dat bepaalde dossiers (met politiegegevens) via systemen, mail, op papier (uitwisseling van de fysieke dossiers), CD's of DVD's ter beschikking worden gesteld.

Indien informatie ter beschikking gesteld via CD's en DVD's wordt zowel een origineel van het onderzoeksdossier als een werkkopie beschikbaar gesteld. Beide exemplaren worden gelijktijdig aan de opdrachtgever overhandigd na kwijting; er blijven geen kopie-exemplaren achter. Na overhandiging is de opdrachtgever verantwoordelijk voor de onderzoeksinformatie

De informatie op de CD's en DVD's is rode informatie (rubricering geheim), niet versleuteld en op geen enkele manier beveiligd. Het verlies van de deze informatie kan tot ernstige schade leiden aan onderzoeken en gevaar opleveren voor betrokkenen (politiemedewerkers, verdachten, informanten) indien niet daartoe geautoriseerde personen kennis kunnen nemen van de gegevens uit het onderzoeksdossier. Desondanks voldoet deze wijze van de ter beschikking stelling van politiegegevens aan de eisen die de WPG daaraan stelt en aan de eisen die het BBNP stelt aan het transport van deze informatie. Dit geldt uitsluitend voorzover betrokkenen deze informatie nodig hebben voor de uitvoering van hun politietaak.

Bij de ter beschikking stelling wordt op verschillende manieren met de identificatie van de vragende partij omgegaan. Dossiers kunnen - op verzoek - rechtstreeks aan het OM verstuurd worden of elektronisch van informatiecentrum aan informatiecentrum verzonden worden. Er wordt daarbij van uitgegaan dat de informatiecentra van de vragende regio te vertrouwen zijn. Wij hebben niet vastgesteld of dit vertrouwen in alle gevallen terecht is. Bij het delen van informatie kunnen de diensten in de voorkomende gevallen een beroep doen op de OvJ of het OM.

Er is een discrepantie tussen de WPG en de Europese wetgeving ten aanzien van de ter beschikking stelling van gegevens. De dienst beoordeelt eerst of aan de WPG en aan de Europese wetgeving wordt voldaan voordat de gegevens aan de buitenlandse politiekorpsen ter beschikking worden gesteld.

De naleving van de WPG is, ten aanzien van het aspect beschikbaarstelling van gegevens, in opzet in beperkte mate gewaarborgd.

Aanbevelingen
Wij adviseren om ondanks dat de procedure aan het BBNP en aan de WPG voldoet, bij het branden van de onderzoeksgegevens op CD of DVD, een vorm van encryptie toe te passen.

Wij adviseren de scope ten aanzien van de eisen die gesteld worden aan de beveiliging van beschikbaar gestelde politiegegevens in samenhang uit te breiden tot het gehele politiedomein.

Wij adviseren via de daartoe geëigende kanalen aan te dringen op harmonisatie van de WPG en EU wet- en regelgeving.

7.17 Verstrekkingen (Art 16 t/m Art 20)

Bevinding

Verstrekken van gegevens kan alleen aan andere instanties dan politie en Kmar. Hier onder wordt verstaan bijvoorbeeld, burgemeesters, ministers, buitengewone opsporingsambtenaren, buitenlandse inlichtingen diensten en iedereen die bij of krachtens een algemene maatregel van bestuur daarvoor is aangewezen.

Wij hebben op basis van interviews en bestudering van de documentatie, vastgesteld dat verstrekkingen slechts bij één dienst voorkomen. Bij een andere dienst wordt er ook informatie gedeeld met niet politiepartners maar dit is geregeld in de "Aanwijzing Opsporingsberichten" van het OM.
De regio stelt informatie aan het KLPD beschikbaar als het om onderzoeken van de regio gaat. Deze beschikbaarstelling van informatie vindt uitsluitend plaats na overleg met de OvJ en dan uitsluitend informatie die reeds eerder bekend is gemaakt (dus geen nieuwe informatie). Bij twijfel en vragen wordt er verwezen naar de aanbrenger (regio politie) van de zaak.

Het KLPD verstrekt - via het OM – gegevens aan advocaten, gemeenten (op basis van de Wet BIBOB), sociale dienst of rechtsreeks via de OvJ. De bevoegd functionaris toetst de aanvraag. Wij hebben een beschrijving van het proces verstrekken aangetroffen.

De naleving van de WPG is, ten aanzien van het aspect verstrekkingen, in opzet voldoende gewaarborgd.

Aanbevelingen
Wij adviseren de procesbeschrijvingen ten aanzien van dit aspect actueel te houden.

7.18 Rechten van betrokkenen (Art 25 t/m Art 31)

Bevinding

Het KLPD is in veel gevallen niet de opdrachtgever van onderzoeken; tevens heeft het KLPD geen baliefunctie. Het komt om deze redenen niet vaak voor dat een betrokkenen inzage vraagt in de gegevens die zijn vastgelegd in politiegegevens aangezien deze door de opdrachtgever zullen worden ontvangen. Voor zover het KLPD wel dergelijke verzoeken ontvangen zal het KLPD - voorzover zij zelf geen opdrachtgever is – naar de opdrachtgever doorverwijzen. Tijdens onze interviews hebben de auditees geen voorbeelden genoemd van dergelijke verzoeken.
De naleving van de WPG is, ten aanzien van het aspect verstrekkingen, in opzet in beperkte mate gewaarborgd.

Aanbevelingen
Wij adviseren:

- op basis van de in de praktijk reeds gehanteerde informele procedure een korpsbrede procedure te ontwikkelen en vast te stellen teneinde een uniforme beantwoording van van vragen die betrokkenen hebben naar aanleiding van de registratie in systemen te kunnen waarborgen;
- deze procedure te implementeren en te borgen binnen de organisatie.

7.19 Privacyfunctionaris

Bevinding

Het KLPD heeft bij alle onderzochte diensten privacyfunctionarissen aangewezen. Alle privacyfunctionarissen zijn bij het CBP aangemeld. De privacyfunctionarissen konden allemaal de rol en de werkzaamheden van de privacyfunctionaris m.b.t. de WPG aangegeven. Niet bij alle diensten konden de privacyfunctionarissen de toezichthoudende rol uitvoeren. Dit kwam doordat:

- de privacyfunctionaris te weinig tijd heeft voor de vervulling van deze taak. Het takenpakket van de privacyfunctionaris is bij een aantal diensten uitgebreid met de beantwoording van informatieverzoeken op grond van de WOB en Kamervragen.
- de privacyfunctionaris geen toegang heeft tot alle systemen (autorisatie). De privacyfunctionaris kan wel door gericht vragen informatie laten opzoeken door een collega.
- de privacyfunctionaris belast is met de verdere implementatie van de WPG binnen de dienst.
- er geen tool beschikbaar is om invulling te geven aan de toezichthoudende rol.

De naleving van de WPG is, door de beperkte mate waarin de privacyfunctionaris invulling kan geven aan zijn/haar toezichthoudende rol, ten aanzien van het aspect privacyfunctionaris, in opzet in beperkte mate gewaarborgd.

Aanbevelingen
Wij adviseren:

- de privacyfunctionaris een meer toezichthoudende rol te laten vervullen. Het is bij sommige diensten ondoenlijk om voor elk systeem autorisatie te krijgen of een systeem zo goed te kennen om de mogelijkheden voldoende te benutten. Dit zou kunnen worden ondervangen door de privacyfunctionaris de vraagregels voor de queries voor elk systeem op te doen stellen en deze met behulp van deze queiries – door tussenkomst Functioneel beheer - periodiek de gewenste informatie op te vragen.
  de privacyfunctionaris de uitgevoerde controles over de registratie, verwerking, verstrekking en vernietiging van persoonsgegevens in het kader van het toezicht op de naleving van de WPG in een dossier zichtbaar te maken.

7.20 Privacyjaarverslag

Bevinding

Artikel 34. (privacyfunctionaris)
De privacyfunctionaris stelt jaarlijks een verslag op van zijn bevindingen.
Door de onderzochte diensten zijn over 2010 jaarverslagen gemaakt. De jaarverslagen zijn niet tot een KLPD jaarverslag gebundeld maar betreft minimaal 6 losse jaarverslagen.

De naleving van de WPG is, ten aanzien van het aspect privacyjaarverslag, in opzet voldoende gewaarborgd.

Aanbevelingen
Het KLPD wordt geadviseerd over 2011 een compleet jaarverslag over de gehele organisatie aan te leveren.

8 Bijlagen

In verband met de omvang van het normenkader KLPD en de wetgeving WPG zijn het normenkader en de wet WPG niet als bijlage opgenomen in deze rapportage en wordt op verzoek elektronisch beschikbaar gesteld.

Bijlage 1: Overzicht gebruikte documentatie

- Wet politiegegevens, juli 2007, Staatsblad 300
- Besluit politiegegevens, december 2007
- Regeling periodieke audit politiegegevens, december 2008, nr. 5578598/08
- De Handreiking Normering Wet politiegegevens, november 2009
- De Handreiking Auditing Wet politiegegevens, november 2009
- PID 2010 Programma Wet Politiegegevens
- Rapport onderzoeksfase WPG IV versie 1.0
- Opleidingsplan WPG fase 1 en 2" 2010
- Plan van Aanpak WPG-IV fase II versie 1.0
- BVH WPG replicatie versie 1.0
- BVH WPG beslotenheid 1.0
- Plan van Aanpak Implementatie WPG DWP
- Opleidingsplan WPG DWP 2010 versie 0.2
- Jaarverslag 2009 Privacyfunctionaris
- Rapportage Procesmodel Verzamelen en Verwerken Veiligheidsinformatie DIKC-water versie 2.0 2010
- Functionele documentatie BVH
- WPG 701 Gegevensbeheer versie 1.0
- BVO Autorisatiemodel versie 0.9 2007
- Autorisatiemodel Uitvoeren Opsporing & Intelligence (concept maart 2010)
- WPG 301 Autorisatiebeleid
- Procesbeschrijving CARIN versie 1.0
- Handreiking Auditing
- Handreiking Normstelling
- Samenwerkingsverbanden: UCIB (binnenvaart); Kreekrak: ladinggegevens en containervervoer); EVOA (overbrenging van afvalstoffen)
- De processen van BVCM, BVH en BVO in samenhang versie 1.0 2007
- Handleiding beheer koppeling BVO <-> Bleu View versie 01032008.
- Risico inventarisatie 2011 Stuurgroepvergadering 12102010
- Status overzicht samenwerkingsverbanden wk39 2010
- Statusoverzicht Art 13 protocollen week 44 2010

Bijlage 2, Totaal overzicht per dienst

		KLPD	BVI	IPOL	DSRT	DNR	DOS	DKDB
7.1	Mandaatregeling	+	+	+	+	+	0	+
7.2	Procesbeschrijvingen	+	+	+	0	+	0	+
7.3	Risico-analyse	0	-	0	0	0	-	+
7.4	Functionele documentatie.	n.v.t.	n.v.t.	n.v.t.	n.v.t.	n.v.t.	n.v.t.	n.v.t.
7.5	Aanwijzing Bevoegd functionaris	0	+	0	0	0	0	+
7.6	Samenwerkingverbanden	+	n.v.t.	n.v.t.	n.v.t.	+	n.v.t.	n.v.t.
7.7	Protocollen	0	n.v.t.	0	+	0	n.v.t.	+
7.8	Opleidingen	+	+	0	+	+	0	+
7.9	Noodzakelijkheid, rechtmatigheid & doelbinding	0	+	0	0	+	0	+
7.10	Juistheid, volledigheid & beveiliging politiegegevens	0	+	0	0	+	0	+
7.11	Autorisatie	0	+	0	+	0	-	+
7.12	Geautomatiseerd vergelijken	0	n.v.t.	n.v.t.	n.v.t.	0	n.v.t.	n.v.t.
7.13	In combinatie verwerken	0	n.v.t.	n.v.t.	n.v.t.	0	n.v.t.	n.v.t.
7.14	Bewaartermijnen & vernietiging	0	+	0	0	0	0	+
7.15	Gegevensbeheer	0	0	0	0	0	0	0
7.16	Ter beschikking stellen	0	+	n.v.t.	-	+	0	0
7.17	Verstrekken	0	n.v.t.	n.v.t.	n.v.t.	+	n.v.t.	-
7.18	Recht van betrokkenen	0	n.v.t.	n.v.t.	n.v.t.	0	n.v.t.	-
7.19	Privacyfunctionaris	0	+	-	0	0	-	+
7.20	Privacyjaarverslag	+	+	+	+	+	+	+
	Totaal	0	+	0	0	+/0	0	+

Bijlage 3, Respondenten

Dienst	Processen
BV&I / Interne onderzoeken	
Gesprek met:	
DOS/KIK	
Gesprek met:	
DKDB / DIK	
Gesprek met:	
DSRT / ULI/TIVRI	
Gesprek met:	
DNR / CIE	
DNR / FIET	
DNR / Tactiek	
DNR / MT	

Dienst	Processen
IPOL / Vertalingen	
IPOL / publiceren kenmerken / opsporingsberichten	
Informatiebeveiliging	
Encryptie	

Bijlage 4: BV&I

1 Inrichting van de organisatie

Inleiding
Bureau Veiligheid & Integriteit is verantwoordelijk voor de uitvoering van de volgende processen binnen het KLPD:

- verzorging van Veiligheids- en Antecedentenonderzoeken (variërend van korte screeningen voor bijvoorbeeld personen die tijdelijk werkzaamheden binnen de muren van het KLPD komen verrichten tot zeer uitgebreide antecedentenonderzoeken en veiligheidsonderzoeken);
- uitvoering van Interne Onderzoeken zoals disciplinaire onderzoeken of strafrechtelijke onderzoeken (indien er sprake lijkt te zijn van of vermoedelijke pleging van strafbare feiten door een medewerker van het KLPD);
- de interne beveiliging van het KLPD: zowel informatiebeveiliging en encryptie als fysieke en organisatorische beveiliging;
- de interne communicatie van (landelijke) integriteitvraagstukken, het ontwikkelen van integriteitbeleid voor het KLPD en de (individuele) ondersteuning bij het oplossen van integriteitsdilemma's;
- de registratie van klachten van burgers over de werkwijze of het optreden van KLPD-personeel

Samenvatting implementatie van de WPG bij BV&I
Naar aanleiding van de bevindingen voortgekomen uit de interne WPG-audit bij BV&I kunnen wij concluderen dat BV&I, middels de implementatie van de WPG, in opzet voldoet aan de eisen van de WPG. Wij hebben, in het kader van deze interne audit, geen onderzoek gedaan naar het bestaan en de werking van de maatregelen.

	WPG aspect	Bevinding	Risico-inschatting
1.1	Mandaatregeling	+	L
1.2	Procesbeschrijvingen	+	L
1.3	Risicoanalyse	-	L
1.4	Functionele documentatie.	n.v.t.	L
1.5	Aanwijzing Bevoegd functionaris	+	L
1.6	Samenwerkingverbanden	n.v.t.	-
1.7	Protocollen	n.v.t.	-
1.8	Opleidingen	+	L
2	Noodzakelijkheid, rechtmatigheid & doelbinding	+	L
3	Juistheid, volledigheid & beveiliging politiegegevens	+	L
4	Autorisatie	+	L
5	Geautomatiseerd vergelijken	n.v.t.	-
6	In combinatie verwerken	n.v.t.	-
7	Bewaartermijnen & vernietiging	+	L
8	Gegevensbeheer	0	L

9	Ter beschikking stellen	+	L
10	Verstrekken	n.v.t.	-
11	Recht van betrokkene	n.v.t.	L
12	Privacyfunctionaris	+	L
13	Privacyjaarverslag	+	L
	(voldoet aan de eisen van de WPG) **Eindconclusie:**	**+**	

Legenda bevindingen:	
+	*voldoet aan de WPG*
o	*voldoet in beperkte mate aan de WPG*
-	*voldoet onvoldoende aan de WPG*
n.v.t.	*WPG aspect niet van toepassing*
Legenda risico-inschatting	
H	*hoog risico, voldoet niet in opzet en/of is niet vastgelegd. Voldoet niet aan de wet.*
M	*gemiddeld risico, voldoet in opzet maar is niet vastgelegd. Voldoet niet volledig aan de wet.*
L	*laag risico, voldoet in opzet maar is niet volledig vastgelegd. Voldoet aan de wet.*
-	*geen risico, of niet van toepassing.*

1.1 Mandaatregeling

De mandaatregeling WPG is bekend en binnen BV&I geïmplementeerd. Er is een overzicht beschikbaar van alle verwerkingen; de WPG is uitsluitend van toepassing op de strafrechtelijke onderzoeken van het eigen personeel. Dit betreft ca. 6 zaken per jaar.
Bevindingen: voldoet aan de WPG

Risico
geen

Risico-inschatting: Laag

Aanbevelingen
geen

1.2 Procesbeschrijvingen

Wij hebben bij BV&I beschrijvingen van de processen aangetroffen waarop de WPG van toepassing is. Deze zijn overzichtelijk van aard.

BV&I voert de onderzoeken uit t.b.v. het OM. BV&I vernietigt de fysieke dossiers zodra het dossier is afgedragen aan het OM. Alleen het zaaknummer met omschrijving blijft bestaan t.b.v. .de managementinformatie. De beheersdoelstellingen t.a.v. de naleving van de WPG zijn geborgd door frequent overleg tussen de Privacyfunctionaris en het Hoofd BV&I.

Voor de registratie van de strafrechtelijke onderzoeken wordt gebruik gemaakt van het systeem "Registratie Interne Onderzoeken BV&I" (in het vervolg: RIO-BV&I). Daarnaast gebruikt BV&I de G:schijf beveiligd t.b.v. de opslag van documenten.
Bevindingen: voldoet aan de WPG

Risico
Geen

Risico-inschatting: Laag

Aanbevelingen
geen

1.3 Risicoanalyse

Wij hebben bij de processen die plaatsvinden bij BV&I een aantal beheersmaatregelen rondom de naleving van de WPG aangetroffen. Deze beheersmaatregelen zijn echter niet getroffen naar aanleiding van een risicoanalyse. Bevinding: voldoet niet aan de WPG.

Risicoanalyse
Door het ontbreken van een uitgewerkte risicoanalyse hebben wij niet vast kunnen stellen dat BV&I een integraal inzicht heeft in de risico's die gelopen worden in de processen. Hierdoor bestaat het risico dat de getroffen beheersmaatregelen de risico's in de processen onvoldoende mitigeren en er, na het nemen van de beheersmaatregelen, alsnog restrisico's blijven bestaan.

Risico-inschatting: laag
- BV&I kent een beperkt aantal overzichtelijke processen;
- het aantal medewerkers van BV&I is beperkt en heeft een hoog veiligheidsbewustzijn;
- BV&I werkt in een beveiligd deel van de geautomatiseerde omgeving;
- de privacyfunctie is geborgd;
- WPG maakt onderdeel uit van de managementcontrolcyclus.

Aanbeveling
Wij adviseren u een risicoanalyse uit te voeren op basis waarvan op samenhangende wijze beheersmaatregelen in de AO en in de systemen getroffen kunnen worden teneinde eventuele risico's in de processen te mitigeren.

1.4 Functionele documentatie

Wij hebben geen functionele documentatie (incl. gebruikershandleidingen) aangetroffen van de applicatie RIO BV&I. Bevinding: voldoet niet aan de WPG.

Risico
Door het ontbreken van functionele documentatie is de betrouwbaarheid van de informatievoorziening in RIO BV&I in opzet onvoldoende gewaarborgd.

Risico-inschatting: laag
- de applicatie biedt ondersteunende informatie; de privacyfunctionaris houdt tevens een hard-copy dossier bij van alle WPG verwerkingen (van aanmelding van de onderzoeken tot en met de controle op de afloop) op basis waarvan de toezichthoudende rol kan worden vervuld;
- het jaarlijkse aantal onderzoeken (ca. 6) is beperkt en daardoor overzichtelijk;
- het aantal medewerkers dat werkt met de applicatie is beperkt, 'on-the-spot' opgeleid en heeft een hoog veiligheidsbewustzijn.

Aanbeveling
Wij adviseren u alsnog een beschrijving van het systeem RIO BV&I uit te werken, vast te stellen, te implementeren en te borgen.

1.5 Aanwijzing bevoegd functionaris
Alle onderzoekers van BV&I zijn tevens bevoegd functionaris. Wij hebben een besluit tot aanwijzing van bevoegd functionaris aangetroffen. Per zaak wordt een bevoegd functionaris aangewezen. Voldoet aan de WPG.

Risico
geen

Risico-inschatting: Laag

Aanbevelingen
geen

1.6 Samenwerkingsverbanden (Art 20)
BV&I heeft uitsluitend een samenwerkingsverband met het OM. Deze samenwerking vloeit voort uit een wettelijke verplichting.

1.7 Protocollen
Met uitzondering van de melding van de art. 9 verwerkingen aan de privacyfunctionaris heeft BV&I geen geprotocolleerde verwerkingen.

1.8 Opleidingen
Wij hebben geen opleidingsplan aangetroffen. Alle nieuwe medewerkers die met de WPG werken worden direct "on the job" opgeleid.

Risico
geen

Risico-inschatting: Laag

Aanbevelingen
Geen

2 Noodzakelijkheid, rechtmatigheid en doelbinding (Art 3)
Het doel van het onderzoek (onderwerp) en het deel van de politietaak waarop het onderzoek is gericht dient binnen een week na aanvang van verwerking schriftelijk vastgelegd en bij de privacyfunctionaris (protocolplicht) gemeld te worden.
Er wordt geen gebruik gemaakt van de landelijke applicatie BVO aangezien er teveel medewerkers toegang hebben tot BVO en het om zeer gevoelige gegevens gaat. Ten

behoeve van onderzoeksgegevens wordt zowel een digitale map (op een afgeschermd deel van de G:/schijf) als een fysieke map aangemaakt. De fysieke map wordt bewaard in de kluis. Er wordt vastgesteld wie de onderzoeksleider is en wat de onderzoekstappen zullen zijn.

BV&I is geen eigenaar van de onderzoeksgegevens aangezien BV&I de onderzoeken - in voorkomende gevallen - uitvoert t.b.v. het Landelijk Parket van het OM. In de overige gevallen zal een Bijzondere Opsporings Dienst (BOD) het onderzoek uitvoeren. BV&I bewaart uitsluitend de kopiedossiers. Bevindingen: voldoet aan de WPG

Risico
Door overdracht van het onderzoek van BV&I naar het OM en ontvangst van afloopberichten van het OM treden ketenrisico's op t.a.v. .de juistheid, tijdigheid en volledigheid van de gegevensverwerking. Deze risico's vormen een KLPD- (of mogelijk politie)breed probleem. Dit veroorzaakt tevens risico's t.a.v. .de naleving van de WPG.

Risico-inschatting: laag
- het risico is bekend en speelt binnen de gehele strafrechtketen;
- door het beperkte aantal onderzoeken en de actieve wijze waarop BV&I in de praktijk met dit risico omgaat is het restrisico beperkt.

Aanbevelingen
Wij adviseren u de controles die de procesmanager resp. de privacyfunctionaris uitvoeren bij de overdracht van de gegevens aan het OM en de ontvangst van de afloopberichten in de administratie - i.c. het WPG dossier van de privacyfunctionaris – nader uit te werken en vast te leggen.

Wij adviseren u de problematiek van de niet tijdige en volledige ontvangst van de afloopberichten centraal (KLPD / politie) te doen bespreken bij het OM.

3 Juistheid, volledigheid en beveiliging politiegegevens (Art 4)

Politiegegevens zijn, gelet op de doeleinden waarvoor zij worden verwerkt, juist en nauwkeurig. De eindcontrole en verantwoordelijkheid van de gegevensverwerking ligt bij de procesmanager. Deze controle wordt zichtbaar gemaakt in het dossier door ondertekening door de procesmanager voor 'gezien en geaccordeerd'. Aangezien BV&I voor de registratie van de strafrechtelijke onderzoeken gebruik maakt van het systeem RIO-BV&I. Dit systeem vervult uitsluitend een ondersteunende rol. Aangezien er van dit systeem geen functionele documentatie beschikbaar is kan geen inzicht worden verkregen in de kwaliteit van de application controls binnen het systeem. Tevens kan op deze wijze geen eenduidige werkwijze door de medewerkers worden afgedwongen. Bevindingen: voldoet aan de WPG.

Risico
De betrouwbaarheid van de informatievoorziening in RIO-BV&I is in opzet onvoldoende gewaarborgd. Door het ontbreken van inzicht in de kwaliteit van de application controls bestaat het risico van onjuiste primaire registratie en verwerking van gegevens in RIO-BV&I.

Risico-inschatting: laag

- RIO-BV&I vervult uitsluitende een ondersteunende rol t.b.v. de voortgangsbewaking van de dossiers; er kan te allen tijde worden teruggevallen op de primaire registratie in het dossier;
- BV&I heeft aanvullende beheersmaatregelen getroffen in de vorm van gebruikerscontroles op basis van de primaire registratie door de procesmanager en de privacyfunctionaris;
- door het zeer beperkte aantal onderzoeken en de actieve wijze waarop BV&I in de praktijk met dit risico omgaat is het restrisico beperkt.

Aanbeveling
Geen

4 Autorisatie (Art 6)

Medewerkers die bij het proces interne onderzoeken werken, het hoofd en het hoofd plv. BV&I zijn voor de gehele G schijf interne onderzoeken geautoriseerd conform autorisatiebeleid. Voor dit doel is een autorisatiematrix opgesteld. De autorisaties worden centraal beheerd. Een uitzondering geldt voor de dienstspecifieke applicaties: hiervoor worden de autorisaties door de afdeling zelf beheerd. Bij uitdiensttreding worden de autorisaties ingetrokken. Bevindingen: voldoet aan de WPG.

Risico
De criteria voor de toekenning van autorisaties in de applicaties en de G:/schijf zijn niet inzichtelijk. Hierdoor bestaat het risico dat ruimere bevoegdheden worden toegekend dan op grond van de functie nodig en dat controletechnische functiescheidingen worden doorbroken. Hierdoor ontstaan risico's voor de betrouwbaarheid van de informatievoorziening t.a.v. de aspecten exclusiviteit, integriteit, beschikbaarheid, controleerbaarheid en compliance.

Risico-inschatting: laag

- BV&I heeft aanvullende beheersmaatregelen getroffen in de vorm van gebruikerscontroles op basis van de primaire registratie door de procesmanager en de privacyfunctionaris
- door het beperkte aantal onderzoeken en de actieve wijze waarop BV&I in de praktijk met dit risico omgaat is het restrisico beperkt.

Aanbeveling
Wij adviseren u het beleid rondom de toekenning van de autorisatie voor RIO-BV&I en de G:/schijf nader uit te werken, vast te stellen en in de organisatie te borgen en de autorisatiematrix in te richten op basis van vastgesteld autorisatiebeleid.

5 Geautomatiseerd vergelijken (Art 11)

BV&I past geen geautomatiseerde vergelijking toe.

6 In combinatie verwerken (Art 11)

BV&I kent geen verwerkingen die gecombineerd met andere verwerkingen plaatsvinden.

7 Bewaartermijnen en vernietiging (art. 14)

Politiegegevens die niet langer noodzakelijk zijn voor het doel van het onderzoek worden vernietigd of gedurende een periode van maximaal een half jaar verwerkt teneinde te bezien of zij aanleiding geven tot een nieuw onderzoek. Na verloop van deze termijn worden deze gegevens verwijderd. In de applicatie RIO-BV&I kan een selectie plaatsvinden van de betreffende zaken aangezien het jaartal onderdeel uitmaakt van het zaaksnummer. Ook de namen van de mappen op de G:/schijf bevatten het jaartal.

