



Ministerie van Veiligheid en Justitie

Audit Wpg politie IJsselland

Rapport

Datum
Status

22 december 2011
Definitief

Colofon

Afzendgegevens

Departementale Auditdienst

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

Contactpersonen

Senior auditors

T 070 370 65 60

Projectnaam

Audit Wet Politiegegevens

Ons kenmerk

DDS/5719714/11

Auteurs

Inhoud

Colofon 3

1 Assuranceverklaring 7

2 Samenvatting 9

3 Inleiding 19

- 3.1 Algemeen 19
- 3.2 Aanleiding 19
- 3.3 Doelstelling, aard en scope van de opdracht 19
- 3.4 Afbakening 20
- 3.5 Normenkader 20
- 3.6 Beperkingen voor de privacy audit 21
- 3.7 Onderzoeksmethoden en werkwijze 21
- 3.8 Doelgroep van het rapport 21

4 Bevindingen 23

- 4.1 Inleiding 23
- 4.2 Verantwoordelijke (artikel 1.f) 24
- 4.3 Kwaliteitsaspecten van politiegegevens (art 3 en 4) 24
- 4.4 Gevoelige gegevens (artikel 5) 27
- 4.5 Autorisatie (art 6) 27
- 4.6 Geautomatiseerd Vergelijken/ In Combinatie Met Elkaar Verwerken (art 11) 28
- 4.7 Bewaartermijnen (art 14) 29
- 4.8 Ter beschikking stellen (art 15) 31
- 4.9 Verstrekken (art 16/24) 32
- 4.10 Rechten van betrokkenen (art 25/28) 34
- 4.11 Protocolplicht (art 32) 35
- 4.12 Audits (art 33) 36
- 4.13 Privacy functionaris (art 34) 36
- 4.14 Functionaris Gegevensbescherming (art 36) 37

1 Assuranceverklaring

In het jaar 2011 heeft de Departementale Auditdienst (DAD) van het ministerie van Veiligheid en Justitie (VenJ) in opdracht van de landelijke stuurgroep implementatie Wpg, waarin de Directeur-Generaal Politie en het Korpsbeheerders Beraad (KBB) zijn vertegenwoordigd, privacy audits op grond van de Wet politiegegevens (Wpg) uitgevoerd naar de verwerkingen die in de Wpg zijn beschreven bij de politiekorpsen. In de maand november 2011 is een privacy audit uitgevoerd bij het korps IJsselland.

Deze privacy audit had tot doel op systematische wijze te toetsen of aan de bepalingen van de Wpg op adequate wijze uitvoering is gegeven ten aanzien van de in de wet genoemde verwerkingen bij het korps IJsselland.

Dit onderzoek is uitgevoerd conform de richtlijn 3600N, 'Assurance-opdrachten met betrekking tot de bescherming van persoonsgegevens (privacy audits)' van juni 2006, van de NIVRA en de NOREA.

Op grond van onze werkzaamheden concluderen wij dat het stelsel van maatregelen en procedures gericht op de bescherming van de politiegegevens, betrekking hebbende op de in de Wpg genoemde artikelen bij het korps IJsselland, naar de stand van medio september 2011, in opzet, bestaan en werking niet volledig heeft voldaan aan de vereisten zoals genoemd in de Wpg.

Deze conclusie is onderworpen aan de inherente beperkingen die elders in dit assurance-rapport zijn genoemd.

Het oordeel heeft betrekking op de zogenaamde verwerkingen genoemd in de Wpg. Het hierbij gehanteerde normenkader omvat de door het korps IJsselland te nemen maatregelen. Ook is gebleken dat het korps IJsselland voor het volledig kunnen voldoen aan de Wpg eisen mede afhankelijk is van besluiten die buiten het korps IJsselland dienen te worden genomen, bijvoorbeeld op landelijk niveau door de minister van VenJ, het KBB of de Raad van Korpschefs. Tekortkomingen op al deze vlakken hebben uiteindelijk geleid tot het geformuleerde oordeel.

De verantwoordelijke, zijnde de korpsbeheerder van het korps IJsselland, 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 audit functie van het korps IJsselland. Het verbeterrapport en de uitgevoerde hercontrole zullen in de navolgende jaren door de privacyauditor worden beoordeeld.