Risico

Bij BV&I bestaat het risico op overschrijding van de wettelijke termijnen doordat de betrouwbaarheid van de informatie in de applicatie RIO-BV&I onvoldoende is gewaarborgd en vooral gesteund dient te worden op aanvullende beheersmaatregelen in de AO.

Risico-inschatting: laag

- de privacyfunctionaris maakt, bij de vervulling van haar toezichthoudende rol, niet alleen gebruik van de RIO-BV&I maar steunt met name op de primaire gegevens in het hard-copy dossier.

Aanbeveling

Wij adviseren u de controle op de handhaving van de bewaartermijnen en vernietiging zichtbaar te maken in het dossier.

8 Gegevensbeheer

Wij hebben de betrouwbaarheid van de informatie in de applicatie RIO-BV&I niet vast kunnen stellen. Hierdoor biedt deze applicatie onvoldoende ondersteuning bij het gegevensbeheer. Bevinding: voldoet niet vooledig aan de WPG.

Risico

Er bestaat een risico van onjuist gegevensbeheer doordat de applicatie RIO-BV&I het gegevensbeheer onvoldoende ondersteunt .

Risico-inschatting: laag

- BV&I maakt ten behoeve van het gegevensbeheer niet alleen gebruik van RIO-BV&I maar steunt met name op de primaire gegevens in het hard-copy dossier.

Aanbeveling

Wij adviseren u bij het gegevensbeheer niet alleen te steunen op informatie uit RIO-BV&I maar m.n. te steunen op de primaire registratie in het dossier buiten het systeem RIO-BV&I en de uitgevoerde controles in dat dossier zichtbaar te maken.

9 Ter beschikking stellen van politiegegevens (Art 15)

BV&I voert haar strafrechtelijke onderzoeken uit op verzoek van het OM. Zij stelt de gegevens uit deze onderzoeken ter beschikking aan het OM. Het OM maakt onderdeel uit van het politiedomein. Buiten deze ketenpartner stelt BV&I geen informatie beschikbaar aan andere partijen.

10 Verstrekkingen (Art 16 t/m Art 20)

Er is slechts sprake van verstrekkingen indien deze plaatsvinden buiten het politiedomein. Bij BV&I is geen sprake van verstrekking maar uitsluitend van beschikbaarstelling aan een partner (het OM) in de strafrechtketen.

11 Rechten van betrokkenen (Art 25 t/m Art 31)

Wij hebben geen procesbeschrijving voor de rechten van betrokken aangetroffen. Uit interviews met medewerkers van BV&I is gebleken dat BV&I dergelijke verzoeken tot op heden nog niet heeft ontvangen. Bevindingen: voldoet niet volledig aan de WPG.

Risico

- een uniforme werkwijze bij het afdoen van kennisnemingsverzoeken is - in de voorkomende gevallen - onvoldoende gewaarborgd.

Risico-inschatting: laag

- het is tot op heden niet voorgekomen dat BV&I dergelijke verzoeken heeft ontvangen;
- de toezichthoudende rol van de privacyfunctionaris is geborgd binnen BV&I

Aanbeveling

Wij adviseren u een procesbeschrijving inzake de rechten van betrokkenen op kennisneming uit te werken en in de organisatie te borgen.

12 Privacyfunctionaris (Art34)

Het bureau BV&I heeft een privacyfunctionaris aangewezen. Zij is aangemeld bij het CBP en is op de hoogte van de inhoud van haar toezichthoudende rol. Bij de uitoefening van deze rol kan zij niet (uitsluitend) steunen op de informatie in RIO-BV&I maar zal vooral op andere wijze (extracomptabel) informatie dienen vast te leggen over de registratie, verwerking, verstrekking en vernietiging van persoonsgegevens in het kader van de WPG. Bevindingen: voldoet aan de WPG.

Risico

Het risico bestaat dat de WPG niet wordt nageleefd indien uitsluitend wordt uitgegaan van de informatie in RIO-BV&I.

Risico-inschatting: laag

- de privacyfunctionaris steunt bij de vervulling van de toezichthoudende rol met name op de primaire registraties in het dossier.

Aanbeveling

Wij adviseren de privacyfunctionaris de uitgevoerde controles in het kader van de naleving van de WPG in het dossier zichtbaar te maken.

13 Privacyjaarverslag (Art 34)

De privacyfunctionaris van BV&I heeft een privacyjaarverslag opgesteld. Hiermee heeft BV&I voldaan aan de wettelijke verplichting vanuit de WPG.

Risico

Geen

Risico-inschatting: laag

Aanbevelingen
Geen

14 Knelpunten verdere implementatie

Door BV&I zijn geen punten genoemd die mogelijk als knelpunt kunnen worden aangerekend bij verdere implementatie van de WPG.

15 Reactie van het Bureau Veiligheid en Integriteit

Naar aanleiding van de op 18 mei 2011 verrichtte interne WPG-audit naar de implementatie en opzet van de Wet Politie Gegevens binnen BV&I, willen wij graag de volgende reactie geven op de audit-rapportage.

Er wordt slechts op die onderwerpen een reactie gegeven waar de auditcie opmerkingen en aanbevelingen voor aangegeven heeft in haar rapportage.

Ad: 1.3 Risico-analyse
Door de interne auditcommissie (verder te noemen auditcie) is aangegeven dat er geen risicoanalyse mbt de BV&I processen is opgesteld danwel aanwezig is. De risico-inschatting hiervan wordt als laag gekwalificeerd.

Aanbeveling auditcie: stel een risicoanalyse op.

Reactie DH BV&I: Er is inderdaad (nog) geen risico analyse opgesteld mbt de BV&I processen. Dit ligt wel in de planning. Getracht wordt dit in 2012 te verwezenlijken.

Ad: 1.4 Functionele documentatie
Auditcie: er is geen functionele documentatie mbt het RIO BV&I aangetroffen. De risico-inschatting hiervan wordt als laag gekwalificeerd.

Aanbeveling auditcie: stel een beschrijving van het RIO-BV&I systeem op.

Reactie DH BV&I: Het opstellen van een beschrijving van het RIO-BV&I systeem zal in 2012 gerealiseerd gaan worden.

Ad: 2 Noodzakelijkheid, rechtmatigheid en doelbinding
Auditcie: De ontvangst van afloopberichten van het landelijke Parket van het OM leveren (door niet tijdige danwel onvolledige ontvangst, noot Bouwmeister) ketenrisico's op tav de juistheid, tijdigheid en volledigheid van de gegevensverwerking. De risico-inschatting hiervan wordt als laag gekwalificeerd.

Aanbeveling auditcie: maak problematiek mbt tijdige en onvolledige ontvangst *kenbaar bij OM*

Reactie DH BV&I: Dit is een alom bekend probleem (KLPD breed). Er wordt door BV&I regelmatig aandacht voor gevraagd. Het blijft de aandacht van BV&I behouden.

Ad: 3 Juistheid, volledigheid en beveiliging politiegegevens (art. 4WPG)
Auditcie: De betrouwbaarheid van de informatievoorziening in RIO-BV&I is in opzet onvoldoende gewaarborgd door het ontbreken van functionele documentatie daarvan. De risico-inschatting wordt als laag gekwalificeerd.

Aanbeveling auditcie: geen

Reactie DH BV&I: Het RIO-BV&I systeem wordt door slechts een beperkt aantal collega's van BV&I gebruikt. De controle van het systeem (gebruikerscontrole) is weggezet/ondergebracht bij de informatieverwerker van het proces Interne Onderzoeken.

Ad: 4 Autorisatie
Auditcie: De criteria voor toekenning van autorisaties in de applicaties en de G:schijf zijn niet inzichtelijk. Hierdoor bestaat het risico dat ruimere bevoegdheden worden toegekend dan op grond van functie nodig is. De risico-inschatting wordt als laag gekwalificeerd.

Aanbeveling auditcie: werk het beleid rondom toekenning van de autorisatie van RIO-BV&I en de G:schijf nader uit, stel deze vast en borg deze in de organisatie.

Reactie DH BV&I: Het opstellen van beleid omtrent de autorisatie van RIO-BV&I en de G:schijf, het vaststellen en borgen daarvan zal in 2012 verwezenlijkt worden.

Ad: 7 Bwaartermijnen en vernietiging (art.14 WPG)
Auditcie: Door het ontbreken van functionele documenten kan de betrouwbaarheid van de informatie van het RIO-BV&I systeem onvoldoende gewaarborgd worden. Risico is dat hierdoor overschrijding van de bewaartermijn(en) plaatsvinden. De risico-inschatting wordt als laag gekwalificeerd.

Aanbeveling auditcie: maak de controle op de handhaving van de bewaartermijnen en vernietiging zichtbaar in het dossier.

Reactie DH BV&I: De bewaartermijnen van de informatie en van de dossiers wordt zeer nauwkeurig door de informatieverwerker van het proces Interne Onderzoeken gemonitord. Zij vergewist zich ervan dat de WPG goed en zorgvuldig wordt uitgevoerd.

Ad: 8 Gegevensbeheer
*Auditcie:*Door het niet kunnen vaststellen van de betrouwbaarheid van het RIO-BV&I systeem wordt verondersteld dat deze het gegevensbeheer van BV&I onvoldoende ondersteund. De risico-inschatting wordt als laag gekwalificeerd.

Aanbeveling auditcie: maak ter controle van het gegevensbeheer tevens gebruik van de hard-copy dossier.

Reactie DH BV&I: Door de privacyfunctionaris van BV&I wordt reeds ter controle van het gegevensbeheer, gebruik gemaakt van een hard-copy overzicht. Daar worden tevens de controles in bijgehouden.

Ad: 11 Rechten van betrokkenen
Auditcie: Er is geen procesbeschrijvingen voor een kennisnemingverzoek aangetroffen bij BV&I. Tot nu toe is er geen gebruik gemaakt van dit recht door een betrokkene. De risico-inschatting wordt als laag gekwalificeerd.

Aanbeveling auditcie: stel een procesbeschrijving inzake rechten betrokkene voor een kennisname verzoek op.
Reactie DH BV&I: Het opstellen van een dergelijke procesbeschrijving is naar de mening van het Diensthoofd BV&I een KLPD brede aangelegenheid. Daar komt nog bij dat de informatie eigenaar van dit BV&I proces het Landelijk Parket is. Daar zullen dan ook de verzoeken tot kennisname binnenkomen.

Ad: 12 Privacyfunctionaris
Auditcie: Door het niet kunnen vaststellen van de betrouwbaarheid van het RIO-BV&I systeem, wordt verondersteld dat deze het gegevensbeheer van BV&I onvoldoende ondersteund. Hierdoor zal de privacyfunctionaris niet slechts op de informatie uit het RIO-BV&I systeem kunnen afgaan maar zal op andere wijze(n) informatie dienen vast te leggen over registratie, verwerking, vestrekking en vernietiging van persoonsgegevens. De risico-inschatting wordt als laag gekwalificeerd.

Aanbeveling auditcie: maak controles door privacyfunctionaris in kader naleving WPG zichtbaar in dossier.

Reactie DH BV&I: Door de privacyfunctionaris van BV&I wordt reeds ter controle van het gegevensbeheer, gebruik gemaakt van een hard-copy overzicht. Daar worden tevens de controles in bijgehouden.

Bijlage 5: DOS

1 Inrichting van de organisatie

Inleiding

De Dienst Operationele Samenwerking (DOS) is de dienst die ondersteuning biedt op een aantal terreinen aan het KLPD, de Nederlandse politie en andere overheidsinstanties. De ondersteuning geschiedt in de vorm van expertise maar ook door het leveren van personele en materiële capaciteit. Tot de taken van de dienst behoort o.a. het opsporen van TBS'ers, expertise bij grote verkeersongevallen, mobiele 112 oproepen, de meldkamer, het verwerken van proces verbalen, inzet van de politie luchtvloot en opleiding en inzet van levende have zoals honden en paarden. Tevens is de dienst het informatieknooppunt voor het gehele korps.

Samenvatting implementatie van de WPG bij DOS

Wij hebben ons, bij de uitvoering van deze interne WPG-audit bij de dienst DOS, beperkt tot onderzoek naar de naleving van de WPG bij het Kennis- en Informatiecentrum. Tevens hebben wij uitsluitend onderzoek gedaan naar de opzet van de beheersmaatregelen; wij hebben geen onderzoek gedaan naar het bestaan en de werking van de maatregelen.

Op basis van de bevindingen naar aanleiding van dit onderzoek kunnen wij concluderen dat DOS/KIC, middels de implementatie van de WPG, in opzet in beperkte mate voldoet aan de eisen van de WPG.

	WPG aspect	Bevinding	Risico-inschatting
1.1	Mandaatregeling	0	M
1.2	Procesbeschrijvingen	0	L
1.3	Risicoanalyse	-	M
1.4	Functionele documentatie.	n.v.t.	-
1.5	Aanwijzing Bevoegd functionaris	0	L
1.6	Samenwerkingverbanden	n.v.t.	-
1.7	Protocollen	n.v.t.	-
1.8	Opleidingen	0	L
2	Noodzakelijkheid, rechtmatigheid & doelbinding	0	M
3	Juistheid, volledigheid & beveiliging politiegegevens	0	M
4	Autorisatie	-	M
5	Geautomatiseerd vergelijken	n.v.t.	-
6	In combinatie verwerken	n.v.t.	-
7	Bewaartermijnen & vernietiging	0	M
8	Gegevensbeheer	0	H
9	Ter beschikking stellen	0	L
10	Verstrekken	n.v.t.	-
11	Recht van betrokkenen	n.v.t.	-
12	Privacyfunctionaris	-	H
13	Privacyjaarverslag	+	L
	(voldoet in beperkte mate aan de eisen van de WPG)	**0**	

	Eindconclusie:		

Legenda bevindingen:	
+	*voldoet aan de WPG*
o	*voldoet in beperkte mate aan de WPG*
-	*voldoet onvoldoende aan de WPG*
n.v.t.	*WPG aspect niet van toepassing*
Legenda risico-inschatting:	
H	*hoog risico, voldoet niet aan de wet; geen risicobeperkende beheersmaatregelen ingericht*
M	*gemiddeld risico, voldoet niet aan de wet; wel risicobeperkende beheersmaatregelen ingericht*
L	*laag risico, voldoet aan de wet*
-	*geen risico; WPG aspect niet van toepassing.*

1.1 Mandaatregeling

De deelnemers aan het gesprek kennen de mandaatregeling en weten wat deze inhoudt. De dienst heeft het mandaat geïmplementeerd betreffende de bevoegdheden van o.a. de Korpschef, de diensthoofden en de doormandatering van de bevoegdheden aan de onderliggende leidinggevende niveaus. De dienst weet vooral de rechten worden goed te verwoorden.

De deelnemers zijn het er over eens dat de mandaatregeling niet helemaal meer past en eigenlijk zou moeten worden herschreven. Uit praktisch oogpunt tekent nu het plaatsvervangend diensthoofd in plaats van het diensthoofd voor verschillende zaken. Ook voor beslissingen over autorisaties zou de unitleiding moeten kunnen tekenen in plaats van het diensthoofd. De mandaatregeling voorziet niet standaard in deze situaties. Art. 3 lid 3 van de mandaatregeling maakt het echter wel mogelijk aan andere in de mandaatregeling genoemde functionarissen bij besluit bevoegdheden toe te kennen ten aanzien van persoonsgegevens en/of politiegegevens die onder de hun verantwoordelijkheid vallen. Wij hebben niet vast kunnen stellen of aan de in het interview genoemde afwijkende gevallen besluiten ten grondslag liggen. De naleving van de WPG is, ten aanzien van het aspect mandaatregeling, in beperkte mate gewaarborgd.

DOS/KIC heeft een schema beschikbaar met organisatorische indeling en een overzicht van de verwerkingen die plaatsvinden in het kader van de WPG.

Risico

Er bestaat een risico dat - buiten het mandaat om - beslissingen worden genomen door niet gemandateerde functionarissen.

Risico-inschatting: gemiddeld

- Aan de bevoegdheden die zijn toegekend aan niet in het mandaat genoemde functionarissen zullen slechts in beperkte mate besluiten ten grondslag liggen.

Aanbeveling

Wij adviseren het mandaat op deze punten korpsbreed te doen aanpassen aan de en vast te stellen zodat op deze wijze niet voor alle niet in het mandaat genoemde situaties besluiten genomen dienen te worden.

1.2 Procesbeschrijvingen

Uit een interview is gebleken dat de processen bij DOS/KIC waarbij de WPG een rol speelt in opzet voldoen aan de WPG. Wij hebben dit niet vast kunnen stellen aangezien de maatregelen rondom de nalevingen van de WPG niet in alle gevallen zijn uitgewerkt. De werkprocessen betreffen de intake van vragen en het zoeken en geven van antwoorden. Dit is voor alle processen globaal hetzelfde; uitsluitend in de detail vertonen de processen minimale verschillen. Dit is in de werkinstructies beschreven. Dit betreft bijv. verschillen in formulieren en routing. De beschreven processen zijn niet door het MT vastgesteld; het Unithoofd heeft de processen wel vastgesteld.

Het MT van DOS heeft aandacht voor de verdere implementatie van de WPG. De projectgroep implementatie WPG heeft in dit verband een presentatie gehouden voor het MT. DOS heeft ook een eigen projectleider Implementatie WPG. De naleving van de WPG is, ten aanzien van de het aspecten procesbeschrijvingen, in opzet in beperkte mate gewaarborgd.

Risico

De procesbeschrijvingen voldoen op dit moment aan de WPG. Het risico is aanwezig dat wijzigingen in werkprocessen niet tijdig in de procesbeschrijvingen worden aangepast.

Risico-inschatting: laag

- de processen zijn niet door het MT vastgesteld; er wordt echter wel gewerkt conform de beschrijving van de processen;
- de maatregelen rondom de naleving van de WPG zijn niet in alle gevallen uitgewerkt;
- DOS heeft een projectleider implementatie WPG - niet zijnde de privacyfunctionaris - aangesteld;
- er is een goede communicatie tussen de procesvoerder, de privacyfunctionarissen en de projectleider implementatie WPG.

Aanbeveling

Wij adviseren de procesbeschrijvingen te evalueren, waar nodig verder uit te werken voor de WPG aspecten, te doen vaststellen, implementeren en binnen de organisatie te borgen.

1.3 Risico-analyse

DOS heeft geen risico-analyse uitgevoerd. DOS heeft hierdoor nog geen zicht op de eventuele risico's in de processen van de dienst. De naleving van de WPG is, ten aanzien van het aspect risico-analyse, onvoldoende gewaarborgd.

Risico

Het mogelijkheid bestaat dat er niet in alle gevallen voldoende zicht is op de aanwezige risico's en op de getroffen maatregelen om deze risico's te mitigeren. Hierdoor kan niet in alle gevallen voldoende gestuurd worden op het terugdringen van deze risico's. De beheersmaatregelen zijn uitsluitend getroffen op basis van een inschatting van de risico's door de verantwoordelijke functionarissen; zij maken echter geen deel uit van een integrale risico-analyse.

Risico-inschatting: gemiddeld

- *In de onderzochte processen zijn beheersmaatregelen ingericht. Deze zijn echter niet gebaseerd op een risico-analyse, maar totstandgekomen op basis van de inschattingen van de verantwoordelijke functionarissen in de processen. Wij hebben niet vast kunnen stellen dat alle risico's in de processen voldoende zijn afgedekt.*

Aanbevelingen

Wij adviseren een dienstbrede risico-analyse uit te doen (laten) uitvoeren op basis waarvan samenhangende maatregelen in de administratieve organisatie en in de systemen getroffen kunnen worden. Op deze wijze kunnen de risico's in de processen tot een aanvaardbaar niveau worden gemitigeerd.

1.4 Functionele documentatie

Alle art 8 verwerkingen bij DOS/KIC worden in BVO vastgelegd en aangezien alle vastleggingen in het kader van een onderzoek in BVO plaatsvinden.

DOS/KIC heeft een overzicht van alle interfaces met systemen waarin gegevens worden vastgelegd of opgeslagen. DOS/KIC maakt voor de registratie rondom haar primaire processen gebruik van het landelijke systeem (BVO) en de standaardapplicaties Windows Verkenner (G:/schijf) en Outlook. Als bronsystemen wordt o.a. gebruik gemaakt van BVH en de PS Handhaving Vreemdelingen. Er zit een knip tussen de zoekvraag en de informatievraag.

De landelijke applicaties worden beheerd door de VtsPN; de standaardprogrammatuur wordt volgens de systematiek van de VtsPN beveiligd. Er is functionele documentatie van de gebruikte systemen. De aanwezigheid van functionele documentatie is geen verplichting *vanuit de WPG. Functionele documentatie is indirect echter wel van invloed op de naleving* van de WPG aangezien op basis van functionele documentatie beoordeeld kan worden welke beheersmaatregelen zijn getroffen in de applicaties. Deze beheersmaatregelen (bijv. validaties, ingebouwde en geprogrammeerde controles) betreffen o.a. de aspecten juistheid, volledigheid en beveiliging van politiegegevens. E.e.a. is is nader toegelicht in paragraaf 3 *van deze rapportage.*

1.5 Aanwijzing bevoegd functionaris

Een bevoegd functionaris is alleen nodig bij art 9 en 10 verwerkingen op voorwaarde dat de dienst opdrachtgever is. DOS/KIC verricht geen zelfstandige onderzoeken; zij is *ondersteunend aan de andere diensten in dit proces. Omdat DOS/KIC geen eigenaar is van* de informatie heeft DOS/KIC geen bevoegd functionarissen nodig. DOS heeft – voorzover nodig - aan haar overige processen - indien DOS opdrachtgever is – wel bevoegd functionarissen aangewezen.

Ten aanzien van DOS/KIC is de opdrachtgever een andere dienst (bijv. de DNR) of een regiokorps. De onderzoeksleider van deze andere dienst of regio is in dat geval de bevoegd functionaris. DOS/KIC onderhoudt in dat verband nauwe contacten met de bevoegd functionarissen.

Dit aspect van de WPG is, ondanks het ontbreken van bevoegd functionaris bij DOS/KIC, in opzet in beperkte mate gewaarborgd doordat te allen tijde afstemming wordt gezocht met de

aanvrager op basis van de verstrekkingenwijzer. Wij hebben op basis van procesbeschrijvingen niet in alle gevallen kunnen vaststellen in welke mate de bevoegd functionaris hierin betrokken wordt.

Risico
Het risico is aanwezig dat de bevoegd functionaris (buiten DOS/KIC) niet in alle gevallen wordt geraadpleegd voor de verstrekking en beschikbaarstelling van informatie.

Risico-inschatting: laag
Doordat te allen tijde afstemming wordt gezocht met de aanvrager wordt het gemis aan een aangewezen bevoegd functionaris bij DOS/KIC een deel ondervangen.

Aanbevelingen
Wij adviseren de procesbeschrijvingen ten aanzien van dit aspect aan te passen.

1.6 Samenwerkingsverbanden (Art 20)
Er zijn bij DOS geen samenwerkingsverbanden in het kader van de WPG met andere organisaties.

1.7 Protocollen
De dienst DOS heeft geen protocollen. De eigenaar van de gegevens is verantwoordelijk. De dienst DOS wordt geen eigenaar van gegevens.

1.8 Opleidingen
DOS heeft geen opleidingsplan. Iedereen die met de WPG in aanraking komt is voor de WPG opgeleid. De Politieacademie verzorgt een standaardopleiding op het gebied van de WPG en heeft de eerste medewerkers van DOS opgeleid. De overige van de medewerkers zijn intern door deze medewerkers opgeleid. De WPG opleiding maakt onderdeel uit van de opleiding tot informatieverwerker.

De laatste ontwikkelingen op het gebied van de WPG worden bijgehouden door de privacyfunctionaris en de procesvoerder WPG. Deze ontwikkelingen worden daarna met de organisatie gedeeld. Er wordt regelmatig aandacht gevraagd voor de WPG via de mail en in briefings door de operationeel chef (iedere ochtend). De communicatie rondom de WPG verschilt in dit opzicht niet van andere processen. De privacyfunctionaris levert informatie aan over nieuwe ontwikkelingen. Functioneel Beheer volgt de wijzigingen in de landelijke systemen.

Risico
Het risico is dat nieuwe medewerkers niet opgeleid worden voor het werken met de WPG of dat nieuwe ontwikkelingen onvoldoende bij de medewerkers bekend zijn.

Risico-inschatting: laag

- de communicatie rondom de ontwikkelingen ten aanzien van de WPG wordt centraal binnen het KLPD – via het programma implementatie WPG - via de procesvoerder en de privacyfunctionaris met de dienst gecommuniceerd
- de privacyfunctionaris is onderdeel van het netwerk van privacyfunctionarissen binnen het KLPD
- nieuwe medewerkers mogen pas met de WPG werken als zij volledig zijn opgeleid.

Aanbevelingen

Wij adviseren het privacynetwerk in stand te houden en centraal in het privacyoverleg de WPG regelmatig op de agenda te zetten.
Wij adviseren de taken van de programmamanager implementatie WPG over te dragen aan de staande organisatie.

2. Noodzakelijkheid, rechtmatigheid en doelbinding (Art 3)

De termen noodzakelijkheid, rechtmatigheid en doelbinding zijn binnen de dienst DOS bekend maar niet in alle gevallen afdoende beschreven in de procesbeschrijvingen. Informatie wordt alleen verzameld indien deze direct aan een zaak te koppelen zijn. DOS bouwt geen eigen informatiepositie op maar maakt gebruik van bronsystemen waaruit de informatie wordt gehaald. Zij gaat er daarbij van uit dat de informatie rechtmatig is verkregen. De naleving van de WPG is, ten aanzien van de aspecten noodzakelijkheid, rechtmatigheid en doelbinding, in beperkte mate gewaarborgd.

Risico

DOS/KIC loopt het risico dat de toets op de noodzakelijkheid, rechtmatigheid en doelbinding niet of niet juist wordt uitgevoerd.

Risico-inschatting: gemiddeld

- DOS/KIC heeft aandacht voor de beschrijving van de werkprocessen
- Er is in deze beschrijving niet in alle gevallen voldoende aandacht voor de beschrijving van de toets op de noodzakelijkheid, rechtmatigheid en doelbinding

Aanbevelingen

Wij adviseren de procesbeschrijvingen voor aspecten noodzakelijkheid, rechtmatigheid en doelbinding de actueel te houden.

3 Juistheid, volledigheid en beveiliging politiegegevens (Art 4)

De termen juistheid, volledigheid en beveiliging zijn niet in alle gevallen afdoende beschreven in de procesbeschrijvingen. Uit het interview en op basis van de documentatie hebben wij vastgesteld de DOS/KIC een aantal maatregelen heeft getroffen om de naleving van de WPG, ten aanzien van de aspecten noodzakelijkheid, rechtmatigheid en doelbinding, te waarborgen. Wij hebben echter niet vast kunnen stellen of deze maatregelen in samenhang zijn getroffen en welke restrisico's er bestaan. De naleving van de WPG is in beperkte mate gewaarborgd.

Risico

DOS/KIC loopt het risico dat de juistheid, volledigheid en beveiliging van politiegegevens onvoldoende is gewaarborgd. Dit levert risico's op voor de naleving van de WPG.

Risico-inschatting: gemiddeld

- DOS/KIC heeft aandacht voor de beschrijving van de werkprocessen;
- Het intern kwaliteitsbureau toetst de kwaliteit van de geregistreerde gegevens en schoont deze waar nodig;
- De dagcoördinator controleert de uitgevoerde werkzaamheden zoals de verstrekking van informatie en de kwaliteit van de vastlegging van de verzoeken en de afhandeling ervan;
- Er is in deze beschrijving niet in alle gevallen voldoende aandacht voor de aspecten juistheid, volledigheid en beveiliging van politiegegevens.

Aanbevelingen

Wij adviseren in de procesbeschrijvingen de aspecten juistheid, volledigheid en beveiliging van politiegegevens nader uit te werken, te implementeren in binnen de organisatie te borgen.

4 Autorisatie (Art 6)

DOS/KIC maakt voor de registratie rondom haar primaire processen gebruik van het landelijke systeem (BVO) en de standaardapplicaties Windows Verkenner (G:/schijf) en Outlook. Als bronsystemen wordt o.a. gebruik gemaakt van BVH en de PS Handhaving Vreemdelingen.
De autorisaties bij DOS/KIC worden op de functie uitgereikt. De medewerkers hebben uitsluitend raadpleegbevoegdheden in de bronsystemen; de wijzigingsbevoegdheden in de bronsystemen zijn voorbehouden aan de gebruikers die deze systemen vullen. Er is onvoldoende controletechnische functiescheiding toegepast.

Voor het toekennen van de autorisatie is er bij FA&G (Bureau Functioneel Applicatie & Gegevensbeheer) een autorisatie matrix aan de hand waaraan autorisaties worden toegekend. De Operationeel chef c.q. de procesvoerder onderhoud de autorisaties en laat het beheer bij FA&G. De operationeel chef c.q. procesvoerder kent de autorisaties toe.

Risico

Wij hebben geen controletechnische functiescheiding aangetroffen op basis van een goedgekeurd autorisatiebeleid uitgewerkt in een autorisatiematrix.

Risico-inschatting: gemiddeld

- De afdelingen bestaan uit een aantal medewerkers die dezelfde functie hebben.
- Er is wel een autorisatiematrix voor het toekennen van autorisaties

Aanbevelingen

Wij adviseren controletechnische functiescheiding toe te passen op basis van goedgekeurd autorisatiebeleid uitgewerkt in een autorisatiematrix.

5 Geautomatiseerd vergelijken (Art 11)

DOS past geen geautomatiseerde vergelijking toe.

6 In combinatie verwerken (Art 11)

DOS past geen in combinatie verwerken toe.

7 Bewaartermijnen en vernietiging (art. 14)

Bewaartermijnen en vernietiging is nog niet automatisch in BVO geregeld. Alle andere relevante gegevens verzamelingen worden met de hand door DOS na 1 jaar verwijderd. De procesvoerder draagt zorg voor deze verwijdering. De informatie die wordt opgeslagen in outlook wordt na 1 jaar verwijderd (achter schot geplaatst). Informatie die achter het schot is geplaatst wordt na 4 jaar (1+4 jaar) vernietigd door de procesvoerder.

DOS maakt nog geen gebruik van SUMM-IT; dit systeem beschikt over een infodeskmodule waarbij rekening is gehouden met de informatiebehoeften van DOS. Tevens ondersteunt SUMM-IT het beheer van informatie, schoning e.d. Ten aanzien van de vernietiging van informatie wordt altijd ruggespraak gehouden met de bevoegd functionaris van de DNR. De dienst DOS heeft behoefte aan een functionaliteit waarmee de (tijdige) vernietiging van gegevens wordt ondersteund. Momenteel is dit een puur handmatig proces.

Politiegegevens die niet meer noodzakelijk zijn worden na een half jaar vernietigd door de procesvoerder. Gegevens die ouder zijn dan 5 jaar worden door DOS niet opnieuw gebruikt. Ook bij DOS is de tijdige ontvangst van afloopberichten (via de unit Operationele informatieverwerking) een probleem. De naleving van de WPG is, ten aanzien van het aspect bewaartermijnen, in beperkte mate gewaarborgd.

Risico

Het achter een schot plaatsen en vervolgens vernietigen van gegevens is een puur handmatig proces. Dit sterk afhankelijk van de procesvoerder; het is niet te controleren of gegevens daadwerkelijk tijdig achter een schot geplaatst worden of vernietigd worden.

Risico-inschatting: gemiddeld

- de procesvoerder voert het proces van het achter een schot plaatsen en vernietigen van gegevens uit in samenwerking met de privacyfunctionaris; dit is een handmatig proces en wordt niet door het systeem ondersteunt;
- de werkwijze is beschreven.

Aanbevelingen

Wij adviseren SUMM-IT op korte termijn te implementeren aangezien dit systeem beschikt over een infodeskmodule en de naleving van de bewaartermijnen ondersteunt door de functionaliteiten op het gebied van beheer van informatie, schoning e.d.

Wij adviseren de problematiek rondom de afloopberichten via de privacyfunctionaris van het KLPD onder de aandacht van het OM te brengen.

8 Gegevens beheer

Alle informatie buiten BVO wordt opgeslagen in Outlook en op de G:/schijf. Alles informatie wordt digitaal opgeslagen; er vindt geen decentrale opslag van gegevens plaats. Er is een afzonderlijke map (ordner) voor gevoelige informatie die aan de DSRT is verstrekt. Deze informatie wordt in de kluis bewaard. Het proces is niet beschreven (ca. 20- 30 zaken per jaar).

Office toepassingen (zoals Outlook) zijn primair geschikt voor single-user toepassingen en voorziet niet standaard in aanvullende beheersmaatregelen om de betrouwbaarheid van de informatievoorziening bij multi-user toepassing voldoende te waarborgen. Hierbij kan gedacht worden aan beheersmaatregelen zoals validaties, ingebouwde en geprogrammeerde controles; deze betreffen o.a. de aspecten juistheid, volledigheid en beveiliging van politiegegevens. De betrouwbaarheid van de informatievoorziening rondom de primaire processen is, door de afhankelijkheid van Office toepassingen, in opzet in beperkte mate gewaarborgd.

Risico
DOS/KIC is voor haar primaire proces voor een belangrijk deel afhankelijk van Office toepassingen (zoals Outlook). De naleving van de bewaartermijn kunnen hierdoor niet worden gecontroleerd. Dit veroorzaakt niet alleen risico's voor de betrouwbaarheid van de informatievoorziening maar ook voor de naleving van de WPG.

Risico-inschatting: hoog
- Office toepassingen voorziet niet in aanvullende beheersmaatregelen (zoals validaties, ingebouwde en geprogrammeerde controles) om de betrouwbaarheid van de informatievoorziening te waarborgen.

Aanbevelingen
Wij adviseren SUMM-IT te implementeren en, op basis van een risico-analyse, aanvullende beheersmaatregelen in de processen te treffen om de betrouwbaarheid van de informatievoorziening te waarborgen.

9 Ter beschikking stellen van politiegegevens (Art 15)

Gegevens worden elektronische ter beschikking gesteld. Er blijven geen papieren versies achter.
DOS/KIC gaat uit van het principe delen tenzij. Ter beschikkingstelling van Infodesk naar Infodesk betreft ter beschikkingstellen buiten KLPD. Binnen KLPD wordt wel aan individuele medewerker ter beschikking gesteld (alleen per mail). Bij het ter beschikking stellen binnen het KLPD wordt nagegaan of de vragen steller bevoegd is deze vraag te stellen. Het mailaccount (beveiligd via een wachtwoord op het netwerk) is voor DOS het bewijs van de identiteit van de vragensteller. Het proces van het beschikbaarstellen van informatie is beschreven. De informatie word uitsluitend beschikbaar gesteld aan functionarissen waarvan bekend is dat zij deze informatie mogen opvragen. Wij hebben dit verband geen overzicht aangetroffen van functionarissen die bevoegd zijn informatie op te vragen en evenmin een beschrijving aangetroffen van de wijze waarop mutaties in dit verband worden bijgehouden en verwerkt. De naleving van de WPG is, ten aanzien van het aspect beschikbaarstelling van gegevens, in beperkte mate gewaarborgd.

Risico
Het risico is aanwezig dat aanvragen tot beschikbaarstelling van informatie ten onrechte worden gehonoreerd.

Risico-inschatting: laag
- Het proces van beschikbaarstelling van informatie is beschreven;

- Wij hebben geen overzicht aangetroffen van functionarissen die bevoegd zijn informatie op te vragen;
- De verwerken van mutaties in dit verband is niet gewaarborgd.

Aanbeveling
Wij adviseren een overzicht bij te houden van functionarissen die bevoegd zijn informatie op te vragen en de verwerking van mutaties in dit overzicht te waarborgen.

10 Verstrekkingen (Art 16 t/m Art 20)
DOS/KIC verstrekt geen gegevens.

11 Rechten van betrokkenen (Art 25 t/m Art 31)
Dit is geen onderdeel van de processen bij DOS/KIC; alle aanvragen gaan via de privacyfunctionaris.

12 Privacyfunctionaris (Art 34)
Binnen de dienst DOS zijn 2 privacyfunctionarissen aangesteld. De taken zijn tussen deze privacyfunctionarissen verdeeld; zij zijn beiden goed op de hoogte van de WPG.

De toezichthoudende rol van de privacyfunctionaris kan, door werk- en tijdsdruk, slechts op hoofdlijnen worden ingevuld. De privacyfunctionarissen werken ook voor de "blauwe" diensten. De verdere implementatie van de WPG kost capaciteit. De privacyfunctionaris heeft geen rechtstreekse toegang tot de systemen, maar kan gebruik maken kan wel gebruik maken van de collega's die autorisaties hebben voor betreffende systemen.

Risico's
Doordat de toezichthoudende rol alleen op hoofdlijnen wordt ingevuld bij DOS, loopt de dienst risico's t.a.v. de naleving van de WPG. Hierdoor voldoet DOS, ten aanzien van het aanstelling van een privacyfunctionaris, in beperkte mate aan de WPG.

Risico-inschatting: hoog
- de privacyfunctionarissen van DOS vervullen geen toezichthoudende rol; de naleving van de WPG is hierdoor uitsluitend afhankelijk van de beheersmaatregelen in het proces;
- de privacyfunctionaris kan niet zelfstandig onderzoek doen (autorisaties, werk- en tijdsdruk) naar de naleving van de WPG.

Aanbevelingen
Wij adviseren, ten aanzien van het aspect aanstelling van een privacyfunctionaris, de WPG volledig na te leven en de privacyfunctionaris zijn toezichthoudende rol te (doen) vervullen.

13 *Privacyjaarverslag (Art 34)*
De Privacyfunctionaris is aangemeld bij de CBP en heeft over 2010 een kort jaarverslag opgesteld. Hiermee heeft de Privacyfunctionaris voldaan aan de WPG.

Risico
Bij afwezigheid van een privacyjaarverslag kan moeilijk een inschatting worden gemaakt van de totale inzet en taken van de privacyfunctionaris en van de voortgang van de implementatie van de WPG.

Risico-inschatting: laag
- Indien geen privacyjaarverslag wordt opgesteld kan niet op een eenvoudige wijze worden ingeschat of de dienst op hoofdlijnen "in control" is t.a.v. de WPG.

14 Knelpunten verdere implementatie

DOS heeft een aantal punten genoemd die mogelijk als knelpunt kunnen worden aangemerkt bij de verdere implementatie van de WPG:
- de automatische schoning van gegevens na verstreken tijdsduur;
- de OvJ dient toestemming te verlenen voor geautomatiseerde vergelijking en in combinatie verwerking. Het KIC maakt nu gebruik van wildcards en jokers in zoektermen zodat alle op het verzoek betrekking hebbende gegevens worden geraadpleegd en doorgeleid aan de verzoeker. E.e.a. dient beter geregeld te worden.
- het proces rondom de verzending en verwerking van afloopberichten beter regelen.

15 Reactie van de dienst DOS

Reactie op de interne audit door het diensthoofd DOS.
Op 28/10/11 is in het kader van de jaarlijkse interne Wpg audit een interview afgenomen bij de afdeling Korps Informatie Knooppunt / Infodesk bij de Unit Informatie van de Dienst operationele Samenwerking (DOS).

De dienstleiding heeft kennis genomen van de conceptrapportage en de conclusies en de aanbevelingen zorgvuldig doorgenomen. Een inhoudelijke reactie per Wpg onderwerp is in de bijlage opgenomen. Naast deze aanvullingen, verbeteringen en verduidelijkingen, zijn echter de volgende aspecten opgevallen:

- De interne audit betreft de fase *opzet* en niet de fasen *bestaan en werking*. In de rapportage vloeien echter de verschillende fasen in elkaar over, waardoor de eindconclusie / risico-inschatting niet altijd enkel de fase *opzet* betreft;

- De scope van de audit betreft de dienstonderdelen KIK en Infodesk bij de DOS, terwijl de scope bij bepaalde onderwerken in de rapportage breder wordt getrokken. Dit betekent dat de risico-inschatting en de bijbehorende aanbeveling verder gaat dan alleen de dienstonderdelen die ge-audit zijn;

- Een aanscherping van de risico-analyse vanuit de context DOS is gewenst omdat volgens de rapportage een aantal Wpg aspecten in het geheel niet van toepassing zijn op de betreffende dienstonderdelen KIK en Infodesk, of zelfs voldoen aan de Wpg.

De concept reactie van de dienstleiding met daarin de aanvullingen, verbeteringen en verduidelijkingen is per 15 december jl. aan jullie gemaild. Wij gaan ervan uit dat de reactie zal worden verwerkt in de definitieve rapportage. Indien hierbij mocht blijken dat het standpunt van de audit afwijkt van deze reactie, dan graag nadere afstemming.

Hoofd van de Dienst Operationele Samenwerking

Drs. Ing. P.J.M. van Loosbroek EMPM.

Deze concept reactie is samengesteld door de geïnterviewden (opgesteld door de privacy functionairs DOS).

Inleiding:
Eens per vier jaar dient middels een externe Audit de naleving van de Wpg te worden gecontro-
leerd. Daarnaast dient jaarlijks (binnen de 4-jaarlijkse cyclus) ter controle op de naleving van de
Wpg een interne Wpg audit plaats te vinden. Hiervoor heeft op 28/10/2011 een interview plaatsgevonden bij DOS -> onderdeel Informatiecoördinatie -> Unit Informatie afdeling Korps Informatie Knooppunt – Infodesk. Vanuit de KLPD FEZ-auditpool is gesproken met: KLPD Programmaleider Implementatie Wpg, Wpg-functionaris DOS, Procesvoerder KIK-Infodesk, privacy functionaris blauwe diensten / DOS.

Proces:
Een intern audit proces kent een aantal stappen. Hieronder een kort overzicht van de acties.

- Samenstellen van een pré-audit dossier door het programma implementatie Wpg. Dossier bevat Wpg gerelateerde korps, dienst en unit documentatie.
- Ten behoeve van de interne audit, is een vragenlijst (quick scan Wpg KLPD 2011) opgesteld door de interne auditpool. Deze vragenlijst is leidend bij het gehouden interview.
- De vragenlijst is door de auditors gevuld met (interpretatie van de) antwoorden. Deze lijst is teruggekoppeld aan genoemde functionarissen voor een inhoudelijke reactie. Voor zover bekend, hebben de procesvoerder en privacy functionaris inhoudelijk gereageerd.
- In onderliggend concept document Interne audit WPG KLPD zijn de vragenlijst reacties summier overgenomen. Het concept is mede hierdoor deels correct. Onder het laatste hoofdstuk, zie inhoudelijke reactie, volgt puntsgewijs nader inhoudelijke behandeling van de onderwerpen indien deze naar overtuiging van de geïnterviewde aanvulling, verduidelijking, verbetering behoeven.

Scope interne audit:
De scope van de interne audit is gericht op het aspect opzet. Dit betekent dat de aspecten bestaan en werking in principe buiten beschouwing kunnen worden gelaten. Tijdens het interview is dit onderscheid niet aangehouden, aangezien de aspecten door de processen heen lopen. Gezien de scope van de audit zal het resultaat (risico's en aanbevelingen) wel weer gericht dienen te zijn op het aspect opzet.
Het auditgebied betreft zowel het KLPD Korps Informatie Knooppunt als de KLPD Infodesk. Beide onderdelen zijn beheersmatig ondergebracht bij de Dienst Operationele Samenwerking.

Inhoudelijke reactie:

Samenvatting tabel:
Op de samenvatting in tabelvorm is de toegekende bevinding niet eensluidend met de tekst bij de onderdelen in het rapport. Als voorbeeld: ondermandaat regeling, procesbeschrijvingen, bevoegd functionaris en privacy functionaris.

1.1. Mandaatregeling is aanwezig, daarmee wordt voldaan aan de opzet. Bij nader inzien voldoet de ondermandaat regeling in de praktijk, het is daarnaast niet wenselijk om privacy gerelateerde onderwerpen op een dieper nivo aan de organisatie te mandateren.

1.2. Procesbeschrijvingen zijn opgemaakt, daarmee wordt voldaan aan aspect opzet.
De vaststelling van processen door het Management Team, wordt benoemd als risico maar dit is geen Wpg mandaat aangelegenheid.

1.5. *Aanwijzing bevoegd functionaris.*
De KIK-Infodesk is belast met de makelaarsfunctie in de informatiekolom.
Hieruit vloeit voort dat de KIK -Infodesk geen eigenaar van de gegevens is, nog dat een bevoegd functionaris aan de orde is.

1.8. Opleidingsplan.
De medewerker op de infodesk volgt twee opleidingen waarbij de Wpg wordt behandeld. Deze opleidingen worden gevolgd voordat de nieuwe medewerker met werkzaamheden aanvangt. Op de afdeling heeft ieder een Wpg-training gevolgd en een opleiding voor de *functie van informatie medewerker (Rinf).*

2. Noodzakelijkheid, rechtmatigheid en doelbinding.
De afdeling is in de makelaarsfunctie geen eigenaar van de gegevens. Genoemde aspecten zijn niet van toepassing bij deze afdeling.

3. Juistheid, volledigheid en beveiliging van politiegegevens.
De afdeling is in de makelaarsfunctie geen eigenaar van de gegevens. Genoemde aspecten zijn niet van toepassing bij deze afdeling. Vanwege het belang van actualiteit in de informatievoorziening, wordt een gericht informatieverzoek uitsluitend afgehandeld met een actuele systeembevraging waarbij de meest recente informatie wordt doorgeleid.
Op eigen initiatief wordt wel een actieve bijdrage geleverd aan kwaliteitverbetering.
Daarbij neemt de medewerker contact op met het Kwaliteitsburo van de DNR. Dit buro kan *daardoor gepaste actie ondernemen.*

4. Autorisatie.
De bronsystemen waar de KIK-Infodesk gebruik van maakt zijn hoofdzakelijk Blue View; BVO, HKS, VROS, BVH, NSIS en -indien gewenst- nog een dertigtal andere systemen of applicaties. Er bestaat geen functiescheiding in de dagelijkse werkzaamheden van de KIK-Infodesk. Alle medewerkers hebben dezelfde autorisatie en hetzelfde autorisatieniveau. Derhalve hoeft er geen controle op functiescheiding te zijn en kan deze derhalve niet onvoldoende zijn. De scheiding van functies zit in andere aspecten (niet WPG- gerelateerd). De operationeel chef c.q. procesvoerder laat niet het beheer van autorisaties bij FA&G, dit beheer is daar immers belegd.

7. *Bewaartermijnen en vernietiging en* **8.** *Gegevens beheer:*
Geautomatiseerde schoning heeft betrekking op de gegevens welke d.t.v. de KIK-Infodesk zijn gedeeld en vastgelegd in BVO registratie.

V.w.b. bestand op de G-schijf, hierin is gedateerd mailverkeer opgeslagen.
T.b.v. interne verantwoording worden verwijderde mails als pst-bestand gedurende maximaal 4 jaar op de G:schijf bewaard.

9. Ter beschikking stellen van politiegegevens.
Conform het NIM model wordt met de regio korpsen (d.t.v. de Infodesk) gecommuniceerd. Intern daarintegen wordt op individueel nivo rechtstreeks tussen de Infodesk en de individuele medewerker gecommuniceerd. Hierbij vertrouwend op de integriteit van de interne collega die het verzoek indient. Ook wordt steeds de vraag gesteld aan verzoeker waarom hij de vraag stelt, voor welk onderzoek, en wat hij met de verkregen informatie gaat doen. Deze antwoorden worden bij de vraag en de gedeelde informatie in de BVO vastgelegd.

12. Privacy functionaris.
De privacy functionaris vervult in de praktijk veelal een gecombineerde advies/toezichthoudende rol. Zo ook de privacy functionaris bij de blauwe diensten / DOS. Al ontbreekt het momenteel aan gepland toezicht en vastlegging van de resultaten in een overzicht.

14. Knelpunten verdere implementatie.
* Automatische schoning:

Zie hiervoor punt 7 en 8. Het is wenselijk de handmatige schoning geautomatiseerd te laten plaatsvinden. Al betreft het een relatief eenvoudige handeling, daar waar ICT-matig ondersteund kan worden, is dit gewenst.
* geautomatiseerd vergelijken:

geautomatiseerd vergelijken / gecombineerd zoeken wordt niet gebruikt ten behoeve van analyse doeleinden. Vandaar dat deze handelingen m.u.v. raadpleging BleuView, niet als zodanig kunnen worden aangemerkt.
* proces terugkoppeling vanuit Openbaar Ministerie (Afloopberichten):

Het proces met betrekking tot de organisatie rondom en de verwerking van afloopbericten dient ICT-matig ondersteund te worden. Dit proces is op dit moment niet volledig sluitend in de praktijk. Centrale ontvangst voor het KLPD vindt bij de afdeling Operationele Informatie verwerking plaats. Door betreffende afdeling is medio 2011 een brief opgesteld waarin OIV als centraal ontvangstloket staat genoemd. Met het verzoek de afloopberichten voor wat betreft KLPD zaken aan deze afdeling te sturen.
De privacy functionaris kan zo nodig aanvullend contact onderhouden met de parketten.

Bijlage 6: DKDB

1 Inrichting van de organisatie

Inleiding

De Dienst Koninklijke en Diplomatieke Beveiliging (DKDB) is specialist op het gebied van persoonsbeveiliging, objectbeveiliging en veiligheidsadviezen in binnen- en buitenland. Door de DKDB worden leden van het Koninklijk Huis, hun gasten, politici, diplomaten en andere aangewezen personen 'op maat' beveiligd zodat zij veilig kunnen wonen, werken en ontspannen. De dienst verzamelt inlichtingen over relevante dreigingsinformatie waarmee persoonsbeveiligers de juiste tactiek, techniek en inzet voor de beveiligingsopdracht kunnen bepalen.

Samenvatting implementatie van de WPG bij DKDB

Wij hebben ons, bij de uitvoering van deze interne WPG-audit bij de dienst DKDB, beperkt tot onderzoek naar het proces DIK. Wij hebben uitsluitend onderzoek gedaan naar de opzet van de beheersmaatregelen; wij hebben geen onderzoek gedaan naar het bestaan en de werking van de maatregelen.

Op basis van de bevindingen naar aanleiding van dit onderzoek kunnen wij concluderen dat de DKDB, middels de implementatie van de WPG, in opzet voldoet aan de eisen van de WPG.

	WPG aspect	Bevinding	Risico-inschatting
1.1	Mandaatregeling	+	L
1.2	Procesbeschrijvingen	+	L
1.3	Risicoanalyse	+	L
1.4	Functionele documentatie.	n.v.t.	-
1.5	Aanwijzing Bevoegd functionaris	+	L
1.6	Samenwerkingverbanden	n.v.t.	-
1.7	Protocollen	+	L
1.8	Opleidingen	+	L
2	Noodzakelijkheid, rechtmatigheid & doelbinding	+	L
3	Juistheid, volledigheid & beveiliging politiegegevens	+	L
4	Autorisatie	+	L
5	Geautomatiseerd vergelijken	n.v.t.	-
6	In combinatie verwerken	n.v.t.	-
7	Bewaartermijnen & vernietiging	+	L
8	Gegevensbeheer	0	L
9	Ter beschikking stellen	0	L
10	Verstrekken	-	L
11	Recht van betrokkenen	-	L
12	Privacyfunctionaris	+	L
13	Privacyjaarverslag	+	L
	(voldoet aan de eisen van de WPG) **Eindconclusie:**	+	

Legenda bevindingen:	
+	*voldoet aan de WPG*
o	*voldoet in beperkte mate aan de WPG*
-	*voldoet onvoldoende aan de WPG*
n.v.t.	*WPG aspect niet van toepassing*
Legenda risico-inschatting:	
H	*hoog risico; voldoet niet aan de wet; geen risicobeperkende beheersmaatregelen ingericht*
M	*gemiddeld risico ; voldoet niet aan de wet; wel risico beperkende maatregelen ingericht*
L	*laag risico; voldoet aan de wet.*
-	*geen risico WPG aspect is niet van toepassing.*

1.1 Mandaatregeling

Het mandaat is door de DKDB feitelijk ingevuld. De DKDB heeft een organisatieschema met de organisatie onderdelen. Buiten het DIK (Dienst informatie knooppunt) werken ook het KEC (Kennis en Expertise Centrum), het IRIS team en de Units (Koninklijke - en diplomatieke beveiliging) met de WPG. Het diensthoofd is verantwoordelijk voor de toepassing en naleving van de WPG. De DKDB heeft ook een aantal taken lager in de organisatie belegd.
De DKDB werkt met de systemen BVO, VIPER en PAPER. Deze systemen kunnen een overzicht genereren waarop alle verwerkingen staan vermeld. In het processchema VVV is inzichtelijk gemaakt welke WPG verwerkingen binnen de dienst plaatsvinden.

Risico

Het risico is aanwezig dat op basis van de mandaatregeling toegekende bevoegdheden aan aangewezen functionarissen niet tijdig worden aangepast bij mutaties in de organisatie

Risico-inschatting: laag

- de DKDB heeft aandacht voor de veranderingen in de organisatie;
- het hoofd DIK is MT lid en regelt met de privacyfunctionaris de verdere implementatie van het mandaat.

Aanbevelingen

Wij adviseren de toekenning van bevoegdheden op basis van de mandaatregeling KLPD breed actueel te houden en, voorzover de werkwijze van de DKDB niet aansluit bij de werkwijze van het KLPD, de mandaatregeling op dit punt te doen aanpassen.

1.3 Procesbeschrijvingen

Alle processen van de DKDB zijn uitvoerig beschreven en door het MT vastgesteld. Hiermee wordt voldaan aan de WPG. De DKDB heeft inzicht in de functionele eisen die zij aan SUMM-IT stelt (zoals o.a. automatische opschoning). De DKDB heeft geen afzonderlijke maatregelen getroffen voor de processen die niet aan de WPG voldoen.

Het project G:\schijf had tot doel de G:\schijf te schonen. Het voorziet in een structuur voor de informatievoorziening en is afgestemd op de uiteindelijke overgang naar SUMM-IT. Het project is ten dele achterhaald doordat SUMM-IT voorziet in een functionaliteit voor automatische opschoning. Tevens heeft SUMM-IT voordelen op het gebied van het

raadplegen en verwerken van informatie. De DKDB zal SUMM-IT op korte termijn uitrollen; de implementatie staat gepland voor de 2e helft van 2012. Na ingebruikname vindt de toets in de praktijk plaats.

De DKDB heeft voor het beschrijven van het primaire proces gebruik gemaakt van de OMP systematiek (MAVIM); dit is een KLPD-breed gebruikte systematiek.