Den Haag, 22 december 2011

De Directeur van de Departementale Auditdienst

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

J.C. van Praat RE RA

2 Samenvatting

Het korps IJsselland heeft een aantal zaken in opzet opgepakt, zoals het ter beschikking stellen van politiegegevens en de interne audit. De korpsleiding toont hiermee en met andere initiërende activiteiten haar aandacht voor de Wpg. Niettemin voldoet het door ons beschouwde stelsel van maatregelen nog niet in opzet, bestaan en werking aan de vereisten zoals genoemd in de Wpg.

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

Criteria:

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

Norm	Aspect	Bevinding en oordeel
Art. 1.f, Verantwoordelijke		
1.f	Mandaatbesluit	Er is een mandaatbesluit en ondermandaatbesluit aanwezig. De verantwoordelijkheden zijn gedelegeerd aan de korpschef en doorgemandateerd aan de proceseigenaren. Hiermee wordt voldaan aan de Wpg.
Art. 3 en 4, Kwaliteitsaspecten van politiegegevens		
8.1 en 9.1	Onderscheid onderzoek Dagelijkse Politietask (8) versus Bepaald geval (9)	Er is geen instructie aangetroffen waarin de criteria voor het onderscheid zijn aangegeven. Vaak begint een zaak in art 8 (BVH) en verandert in loop der tijd in art 9 onderzoek. Niet alle art 9 onderzoeken worden vanuit BVH overgezet naar BVO. De systemen faciliteren hierin niet. Het onderscheid is in het begin stadium van een onderzoek lastig te maken. Het OM kan vaak geen duidelijk onderscheid maken tussen art. 8 en 9 politiegegevens. Beide soorten worden in BVH opgeslagen. Binnen de politie zijn geen vuistregels opgesteld om het onderscheid te bepalen. Daarmee is sturing vanuit OM problematisch. Hiermee wordt deels voldaan aan de Wpg.
3.1 t/m 3.3 (8) 4.1 (8)	Noodzakelijkheid (8) Doelbinding Rechtmatigheid Juistheid Volledigheid	Er zijn geen procesbeschrijvingen, procedures of richtlijnen voor het waarborgen van de rechtmatigheid, doelbinding, noodzakelijkheid, volledigheid en juistheid. Het is moeilijk vast te stellen of aan criteria wordt voldaan. Er is voorzien in een aantal beheersmaatregelen die er voor moeten zorgen dat aan de criteria wordt voldaan. Aandacht voor kwaliteitscriteria van informatie wordt vooral gegeven in de basisteams en is een lijnverantwoordelijkheid. Er wordt op gestuurd door de assistent team chefs; die controleren de

Norm	Aspect	Bevinding en oordeel
		Informatie op kwaliteitscriteria. Verder vindt er in BVH een controle plaats op personalia met behulp van GBA. Voorts vindt er in het systeem een beperkte check plaats op juistheid en volledigheid. Tot slot komt de Afdeling analyse en beheer in actie bij geconstateerde onjuistheden; zij hanteert hiervoor en geeft opdracht tot corrigeren. Medewerkers verzamelen zoveel mogelijk informatie voor het onderzoek maar houden hierbij geen rekening met aspecten als ter zake dienend en niet bovenmatig. Hiermee wordt deels voldaan aan de Wpg.
3.1 t/m 3.3 (9) 4.1 (9)	Noodzakelijkheid (9) Doelbinding Rechtmatigheid Herkomst en wijze van verkrijging Juistheid Nauwkeurig Volledigheid	Er zijn geen procesbeschrijvingen maar wel werkinstructies voor de medewerkers beschikbaar. Wanneer dagelijks politiewerk (art 8) opsporingswerk wordt (art 9), moet de zaak in BVO worden aangemaakt en moeten gegevens vanuit BVH naar BVO worden getransporteerd. Technisch vormt dit een probleem. Het overzetten dient derhalve nog handmatig te gebeuren. Door deze arbeidsintensieve handeling komt het voor dat opsporingsonderzoeken in BVH worden afgerond. De juistheid en volledigheid van informatie wordt niet automatisch in het systeem gecontroleerd. Medewerkers verzamelen veelal zoveel mogelijk informatie voor het onderzoek maar houden zich hierbij doorgaans niet bezig met de aspecten ter zake dienend en niet bovenmatig. Er is ook geen middel voor handen om de rechtmatigheid van gegevens te toetsen. Hiermee wordt deels voldaan aan de Wpg.
3.4 (9)	Noodzakelijkheid (10 en 12) Doelbinding Rechtmatigheid Herkomst en wijze van verkrijging Juistheid Nauwkeurig Volledigheid	In verband met de aard van de werkzaamheden zijn de kwaliteitscriteria goed ingeregeld. Bij de CIE gebeurt dat door het landelijk proceshandboek CIE en de toezichthoudende rol CIE OvJ. Dit handboek is Wpg compliant. Bij de RID liggen de kwaliteitscriteria al in het doel van de taak vast. In de werkprocessen is beschreven hoe om te gaan met noodzakelijkheid, doelbinding, rechtmatigheid en volledigheid. Informatie wordt voor opname in BVO door leidinggevende gecontroleerd. Hiermee wordt aan de Wpg voldaan.
4.3	Beveiliging	De landelijke systemen en regionale applicaties zijn nog niet Wpg proof. Een aantal systemen waaronder BVH voldoet niet aan de door de Wpg gestelde bewaartermijnen. Hierdoor is kans op onrechtmatig