De dienst DKDB is meegenomen in het hele proces van de implementatie van de WPG. Er is vaak gecommuniceerd via intranet en in briefings zijn casussen aan de medewerkers voorgelegd. Deze casussen zijn voor studie nog steeds beschikbaar via intranet.

De WPG staat niet standaard op de agenda van het MT maar wel op de agenda van het OBB (Operationeel overleg Bewaken & Beveiligen). De WPG issues kunnen altijd worden besproken met het MT of met het diensthoofd.

De DKDB hanteert een disclaimer waarin het doel van de verzameling van informatie is beperkt tot het proces bewaking en beveiligen; informatie kan niet worden gebruikt voor opsporingsdoeleinden.

Risico
Het risico is dat de huidige systemen de WPG niet of onvoldoende ondersteunen en dat de ontwikkelingen voor de systemen die niet aan de WPG zijn aangepast worden stopgezet.

Risico-inschatting: laag
- De DKDB hanteert een disclaimer die de naleving van de WPG bevordert. In deze disclaimer is het doel van de informatievoorziening omschreven en beperkt tot het proces bewaken en beveiligen; het gebruik van de informatie voor opsporingsdoeleinden is niet toegestaan.
- De DKDB heeft zicht op het proces en op de manco's voor de WPG in die processen en systemen.

Aanbevelingen
Wij adviseren om de procesbeschrijvingen aan te passen bij implementatie van SUMM-IT.

1.3 Risicoanalyse
De DKDB heeft een risico-analyse uitgevoerd; deze is vastgelegd ter voorbereiding op de interne audit en geënt op de systematiek van de infoproducten. De risico-analyse is niet door het MT vastgesteld. De DKDB, wil voor de overgang naar de nieuwe standaard SUMM-IT, opnieuw een risico-analyse uitvoeren. Hierbij dient rekening te worden gehouden met schoning van het systeem.

De WPG maakt geen vast onderdeel uit van de agenda. Vanuit het OBMP is committment gezocht met het hoofd DKDB door het delen van informatie (bijv. het uitwisselen van praktijkcasussen). De bevoegdheden rondom de implementatie van de WPG zijn doorgemandateerd; de uiteindelijke verantwoordelijkheid ligt bij de KL en de diensthoofden. Ten aanzien van de overgang naar SUMM-IT zijn er diverse opties: een afbouw van het huidige systeem (wel raadpleging) of gefaseerde uitfasering (waarbij alleen gevalideerde informatie overgaat naar SUMM-IT).

4 specialisten zijn verantwoordelijk voor de invoer van gegevens. De DKDB zal 1 medewerker (gegevensbeheerder) belasten met de controle op de kwaliteit van de ingevoerde gegevens.

Risico
Het risico is dat de dienst onvoldoende zicht heeft op de risico's die de WPG met zich meebrengt. De effectiviteit en efficiëntie van de getroffen maatregelen is op deze wijze onvoldoende gewaarborgd.

Risico-inschatting: laag
- DKDB heeft een risicoanalyse uitgevoerd.
- DKDB is van plan opnieuw een risicoanalyse uit te voeren bij de implementatie van SUMM-IT

Aanbevelingen
Wij adviseren de DKDB bij de implementatie van SUMM-IT een integrale risico-analyse uit te voeren en door het MT te doen vaststellen.

1.4 Functionele documentatie
De DKDB maakt gebruik van o.a. de bekende landelijke applicaties zoals BVO en standaard pakketten zoals Office. De landelijke applicaties worden beheerd door de VtsPN. De standaard pakketten worden volgens de systematiek van de VtsPN beveiligd. Tevens maakt de DKDB voor de verwerking van informatie gebruik van de applicaties VIPER en PAPER. Deze systemen bevatten een overzicht van alle systemen die de verwerking ondersteunen; er is geen functionele documentatie beschikbaar. VIPER en PAPER hebben geen interfaces met andere systemen voor de uitwisseling van informatie.

Van de overige systemen die de DKDB gebruikt is functionele documentatie beschikbaar. Uitgangspunt bij de registratie is het delen van kennis en het verbeteren van de kwaliteit..Ongeveer 10 medewerkers verwerken politiegegevens binnen de systemen.

De aanwezigheid van functionele documentatie is geen verplichting vanuit de WPG en is niet direct van invloed op de mate waarin aan de WPG wordt voldaan. Functionele documentatie is indirect echter wel van invloed op de naleving van de WPG aangezien op basis van functionele documentatie beoordeeld kan worden welke beheersmaatregelen zijn getroffen in de applicaties. Deze beheersmaatregelen (bijv. validaties, ingebouwde en geprogrammeerde controles) betreffen o.a. de aspecten juistheid, volledigheid en beveiliging van politiegegevens. E.e.a. is nader toegelicht in paragraaf 3 van deze rapportage.

De DKDB heeft geen zicht op de naleving van de WPG in de systemen die in eigen beheer zijn gebouwd. De DKDB kent wel de beperkingen van deze systemen. De bedoeling is deze systemen op den duur uit te faseren en te vervangen door systemen wel aan de WPG voldoen.

1.5 Aanwijzing bevoegd functionaris
Binnen de DKDB zijn 5 personen (4 specialisten informatie voorziening en 1 leidinggevende) als bevoegd functionaris aangewezen. De rol van bevoegd functionaris wordt conform de

aanstelling en de "Handreiking bevoegd functionaris" uitgevoerd. De taken, bevoegdheden en verantwoordelijkheden zijn bij de bevoegd functionarissen bekend.

Risico
Bij het niet aanwijzen van bevoegd functionarissen bestaat het risico dat een aantal verplichtingen uit de WPG niet juist worden uitgevoerd.

Risico-inschatting: laag
- DKDB heeft 5 bevoegd functionarissen aangewezen;
- De taken en bevoegdheden van bevoegd functionarissen zijn bekend en geïmplementeerd.

Aanbevelingen
Geen

1.6 Samenwerkingsverbanden (Art 20)
De DKDB is geen samenwerkingsverbanden met andere partijen aangegaan.

1.7 Protocollen
De DKDB heeft een art. 13 protocol opgesteld. Het protocol is getekend door het diensthoofd en is, vanuit een juridische noodzaak, opgesteld in samenwerking met de juristen van het KLPD.

Risico's
Het risico bestaat dat het protocol voor art. 13 verwerkingen onvoldoende wordt onderhouden en dat zich nieuwe knelpunten voordoen waarbij een nieuw protocol beschreven zou moeten worden.

Risico-inschatting: laag
- De processen van de DKDB zijn overzichtelijk en de privacyfunctionaris van de DKDB heeft voldoende oog voor veranderingen in het proces of de WPG die het noodzakelijk maakt een art. 13 protocol te onderhouden.

Aanbevelingen
Wij bevelen aan om art. 13 protocollen één maal per jaar met de afdelingshoofden op hun actualiteit te beoordelen en waar nodig aan te passen.

1.8 Opleidingen
De behoefte aan een WPG opleiding is ontstaan vanuit een juridisch noodzaak aangezien medewerkers van de DKDB met juridische vraagstukken omtrent de WPG werden geconfronteerd. Door middel en opleiding en communicatie rondom de WPG is de bewustwording bij de medewerkers geborgd. Er is een werkgroep samengesteld met daarin een unithoofd in de lijn naar het Managementteam van de dienst. In 2012 is er een cursus voor nieuwe instromers bij de DKDB. De WPG is tegenwoordig ook opgenomen in de basis opleiding van de Politie Academie. Op intranet wordt een WPG zelftest aangeboden. Bij indiensttreding van nieuwe medewerkers krijgt iedere nieuwe medewerker opleiding waar de WPG onderdeel van uitmaakt. Er ligt een voorstel om iedere beveiliger één keer per jaar de E-learning test te laten doen. Momenteel is iedereen bij de DKDB die met de WPG werkt

opgeleid. De privacyfunctionaris en Hoofd DIK houden de laatste ontwikkelingen rondom de WPG bij en communiceren deze via de gebruikelijke kanalen..

Risico
Na het opleiden van medewerkers moet de kennis over de WPG bij de medewerkers worden bijgehouden. Indien de kennis niet wordt bijgehouden is het voor de organisatie onvoldoende te meten of er volgens de WPG gewerkt wordt.

Risico-inschatting: laag
- DKDB wil met een E-learning test één maal per jaar de kennis over de WPG testen;
- Ontwikkelingen worden in de organisatie gedeeld;
- Nieuwe medewerkers worden opgeleid.

Aanbevelingen
Wij adviseren het voorstel de medewerkers jaarlijks te testen op hun kennis van de WPG via E-learning te implementeren en, na evaluatie, ook binnen het KLPD onder de aandacht te brengen.

2 Noodzakelijkheid, rechtmatigheid en doelbinding (Art 3)

Deze begrippen zijn bij de geïnterviewden van de DKDB bekend. Alle processen worden gerelateerd aan de taken en doelstellingen van de DKDB. De DKDB heeft een disclaimer opgenomen om de noodzakelijkheid en rechtmatigheid af te dekken door in de disclaimer het doel van de verzameling van informatie te beperken tot het proces bewaking en beveiligen en daarmee het gebruik van informatie voor opsporingsdoeleinden uit te sluiten.
De bevoegd functionarissen zijn de enige functionarissen die met derden communiceren over de beschikbare informatie.

De onderzoeken van de DKDB kunnen worden beschouwd als projecten. De privacyfunctionaris heeft overzicht door een actuele lijst met alle projecten en heeft in dit verband een passieve rol. De registratie van projecten en incidentele beveilingsopdrachten vindt plaats binnen een week. De privacyfunctionaris beschikt over extra mogelijkheden in het kader van de WPG om inzicht en overzicht te verkrijgen in het kader van zijn toezichthoudende rol.

Het toezicht kenmerkt zich onder andere door:
- de code planning in BVCM;
- van iedere incidentele beveiligingsopdracht wordt een opdracht geregistreerd in VIPER (dit geeft antwoord op de WAT-vraag);
- er wordt een levend document aangemaakt met een overzicht van alle relevante informatie (incl. de status; dit geeft antwoord op de HOE-vraag).

Risico
Het risico is dat politiegegevens voor een ander doel of een niet noodzakelijk doel worden verwerkt.

Risico-inschatting: laag

- DKDB heeft een duidelijke visie en beleid omtrent het delen van informatie met andere partijen;
- informatie die niet meer relevant is wordt vernietigd.

Aanbevelingen

Wij adviseren in het kader van noodzakelijkheid en doelbinding vast te houden aan het eigen beleid en dit afhankelijk te maken van het beleid rondom Bewaken en Beveiligen.

3 Juistheid, volledigheid en beveiliging politiegegevens (Art 4)

De specialisten van het DIK controleren of de politiegegevens juist en volledig zijn. In de toekomst zal deze taak door gegevensbeheer worden uitgevoerd. Alle informatie die door DIK wordt geleverd is geverifieerd; er wordt van uitgegaan dat deze informatie juist en volledig is. De informatie uit eigen DKDB bronnen wordt ook als juist aangemerkt. De informatie uit andere bronnen worden vergezeld van een bronvermelding.

Als bij navraag bij de aanleverende collega de gegevens niet juist of onvolledig zijn wordt dit hersteld; de onjuiste informatie blijft beschikbaar. Als de informatie toch nog relevant is wordt deze in VIPER geregistreerd.
Deze worden aangevuld of vernietigd door de specialisten van DIK in overleg met de privacyfunctionaris. Indien informatie onjuist is wordt dit ook aan de betreffende collega gemeld. De controle vindt handmatig plaats en wordt niet door systemen ondersteund. Alle data van de DKDB staan in een beveiligde omgeving (achter datafort). Het is beleid dat er uitsluitend beveiligde USB-sticks worden gebruikt (uitzonderingen daargelaten). Tijdens de operationele uitvoering wordt informatie opgeborgen in beveiligde koffers..

Andere informatie wordt op de persoon uitgereikt en ingenomen. Er wordt alleen die informatie verstrekt die men nodig heeft plus een evaluatie formulier. Er zijn tot nog toe geen incidenten gemeld rondom het verlies van informatie. Het uitgangpunt van de DKDB is: informatie die binnen is blijft binnen. De DKDB heeft beleid ontwikkeld rondom de wijze waarop met informatie moet worden omgegaan en hoe de betrouwbaarheid van de informatie gewaarborgd dient te worden. De data zijn beveiligd en afgeschermd. Informatie wordt slechts op de man verstrekt en weer ingenomen.

Risico

Het risico is dat informatie niet juist of niet volledig is. Een ander risico is niet daartoe geautoriseerde personen kennis nemen van de informatie of dat informatie verloren gaat.

Risico-inschatting: laag

- De DKDB heeft de aanname dat de eigen informatie juist is.
- Informatie van andere wordt als juist gezien maar er wordt een bron vermelding toegevoegd.

Aanbevelingen
Geen

4 Autorisatie (Art 6)

De autorisaties zijn functioneel ingericht; niet iedereen heeft dezelfde functie. Zowel de uitreiking van de bevoegdheden als de inname van de bevoegdheden vinden plaats op de persoon. Tevens is er een onderscheid tussen twee groepen medewerkers, namelijk de Koninklijke en de diplomatieke beveiliging. In een aantal gevallen zijn medewerkers geautoriseerd voor beide groepen.

De functiescheiding wordt gewaarborgd door gebruik te maken van een autorisatiematrix. De autorisatiematrix moet nog door het diensthoofd van de DKDB worden geaccordeerd. Bij het toekennen van de autorisatie is de functie leidend. De gemandateerde leidinggevende kent de autorisaties toe. Functioneel beheer zal de autorisatieaanvragen verwerken op basis van door het diensthoofd goedgekeurde functies (conform autorisatiebeleid) en vervolgens in beheer nemen.

De DKDB heeft functiescheiding toegepast t.a.v. de inrichting van de autorisatiematrix en de toekenning van de autorisaties conform het autorisatiebeleid. De korpsleiding heeft dit autorisatiebeleid vastgesteld..

Risico
Er bestaat een risico bij het toekennen van autorisatie bij nieuwe functies en bij overstappen van de Koninklijke naar de diplomatieke tak en omgekeerd. De autorisatiematrix is niet door het diensthoofd vastgesteld.

Risico-inschatting: laag
- de DKDB heeft een overzichtelijk proces waarin de twee verschillende takken goed zijn te onderscheiden;
- er is een autorisatiematrix.

Aanbevelingen
Wij adviseren om de autorisatiematrix door het diensthoofd vast te laten stellen.

5 Geautomatiseerd vergelijken (Art 11)

De DKDB past geen automatische vergelijking toe. In de gevallen dat de informatie niet duidelijk of niet volledig is vindt bevraging van HKS plaats. Dit proces is beschreven en ingeregeld in het VVV proces.

6 In combinatie verwerken (Art 11)

De DKDB past geen in combinatie met elkaar verwerking toe.

7 Bewaartermijnen en vernietiging (art. 14)

De privacyfunctionaris controleert maandelijks op de naleving van de bewaartermijnen met behulp van de systemen VIPER en PAPER. De gegevens die te oud zijn (op basis van de datum van de laatste verwerking) worden, in overleg met het DIK, verwijderd of overgezet naar art. 13 zodat de bewaartermijn kon worden verlengd. De informatie uit art. 8

verwerkingen gaat snel over naar art. 13 als op deze manier de informatie langer kan worden bewaard.. Voor zover gegevens niet langer relevant zijn verwijdert Functioneel beheer de gegevens uit de systemen. De privacyfunctionaris plaatst gegevens in de voorkomende gevallen achter een "schot".

Hoewel de controle op de naleving van de bewaartermijnen een handmatig proces is worden de bewaartermijnen goed gehandhaafd. De privacyfunctionaris begeleid dit proces.

Risico's
De DKDB heeft zicht op de naleving van de bewaartermijnen; dit is echter geheel afhankelijk van één functionaris. De systemen bevatten geen functionaliteit voor automatische schoning en evenmin een signaleringsfunctie.

Risico-inschatting: laag
- de privacyfunctionaris heeft zicht op de naleving van de bewaartermijnen;
- de gegevens die niet meer relevant zijn worden vernietigd;
- informatie kan één jaar of langer bewaard worden, zolang de privacyfunctionaris geen actie onderneemt.

Aanbevelingen
Wij adviseren bij de komst van SUMM-IT de functionaliteit voor automatische opschoning (signalering en vernietiging) te gebruiken.

8 Gegevens beheer

De DKDB is nog in afwachting van Korpsbesluit om op dienstniveau gegevensbeheer in te richten. Alle gegevens worden zoveel mogelijk digitaal geregistreerd en bewaard.
Papieren informatie wordt "op de man" uitgereikt. Na de inzet neemt de dienst de informatie weer in ter vernietiging. Wanneer gegevens buiten de DKDB meegenomen worden, worden deze in een kluis opgeslagen.

Risico
Er bestaat een risico dat het beheer van politiegegevens in hardcopy vorm niet op de juiste wijze plaatsvindt. Informatie wordt in mappen aan medewerkers meegegeven.

Risico-inschatting: laag
- de DKDB heeft een protocol voor het uitgeven en weer innemen van informatie;
- medewerkers worden aangesproken als informatie niet wordt ingeleverd;
- informatie wordt buiten de DKDB vestigingen in een kluis bewaard.

Aanbevelingen
Wij adviseren het huidige beleid om informatie op de man uit te geven en weer in te nemen te handhaven en een audit te doen uitvoeren naar dit proces.

9 Ter beschikking stellen van politiegegevens (Art 15)

De DKDB stelt alleen gegevens ter beschikking voorzover dit in overeenstemming is met de taken en doelstellingen van de DKDB. Het DIK is belast met de beoordeling en - voorzover van toepassing - feitelijke beschikbaarstelling. De DKDB heeft geen convenant afgesloten

waarin de afspraken zijn vastgelegd. Wij hebben niet kunnen vaststellen op welke wijze wordt beoordeeld of de ter beschikking stelling van informatie in overeenstemming met de taken en doelstellingen van de DKDB heeft plaatsgevonden..

Risico
Het risico bestaat dat de beoordeling van de ter beschikking gestelde informatie niet in alle gevallen conform de taken en doelstellingen van de DKDB en conform de WPG plaatsvindt indien voor deze beoordeling niet in alle gevallen dezelfde criteria worden gehanteerd.

Risico-inschatting: laag
- DKDB overweegt met argumenten welke informatie ter beschikking wordt gesteld;
- DKDB is erg terughoudend met ter beschikking stellen van informatie.

Aanbevelingen
Wij adviseren nadere richtlijnen op te stellen voor de beschikbaarstelling van informatie om te voorkomen dat de definitie niet eenduidig wordt toegepast en de grenzen worden opgerekt.

10 Verstrekkingen (Art 16 t/m Art 20)

Bij de DKDB wordt er in principe niet buiten het politiedomein verstrekt. In voorkomende gevallen zal de bevoegd functionaris hierover oordelen. Bij verstrekken zal worden vastgelegd aan wie, wanneer en welke informatie is verstrekt. Dit proces is niet beschreven en is ook nog niet eerder voorgekomen. Hiermee is niet voldaan aan de WPG.

Risico
Er is geen procedure voor het verstrekken van politiegegevens buiten het politiedomein. In interview is aangegeven dat dit waarschijnlijk niet vaak zal voorkomen.

Risico-inschatting: laag
- er is geen procedure voor verstrekken van politiegegevens buiten het politiedomein;
- in voorkomende gevallen wordt de bevoegd functionaris ingeschakeld.

Aanbevelingen
Wij adviseren deze procedure alsnog te beschrijven of voor deze procedure aan te haken bij andere diensten.

11 Rechten van betrokkenen (Art 25 t/m Art 31)

Het is bij de DKDB nog nooit voorgekomen dat betrokkenen inzage in de politiegegevens wil hebben. Alleen worden er WOB verzoeken ingediend. Indien er vragen binnenkomen bij de DKDB worden deze direct bij de privacyfunctionaris neergelegd. Dit proces is niet beschreven.

Risico's
Er is geen procedure voor het omgaan van het recht van betrokkenen. In het interview is aangegeven dat dit waarschijnlijk niet zal voorkomen.

Risico-inschatting: laag

- er is geen procedure voor de inzage, mutatie of vernietiging van dossiers van betrokkenen. In voorkomende gevallen wordt de privacyfunctionaris ingeschakeld.

Aanbevelingen

Wij adviseren een korpsbrede procedure te ontwikkelen voor de rechten van betrokkenen.

12 Privacyfunctionaris (Art 34)

Bij de DKDB is een privacyfunctionaris aangesteld. De privacy functionaris is goed inhoudelijk op de hoogte van zijn taken, verantwoordelijkheden en bevoegdheden en van de werkzaamheden in het operationele proces van de DKDB.

De privacyfunctionaris borgt de voortgang en de implementatie binnen de dienst. Hij neemt deel aan het privacyoverleg van het KLPD. De voortgang wordt gecommuniceerd via het Hoofd DIK; bevoegd functionarissen verzorgen de implementatie. Er is een nazorgtraject waarin casusvoorbeelden worden gehanteerd i.s.m. een jurist en de centrale privacyfunctionaris van het KLPD. Er wordt proactief op de implementatie van de WPG ingespeeld.

De privacyfunctionaris heeft de hoogste autorisatie voor inzage in de systemen. Alle WPG aangelegenheden met betrekking tot de WPG worden aan de privacyfunctionaris gemeld. De privacyfunctionaris houd toezicht op en in alle systemen en geeft adviezen om deze te verbeteren. De privacyfunctionaris is met het hoofd DIK nauw betrokken bij de implementatie van SUMM-IT binnen de DKDB.

Risico

Er bestaat een risico dat de privacyfuntionaris door werkdruk onvoldoende invulling kan geven aan zijn toezichthoudende rol.

Risico-inschatting: laag

- de privacyfunctionaris van de DKDB vult de toezichthoudende rol in.
- de privacyfunctionaris werkt - als waarborg voor de continuïteit - nauw samen met het hoofd DIK.

Aanbevelingen

Geen aanbeveling

13 Privacyjaarverslag (Art 34)

De Privacyfunctionaris DKDB is aangemeld bij de CBP en heeft over 2010 een kort jaarverslag opgesteld. Hiermee heeft de privacyfunctionaris voldaan aan de WPG.

Risico

Door het niet opleveren van een jaarverslag wordt niet aan de WPG voldaan.

Risico-inschatting: laag

- De DKDB heeft een jaarverslag over 2010 opgeleverd

		Eindconclusie:	

Legenda bevindingen:	
+	*voldoet aan de WPG*
0	*voldoet in beperkte mate aan de WPG*
-	*voldoet niet aan de WPG*
n.v.t.	*WPG aspect niet van toepassing*
Legenda risico-inschatting:	
H	*hoog risico; Voldoet niet aan de wet; geen risicobeperkende beheersmaatregelen ingericht*
M	*gemiddeld risico ; Voldoet niet aan de wet; wel risico beperkende maatregelen ingericht*
L	*laag risico; Voldoet aan de wet.*
-	*geen risico WPG aspect is niet van toepassing.*

1.1 Mandaatregeling

Wij hebben, op basis van interviews en bestudering van de documentatie, vastgesteld dat de mandaatregeling bij de DSRT bekend is en binnen de dienst is geïmplementeerd.
De privacyfunctionaris kent de globale inhoud van het mandaat. Er is geen overzicht van alle verwerkingen op de afdeling. Het werk van de DSRT is omgeven met het label "geheim"; dit maakt transparantie moeilijk. De diensthoofden zijn verantwoordelijk voor de implementatie en de naleving van de WPG. De feitelijke uitvoering van de implementatie is belegd bij de privacyfunctionaris.

De DSRT werkt in een keten en doet geen zelfstandige onderzoeken. De WPG heeft de aandacht van de dienstleiding van DSRT.
Dit aspect, mandaatregeling, voldoet aan de WPG.

Risico

De DSRT is van mening dat de wetgever onvoldoende duidelijkheid schept voor de specifieke processen die bij de DSRT plaatsvinden aangezien onderdelen van de WPG op diverse wijze geïnterpreteerd kunnen worden. De DSRT weet om die reden niet of zij in alle opzichten aan de WPG voldoet.

Risico-inschatting: hoog

- Hoewel de WPG regelmatig op de agenda staat is de naleving van de WPG echter niet geborgd in de managementcyclus.

Aanbeveling

Wij adviseren nader onderzoek te doen naar de interpretatie van de WPG en in de voorkomende gevallen bij de wetgever aan te dringen op een nadere toelichting over de interpretatie van de WPG (bijvoorbeeld in de vorm van uitvoeringsvoorschriften).

1.2 Procesbeschrijvingen

De processen van de DSRT zijn op hoofdlijnen beschreven. De beschrijving van de taken, verantwoordelijkheden en bevoegdheden in de procesbeschrijvingen beperkt zich in het algemeen tot een beschrijving op teamniveau en zijn niet gedetailleerd tot het niveau van de individuele functionaris.

Wij hebben evenmin een beschrijving aangetroffen van de processen tussen de ketenpartners van de DSRT binnen de strafrechtketen. Door de beperkte detaillering in de procesbeschrijvingen van de DSRT worden processen mogelijk verschillend geïnterpreteerd en niet op een eenduidige wijze gevolgd. Tevens zijn de beheersmaatregelen in de processen onvoldoende uitgewerkt en geborgd. De afwezigheid van beschrijvingen van de processen tussen de ketenpartners van de DSRT binnen de strafrechtketen veroorzaakt eenzelfde risico binnen de strafrechtketen. Hierdoor is – zowel binnen de DSRT als binnen de strafrechtketen - niet bekend welke risico's worden gelopen t.a.v. de naleving van de WPG.
Dit aspect, procesbeschrijvingen, voldoet in beperkte mate aan de WPG.

Risico
De processen van de DSRT en tussen de DSRT en haar ketenpartners zijn niet in alle gevallen voldoende uitgewerkt; dit veroorzaakt risico's voor de naleving van de WPG.

Risico-inschatting: hoog
- De naleving van de WPG - zowel binnen de DSRT als binnen de strafrechtketen - is niet in alle gevallen voldoende gewaarborgd.

Aanbevelingen
Wij adviseren de procesbeschrijvingen binnen de DSRT verder te detailleren (tot het niveau van de individuele functionaris), te implementeren en binnen de organisatie te borgen zodat de naleving van de WPG is gewaarborgd.

Wij adviseren de processen tussen de DSRT en haar ketenpartners binnen de strafrechtketen te beschrijven, te implementeren en binnen (de ketenpartners van) de strafrechtketen organisatie te borgen.

1.3 Risico-analyse
Wij hebben bij de DSRT een risico-analyse aangetroffen. Deze is, op verzoek van het diensthoofd, uitgevoerd door de afdeling Kwaliteit maar (nog) niet door het MT vastgesteld. Op basis van deze risico-analyse is een aantal maatregelen getroffen die tot doel hebben de betrouwbaarheid van de informatievoorziening en de naleving van de WPG te waarborgen. Wij hebben, op basis van de interviews en op basis van onderzoek van de documentatie, niet vast kunnen stellen dat deze maatregelen in samenhang zijn getroffen. Dit aspect risico analyse, voldoet hiermee in beperkte mate aan de WPG.

Risico
De maatregelen rondom de betrouwbaarheid van de informatievoorziening en de naleving van de WPG zijn niet in samenhang getroffen. Wij hebben om deze reden niet vast kunnen stellen welke restrisico's de DSRT loopt ten aanzien van de betrouwbaarheid van de informatievoorziening en de naleving van de WPG.

Risico-inschatting: hoog
- De betrouwbaarheid van de informatievoorziening en de naleving van de WPG zijn niet in alle gevallen voldoende gewaarborgd.

Aanbevelingen
Wij adviseren de risicoanalyse verder uit te werken, door het MT te laten vaststellen en - op basis van de risico-analyse - beheersmaatregelen te treffen (in samenhang) om de gesignaleerde risico's te mitigeren.

1.4 Functionele documentatie

Bij DSRT wordt gebruik gemaakt van diverse applicaties. DSRT heeft een aantal van deze applicaties in eigen beheer gebouwd en verzorgt ook het onderhoud van de applicaties in eigen beheer. Over het algemeen zijn uitsluitend fabrieksbeschrijvingen beschikbaar en geen overige documentatie.
Het ontbreken van functionele documentatie van applicaties kan een risico vormen voor de naleving van de WPG aangezien hierdoor niet kan worden beoordeeld welke beheersmaatregelen in de applicaties zijn getroffen. Deze beheersmaatregelen (bijv. validaties, ingebouwde en geprogrammeerde controles) betreffen o.a. de aspecten juistheid, volledigheid en beveiliging van politiegegevens. E.e.a. is is nader toegelicht in paragraaf 3 van deze rapportage. Tevens kan, bij het ontbreken van functionele documentatie, niet worden ingeschat of de applicaties in opzet voldoende aansluiten op de processen van de DSRT. Hoewel deze bevinding geen directe invloed heeft op de mate waarin aan de WPG wordt voldaan, adviseren wij toch de functionele documentatie van de applicaties uit te werken en binnen te organisatie te borgen.

1.5 Aanwijzing bevoegd functionaris

Bij de DSRT is sprake van gerubriceerde gegevens tot het niveau van zeer geheim (paarse informatie). Uit interviews is gebleken dat de DSRT geen bevoegd functionarissen heeft aangewezen aangezien de DSRT uitsluitend opdrachten uitvoert van andere diensten (zoals de DNR, regiokorpsen, FIOD, ECD, MIVD, AIVD en BOD's). De DSRT staat op het standpunt dat de onderzoeksleider (bijv. van de DNR) de bevoegd functionaris is en de DSRT in dat geval dan geen bevoegd functionaris nodig heeft. Hierbij is ervan uitgegaan dat de DSRT werkzaamheden uitvoert in een keten waarmee de onderzoeksleider (buiten het KLPD) de bevoegd functionaris is. De DSRT is geen eigenaar van de gegevens die zij verzamelt.

In de art.13.2 protocollen TGB (Getuigenbescherming) en WOD (Werken onder Dekmantel) zijn echter wel bevoegd functionarissen van de DSRT genoemd: de teamleider alsmede de daartoe opgeleide en aangestelde functionarissen van de Unit TGB (Getuigenbescherming) resp. WOB (Werken onder Dekmantel). De bevoegd functionaris bepaalt, in afstemming met de Officier van Justitie van het Landelijk Parket, aan wie de gegevens beschikbaar worden gesteld.
Het aspect aanwijzing bevoegd functionaris voldoet in beperkte mate aan de WPG.

Risico
Bij de DSRT worden politiegegevens verwerkt op verzoek van andere diensten binnen de strafrechtketen (zowel binnen als buiten het KLPD). Deze andere dienst levert de onderzoeksleider die tevens de rol van bevoegd functionaris vervult. Het is vraag in hoeverre een bevoegd functionaris in dit geval (ten aanzien van de verstrekking van gegevens) over de grenzen van de eigen organisatie kijkt en toezicht kan uitoefenen op de naleving van de WPG bij de overige ketenpartners (buiten de eigen organisatie, zoals de DSRT).

Tevens kan de in het voorgaande geconstateerde onduidelijkheid omtrent bevoegd functionarissen risico's met zich meebrengen voor de naleving van de WPG.

Risico-inschatting: hoog

- De naleving van de WPG – zowel binnen de DSRT als in de strafrechtketen - is niet in alle gevallen voldoende gewaarborgd.

Aanbevelingen

Wij adviseren zowel de rol van de bevoegd functionaris als de rol van de privacyfunctionaris in ketenprocessen te (doen) verduidelijken en in dit verband nadere afspraken te maken over de taken, verantwoordelijkheden en bevoegdheden van betreffende functionarissen in ketenprocessen.

1.6 Samenwerkingsverbanden (Art 20)

Er zijn geen samenwerkingsverbanden. Het OM geldt als (uiteindelijke) opdrachtgever.

1.7 Protocollen

De DSRT kent 2 protocollen voor art. 13.2 verwerkingen: TGB en WOD. De DSRT heeft, met de voornoemde protocollen, voldaan aan de wet. Uit de interviews is gebleken dat niet iedere relevante functionaris in dit verband kennis heeft genomen van het bestaan van deze protocollen. In dit geval bestaat een risico dat wordt afgeweken van de in het protocol beschreven werkwijze. Dit kan risico's opleveren voor de naleving van de WPG.

Risico-inschatting: gemiddeld

- De DSRT heeft, met het uitwerken van de protocollen voor TGB en WOD, ten dele voldaan aan haar wettelijke verplichting.
- Wij hebben niet vast kunnen stellen dat deze protocollen zijn vastgesteld en dat iedere in het kader van de WPG relevante functionaris kennis heeft genomen van deze protocollen.

Aanbevelingen

Wij adviseren de artikel 13 protocollen, voor zover van toepassing, vast te stellen en dit onder de aandacht te brengen van de in het kader van de WPG relevante functionarissen.

1.8 Opleidingen

Bij DSRT is iedereen die met de WPG werkt opgeleid. Wij hebben geen opleidingsplan aangetroffen. Wij hebben door middel van interviews vastgesteld dat iedere medewerker die met de WPG werkt is opgeleid.

Risico

Door het ontbreken van een opleidingsplan bestaat in opzet het risico dat niet iedere medewerker is opgeleid; dit kan risico's veroorzaken voor de naleving van de WPG.

Risico inschatting: laag

- Op basis van interviews is gebleken dat de medewerkers die met de WPG werken zijn opgeleid.
- De privacyfunctionaris houdt de ontwikkelingen op het gebied van de WPG bij en ziet er op toe dat iedere nieuwe medewerker wordt opgeleid.

Aanbeveling
Wij adviseren het proces rondom de opleiding van te medewerkers te beschrijven, vast te stellen, te implementeren en binnen de organisatie te borgen.

2 Noodzakelijkheid, rechtmatigheid en doelbinding (Art 3)

De DSRT valt onder het regime van art. 9, 10 en 13 WPG. De begrippen noodzakelijkheid, rechtmatigheid en doelbinding zijn bekend bij de relevante functionarissen van de DSRT. Wij hebben niet in alle gevallen procesbeschrijvingen aangetroffen die de noodzakelijkheid, rechtmatigheid en doelbinding van de verwerking van politiegegevens waarborgen. De naleving van de WPG is hierdoor niet in alle gevallen gewaarborgd.

Risico
In de procesbeschrijvingen is niet in alle gevallen voldoende aandacht voor de aspecten noodzakelijkheid, rechtmatigheid en doelbinding. Dit veroorzaakt risico's voor de naleving van de WPG.

Risico inschatting: gemiddeld
- De medewerkers zijn bekend met de begrippen noodzakelijkheid, rechtmatigheid en doelbinding.
- Wij hebben in dit verband niet in alle gevallen procesbeschrijvingen aangetroffen;dit veroorzaakt mogelijk mogelijk interpretatieverschillen ten aanzien van de genoemde begrippen.

Aanbevelingen
Wij adviseren de procesbeschrijvingen en werkinstructies nader uit te werken met als doel de noodzakelijkheid, rechtmatigheid en doelbinding van de verwerking van politiegegevens te waarborgen.

3 Juistheid, volledigheid en beveiliging politiegegevens (Art 4)

De DSRT gebruikt informatie afkomstig van derden. De DSRT gaat er van uit dat de aangeleverde informatie volledig, correct en rechtmatig is. Wij hebben niet vastgesteld in hoeverre dit uitgangpunt in alle gevallen juist is. In de procesbeschrijvingen – zowel binnen de DSRT als tussen de DSRT en haar ketenpartners - zijn de aspecten juistheid, volledigheid en beveiliging van politiegegevens niet in alle gevallen voldoende uitgewerkt. De naleving van de WPG is hierdoor in beperkte mate gewaarborgd.

Risico
Het risico bestaat dat de betrouwbaarheid van de gegevens die de DSRT verwerkt -ten aanzien van de aspecten exclusiviteit, integriteit en beschikbaarheid - onvoldoende is gewaarborgd.

Risico inschatting: gemiddeld
- Het is niet bekend of de DSRT er terecht van uitgaat dat alle door derden aangeleverde informatie in alle gevallen juist is.
- Wij hebben de kwaliteit van de beheersmaatregelen in de applicatie VZBS, door het ontbreken van functionele documentatie van VZBS, niet vast kunnen stellen.

- In de procesbeschrijvingen – zowel intern DSRT als tussen de DSRT en haar ketenpartners - is niet in alle gevallen voldoende aandacht geweest voor de betrouwbaarheid van de informatievoorziening.
- De medewerkers van de DSRT hebben een hoog veiligheidsbewustzijn en veel aandacht voor de betrouwbaarheid van informatievoorziening.

Aanbeveling
Wij adviseren, op basis van een risico-analyse, waar nodig aanvullende beheersmaatregelen te treffen in de processen en de applicaties.

4 Autorisatie (Art 6)

Op 9 november 2010 is het autorisatiebeleid voor KLPD door de Korpsleiding vastgesteld. DSRT heeft een autorisatiematrix beschikbaar van geldende autorisaties en rollen. De DSRT past controletechnische functiescheiding toe en heeft maatregelen getroffen om functievermenging te voorkomen. Hiermee voldoet het aspect autorisaties aan de WPG.

Risico
Het inrichten van een autorisatiematrix en voeren van autorisatiebeleid geeft invloed op het kwaliteitsaspect exclusiviteit (uitsluitend de daartoe geautoriseerde medewerkers krijgen toegang tot de gegevens) maar ook op het kwaliteitsaspect integriteit: door het toepassing van functiescheidingen zullen medewerkers elkaar – vanuit een tegengesteld belang rol – controleren.

Risico-inschatting: gemiddeld
- De functies van de medewerkers die de informatie in het systeem gebruiken zijn identiek.
- Het aantal betrokken medewerkers is beperkt.
- De medewerkers hebben een hoog veiligheidsbewustzijn.
- De autorisaties worden door de afdeling geregeld en door het diensthoofd toegekend.
- Tijdelijke medewerkers van binnen en buiten het KLPD krijgen geen toegang tot het systeem.

Aanbevelingen
Wij adviseren de DSRT de autorisatiematrix actueel te houden.

5 Geautomatiseerd vergelijken (Art 11)

De DSRT past geen geautomatiseerde vergelijking toe.

6 In combinatie verwerken (Art 11)

De DSRT kent geen verwerkingen die gecombineerd met andere verwerkingen plaatsvinden.

7 Bewaartermijnen en vernietiging (art. 14)

De DSRT heeft beleid voor het vernietigen van informatie. De vernietiging van informatie wordt uitgevoerd op bevel van de OvJ; de DSRT is geen eigenaar van de informatie. De afgehandelde zaken worden inhoudelijk uit het systeem gewist zodat alleen de kop overblijft om te gebruiken in managementrapportages.
Het OM stuurt niet in alle gevallen tijdig afloopberichten naar de DSRT. Voorzover het OM afloopberichten verstuurt kunnen deze niet in alle gevallen aan de onderzoeksdossiers

worden gekoppeld doordat de gebruikte nummering bij de onderzoeken verschilt van de nummering bij het OM. Handmatige schoning wordt om deze reden slechts fragmentarisch of niet tijdig uitgevoerd. De naleving van de WPG is, ten aanzien van de bewaartermijnen, niet in alle gevallen gewaarborgd.

Risico
Door het niet (kunnen) naleven van vernietigingstermijnen is het mogelijk dat informatie te vroeg of te laat wordt vernietigd.

Risico-inschatting: hoog
- De naleving van de bewaartermijnen uit de WPG is, door de problematiek van de afloopberichten, niet in alle gevallen gewaarborgd.
- De DSRT heeft in dit verband geen mitigerende maatregelen getroffen.

Aanbevelingen
Wij adviseren het proces bewaartermijnen te implementeren en in dit verband nadere afspraken met het OM te maken omtrent de verstrekking van afloopberichten.

8 Gegevens beheer

Alle informatie is digitaal en wordt op het eigen netwerk in een rode omgeving bewaard. Na de ontvangst van een afloopbericht of na bevel van de OVJ wordt de inhoud vernietigd. De afloopberichten van het OM worden niet in alle gevallen tijdig ontvangen of zijn niet in alle gevallen te relateren aan de onderzoeksdossiers. De naleving van de WPG is hierdoor niet in alle gevallen gewaarborgd.

Risico
Door een niet tijdige ontvangst van afloopberichten is het mogelijk dat gegevens mogelijk te vroeg of te laat wordt vernietigd.

Risico-inschatting: gemiddeld
- De naleving van de WPG is, ten aanzien van het gegevensbeheer, niet in alle gevallen gewaarborgd.
- De gegevens worden bewaard in een rode omgeving; de toegang tot de rode omgeving is beperkt tot een daartoe geautoriseerde groep. Dit beperkt de schade Is gevolg van het op dit punt niet naleven van de WPG.

Aanbevelingen
Wij adviseren het proces bewaartermijnen te implementeren en in dit verband nadere afspraken met het OM te maken omtrent de verstrekking van afloopberichten met als doel de betrouwbaarheid van het gegevensbeheer te waarborgen.

9 Ter beschikking stellen van politiegegevens (Art 15)

De door de DSRT opgestelde dossiers blijven altijd binnen het politiedomein. De DSRT stelt de gegevens van de onderzoeken, die zij op verzoek van een opdrachtgever heeft verricht, aan de opdrachtgever beschikbaar door middel van een fysiek dossier, een CD of DVD. De DSRT voldoet hierbij op een goede wijze aan deze wettelijke verplichting van het ter beschikking stellen van politiegegevens aan personen die zijn geautoriseerd voor de verwerking van politiegegevens voor zover zij deze nodig hebben voor de uitvoering van hun

taak. Er is zowel een origineel van het onderzoeksdossier als een werkkopie beschikbaar. Bij de informatie op de CD's/DVD's is geen encryptie toegepast. Beide exemplaren worden gelijktijdig aan de opdrachtgever overhandigd na kwijting. Na overhandiging is de opdrachtgever verantwoordelijk voor de onderzoeksinformatie. De DSRT houdt geen kopie-exemplaren achter.

De CD's/DVD bevatten rode informatie (rubricering geheim). Het betreft informatie (politiegegevens) zoals beelden van heimelijke opnames, afgeluisterde gesprekken en, informatie van bakens die in het kader van een onderzoek zijn verzameld. De werkwijze die de DSRT gebruikt voor het transport van onderzoeksgegevens voldoet aan het BBNP. Wij signaleren echter aanzienlijke risico's die optreden bij het verlies van de gegevens op de CD's/ DVD's na overdracht aan de opdrachtgever. Dit is geen risico voor de DSRT maar wel voor de strafrechtketen. Het verlies van CD's/DVD's kan schade veroorzaken aan onderzoeken doordat onderzoeken beëindigd dienen te worden (waardoor de geïnvesteerde personele capaciteit verloren gaat) en gevaar voor betrokkenen opleveren (politiemedewerkers, verdachten, informanten) indien niet daartoe geautoriseerde personen kennis kunnen nemen van de gegevens uit het onderzoeksdossier. De exclusiviteit van informatievoorziening en daarmee de naleving van de WPG zijn onvoldoende gewaarborgd.

Risico
Het afzien van de toepassing van encryptie voor de informatie op CD of DVD wordt als een groot risico beschouwd tijdens het transport.

Risico-inschatting: hoog
- Hoog politiek risico door schade aan onderzoeken en gevaar voor betrokkenen.

Aanbevelingen
Wij adviseren, bij het branden van de onderzoeksgegevens op CD of DVD, encryptie toe te passen.
Wij adviseren de scope ten aanzien van de eisen die gesteld worden aan de beveiliging van beschikbaargestelde politiegegevens in samenhang uit te breiden tot het gehele politiedomein.

10 Verstrekkingen (Art 16 t/m Art 20)
Binnen de DSRT vindt geen verstrekking van politiegegevens plaats. Uitsluitend de bevoegd functionaris (art. 9/10: bevoegd functionaris buiten de DSRT; art. 13: de bevoegd functionaris van de DSRT/ TGB of WOD i.o.m. de OvJ Landelijk Parket) beslist over de verstrekking van politiegegevens.

11 Rechten van betrokkenen (Art 25 t/m Art 31)
Voor de procesbeschrijving voor de rechten van betrokken steunt DSRT op de beschrijving bij IPOL. Dit aspect is in mindere mate van toepassing omdat DSRT een uitvoerende rol heeft in dit proces. Uit interviews met medewerkers van DSRT is gebleken dat DSRT dergelijke verzoeken tot op heden nog niet heeft ontvangen.

Risico
Bij het niet naleven van dit aspect, wordt de WPG niet nageleefd.

Risico inschatting: laag
- Het is nog niet voorgekomen dat de DSRT dergelijke verzoeken heeft ontvangen
- De privacyfunctionaris zal dergelijke verzoeken in voorkomende gevallen beoordelen en afhandelen.

Aanbeveling
Wij adviseren aandacht te geven aan wijzigingen in de procesbeschrijvingen en de communicatie hiervan.

12 Privacyfunctionaris (Art 34)

Bij de DSRT is een privacyfunctionaris aangesteld; hij is bekend met de taken, verantwoordelijkheden en bevoegdheden van de privacyfunctionaris en is goed bekend met de werkzaamheden van de DSRT.

De privacyfunctionaris vervult een adviserende rol en is daarnaast belast met de feitelijke implementatie van de WPG bij de DSRT.

De privacyfunctionaris krijgt bij de DSRT alle medewerking en kan voldoende aan informatie komen. Hij beschikt echter niet over alle autorisaties die nodig zijn om zelfstandig onderzoek te doen in het kader van zijn toezichthoudende rol in het kader van de naleving van de WPG. De privacyfunctionaris heeft in een interview aangegeven dat hij, gezien het aantal aangemelde zaken (10-50 zaken per dag), te weinig invulling kan geven aan zijn toezichthoudende rol. Daarnaast kan hij in dit verband ook geen gebruik maken van een tool of een systeem om invulling te geven aan die toezichthoudende rol. Deze toezichthoudende rol is een essentieel onderdeel van de taak van de privacyfunctionaris.

Risico
Het toezicht op de naleving van de WPG is hierdoor niet gewaarborgd. De dienst laat de implementatie van de WPG volledig over aan de privacyfunctionaris.

Risico-inschatting: hoog
- De DSRT geeft geen invulling aan de toezichthoudende rol van de privacyfunctionaris. De naleving van de WPG is op dit punt onvoldoende gewaarborgd.
- De feitelijke uitvoering van de implementatie van de WPG is te veel afhankelijk van uitsluitend de privacyfunctionaris.

Aanbevelingen
Wij adviseren de DSRT feitelijk invulling te doen geven aan de toezichthoudende rol van de privacyfunctonaris zodat en de naleving van de WPG op deze wijze beter te waarborgen.

Wij adviseren de implementatie van de WPG bij WPG minder afhankelijk te maken van uitsluitend de privacyfunctionaris.

13 Privacyjaarverslag (Art 34)

De privacyfunctionaris is aangemeld bij de CBP. De privacyfunctionaris van de DSRT heeft over 2010 een jaarverslag opgesteld.

Risico
Bij afwezigheid van een privacyjaarverslag kan KLPD breed moeilijk een inschatting worden gemaakt van de totale inzet en taken van de verschillende privacyfunctionarissen en van de voortgang van de implementatie van de WPG.

Risico-inschatting: laag
- Indien geen geen privacyjaarverslag wordt opgesteld kan niet op eenvoudige wijze worden ingeschat op de dienst op hoofdlijnen "in control" is t.a.v. de WPG.

Aanbeveling
Geen

14 Knelpunten verdere implementatie

- De feitelijke implementatie van de WPG bij de DSRT is te veel afhankelijk van uitsluitend de privacyfunctionaris.
- De privacyfunctionaris kan geen invulling geven aan zijn toezichthoudende rol.
- De DSRT maakt onderdeel uit van de strafrechtketen en is, bij de naleving van de WPG, deels afhankelijk van ketenpartners binnen de strafrechtketen.

15 Reactie van de dienst DSRT

De management reactie van de dienst was op het moment van opstellen van deze rapportage nog niet ontvangen.

Bijlage 8: DNR

1 Inrichting van de organisatie

Inleiding

De dienst Nationale Recherche (DNR) houdt zich bezig met het bestrijden van zware en georganiseerde criminaliteit in binnen en buitenland en werkt daartoe intensief samen met internationale politiediensten. Het bevoegd gezag heeft een aantal aandachtsgebieden benoemd zoals synthetische drugs, heroïne, cocaïne, mensenhandel/mensensmokkel, wapens/explosieve, terreur, witwassen en oorlogsmisdrijven. Hiervoor heeft de DNR expertise in huis en onderhoudt deze expertise. Tevens onderzoekt de dienst strategieën om criminaliteit tegen te houden.

Samenvatting implementatie van de WPG bij DNR

Bij de uitvoering van deze interne WPG-audit bij de dienst DNR, hebben wij ons beperkt tot onderzoek naar de processen CIE, FIET, Tactiek en het MT. Wij hebben uitsluitend onderzoek gedaan naar de opzet van de beheersmaatregelen; het bestaan en de werking van de maatregelen is niet in dit onderzoek betrokken.

Op basis van de bevindingen naar aanleiding van dit onderzoek kunnen wij concluderen dat de DNR, middels de implementatie van de WPG, in opzet voldoet aan de eisen van de WPG met uitzondering van de controle op de naleving van de bewaartermijnen en de invulling van de toezichthoudende rol van de privacyfunctionaris.

	WPG aspect	Bevinding	Risico-inschatting
1.1	Mandaatregeling	+	L
1.2	Procesbeschrijvingen	+	L
1.3	Risicoanalyse	0	M
1.4	Functionele documentatie.	n.v.t.	-
1.5	Aanwijzing Bevoegd functionaris	0	L
1.6	Samenwerkingverbanden	+	L
1.7	Protocollen	0	L
1.8	Opleidingen	+	L
2	Noodzakelijkheid, rechtmatigheid & doelbinding	+	L
3	Juistheid, volledigheid & beveiliging politiegegevens	+	L
4	Autorisatie	0	L
5	Geautomatiseerd vergelijken	0	L
6	In combinatie verwerken	0	L
7	Bewaartermijnen & vernietiging	0	H
8	Gegevensbeheer	0	M
9	Ter beschikking stellen	+	L
10	Verstrekken	+	L
11	Recht van betrokkenen	0	L
12	Privacyfunctionaris	0	H
13	Privacyjaarverslag	+	L

	(voldoet/ - in beperkte mate aan de eisen van de WPG) **Eindconclusie:**	+/0	

Legenda bevindingen:	
+	*voldoet aan de WPG*
o	*voldoet in beperkte mate aan de WPG*
-	*voldoet niet aan de WPG*
n.v.t.	*WPG aspect niet van toepassing*
Legenda risico-inschatting:	
H	*hoog risico; voldoet niet aan de wet; geen risicobeperkende beheersmaatregelen ingericht*
M	*gemiddeld risico ; voldoet niet aan de wet; wel risico beperkende maatregelen ingericht*
L	*laag risico; voldoet aan de wet.*
-	*geen risico WPG aspect is niet van toepassing.*

1.1 Mandaatregeling

Wij hebben, op basis van interviews en bestudering van documentatie, vastgesteld dat de mandaatregeling bij de DNR bekend is en binnen de dienst is geïmplementeerd. De geinterviewden kennen de inhoud van het mandaat. Het MT vindt het van belang dat de mandaatregeling transparant is en dat de checks en balances die betrekking hebben op de implementatie van de WPG zijn ingeregeld. Het MT volgt aandachtig het proces rond de WPG. Het MT maakt het volgende onderscheid: de verantwoordelijkheid voor de implementatie van de WPG ligt bij het MT; de Unit- en Teamleiding is verantwoordelijk voor de feitelijke uitvoering van de WPG. De naleving van de WPG is ten aanzien van dit aspect voldoende gewaarborgd.

Risico

Het risico is aanwezig dat de op basis van de mandaatregeling toegekende bevoegdheden aan aangewezen funcionarissen niet tijdig worden aangepast naar aanleiding van mutaties in de organisatie.

Risico-inschatting: laag

- Door de verantwoordelijken mbt het uitvoeren van de WPG als kennisteam aan te wijzen is het risico beperkt dat door mutaties bij de medewerkers de WPG niet goed wordt uitgevoerd.

Aanbevelingen

Wij adviseren de toekenning van bevoegdheden op basis van de mandaatregeling KLPD-breed actueel te houden.

1.2 Procesbeschrijvingen

De DNR heeft haar processen beschreven; er zijn geen landelijke procesbeschrijvingen van een WPG proof Opsporingsproces. De procesbeschrijvingen van de DNR zijn aangepast aan de WPG en het nieuwe functiehuis. De naleving van de WPG in hierdoor in opzet voldoende gewaarborgd.

Risico
Hoewel de DNR de processen goed beschreven heeft bestaat de kans dat de borging onvoldoende wordt uitgevoerd. Het is van belang dat de beschrijvingen up to date gehouden worden.

Risico-inschatting: laag
- De DNR heeft veel aandacht voor de juiste beschrijving, het actueel houden en het borgen van de processen in de organisatie
- De DNR heeft een intern kwaliteitsbureau; deze toetst permanent in hoeverre de kwaliteitsnormen zijn gehandhaafd en controleert daarbij tevens de procesbeschrijvingen (soll- en ißt situatie).
- Hierbij wordt voortdurend overleg gepleegd met het Landelijke Parket. Onlangs zijn nog diverse processen zoals dossier opbouw en inzet van BOB middelen landelijk als standaard van de DNR vastgesteld. Hierop wordt wekelijks gerapporteerd aan het MT.
- De borging van de strafrechterlijke processen en de WPG processen zijn in de procesbeschrijvingen opgenomen. Hiervan zijn de productbeschrijvingen bekend en deze worden toegepast.

Aanbevelingen
Wij adviseren de procesbeschrijvingen actueel te houden.

1.3 Risico-analyse
De DNR heeft in 2008 een risico-analyse uitgevoerd. Deze analyse is voor het MT aanleiding geweest om maatregelen te nemen en verbeteringen door te voeren. Door de uitvoering van deze risico-analyse wilde men de organisatie enerzijds bewust maken van de risico's rondom de naleving van de WPG en anderzijds de privacyfunctionaris betere in positie brengen.
Er is geen proces ingericht om de maatregelen en de risico's te volgen. Desondanks verwacht de DNR dat de toen uitgesproken risico's onveranderd zijn gebleven. De naleving van de WPG is, ten aanzien van de uitgevoerde risico-analyse, in opzet in beperkte mate gewaarborgd.

Risico
Door het ontbreken van een uitgewerkte actuele risicoanalyse hebben wij niet vast kunnen stellen dat DNR een integraal inzicht heeft in de risico's die gelopen worden in de onderzochte processen. Hierdoor bestaat het risico dat de getroffen beheersmaatregelen de risico's in de processen onvoldoende mitigeren en er, na het nemen van de beheersmaatregelen, alsnog restrisico's blijven bestaan.
De risico's zijn 3 jaar geleden wel inzichtelijk gemaakt; er heeft echter geen evaluatie plaatsgevonden.Het is daardoor niet duidelijk of de geldende risico's nog bestaan en of de getroffen maatregelen efficiënt en effectief zijn geweest.

Risico-inschatting: gemiddeld
- De DNR heeft 3 jaar geleden één risico-analyse uitgevoerd en op basis daarvan maatregelen getroffen. Deze maatregelen zijn echter niet geëvalueerd.

Aanbevelingen
Wij adviseren opnieuw een dienstbrede risicoanalyse uit te laten voeren op basis waarvan samenhangende maatregelen in de administratieve organisatie, interne controle en systemen getroffen kunnen worden. Daarnaast adviseren wij de DNR de effectiviteit en de efficiëntie van de maatregelen te testen en te onderzoeken.

1.4 Functionele documentatie

De DNR maakt gebruik van de reguliere landelijke applicaties en van standaard pakketten zoals Office. De landelijke applicaties worden beheerd door de VtsPN; de standaardprogrammatuur wordt volgens de systematiek van de VtsPN beveiligd. Er is functionele documentatie van de gebruikte systemen. De aanwezigheid van functionele documentatie is geen verplichting vanuit de WPG. Functionele documentatie is indirect echter wel van invloed op de naleving van de WPG aangezien op basis van functionele documentatie beoordeeld kan worden welke beheersmaatregelen zijn getroffen in de applicaties. Deze beheersmaatregelen (bijv. validaties, ingebouwde en geprogrammeerde controles) betreffen o.a. de aspecten juistheid, volledigheid en beveiliging van politiegegevens. E.e.a. is is nader toegelicht in paragraaf 3 van deze rapportage.

1.5 Aanwijzing bevoegd functionaris

De DNR heeft de bevoegd functionarissen (nog) niet formeel aangewezen. In het interview is aangegeven dat de organisatie met een achterstand kampt omdat DPO de besluiten in dit verband nog niet heeft afgewikkeld. Alle unithoofden en teamleiders zijn aangewezen als bevoegd functionaris. Het management onderschrijft dat de DNR met de huidige werkwijze alvast vooruitloopt op de werkwijze die zal worden gevolgd zodra de formele aanwijzing van de bevoegd functionarissen heeft plaatsgevonden. De DNR is tevens van mening dat de "rol" van bevoegd functionaris moet blijven bestaan wanneer een functionaris een andere functie binnen de organisatie accepteert. Deze informele werkwijze is reeds binnen de DNR gecommuniceerd; in de praktijk is het duidelijk wie de bevoegde personen zijn; binnen het proces wordt hier naar gehandeld. Wij constateren dat de DNR, ten aanzien van de formele aanwijzing van bevoegd functionarissen, nog niet volledig voldoet aan de WPG, omdat de medewerkers nog geen functiebeschrijving hebben gekregen waarin hun WPG bevoegdheid formeel is vastgesteld.

Risico
Er is een risico dat de bevoegdfunctionarissen niet tijdig hun aangepaste functiebeschrijving ontvangen en in het strafproces zou kunnen worden gesteld dat de bevoegdfunctionarissen via deze aanstelling niet bevoegd zouden kunnen zijn.

Risico-inschatting: laag
- Informeel wordt wel reeds conform de WPG gewerkt

Aanbevelingen
Wij adviseren de formele aanwijzing van bevoegd functionarissen, in afstemming met DPO alsnog met spoed te doen plaatsvinden.

1.6 Samenwerkingsverbanden (Art 20)

In samenwerkingsverbanden tussen de DNR en ketenpartners is de wet leidend, ook al is er voor deze samenwerking wel een convenant (nadere regelgeving) afgesloten. De wet gaat altijd voor de daaruit volgende regelgeving. In ons onderzoek is niet vastgesteld welke specifieke wrijvingen er zijn tussen de nadere regelgeving en de WPG.
De DNR werkt samen met o.a. het LIEC, Riec en diverse opsporingsdiensten zoals de Belastingdienst. Voor deze samenwerkingsverbanden heeft de DNR convenanten afgesloten en voldoet daarmee aan de WPG.

Risico
Het risico is aanwezig dat de inhoud van samenwerkingsverbanden niet aansluit bij wetgeving (o.a. de WPG). Hierdoor bestaan risico's ten aanzien van de naleving van de WPG. Tevens kunnen nieuwe samenwerkingsverbanden ontstaan waarvoor niet tijdig convenanten worden afgesloten.

Risico-inschatting: laag
- De DNR heeft de WPG in het geval van convenanten hoog op de agenda staan en overlegd in het geval van twijfel met het OM.
- In deze convenanten is met name het WPG aspect bijzonder belicht. Hierdoor is het risico minimaal dat er op het gebied van de WPG procedurefouten worden gemaakt. In het geval van twijfel wordt altijd het OM / OVJ geraadpleegd.

Aanbevelingen
Wij adviseren de ingeslagen weg te continueren en de inhoud van de convenanten periodiek te toetsen aan de wetgeving en – bij het ontstaan van nieuwe samenwerkingsverbanden - de convenanten op volledigheid te beoordelen

1.7 Protocollen

Binnen de DNR wordt de WPG wetgeving gehanteerd via de productbeschrijvingen. Voor zover protocollen nodig zijn, zijn deze uitgewerkt; zij zijn echter nog niet door de dienstleiding van de DNR vastgesteld. Er wordt wel volgens deze protocollen gewerkt.

Risico
Het uitwerken en vaststellen van protocollen is een verplichting vanuit in de WPG. Het niet voldoen aan deze verplichting leidt tot het overtreden van de wet. Daarbij is het noodzakelijk dat de protocollen door de dienstleiding worden vastgesteld.

Risico-inschatting: laag
- De DNR heeft de art.13 protocollen uitgewerkt maar nog niet vastgesteld.
- Er wordt binnen de DNR wel al met de niet vastgestelde protocollen gewerkt.

Aanbevelingen
Wij adviseren de protocollen (art. 13) door het MT te laten vaststellen.

1.8 Opleidingen

De DNR heeft een opleidingsplan uitgewerkt. De deelname aan de WPG-opleiding is door de dienstleiding verplicht gesteld; de dienstleiding heeft hier actief op gestuurd. Dit heeft er toe geleid dat iedere medewerker van de DNR - voorzover hij/zij met de WPG werkt - is opgeleid. Iedere unit van de DNR beschikt over een kernteam van medewerkers die zijn opgeleid door de Politieacademie. Dit kernteam bestaat uit een teamleider, plv. teamleider, dossiervormer en analist. Deze kernteams hebben iedere medewerker van de DNR, voor zover nodig opgeleid. Deze kernteams beantwoorden in de voorkomende gevallen vragen van medewerkers. Ook worden vragen door de privacyfunctionaris afgehandeld. De naleving van de WPG is ten aanzien van het aspect opleidingen in opzet voldoende gewaarborgd.

Risico

Bij het ontbreken van een opleidingsplan is niet gewaarborgd dat alle medewerkers die met de WPG werken zijn opgeleid.

Risico-inschatting: laag

- De DNR heeft een opleidingsplan uitgewerkt, volledig uitgevoerd en in de organisatie geborgd, door het instellen van kennisteams. De dienstleiding stuurt actief op de deelname aan de WPG opleiding.

Aanbevelingen

Wij adviseren de voorgenomen uitvoering van de productbeschrijvingen op het gebied van het "verbeteren" het opleidingsplan periodiek te monitoren en te evalueren.

2 Noodzakelijkheid, rechtmatigheid en doelbinding (Art 3)

De begrippen noodzakelijkheid, rechtmatigheid en doelbinding zijn bekend. Er is een vaste dossieropbouw conform de landelijke standaard. Voor de Criminele Inlichtingen Eenheid (CIE) is dit minder van toepassing aangezien de CIE met "zachte" informatie werkt en het op dat moment nog niet bekend is of deze informatie noodzakelijk is en voor welk doel deze informatie kan worden gebruikt. Het opslaan van deze informatie geschiedt conform een rood NSIS account en het landelijke autorisatie model.

Alle art 9 onderzoeken worden bij de privacyfunctionaris gemeld; het proces is beschreven. De DNR heeft de processen goed beschreven en daarbij aandacht gehad voor de aspecten noodzakelijkheid, rechtmatigheid en doelbinding. Het is van belang dat de beschrijvingen actueel worden gehouden. De naleving van de WPG is ten aanzien van de aspecten noodzakelijkheid, rechtmatigheid en doelbinding, in opzet voldoende gewaarborgd.

Risico-inschatting: laag

- De DNR heeft veel aandacht voor de juiste beschrijving, het actueel houden en het borgen van de processen in de organisatie
- De DNR heeft een intern kwaliteitsbureau; dit toetst in hoeverre de kwaliteitsnormen zijn gehandhaafd en controleert daarbij tevens de procesbeschrijvingen (soll- en iβt situatie).

Aanbevelingen
Wij adviseren de procesbeschrijvingen actueel te houden.

3 Juistheid, volledigheid en beveiliging politiegegevens (Art 4)

Het kwaliteitsbureau verzorgt de schoning van informatie om te garanderen dat informatie juist en volledig wordt verzameld, vastgelegd en verwerkt. Indien bij controle blijkt dat de informatie niet volledig is - bijvoorbeeld de geboortedatum - wordt deze alsnog toegevoegd. Bij "zachte" informatie is niet vast te stellen of de informatie juist en volledig is aangezien het in dit geval hier juist over informatie gaat die nog verder onderzocht dient te worden. Alle informatie wordt kritisch bekeken en steeds verder veredeld. De informatie wordt, na goedkeuring door de teamleider,als art 10 informatie opgenomen in BVO (Basisvoorziening Opsporing Bruto).

De volledigheid en juistheid van de informatie is gewaarborgd doordat verschillende bronnen worden onderzocht. Bij de afdeling tactiek is dit nog niet geregeld. De verstrekte informatie is getoetst door het OM en in een projectvoorstel / proces verbaal aan het tactisch team ter beschikking gesteld. Dit aspect, juistheid, volledigheid en beveiliging politiegegevens voldoet aan de WPG.
De DNR heeft de processen goed beschreven en daarbij aandacht gehad voor de aspecten juistheid, volledigheid en beveiliging. Het is van belang dat de beschrijvingen actueel worden gehouden. De naleving van de WPG is ten aanzien van de aspecten juistheid, volledigheid en beveiliging, in opzet voldoende gewaarborgd.

Risico-inschatting: laag

- De DNR heeft veel aandacht voor de juiste beschrijving, het actueel houden en het borgen van de processen in de organisatie
- De DNR heeft een intern kwaliteitsbureau; dit toetst in hoeverre de kwaliteitsnormen zijn gehandhaafd en controleert daarbij tevens de procesbeschrijvingen (soll- en ißt situatie).

Aanbevelingen
Wij adviseren de procesbeschrijvingen actueel te houden.

4 Autorisatie (Art 6)

De DNR maakt, voor de registratie van opsporingsinformatie, gebruik van BVO. Voor de toekenning van de autorisaties in BVO maakt de DNR gebruik van het landelijke model BVO 2007. In dit model is onderscheid gemaakt naar verschillende rollen en functies waarbij taken en autorisaties elkaar volgen. Per onderzoek wordt vastgesteld welke medewerkers geautoriseerd dienen te worden en welke autorisaties zij – op basis van het landelijke model BVO - dienen te krijgen.

Bij de DNR komen superregistraties voor. De afdeling CIE moet bijvoorbeeld, vanuit haar taak, over alle onderzoeken kunnen kijken. Het is, met behulp van deze superregistraties, alleen mogelijk om de informatie te zien; het bewerken of verwijderen van informatie is niet mogelijk. Het diensthoofd kent de autorisaties toe; functioneel beheer is belast met de uitvoering. De toegekende autorisaties worden periodiek gecontroleerd. Nieuwe medewerkers worden conform hun rol geautoriseerd. Wij hebben geen beleid aangetroffen ten aanzien van het intrekken van bevoegdheden van niet actieve gebruikers in BVO.

Het autorisatiemodel is ingericht om gestandaardiseerde werkprocessen te implementeren en tevens de informatiehuishouding van de opsporingsprocessen op een hoger peil te brengen uitgaande van het besef dat het delen van opsporingsinformatie noodzakelijk is om de opsporing effectiever en efficiënter te laten verlopen.

Het huidige autorisatiemodel kent de volgende beperkingen:
- Het autorisatiemodel is niet WPG proof
- Het autorisatiemodel sluit niet goed aan op de functies van het KLPD aangezien de regionale functiebeschrijvingen als uitgangspunt zijn genomen en het model in opzet onvoldoende voorziet in de eisen die daar, vanuit de specialistische processen van het KLPD, aan worden gesteld
- Het autorisatiemodel maakt onderscheid tussen 4 categorieën opsporingsgegevens. Deze classificatie dient als uitgangspunt te worden genomen voor de toekenning van autorisaties en het delen van opsporingsinformatie. In de praktijk blijken deze categorieën niet te voldoen omdat bij het classificeren van opsporingsinformatie diverse interpretaties mogelijk zijn.

Dit vormde de aanleiding voor het uitwerken van:
- Nationaal Intelligence Model (2008): in dit model zijn de niveaus van sturing op (veiligheids)informatie beschreven. In dit model is de classificatie van opsporingsinformatie nader uitgewerkt;
- het "Autorisatiemodel Uitvoeren Opsporing en Intelligence" (concept; maart 2010): dit model voldoet in opzet aan de eisen die daar, vanuit de WPG, het Nationaal Intelligence Model (NIM) en de werkprocessen van het KLPD aan worden gesteld. Het model ligt vanaf 2010 ter goedkeuring bij de RKC board opsporing maar is tot op heden nog niet vastgesteld.

Verder maakt de DNR gebruik van registratie op de G/: schijf beveiligd. Voor het beheer van de mappenstructuur op de G/:schijf beveiligd ontbreekt nog KLPD breed beleid. BVO maakt gebruik van een aantal andere applicaties

Wij komen tot de conclusie dat de naleving van de WPG bij de DNR, ten aanzien van het aspect autorisaties, een beperkte mate is gewaarborgd.

Risico
Er is een risico dat de toekenning van bevoegdheden in BVO aan medewerkers, door de beperkingen van het huidige autorisatiemodel, in opzet en bestaan niet voldoet aan de eisen die daar op grond van de functie, rol en competenties aan worden gesteld. Bij te ruime bevoegdheden is de exclusiviteit van de informatievoorziening onvoldoende gewaarborgd en wordt de onderzoeksinformatie met teveel medewerkers gedeeld; bij te beperkte bevoegdheden bestaat het risico dat de medewerker zijn functie niet op de juiste wijze kan vervullen omdat onderzoeksinformatie niet met betreffende medewerker wordt gedeeld.

Risico-inschatting: laag
De DNR gaat - ondanks de beperkingen van het huidige model – op een uiterst zorgvuldige wijze om met de toekenning van autorisaties. De DNR hanteert hiertoe intern beleid

vooruitlopend op vaststelling van het "Autorisatiemodel Uitvoeren Opsporing en Intelligence"autorisatiemodel.

Aanbevelingen
Wij adviseren
- het "Autorisatiemodel Uitvoeren Opsporing en Intelligence te doen vaststellen, implementeren en binnen de organisatie te borgen;
- de criteria voor de toekenning van superregistraties nader te doen uitwerken en implementeren binnen de organisatie.

5 Geautomatiseerd vergelijken (Art 11)

Wij hebben, op basis van interviews, vastgesteld dat de afdeling FIET van de DNR geautomatiseerde vergelijking toepast. De andere afdelingen van de DNR hebben niet te maken met geautomatiseerd vergelijken. De verdere verwerking van de verkregen informatie voor het onderzoek vindt plaats in overleg met de bevoegd functionaris. Wij hebben geen procesbeschrijving inzake het geautomatiseerd vergelijken aangetroffen. De naleving van de WPG is ten aanzien van dit aspect in beperkte mate gewaarborgd.

Risico
Door het ontbreken van procesbeschrijvingen bestaat het risico dat niet de juiste process wordt gevolgd; dit kan risico's met zich meebrengen voor de naleving van de WPG.

Risico-inschatting: laag
- uitsluitend de afdeling FIET heeft te maken met geautomatiseerd vergelijken
- de medewerker van deze afdeling zijn goed opgeleid en hebben een hoog veiligheidsbewustzijn

Aanbevelingen
Wij adviseren het proces geautomatiseerd vergelijken uit te werken, vast te stellen, te implementeren en binnen de organisatie te borgen.

6 In combinatie verwerken (Art 11)

O.a. de afdeling CIE verwerkt in combinatie op basis van hit/no hit in opdracht van de OvJ en het bevoegd gezag. Het betreft 'zachte' informatie waarvoor onvolledige sleutels uit diverse bronnen wordt gebruikt. Het is een gevoelig proces aangezien personen, op basis van het gebruik van deze onvolledige sleutel, ten onrechte als verdacht kunnen worden aangemerkt. De gecombineerde informatie wordt tot één document gemaakt te behoeve van art 9 en art 10 verwerkingen. Wij hebben geen beschrijving van dit proces aangetroffen. De naleving van de WPG is ten aanzien van het aspect in combinatie verwerken in beperkte mate gewaarborgd.

Risico
Het risico is aanwezig dat het bevoegd gezag geen toestemming heeft verleend voor het in combinatie verwerken of dat het bevoegd gezag wel toestemming heeft verleend voor het in combinatie verwerken en maar dat dit niet kan worden aangetoond. In beide gevallen kunnen daardoor onderzoeken onderuit worden gehaald door de uit deze verwerking verkregen informatie op onrechtmatige wijze is verkegen en daardoor niet in

Risico-inschatting: laag
De OvJ zal in de praktijk reeds bij het onderzoek betrokken zijn en in de praktijk zijn toestemming hebben verleend voor het in combinatie verwerken.

Aanbevelingen
Wij adviseren het proces in combinatie verwerken uit te werken, vast te stellen, te implementeren en binnen de organisatie te borgen.

7 Bewaartermijnen en vernietiging (art. 14)

Teamleiders krijgen niet automatisch bericht van een hoger beroep. Er zijn evenmin maatregelen getroffen voor het volgen van zaken die onder de rechter zijn. Dit kan gevolgen voor de naleving van de bewaartermijnen.

De dienst heeft niet in alle gevallen zicht op de naleving van de bewaartermijnen. Dit speelt in het bijzonder bij rest- en zijtakinformatie. De bewaartermijnen worden - waar mogelijk - door de privacyfunctionaris gemonitord. Bij afsluiting van een onderzoek wordt een formulier "MRO sluiten" verstuurd naar functioneel beheer met het verzoek het betreffende onderzoek te sluiten. Het formulier bevat ook de namen van de onderzoekers die toegang hebben tot het onderzoek. De melding wordt ook gemaakt aan de privacyfunctionaris.

Teamleiders zijn bewaarders; het gevaar is aanwezig dat informatie niet tijdig wordt geschoond met name indien men zich te veel laat leiden door persoonlijke opvattingen. Het is van belang te zoeken naar themawaardige onderwerpen (onderwerpen die in één van de DNR thema's past) en strikt rechtmatig conform de WPG te werken. Er wordt daarbij specifieke aandacht gevraagd voor de rest- en zijtak informatie die voor het sluiten van het onderzoek opgewaardeerd dient te worden om aan vernietiging te ontkomen. Deze informatie wordt, vanuit het onderzoek, naar (art 10) overgeheveld.

De informatie verkregen uit BOB middelen in onderzoeken mag, op grond van artikel 1.26, rechtmatig gebruikt worden in andere onderzoeken. De DNR heeft het proces bewaartermijnen en vernietiging beschreven. De controle op de naleving van de bewaartermijnen, het plaatsen achter een schot en de tijdige vernietiging vindt op ad-hoc basis plaats en is onvoldoende in het proces geborgd. De naleving van de WPG is, ten aanzien van het aspect bewaartermijnen, in beperkte mate gewaarborgd. DNR ziet in deze de voordelen van SUMM-IT voor het beheer en de opschoning van informatie.

Risico
De DNR heeft niet in alle gevallen zicht op de naleving van de bewaartermijnen. De informatie kan na afronding van een zaak te lang bewaard worden. De controle op de bewaartermijnen en feitelijke vernietitging van informatie vinden op ad-hoc basis plaats. Het risico is aanwezig dat de feitelijke vernietiging niet in alle gevallen tijdig plaatsvindt. De naleving van de bewaartermijnen is op deze wijze niet in alle gevallen gewaarborgd.

Risico-inschatting: hoog
- het bewaken van de bewaartermijnen wordt op ad-hoc basis bijgehouden door de privacyfunctionaris
- de privacyfunctionaris is niet in de gelegenheid om voldoende invulling te geven aan de toezichthoudende rol

- onvoldoende kennis van BOB wetgeving in huis (zie samenvatting einde rapportage)

Aanbevelingen
Wij adviseren het proces bewaartermijnen te beschrijven, vast te stellen, te implementeren en binnen de organisatie te borgen. Tevens adviseren wij gebruik te maken van een systeem om dit proces te ondersteunen. De DNR wil daartoe het systeem SUMM-IT implementeren.

8 Gegevensbeheer

De dossiers en andere informatie worden in een kluis bewaard. De toegang tot de informatie is beperkt tot een selecte groep van medewerkers. De naleving van de WPG is ten aanzien van het aspect gegevensbeheer in beperkte mate gewaarborgd.

Risico
Er bestaat een risico van onjuist gegevensbeheer omdat er onvoldoende zicht is op het beheer van dossiers e.d. Wij hebben gedurende de audit niet kunnen vaststellen of er rond gegevensbeheer een sluitende administratie wordt bijgehouden.

Risico-inschatting: gemiddeld
- Er heerst een groot veiligheidsbewustzijn binnen de DNR.
- De groep met toegang tot de gegevens is beperkt tot een selecte groep van medewerkers.

Aanbevelingen
Wij adviseren de procedure rondom de opslag van dossiers in de kluis te beschrijven,vast te stellen, te implementeren en in de organisatie te borgen.

9 Ter beschikking stellen van politiegegevens (Art 15)

De CIE geeft gevraagd en ongevraagd advies. Dit wordt in een proces verbaal door de bevoegd functionaris vastgelegd. Het delen van informatie loopt altijd via de OvJ. Er is een kentering van "delen als" naar "delen tenzij".

Informatie dient, op basis van EU regelgeving, soms gedeeld te worden met buitenlandse korpsen. Hiervoor wordt gebruik gemaakt van de applicatie EIS; het betreft een applicatie van IPOL. De DNR ervaart het uitsluitend baseren op de informatie vanuit EIS als een risico aangezien EIS zich baseert op de EU regelgeving. De WPG en EU regelgeving zijn echter niet eenduidig en niet op elkaar afgestemd. De DNR beschouwt dit als een risico voor de naleving van de WPG. Bij de verwerking van politiegegevens zal de DNR zich, om die reden niet uitsluitend baseren op de informatie uit EIS de politiegegevens altijd op basis van de WPG verwerken.
Wij hebben een procesbeschrijving aangetroffen inzake het ter beschikking stellen van gegevens.

De naleving van de WPG is, ten aanzien van het aspect ter beschikking stellen van politiegegevens voldoende gewaarborgd ondanks het ontbreken van eenduidigheid tussen WPG en EU regelgeving

Risico
De WPG en de EU wet- en regelgeving zijn niet eenduidig en niet op elkaar afgestemd. De beschikbaarstelling van politiegegevens aan buitenlandse politiekorpsen in EU verband dient van geval tot geval beoordeeld te worden. Het risico is aanwezig dat gegevens op basis van EU regelgeving terecht beschikbaar worden gesteld terwijl dit niet voldoet aan de WPG.

Risico-inschatting: laag
De DNR is onderkent dit risico en zal zich, bij de verwerking van politiegegevens, om die reden niet uitsluitend baseren op de informatie uit EIS (dat uitgaat van de EU regelgeving) maar de politiegegevens altijd op basis van de WPG verwerken.

Aanbevelingen
Wij adviseren via de daartoe geëigende kanalen aan te dringen op harmonisatie van de WPG en EU wet- en regelgeving.

10 Verstrekkingen (Art 16 t/m Art 20)

De DNR verstrekt - via het OM – gegevens aan advocaten, gemeenten (op basis van de Wet BIBOB), sociale dienst of rechtsreeks via de OvJ. De Bevoegd Functionaris toetst de aanvraag. Wij hebben een beschrijving van het proces verstrekken aangetroffen. De naleving van de WPG is, ten aanzien van het aspect verstrekkingen, voldoende gewaarborgd.

Risico
Het risico is aanwezig dat werkprocessen worden aangepast en procesbeschrijvingen niet tijdig worden geactualiseerd. Het is in dat geval mogelijk dat gegevens hierdoor ten onrechte worden verstrekt.

Risico-inschatting: laag
- De DNR heeft veel aandacht voor de juiste beschrijving, het actueel houden en het borgen van de processen in de organisatie
- De DNR heeft een intern kwaliteitsbureau; dit toetst in hoeverre de kwaliteitsnormen zijn gehandhaafd en controleert daarbij tevens de procesbeschrijvingen (soll- en ißt situatie).

Aanbevelingen
Wij adviseren de procesbeschrijvingen ten aanzien van dit aspect actueel te houden.

11 Rechten van betrokkenen (Art 25 t/m Art 31)

Het kan voorkomen dat een betrokkenen inzage wil in eigen politiegegevens. Het hoofd CIE maakt in overleg met de OvJ een afweging om hieraan gehoor te geven. In gevallen waarin dit niet duidelijk is wordt de betrokkenen doorverwezen naar de privacyfunctionaris. Dit staat echter niet beschreven. De naleving van de WPG is, ten aanzien van de rechten van betrokkenen, in beperkte mate gewaarborgd.

Risico's
Wij hebben geen procedure voor het omgaan van het rechten van betrokkenen aangetroffen. Het risico bestaat dat de WPG op dit punt niet wordt nageleefd. Inzageverzoeken komen echter niet of nauwelijks voor.

Risico-inschatting: laag
- De naleving van de WPG is, ten aanzien van de rechten van betrokkenen op inzage, mutatie of vernietiging van dossiers, niet door middel van een procedure gewaarborgd.
- In voorkomende gevallen zal echter de privacyfunctionaris worden ingeschakeld.

Aanbevelingen
Wij adviseren om in dit verband korpsbreed een procedure te ontwikkelen, vast te stellen, te implemteren en binnen de organisatie te borgen.

12 Privacyfunctionaris (Art 34)

Bij de DNR is een privacyfunctionaris aangesteld. De privacyfunctionaris is goed inhoudelijk op de hoogte van de taken, verantwoordelijkheden en bevoegdheden en van de werkzaamheden binnen de DNR.

Uit een interview is gebleken dat de privacyfunctionaris, door gebrek aan capaciteit, in het geheel niet toe komt aan de toezichthoudende rol die zij in het kader van de WPG dient te vervullen. De privacyfunctionaris richt zich in eerste instantie op het verder implementeren van de WPG bij de DNR. De naleving van de WPG is hierdoor uitsluitend afhankelijk van de beheersmaatregelen in het proces; er is geen extra waarborg voor naleving van de WPG in de vorm van toezicht door de privacyfunctionaris.

De privacyfunctionaris is momenteel niet geautoriseerd voor alle systemen waar de registratie van politiegegevens plaatsvindt. Dit is volgens de privacyfunctionaris niet gebaseerd op bewust beleid, maar wordt veroorzaakt doordat het haar aan tijd ontbreekt om zelf onderzoek te doen in de systemen. Bij de DNR worden alle art 9 verwerkingen en alle toekenningen van autorisaties aan de privacyfunctionaris gemeld.

De naleving van de WPG is, ten aanzien van de aanwijzing van een privacyfunctionaris, in beperkte mate gewaarborgd aangezien de privacyfunctionaris een belangrijk onderdeel van de taak van de privacyfunctionaris - het toezicht op de naleving van de WPG - niet uitvoert.

Risico's
Doordat de privacyfunctionaris de toezichthoudende rol momenteel niet vervult loopt DNR risico's ten aanzien van de naleving van de WPG. Hierbij wordt in beperkte mate voldaan aan de wettelijke verplichting vanuit de WPG een privacyfunctionaris toe te wijzen.

Risico-inschatting: hoog
- De privacyfunctionaris is zich bewust van de toezichthoudende rol binnen de WPG.

Aanbevelingen
Wij adviseren de privacyfunctionaris in staat te (doen) stellen de toezichthoudende rol in het kader van de naleving van de WPG te vervullen.

13 Privacyjaarverslag (Art 34)

De privacyfunctionaris DNR is aangemeld bij de CBP. De privacyfunctionaris heeft over 2010 een kort jaarverslag opgesteld. Hiermee heeft de privacyfunctionaris voldaan aan de WPG.

Risico
Door de afwezigheid van een privacyjaarverslag kan moeilijk een inschatting worden gemaakt van de totale inzet en taken van de privacyfunctionaris en van de voortgang van de implementatie van de WPG.

Risico-inschatting: laag
- Indien geen privacyjaarverslag wordt opgesteld kan niet op een eenvoudige wijze worden ingeschat of de dienst op hoofdlijnen "in control" is t.a.v. de WPG.

Aanbevelingen
Geen aanbevelingen

14 Knelpunten verdere implementatie

Door de DNR is een aantal punten genoemd die mogelijk als knelpunt kunnen worden aangerekend bij de verder implementatie van de WPG:
- Regels en protocollen zijn nodig maar het moet wel werkbaar blijven. De creativiteit moet we niet dood slaan. Meer kijken naar wat kan dan naar wat niet kan.
- Er is onvoldoende kennis van BOB wetgeving.
- Beter gebruik maken van wat de WPG bied op het gebied van rest- en zijtak informatie. Er bestaat de veronderstelling dat informatie na 5 jaar zomaar verdwijnt (opschoning).
- Het beheer is in het algemeen omvangrijk. Het genereert veel formulieren en het proces is bureaucratisch. De eis is dat het proces controleerbaar en beheersbaar is.
- De afloopberichten komen niet of nauwelijks door bij de DNR. Het eerste vonnis gaat nog wel goed, maar bij hoger beroep is de volledigheid en juistheid van de ontvangst van afloopberichten onvoldoende gewaarborgd.
- Het is voor medewerkers van de DNR onverteerbaar dat (misschien) belangrijke informatie uit onderzoeken na een aantal jaren wordt vernietigd. Het langer bewaren van deze informatie zou wenselijk kunnen zijn.

15 Reactie van de dienst DNR

Door de DNR is de volgende reactie op de audit ingebracht:

Aanbevelingen
Wij adviseren opnieuw een dienstbrede risicoanalyse uit te laten voeren op basis waarvan samenhangende maatregelen in de administratieve organisatie, interne controle en systemen getroffen kunnen worden. Daarnaast adviseren wij de DNR de effectiviteit en de efficiëntie van de maatregelen te testen en te onderzoeken.

DNR: Door deze voortdurende interne audits worden de processen getoetst en actueel gehouden. Via de mailfunctie en de kwaliteitskringen worden de medewerkers voortdurend op de hoogte gehouden van wettelijke en proces veranderingen

Bij de DNR is een permanente risico analyse aanwezig per onderdeel van de uitgevoerde werkzaamheden.
De risico's worden permanent inzichtelijk gemaakt. De afgelopen drie jaar zijn er vier DNR brede risico's analyses gemaakt. De adviezen zijn door het MT uitgevoerd.
Via het kwaliteitsbureau zullen de processen voortdurend worden gemonitoord en door het MT maatregelen getroffen worden om de risico's te beperken dan wel uit te sluiten.

- De DNR heeft in de afgelopen 3 jaar 4 risico-analyses uitgevoerd en op basis daarvan maatregelen getroffen. Deze maatregelen zijn geëvalueerd en maatregelen getroffen.

Ad 1.5
Aanbevelingen
Wij adviseren de formele aanwijzing van bevoegd functionarissen, in afstemming met DPO alsnog met spoed te doen plaatsvinden.

DNR: In de maand december 2012 hebben de BF functionarissen hun nieuwe functiebechrijving ontvangen .

De reactie van de DNR is nog niet compleet

Bijlage 9: IPOL

1 Inrichting van de organisatie

Inleiding

De dienst IPOL is het knooppunt voor de uitwisseling van informatie tussen de politie in binnen- en buitenland. Bij IPOL wordt informatie verzameld, geanalyseerd, veredeld en verspreid met als doel het inzicht in de nationale en internationale veiligheidssituatie te verbeteren. Jaarlijks maakt de dienst een aantal Criminaliteitsbeeldanalyses teneinde aandachtsgebieden voor politie, politiek en veiligheidsdiensten zichtbaar te maken.

Samenvatting implementatie van de WPG bij IPOL

Bij de uitvoering van deze interne WPG-audit bij de dienst IPOL, hebben wij ons beperkt tot onderzoek naar de processen Vertalingen en Publiceren, Kenmerken en Opsporingsberichten. Wij hebben onderzoek gedaan naar de opzet van de beheersmaatregelen; het bestaan en de werking van de maatregelen is niet in dit onderzoek betrokken.

Op basis van de bevindingen naar aanleiding van dit onderzoek concluderen wij dat IPOL, voor wat betreft de processen Vertalingen en Publiceren, Kenmerken en Opsporingsberichten in opzet in beperkte mate voldoet aan de eisen van de WPG.

	WPG aspect	Bevinding	Risico-inschatting
1.1	Mandaatregeling	+	H
1.2	Procesbeschrijvingen	+	M
1.3	Risico-analyse	0	H
1.4	Functionele documentatie	n.v.t.	-
1.5	Aanwijzing Bevoegd functionaris	0	L
1.6	Samenwerkingverbanden	n.v.t.	-
1.7	Protocollen	0	H
1.8	Opleidingen	0	L
2	Noodzakelijkheid, rechtmatigheid & doelbinding	0	M
3	Juistheid, volledigheid & beveiliging politiegegevens	0	L
4	Autorisatie	0	M
5	Geautomatiseerd vergelijken	n.v.t.	-
6	In combinatie verwerken	n.v.t.	-
7	Bewaartermijnen & vernietiging	0	M
8	Gegevensbeheer	0	H
9	Ter beschikking stellen	n.v.t.	-
10	Verstrekken	n.v.t.	-
11	Recht van betrokkenen	n.v.t.	-
12	Privacyfunctionaris	-	H
13	Privacyjaarverslag	+	L
	(voldoet in beperkte mate aan de eisen van de WPG) **Eindconclusie:**	**0**	

Legenda bevindingen:	
+	voldoet aan de WPG
o	voldoet in beperkte mate aan de WPG
-	voldoet niet aan de WPG
n.v.t.	WPG aspect niet van toepassing
Legenda risico-inschatting:	
H	hoog risico; voldoet niet aan de wet; geen risicobeperkende beheersmaatregelen ingericht
M	gemiddeld risico ; voldoet niet aan de wet; wel risico beperkende maatregelen ingericht
L	laag risico; voldoet aan de wet.
-	geen risico WPG aspect is niet van toepassing.

1.1 Mandaatregeling

De mandaatregeling is bekend en binnen de dienst geïmplementeerd. De privacyfunctionaris kan de globale inhoud van het mandaat aangeven. Er is geen overzicht van alle verwerkingen; beide processen werken sterk productgericht. Hierbij heeft het proces Vertalingen zicht op alle vertalingen; het proces Publiceren, Kenmerken en Opsporingsberichten heeft zicht op de onderwerpen uit het AVRO (publieke omroep) programma "Opsporing verzocht". Eveneens zijn er contracten met SBS6 (commerciele omroep) voor het aanleveren van materiaal voor programma's. Er is een organisatieschema van de dienst en de units aanwezig. De diensthoofden zijn verantwoordelijk voor het uitvoeren van de WPG.

IPOL maakt onderdeel uit van de strafrechtketen; hierbij wordt veel in opdracht van ketenpartners gewerkt (zoals andere diensten van het KLPD, het OM, de regiokorpsen) die al dan niet behoren tot het politiedomein. In interviews is aangegeven dat de dienstleiding van IPOL onvoldoende aandacht heeft voor de WPG. Op basis van interviews, hebben wij vastgesteld dat de WPG op het niveau van de unitleiding wel onder de aandacht is. Het kwaliteitsbureau levert periodiek voortgangsrapportages op aan de dienstleiding en heeft hier regelmatig overleg over. De verdere implementatie van de WPG is belegd bij de privacyfunctionaris.
De opzet van de mandaatregeling voldoet in opzet aan de WPG.

Risico
Indien de WPG niet op de agenda van de leiding van IPOL staat is de naleving en de verdere implementatie van de WPG bij IPOL onvoldoende gewaarborgd.

Risico-inschatting: hoog
- Het niet voldoen aan de eisen gesteld in de wet leidt tot een hoge risico inschatting.

Aanbeveling
Wij adviseren de (verdere) implementatie van de WPG op te nemen in de beheersdoelstelllingen van de managementcyclus van IPOL.

1.2 Procesbeschrijvingen
IPOL heeft haar processen Vertalingen en Publiceren, Kenmerken en Opsporingsberichten beschreven op basis van de RBP-methode. Tijdens de interviews was het bestaan van de

procesbeschrijvingen niet bekend bij de audittees. Wij hebben niet vastgesteld dat de IPOL processen in de strafrechtketen deel uitmaken van deze beschrijving. De opzet voldoet aan de WPG, deze opzet is echter onvoldoende bekend op de werkvloer.

Risico
Het niet bekend zijn van procesbeschrijvingen vormt een risico aangezien daardoor de mogelijkheid bestaat dat iedere medewerker het proces op een eigen manier invult.

Risico-inschatting: midden
- Bij de onderzochte processen wordt slechts in beperkte mate met politiegegevens gewerkt.

Aanbeveling
Wij adviseren de procesbeschrijvingen te implementeren, in de organisatie te borgen en daarbij aan te sluiten op de processen in de strafrechtketen.

1.3 Risico-analyse
Wij hebben, bij de uitvoering van ons onderzoek van de processen Vertalingen en Publiceren, Kenmerken en Opsporingsberichten bij de dienst IPOL, geen risico-analyse aangetroffen waarbij de WPG als uitgangspunt is genomen.. Daarnaast hebben wij wel beheersmaatregelen aangetroffen; deze zijn echter niet gebaseerd op een risico-analyse maar op basis van inschattingen van de verantwoordelijke functionarissen in de processen. De opzet van dit aspect voldoet in beperkte mate aan de WPG.

Risico
Het mogellijkheid bestaat dat er onvoldoende zicht is op de aanwezige risico's en op de getroffen maatregelen om deze risico's te mitigeren. Hierdoor kan onvoldoende gestuurd worden op het terugdringen van deze risico's. De beheersmaatregelen zijn uitsluitend getroffen op basis van een inschatting van de risico's door de verantwoordelijke functionarissen; zij maken echter geen deel uit van een integrale risico-analyse.

Risico-inschatting: hoog
- In de onderzochte processen zijn beheersmaatregelen ingericht. Deze zijn echter niet gebaseerd op een risico-analyse, maar totstandgekomen op basis van de inschattingen van de verantwoordelijke functionarissen in de processen. Voorbeelden zijn o.a. het afsluiten van convenanten en de screening van externe medewerkers als onderdeel van het aanbestedingsproces. Wij hebben niet vast kunnen stellen dat alle risico's in de processen voldoende zijn afgedekt.

Aanbevelingen
Wij adviseren een dienstbrede risico-analyse uit te doen (laten) uitvoeren op basis waarvan samenhangende maatregelen in de administratieve organisatie en in de systemen getroffen kunnen worden. Op deze wijze kunnen de risico's in de processen tot een aanvaardbaar niveau worden gemitigeerd.

1.4 Functionele documentatie

Functionele documentatie bevat een beschrijving van de beheersmaatregelen in een applicatie. IPOL beschikt niet over een applicatie ten behoeve van de registratie rondom de primaire processen maar maakt voor dit doel uitsluitend gebruik van een standaard Officepakket; dit is beveiligd volgens de systematiek van de VtsPN. Office is primair geschikt voor single-user toepassingen en voorziet niet standaard in aanvullende beheersmaatregelen om de betrouwbaarheid van de informatievoorziening bij multi-user toepassing voldoende te waarborgen. Hierbij kan gedacht worden aan beheersmaatregelen zoals validaties, ingebouwde en geprogrammeerde controles; deze betreffen o.a. de aspecten juistheid, volledigheid en beveiliging van politiegegevens. De betrouwbaarheid van de informatievoorziening rondom de primaire processen is, door de afhankelijkheid van Office toepassingen, in opzet onvoldoende gewaarborgd.

In de onderzochte processen Vertalingen en Publiceren, Kenmerken en Opsporingsberichten zijn de volgende risicobeperkende maatregelen aanwezig:

- een beperkte groep van medewerkers heeft toegang tot de bestanden op de G:/schijf beveiligd;
- de toegang tot de fysieke dossiers is beperkt tot een specifieke groep van medewerkers;
- wij hebben niet vastgesteld dat er, t.a.v. de toegang tot de fysieke dossiers, een sleutelprocedure wordt gehanteerd;
- IPOL hanteert voor de toegangsbeveiliging het principe van compartimentering: d.w.z. voor de toegang tot de afdelingen zijn de autorisaties van de medewerkers als uitgangspunt genomen;
- de medewerkers van IPOL hebben een hoog veiligheidsbewustzijn.

Hoewel bovenstaande bevinding geen directe invloed heeft op het oordeel over WPG, adviseren wij toch op basis van een risico-analyse, aanvullende beheersmaatregelen in de processen te treffen om de betrouwbaarheid van de informatievoorziening te waarborgen.

1.5 Aanwijzing bevoegd functionaris

Een bevoegd functionaris is alleen nodig bij art 9 en 10 verwerkingen. IPOL staat op het standpunt dat binnen IPOL geen bevoegd functionaris nodig is indien IPOL geen opdrachtgever is.

IPOL heeft aan haar processen waar nodig – indien IPOL opdrachtgever is - bevoegd functionarissen aangewezen.

Voor de in het onderzoek betrokken processen Vertalingen en Publiceren, Kenmerken en Opsporingsberichten geldt dat IPOL geen opdrachtgever. Deze processen zijn echter wel onderdeel van de processen in de strafrechtketen. In dit geval zou de OvJ (bij het OM) beschouwd kunnen worden als de opdrachtgever en ketenregisseur. IPOL heeft om deze reden geen bevoegd functionarissen aangewezen voor deze processen. De wet sluit op dit punt niet aan bij de praktijk.

Dit betekent ook dat de bevoegd functionaris (buiten IPOL) verantwoordelijk is voor de naleving van de WPG bij IPOL. Bijv. de OvJ dient in dit geval de beheersmaatregelen in de

processen in te regelen en te borgen. Tevens dient de OvJ toezicht uit te oefenen op de naleving van de WPG.

Wij stellen ons op het standpunt dat de processen binnen IPOL onderdeel uitmaken van de processen in de strafrechtketen en dat het van belang aan al deze processen een bevoegd functionaris toe te wijzen. Wij hebben niet vastgesteld dat deze toewijzing in opzet aan alle processen in samenhang heeft plaatsgevonden.
Dit aspect van de WPG is in opzet, ondanks het ontbreken van bevoegd functionaris, op hoofdlijnen in beperkte mate gewaarborgd doordat te allen tijde afstemming wordt gezocht met het OM.

Risico
Het risico is aanwezig dat de processen van IPOL in opzet niet aan de WPG voldoen. Dit staat los van de vraag waar de verantwoordelijkheid voor de toewijzing van de bevoegd functionaris in de strafrechtketen ligt.

Risico-inschatting: laag
- Doordat te allen tijde afstemming wordt gezocht met het OM, wordt het gemis aan een aangewezen bevoegd functionaris bij IPOL ondervangen.

Aanbevelingen
Wij adviseren deze problematiek onder de aandacht van de ketenregisseur / het OM te brengen en hierover nadere afspraken te maken en deze in het proces te borgen

1.6 Samenwerkingsverbanden (Art 20)
IPOL werkt inzake de processen Vertalingen en Publiceren, Kenmerken en Opsporingsberichten samen met vertaalbureaus en met o.a. de AVRO (bij de productie van het programma "Opsporing Verzocht") en SBS6. Dit is vastgelegd in de vorm van een aanbesteding en een convenant. Er is echter geen sprake van een samenwerkingverband in de betekenis van art. 20 WPG aangezien er geen politie-informatie wordt uitgewisseld (valt niet onder de WPG maar onder de wet Strafvordering).

1.7 Protocollen
Er worden bij IPOL in de praktijk voornamelijk art. 13 protocollen gebruikt. Voor het onderwerp opsporingsberichtgeving moet nog een art. 13.2 protocol uitgewerkt en vastgesteld worden. Door het ontbreken van protocollen voor art. 13 verwerkingen is in beperkte mate voldaan aan wettelijke verplichting vanuit de WPG.

Risico
Het beschrijven van protocollen is een verplichting in de WPG. Het niet voldoen aan deze beschrijving leidt tot overtreding van de wet. Tevens bestaat het risico dat medewerkers het protocol niet naleven.

Risico-inschatting: hoog
- Het niet voldoen aan de eisen gesteld in de wet leidt tot een hoge risico inschatting.

Aanbevelingen
Het wordt aanbevolen om de artikel 13 protocollen te (doen) beschrijven, vaststellen, implementeren en binnen de organisatie te borgen.

1.8 Opleidingen

Bij IPOL wordt iedereen die met de WPG werkt opgeleid; wij hebben echter geen opleidingsplan aangetroffen. Het MT heeft besloten alle medewerkers een opleiding WPG te laten volgen. Deze opleiding is gedifferentieerd naar functie. De ontwikkelingen op het gebied van de WPG worden door de PF en het kwaliteitsbureau bijgehouden. In totaal betreft het 2 medewerkers die nog niet zijn opgeleid.
Vanwege het ontbreken van een opleidingsplan is aan dit aspect van de WPG in beperkte mate voldaan.

Risico
Het risico bestaat dat niet alle medewerkers voor de WPG zijn opgeleid en als gevolg daarvan de WPG niet wordt nageleefd.

Risico-inschatting: laag
- De afwezigheid van een opleidingsplan vormt, door de beperkte grootte van de team, in de praktijk een beperkt (laag) risico.

Aanbevelingen
Wij adviseren alsnog een opleidingsplan uit te werken en de controle op de realisatie in de organisatie te borgen. Daarnaast is ons advies om de betreffende medewerkers die nog niet voor de WPG zijn opgeleid de training te laten volgen.

2 Noodzakelijkheid, rechtmatigheid en doelbinding (Art 3)

De begrippen noodzakelijkheid, rechtmatigheid en doelbinding zijn bekend bij de privacyfunctionaris. De WPG verandert, t.o.v. de WpolR, niets aan de wijze waarop IPOL met de gegevens omgaat Wij hebben niet in alle gevallen procesbeschrijvingen aangetroffen die de noodzakelijkheid, rechtmatigheid en doelbinding van de verwerking van politiegegevens waarborgen. De naleving van de WPG is hierdoor niet in alle gevallen gewaarborgd.

Risico
In de procesbeschrijvingen is niet in alle gevallen voldoende aandacht voor de aspecten noodzakelijkheid, rechtmatigheid en doelbinding. Dit veroorzaakt risico's voor de naleving van de WPG.

Risico-inschatting: gemiddeld
- Er is binnen de afdeling geen sprake van art. 9 onderzoeken.
- Er wordt geen gebruik gemaakt van landelijke applicaties en systemen.
- IPOL is geen eigenaar van de informatie; zij faciliteert uitsluitend de vertaling van de informatie en is intermediair tussen de regio's en de AVRO.
- De medewerkers zijn bekend met de begrippen noodzakelijkheid, rechtmatigheid en doelbinding.

- Wij hebben in dit verband niet in alle gevallen procesbeschrijvingen aangetroffen;dit veroorzaakt mogelijk mogelijk interpretatieverschillen ten aanzien van de genoemde begrippen.

Aanbevelingen
Wij adviseren de procesbeschrijvingen en werkinstructies nader uit te werken met als doel de noodzakelijkheid, rechtmatigheid en doelbinding van de verwerking van politiegegevens te waarborgen.

3 Juistheid, volledigheid en beveiliging politiegegevens (Art 4)

In de procesbeschrijvingen is niet in alle gevallen voldoende aandacht geweest voor de aspecten juistheid, volledigheid en beveiliging van politiegegevens. Dit veroorzaakt risico's voor de naleving van de WPG aangezien er evenmin gesteund kan worden op beheersmaatregelen in een applicatie. In de praktijk zijn er echter wel een aantal maatregelen getroffen die er van zorgen dat het risico's van het niet naleven van de WPG beperkt is.

De afdeling vertalingen vertaalt gegevens en interpreteert de gegevens niet. De afdeling is niet verantwoordelijk voor de inhoud van de berichten. Binnen de afdeling is, door middel van een collegiale toetsing, de juistheid van de vertaling gewaarborgd

Tevens is in interviews aangegeven dat in de opsporingsberichten een uitgebreide kwaliteitscontrole plaatsvindt op de informatie/gegevens. Bij de intake wordt de aangeleverde informatie voor registratie gecontroleerd op juistheid en volledigheid. Ontbrekende gegevens om de vraag in behandeling te kunnen nemen worden verzameld. Waar nodig wordt het verzoek verder aangescherpt. Tevens vinden aanvullende controles plaats bij de verdere voorbereiding en bij publicatie. Na publicatie wordt beoordeeld of archivering vanuit wet- of regelgeving nodig is. Zo niet dan vindt vernietiging van de berichten plaats. Hier is een procedure voor geschreven; dit hebben echter niet vast kunnen stellen. Om gegevens te beschermen tegen verlies en diefstal hebben de politieproducers een kluiskoffer in de auto en een kluis thuis.

Risico
De juistheid, volledigheid en beveiliging is, ten aanzien van de opsporingsberichten, geheel afhankelijk van controles door de gebruikers. De kans bestaat dat deze controles niet of niet juist worden uitgevoerd. Dit veroorzaakt beperkte risico's voor de naleving van de WPG aangezien IPOL een aantal mitigerende maatregelen heeft getroffen.

Risico-inschatting: laag
- De medewerkers van IPOL hebben een hoog veiligheidsbewustzijn.
- IPOL past collegiale toetsing en kwaliteitscontrole en aanvullende controles toe bij de verwerking van politiegegevens.
- Papieren dossiers worden bewaard in een afgesloten kast in een afgesloten ruimte.
- IPOL past voor de toegangsbeveiliging het principe van compartimentering toe.

Aanbevelingen
Voor zover IPOL voor de ondersteuning van haar processen in de toekomst gebruik maakt van een applicatie adviseren wij in dat geval een aantal controles in deze applicatie in te richten. Tevens adviseren wij de procesbeschrijvingen waar nodig aan te passen en daarbij aandacht te besteden aan de juistheid, volledigheid en beveiliging van politiegegevens.

4 Autorisatie (Art 6)

Het proces Vertalingen registreert haar documenten in mappen op de G:/Schijf. Alleen medewerkers van deze afdeling hebben toegang tot alle mappen op het betreffende deel van de G:/Schijf. De afdeling bestaat uit vertalers en coördinatoren. De medewerkers hebben zicht op elkaars werkzaamheden en hebben dezelfde rechten. De autorisaties worden door de afdeling geregeld en door het diensthoofd toegekend. De autorisaties op de G:/Schijf worden door de mapeigenaar toegekend en onderhouden. Hier is bij IPOL vastgelegd beleid voor geschreven.

Op 9 november 2010 is door de korpsleiding KLPD breed autorisatiebeleid vastgesteld. Wij hebben bij IPOL een autorisatiematrix aangetroffen bij de Afdeling Publiceren, Kenmerken en Opsporingsberichten.

IPOL past in haar processen het principe van controletechnische functiescheiding toe. Bij de in het onderzoek betrokken processen Vertalingen en Publiceren, Kenmerken en Opsporingsberichten was de controletechnische functiescheiding echter niet in alle gevallen voldoende gewaarborgd. Op basis hiervan zijn wij van mening dat IPOL ten aanzien van de in het onderzoek betrokken processen, op dit aspect in beperkte mate voldoet aan de WPG.

Risico
Wij hebben niet in alle gevallen formele functiescheiding aangetroffen op basis van een goedgekeurd autorisatiebeleid uitgewerkt in een autorisatiematrix. Het risico wordt beperkt doordat de afdelingen uit een beperkt aantal medewerkers bestaan.

Risico-inschatting: gemiddeld
- De naleving van de WPG is, door het ontbreken van voldoende controletechnische functiescheiding, in opzet onvoldoende gewaarborgd. Dit wordt enigszins gecompenseerd door het beperkte aantal medewerkers.

Aanbevelingen
Wij adviseren een risicomatrix per proces op te stellen en bij de toewijziging van autorisaties aansluiting te zoeken bij het KLPD brede autorisatiebeleid.

5 Geautomatiseerd vergelijken (Art 11)

IPOL past geen geautomatiseerde vergelijking toe.

6 In combinatie verwerken (Art 11)

IPOL past geen in combinatie verwerken toe

7 Bewaartermijnen en vernietiging (art. 14)

IPOL, voor wat betreft de processen Vertalingen en Publiceren, Kenmerken en Opsporingsberichten, voldoet ten aanzien van het aspect de bewaar- en vernietigingstermijnen in beperkte mate aan de WPG. Bij het proces Vertalingen dient de borging van de naleving van de termijnen nog te worden geregeld. Daar is nu geen systeem voor. Deze processen vallen onder art. 13. De bewaartermijn moet in het nog op te stellen art. 13 protocol zijn vastgelegd. Als er een termijn van 2 jaar in het protocol wordt vastgelegd voldoen deze processen aan de bewaartermijn. IPOL heeft een aantal compenserde maatregelen getroffen die de naleving van de bewaartermijnen en tjidige vernietiging dienen te waarborgen.

IPOL plaatst de documenten in een mappen op de G:/schijf beveiligd; deze is per jaarmap ingedeeld. Documenten die daarvoor in aanmerking komen niet achter een schot. Informatie wordt na vertaling in principe niet bewaard voor nieuwe bewerking maar blijft wel achter als "studieobject" voor toekomstige vertalingen. De informatie wordt daarbij niet geanonimiseerd. Er is geen zicht op het vernietigen van gegevens bij externe vertaalbureaus.

IPOL verwerkt uitsluitend elektronische informatie. Verreweg de meeste documenten worden digitaal ontvangen. Als er toch een opdracht op papier wordt ontvangen wordt deze direct ingescand. De papieren versie wordt vervolgens de shredder vernietigd. De coördinator vernietigt daarna de betreffende bestanden en mappen op de G:/schijf.

De afdeling Publiceren, Kenmerken en Opsporingsberichten bewaart mailtjes van zaken in een map op de G:/schijf. De hard-copy informatie wordt bewaard in mappen in een afgesloten kast op een afdeling die is voorzien van toegangsbeveiliging. Het volledig digitaliseren van zaken is nog niet gelukt. Via ROVER (verwijsindex met regio/zaaksdatum/zaaksbehandelaar/ uitzenddatum/OvJ/datum) worden zaken gelogd.

De naleving van de bewaartermijn is nog niet geborgd. "Oude" zaken worden na in principe na 2 jaar vernietigd. Voorzover gegevens worden aangeleverd door de regio worden deze door het KLPD geleverd aan de AVRO. Het KLPD is echter geen eigenaar van de gegevens; deze blijven eigendom van de regio.

Risico

Informatie uit het proces wordt in niet alle gevallen tijdig vernietigd; schoning vindt incidenteel plaats. Het is mogelijk dat informatie, door het niet naleven van vernietigingstermijnen, te vroeg of juist te laat wordt vernietigd.

Risico-inschatting: gemiddeld

IPOL loopt, doordat het proces bewaartermijnen nog niet in geïmplementeerd, beperkte risico's t.a.v. de naleving van WPG doordat IPOL de volgende compenserende maatregelen heeft getroffen:

- De medewerkers van IPOL hebben een hoog veiligheidsbewustzijn.
- Alle gedigitaliseerde Informatie wordt op een gestructureerde wijze bewaard op de G:/;schijf beveiligd.
- Papieren dossiers worden achter slot en grendel in een afgesloten ruimte bewaard en na 2 jaar vernietigd.

- Informatie wordt in principe na 2 jaar vernietigd; dit is ruim binnen de wettelijke termijn van 5 jaar.

Aanbevelingen
Wij adviseren om voor de processen Vertalingen en Publiceren, Kenmerken en Opsporingsberichten bewaartermijnen te implementeren.

8 Gegevens beheer

Alle informatie die het karakter van politiegegevens hebben is digitaal of wordt digitaal gemaakt. Papieren versies worden vervolgens via de "Grijze afval stroom" met behulp van een shredder vernietigd.

Het proces vertalingen gebruikt de G:/schijf voor opslag en archivering. Er wordt verder geen andere applicatie gebruikt. De vertalingen, zowel het bron document als het product, worden altijd via internet met de mail verstuurd.

De informatie t.b.v. de uitzendingen van "Opsporing verzocht" wordt gedurende 2 jaar in mappen bewaard. Na 2 jaar wordt de informatie verplaatst en naar een afgesloten ruimte en daar bewaard. Dit aspect voldoet in beperkte mate aan de WPG.

Risico
Omdat alle informatie via het openbare internet, niet encrypted, wordt verstuurd bestaat er risico dat documenten onderschept en/of gemanipuleerd worden.

Risico-inschatting: hoog

- De betrouwbaarheid van de informatievoorziening is, door het versturen van niet encrypte gegevens over het openbare internet, onvoldoende gewaarborgd. Dit veroorzaakt risico's ten aanzien van de naleving van de WPG.

Aanbevelingen
Wij sluiten aan bij de wens van IPOL om het uitwisseling van gegevens met vertaalbureaus uitsluitend via een beveiligde lijn te laten plaatsvinden of voor dat doel een beveiligde omgeving te creëren.

9 Ter beschikking stellen van politiegegevens (Art 15)

Ter beschikking stellen van informatie betreft de uitwisseling van informatie binnen het politie-domein. IPOL stelt geen politiegegevens ter beschikking.

10 Verstrekkingen (Art16 t/m Art 20)

Het proces Publiceren Kenmerken en Opsporingsberichtgeving verstrekt informatie aan derden. Dit is geregeld in de "Aanwijzing Opsporingsberichten" van het OM. De regio stelt informatie aan IPOL beschikbaar als het om onderzoeken van de regio gaat. Deze beschikbaarstelling van informatie vindt uitsluitend plaats na overleg met de OvJ en dan uitsluitend informatie die reeds eerder bekend is gemaakt (dus geen nieuwe informatie). Bij twijfel en vragen wordt er verwezen naar de aanbrenger (regio politie) van de zaak.

11 Rechten van betrokkenen (Art 25 t/m Art 31)

Het proces Vertalingen heeft niet te maken met betrokkenen. Zij voeren in opdracht van opdrachtgevers binnen en buiten het KLPD vertalingen uit. Indien nodig worden betrokkenen verwezen naar de opdrachtgever.
Het proces Publiceren, Kenmerken en Opsporingsberichten heeft niet te maken met betrokkenen. Indien nodig worden betrokkenen doorverwezen naar de aanleverende regio of naar de opdrachtgever de AVRO.

12 Privacyfunctionaris (Art 34)

Bij IPOL is een privacyfunctionaris aangesteld. Hij is inhoudelijk op de hoogte van zijn taken, verantwoordelijkheden en bevoegdheden en van de werkzaamheden van verschillende units. Hij heeft echter geen echte werkrelatie met een aantal units omdat het onderwerp privacy bij sommige units niet speelt.

Het aanstellen van een privacyfunctionaris is een wettelijke verplichting vanuit de WPG. Een belangrijke taak van de privacyfunctionaris is het uitoefenen van toezicht op de naleving van de WPG. IPOL heeft een privacyfunctionaris; hij komt echter niet toe aan de toezichthoudende rol. Dit wordt veroorzaakt doordat andere taken, zoals informatieverzoeken op grond van de WOB (250 stuks per maand), te veel tijd kosten. Deze informatie is uitsluitend gebaseerd op het interview met de privacyfunctionaris; wij hebben deze uitspraak niet getoetst.

De privacyfunctionaris is momenteel niet geautoriseerd voor de systemen waar de registratie van politiegegevens plaatsvindt. Dit is echter niet gebaseerd op bewust beleid: de privacyfunctionaris krijgt - op aanvraag – alle autorisaties die hij nodig heeft voor zijn functie en om invulling te geven aan zijn toezichthoudende rol. Verder geeft betrokkene adviezen m.b.t. de implementatie van de WPG. Bij afwezigheid van de privacyfunctionaris worden de taken intern binnen IPOL waargenomen.
Het toezicht op de naleving van de WPG door de privacyfunctionaris is momenteel niet ingericht. Hierdoor wordt niet voldaan aan een belangrijk onderdeel van de wettelijke verplichting vanuit de WPG.

Risico
Doordat de privacyfunctionaris zijn toezichthoudende rol momenteel niet vervult loopt IPOL risico's t.a.v. de naleving van de WPG. De naleving van de WPG is hierdoor uitsluitend afhankelijk van de beheersmaatregelen in het proces.

Risico-inschatting: hoog

- Er is geen extra waarborg voor naleving van de WPG in de vorm van toezicht door de privacyfunctionaris.

Aanbevelingen
Wij adviseren de WPG na te leven en de privacyfunctionaris zijn toezichthoudende rol te (doen) vervullen.

13 Privacyjaarverslag (Art 34)

De privacyfunctionaris is aangemeld bij de CBP en heeft over 2010 een kort jaarverslag opgesteld. Hiermee is met dit aspect, het opstellen van een privacyjaarverslag, voldaan aan de WPG.

Risico

Bij afwezigheid van een privacyjaarverslag kan moeilijk een inschatting worden gemaakt van de totale inzet en taken van de privacyfunctionaris en van de voortgang van de implementatie van de WPG.

Risico-inschatting: laag

- Indien geen privacyjaarverslag wordt opgesteld kan niet op een eenvoudige wijze worden ingeschat of de dienst op hoofdlijnen "in control" is t.a.v. de WPG.

Aanbevelingen

Geen aanbevelingen

14 Knelpunten verdere implementatie

Door IPOLinzake de processen Vertalingen en Publiceren, Kenmerken en Opsporingsberichten zijn een aantal punten genoemd die mogelijk als knelpunt kunnen worden aangerekend bij de verder implementatie van de WPG:

- een beschermde en beveiligde lijn met de vertaalbureaus ontbreekt;
- bij de externe vertaalbureaus dient een beveiligde omgeving te worden ingericht waar op betrouwbaarheid van de informatievoorziening voldoende is gewaarborgd;
- de dienst IPOL - m.n. de art. 13 verwerkingen – past niet in de WPG. De art. 13 verwerkingen zijn speciaal geschreven voor IPOL. Voor het schrijven van de (voor art. 13 verplichte) protocollen heeft IPOL onvoldoende personele capaciteit;
- het Proces vertalingen binnen IPOL is niet te vergelijken met een gewone politie regio. IPOL probeert het WPG proces in een vorm te organiseren maar zijn in deze uniek waardoor spiegelen met anderen (korpsen of diensten) niet mogelijk is;
- de privacyfunctionaris komt, door teveel overige werkzaamheden, niet toe aan zijn toezichthoudende rol.

15 Knelpunten verdere implementatie

<u>Algemeen</u>

Deze reactie is tot stand gekomen na consultatie van de privacyfunctionaris die de audit van beide processen heeft bijgewoond.

<u>Ten aanzien van de inleiding.</u>

Daar dit slechts dient om een algemeen beeld van de dienst IPOL te schetsen, komt het wat vreemd voor dat hier slechts een van de zeer vele producten van de dienst wordt genoemd. Wellicht is het handiger om hier gebruik te maken van de tekst zoals die op het Intranet wordt gebruikt: "*De Dienst IPOL is het verbindingspunt van de politie voor nationale en internationale partners die werken aan een veilige samenleving. De dienst brengt informatiestromen bij elkaar, waarbij wederkerigheid het uitgangspunt is. Met andere woorden: IPOL verzamelt, analyseert, veredelt en verspreidt informatie waardoor beter overzicht en inzicht ontstaat in de nationale en internationale veiligheidssituatie.*"

Ad 1.1 Mandaatregeling
Ten aanzien van de door u gestelde aanbeveling kan ik melden dat de voortgang van de implementatie van de WPG maandelijks aan de orde wordt gesteld in het beheers-MT. Daarnaast wordt in het KLPD-privacy-overleg momenteel gesproken op welke wijze 'privacy' kan worden geborgd in een management-informatie-systeem binnen het KLPD. Indien aanvullende maatregelen nodig zijn zal de dienst IPOL zich hieraan conformeren.

Ad 1.3 Risico-analyse
Op dit moment richt de dienst IPOL zich op de implementatie van de WPG. Door middel van onze maandelijkse voortgangsrapportage heb ik zicht op de openstaande activiteiten en de grootste risico's. Zolang deze implementatiefase nog niet is afgerond zal ik nog geen opdracht geven voor een dienstbrede risico-analyse.

Ad 1.4 Functionele documentatie
Door middel van uw aanbeveling suggereert u dat de door mij genomen beheersingsmaatregelen onvoldoende het risico afdekken. Ik kan echter niet uit de tekst opmaken over welke risico's het gaat, graag ontvang ik van u hierover een nadere toelichting.

Ad 1.5 Aanwijzing bevoegd functionaris.
Ten opzichte van de vragen die zijn gesteld, is de rapportage afwijkend daarvan. Verder is de werkelijkheid genuanceerder dan in het rapport gesteld.

In de tweede zin van deze paragraaf wordt gesteld: "IPOL staat op het standpunt dat binnen IPOL geen bevoegd functionaris nodig is indien IPOL geen opdrachtgever is." Het gaat echter niet om het standpunt van de dienst IPOL, maar om het feit dat hierin door de WPG niet is voorzien. Beide onderzochte onderdelen verwerken gegevens onder de verantwoordelijkheid van een regio of andere onderdelen van het KLPD.

Het klopt dat voor deze onderdelen geen bevoegd functionarissen zijn aangesteld. Bevoegd functionarissen worden, zoals in de conceptrapportage terecht is gesteld, alleen aangewezen door de verantwoordelijke indien sprake is van verwerkingen als bedoeld in artikel 9 of 10 van de WPG. Het spreekt voor zich dat de verantwoordelijke dit alleen kan doen voor verwerkingen die onder zijn verantwoordelijkheid vallen. Bij geen van beide processen is sprake van zelfstandig gevoerde verwerkingen ex artikel 9 of 10 van de WPG, waarvoor het hoofd van de dienst IPOL verantwoordelijk is. Derhalve is er geen juridische grond voor het hoofd van de dienst IPOL om bevoegd functionarissen aan te wijzen voor verwerkingen noch is de noodzaak daartoe aanwezig.

Ik deel derhalve niet het onderdeel van het standpunt van de auditors in deze dat het van belang is aan al deze processen een bevoegd functionaris toe te wijzen. Het gaat hier om een lijnverantwoordelijkheid in de uitvoering van taken ten behoeve van een andere verantwoordelijke.

In aansluiting hierop wil ik het volgende opmerken. Onder "Risico" wordt in z'n algemeenheid gesteld dat het risico aanwezig is "dat de processen van IPOL in opzet niet aan de WPG voldoen.". Tegen de achtergrond van de hierboven door mij aangegeven argumenten deel ik het hier geformuleerde risico zeker niet. Het verhoudt zich niet met het feit dat de WPG niet voorziet in de aanwijzing van een bevoegd functionaris voor een verwerking, waarvoor een

andere verantwoordelijke verantwoordelijk is. Hoe dit wel is geregeld, is te vinden in artikel 6, zevende lid, WPG.

De aanbeveling lijkt mij niet aan te sluiten bij de daarvoor genoemde risico-inschatting. Enerzijds is daarin vermeld dat, doordat te allen tijde afstemming wordt gezocht met het OM, het gemis aan een aangewezen bevoegd functionaris bij IPOL wordt ondervangen, terwijl anderzijds in de aanbeveling wordt gesteld deze problematiek onder de aandacht van de ketenregisseur / het OM te brengen en hierover nadere afspraken te maken en deze in het proces te borgen.

Juist vanwege het feit dat alle werkzaamheden binnen het proces Publiceren van kenmerken (opsporingsberichtgeving) altijd worden verricht op basis van de Aanwijzing opsporingsberichtgeving en met uitdrukkelijke toestemming van, en in overleg met, het OM, neem ik de aanbevelingen op dit punt voor beide processen niet over.

Ad 1.7 Protocollen
Hetgeen in deze paragraaf is verwoord onderschrijf ik in z'n geheel voor zover dat toeziet op het proces Opsporingsberichtgeving. Ondanks dat bij dit onderdeel geen sprake is van een eigen verwerking ex artikel 9 of 10 WPG, is wel degelijk sprake van een verdere verwerkingen van gegevens als bedoeld in artikel 13 WPG, namelijk de verwerking van gegevens ten behoeve van Publiceren van kenmerken (opsporingsberichtgeving) in het algemeen en de verwerking van gegevens over vermiste personen in het bijzonder. Ten aanzien van de daarvoor verplichte protocollen kan ik meedelen dat deze in een zeer ver gevorderd stadium van ontwikkeling zijn. De vaststelling verwacht ik in het eerste kwartaal van 2012.

Ten aanzien van het proces Vertalingen geldt dat geen politiegegevens in de zin van artikel 13 WPG worden verwerkt. De overige gegevens die binnen dit proces worden verwerkt, vallen onder de verantwoordelijkheid van de verzoekende interne dan wel externe instantie en kan het team worden gezien als een bewerker in de zin van artikel 1, onder i, WPG.

Ad 1.8 Opleidingen
Ten aanzien van de opleiding van de medewerkers van de onderzochte onderdelen, kan ik meedelen dat deze allemaal de WPG-cursus hebben gevolgd. Het is derhalve niet meer nodig om hiervoor in een opleidingsplan te voorzien.

Voor wat betreft de WPG-cursus voor de dienst IPOL als geheel kan ik meedelen dat nog slechts 7 personen de cursus dienen te volgen. Het betreft in al deze gevallen de basiscursus voor de WPG. Deze personen zijn bekend en inmiddels geïnformeerd over het feit dat zij de cursus dienen te volgen. Dat zal gebeuren met een laatste "veegklas".

De WPG-opleidingen zijn vanaf enig moment verzorgd door daartoe opgeleide kerninstructeurs. Daar hiermee, anders dan kleine kosten voor koffie, thee en fris, geen kosten zijn gemoeid, maakt de WPG-cursus geen onderdeel uit van een algemeen opleidingsplan. Dat verklaart ook dat er geen opleidingsplan voor de WPG voorhanden was tijdens de audit zelf. Gezien de huidige stand van zaken ten aanzien van de WPG, zal ik ook niet meer voorzien in een opleidingsplan hiervoor.

In aanvulling hierop kan ik meedelen dat kennis van de WPG wel aandacht zal krijgen in het in ontwikkeling zijnde beleid ten aanzien van nieuwe medewerkers in het primaire proces.

Ad 2 noodzakelijkheid, rechtmatigheid en doelbinding (Art 3)
Ook hier onderschrijf ik de constatering dat in de procesbeschrijvingen niet in alle gevallen voldoende aandacht bestaat voor de aspecten noodzakelijkheid, rechtmatigheid en doelbinding. Zoals ook is geconstateerd zijn de medewerkers wel bekend met deze begrippen. In hun dagelijks taakuitvoering zullen deze begrippen dan ook worden toegepast. Dat ontslaat ons echter niet van de plicht om dit te borgen in de procesbeschrijvingen en werkinstructies.
Ik zal opdracht geven om de aanbeveling uit te voeren. Deze opdracht is echter beperkt tot de beschrijvingen van het proces Opsporingsberichtgeving, daar het Team Vertalingen helemaal geen zelfstandige gegevensverwerking heeft.

Ad 3 Juistheid, volledigheid en beveiliging politiegegevens (Art 4)
Ten aanzien van de aanbevelingen.
Gezien de huidige ontwikkelingen richting de Nationale politie en het daaraan verbonden beleid ten aanzien van ITC, ligt het niet in de lijn der verwachtingen dat veel invloed zal kunnen worden uitgeoefend op de inrichting van toekomstige applicaties. Uiteraard zal dat, waar mogelijk, wel gebeuren. Voor wat betreft de procesbeschrijvingen zal ik opdracht geven om na te gaan in hoeverre deze ten aanzien van de betreffende aspecten dienen te worden aangepast.

Ad 4 Autorisatie (Art 6)
De G:schijf is bedoeld voor alle medewerkers. Het is inderdaad zo dat medewerkers zicht hebben op elkaars werkzaamheden. Verdere functiescheiding en differentiatie ten aanzien van de toegang tot deze gegevens is echter niet wenselijk. Binnen dergelijke kleine teams met relatief weinig medewerkers werkt dat contraproductief en staat het de continuïteit van het werk in de weg.

Ad 5 Geautomatiseerd vergelijken (Art 11) en 6 In combinatie verwerken (Art 11)
Voor beide onderdelen geldt dat aan de constatering na het woord "toe" moet worden toegevoegd: "binnen de onderzochte processen".

Ad 7 Bewaartermijnen en vernietiging (Art 14)
Hier wil ik eerst opmerken dat niet duidelijk is welke bewaartermijnen worden bedoeld. Artikel 14 WPG wordt hier kennelijk als bepalend beschouwd, terwijl dat om twee redenen niet juist is. Ten eerste ziet artikel 14 WPG, ondanks de titel "bewaartermijnen", slechts toe op de termijnen voor het bewaren of het gebruik van gegevens <u>ná</u> de verwerking voor de doelen als beschreven in de artikelen 8, 9 en 10 WPG. Ten tweede is, zoals uit het hiervoor gestelde blijkt, artikel 14 niet van toepassing op gegevens die ex artikel 13 worden verwerkt.

Het voorgaande neemt niet weg dat voor het proces Publiceren van kenmerken (opsporingsberichtgeving) wel degelijk bewaartermijn van toepassing zijn. Deze termijnen zijn vastgelegd in 2 protocollen ex artikel 13, vierde lid, WPG die, zoals ik onder ad 1.7 heb vermeld, kort na de jaarwisseling zullen worden vastgesteld. Deze nog niet vastgestelde protocollen zal ik ter illustratie van de termijnen aan mijn reactie toevoegen.

Ten aanzien van het proces Vertalingen is mij niet duidelijk waarom een bewaartermijn van 2 jaar wordt voorgesteld. Zoals al duidelijk is geworden, vinden onder de eigen verantwoordelijkheid binnen het proces Vertalingen geen zelfstandige verwerkingen van politiegegevens plaats, waarvoor termijnen zouden moeten worden vastgesteld.

Aan de aanbeveling om bewaartermijnen te implementeren is naar mijn mening voldaan. Voor het overige zal ik voor wat betreft het proces Publiceren van kenmerken (opsporingsberichtgeving) laten nagaan of verbetering mogelijk is op het naleven van de termijnen.

Ad 8 Gegevensbeheer
Ten aanzien van de aanbevelingen wil ik opmerken dat het inrichten van een beveiligde omgeving bij een vertaalbureau nooit kan worden afgedwongen. Zou de dienst IPOL vasthouden aan een dergelijke eis, bestaat de kans dat het vertaalbureau hetzij bedankt voor de klandizie, hetzij dat kosten voor vertaling dermate hoog worden, dat dit niet meer is te verantwoorden. Werkbaarder is het om dit procedureel te regelen, waarbij een vertaalbureau zich contractueel verbindt om aan bepaalde eisen van beveiliging te voldoen en daarvoor bepaalde door de dienst IPOL opgestelde procedures/werkinstructies in acht neemt.

Ad 9 Ter beschikking stellen van politiegegevens (Art 15)
Voor dit punt stel ik vast dat artikel 15 de algemene opdracht in de WPG is, op basis waarvan gegevens binnen het politiedomein moeten worden gedeeld. De stelling dat de dienst IPOL geen gegevens ter beschikking stelt, deel ik niet; ook niet voor wat betreft het onderzochte proces Opsporingsberichtgeving. Vanuit de dienst alsook vanuit het proces Publiceren van kenmerken (opsporingsberichtgeving) worden juist veelvuldig gegevens binnen het politiedomein ter beschikking gesteld. Vanuit het proces Vertalingen zullen inderdaad geen gegevens ter beschikking worden gesteld. Dit laatste vindt zijn oorsprong overigens niet in de WPG, maar in de wijze waarop dit proces bij de dienst IPOL is ingericht (geen zelfstandige gegevensverwerking).

Ad 11 (Rechten van betrokkenen)
De constatering dat de onderzochte processen niet te maken hebben met betrokkenen is apert onjuist. Beide processen verwerken immers politiegegevens over betrokkenen (artikel 1, onder a en g, WPG). Zou dat niet zo zijn, dan zou de WPG niet van toepassing zijn en zou er ook geen grond zijn voor een audit in de zin van de WPG. Beide processen zijn derhalve niet uitgezonderd van de toepassing van de rechten van betrokkenen.

Voor het proces Publiceren van kenmerken (opsporingsberichtgeving) geldt, dat ondanks dat alle gegevens van andere politie-instanties afkomstig zijn, binnen dit proces sprake is van 2 zelfstandige verwerkingen, waarvoor de verantwoordelijke kan worden aangesproken ten behoeve van de uitoefening van de rechten van betrokkenen. Als een dergelijk verzoek wordt ingediend, zal het namens de verantwoordelijke door de privacyfunctionaris van de dienst IPOL worden behandeld, waarbij hij in contact treedt en overleg pleegt met alle betrokken partijen om uiteindelijk een gewogen beslissing te kunnen nemen. Ten aanzien van het proces Vertalingen geldt mutatis mutandis hetzelfde.

Ad 12 Privacyfunctionaris (Art 34)
De opmerking dat de privacyfunctionaris geen echte werkrelatie met een aantal units zou hebben omdat het onderwerp privacy bij sommige units niet speelt, is onjuist.

Toch wil ik hier wel ingaan op de beschreven constateringen van meer algemene strekking, omdat ik dat van belang acht voor de invloed op de relatie van de privacyfunctionaris tot de onderzochte onderdelen.

De functie van de privacyfunctionaris is nog niet geborgd in de organisatie van de dienst IPOL. De functie is nog steeds niet geformaliseerd en de formatieplaats van de huidige privacyfunctionaris is door 2 reorganisaties (IPOL en centralisering bedrijfsvoering) volledig wegvallen. Vanwege de genoemde reorganisaties heeft de privacyfunctionaris vanaf het eerste kwartaal 2009 te maken met een onderbezetting van 50%.

In de formatiebijstelling van 2012 zal binnen de dienst IPOL voor het eerst worden voorzien in formatieruimte voor deze functie. Ik merk op dat met deze formatieve voorziening de onderbezetting niet zal zijn opgelost. Voor het ontstaan van de dienst IPOL uit de dienst Nationale recherche Informatie en dienst Internationale Politiesamenwerking werden de werkzaamheden verricht door 2 privacyfunctionarissen. Door de samenvoeging is het werkaanbod niet afgenomen, omdat de functionaliteiten van de beide voormalige diensten zijn blijven bestaan en ook het exogene werkaanbod niet is gewijzigd.

De onderbezetting en daarmee gepaard gaande werkdruk heeft er toe geleid dat keuzen moesten worden gemaakt ten aanzien van de taken die door de privacyfunctionaris worden verricht. In overleg met de privacyfunctionaris is er voor gekozen om, vanwege het grote afbreukrisico, voorrang te geven aan het behandelen van de verzoeken van betrokkenen. Dat zijn er, in tegenstelling tot hetgeen in het rapport is vermeld, geen 250 per maand, maar 250 per jaar. Bovendien zijn dit geen verzoeken op grond van de WOB, maar op grond van de WPG.

Naast de behandeling van de verzoeken houdt de privacyfunctionaris zich zo veel mogelijk bezig met het geven van advies ten behoeve van de primaire processen van de dienst. Het spreekt voor zich dat de privacyfunctionaris derhalve niet toekomt aan de uitvoering van alle aan hem door de WPG opgelegde werkzaamheden en dat vooral toezicht, controle en de rapportage daarover er bij inschieten.

Wat de aanbeveling betreft kan ik aangeven dat thans ontwikkelingen gaande zijn om in elk geval de functie eerst formatief te regelen en dat vervolgens zal worden gekeken naar de verdere borging, rekening houdend met het Landelijk Functiehuis Nationale Politie en het voorstel van het landelijke project implementatie wet politiegegevens (PIWPG) en de NPA.

Ad 14 Knelpunten verdere implementatie
Ten aanzien van het eerste punt wil ik opmerken dat het hier gaat om een streven. Hoe hier uitvoering aan kan worden gegeven, is nu sterk afhankelijk van de landelijke ontwikkelingen op het gebied van ICT tegen de achtergrond van afspraken die worden beïnvloed door de ontwikkeling van de nationale politie.
Het eerste deel van het derde punt is niet duidelijk geformuleerd en verder op zich niet relevant voor de onderzochte onderdelen. De onvoldoende personele capaciteit voor het schrijven van protocollen ex artikel 13 WPG is opgelost. Ter ondersteuning van de privacyfunctionaris is voor dit doel een externe juriste ingehuurd. Dat heeft erin geresulteerd dat een groot deel van de benodigde protocollen inmiddels in concept gereed is, waaronder, zoals onder ad 1.7 is opgemerkt, ook de protocollen voor het proces Opsporingsberichtgeving.
Het vierde punt is dezerzijds niet duidelijk, niet in z'n algemeenheid en ook niet in relatie tot de audit.
Voor het laatste punt verwijs ik naar hetgeen is verwoord onder ad 12.

Het hoofd van de dienst IPOL,
voor deze,
het plaatsvervangend hoofd van de dienst IPOL,

Vaststelling:

Datum :

Korpsleiding :

220220120144