II

Norm	Aspect	Bevinding en oordeel
		gebruik. Binnen het korps zijn politiegegevens op basis van een autorisatiesysteem afgeschermd. Tevens is sprake van fysieke beveiliging van de gebouwen in de vorm van toegangssystemen. Informatie buiten de landelijke systemen wordt opgeslagen in zogenaamde . Deze worden ook verwerkt in het en daarbij wordt gebruik gemaakt van l . Het opslaan van gegevens in heeft wel tot gevolg dat schoning en bewaring niet is gewaarborgd en dat het delen van gegevens, een doelstelling van de Wpg, niet gerealiseerd kan worden. Hiermee wordt deels voldaan aan de Wpg.
Art. 5, Gevoelige gegevens		
	Gevoelige gegevens	Er zijn geen procesbeschrijvingen aangetroffen waarin is opgenomen op welke wijze de zorg voor het voldoen aan de criteria voor de verwerking van gevoelige gegevens dient plaats te vinden. Kennis en bewustzijn over opslag en verwerking van gevoelige gegevens zijn summier aanwezig. Niettemin geeft men aan en blijkt ook uit de interne audit dat gegevens over afkomst, ras, godsdienst of seksuele- of politieke voorkeur zelden worden geregistreerd. Slechts een beperkt deel doet dit op regelmatige basis. Medewerkers CIE leggen alleen gevoelige informatie vast indien hier noodzaak voor is. Hiermee wordt niet voldaan aan de Wpg.
Art. 6, Autorisatie		
	Korpsautorisatiematrix	Het korps beschikt wel over een autorisatiematrix, waarin rechten aan functies en taken gekoppeld zijn, maar die is niet actueel. Update gaat plaatsvinden met de implementatie van het functiehuis. Hiermee wordt deels voldaan aan de Wpg.
	Aanvraagproces	Het handboek autorisaties beschrijft het aanvraagproces. Verder is er een autorisatiebeheerder aangesteld binnen de afdeling analyse en beheer, die ook verantwoordelijk is voor beheer en schoning. Hiermee wordt voldaan aan de Wpg.
	Wijziging en verwijdering	De autorisatiematrix wordt gevoed met gegevens uit het . Op basis hiervan worden mutaties up-to-date verwerkt, waardoor onterechte autorisaties voorkomen worden. Het proces om autorisaties te verwijderen of aan te passen als gevolg van uitdiensttreding of

II

II

Norm	Aspect	Bevinding en oordeel
		functiewijziging is inmiddels verbeterd. Bij de autorisatiebeheerder worden alle mutaties ingeleverd en getoetst. Proceseigenaren dienen minimaal controle uit te voeren op de toegekende autorisaties. Vanuit het korps worden echter geen autorisatieoverzichten opgevraagd om de toebedeelde autorisaties te controleren. Ook door de privacyfunctionaris wordt nauwelijks controle op de autorisaties uitgevoerd en worden geen rapportages opgeleverd. Hiermee wordt deels voldaan aan de Wpg.
	• Autorisatiebeheer CIE en RID	Autorisaties CIE worden toegekend door hoofd CIE, waarvan sommige goedgekeurd door OvJ. Autorisaties RID worden toegekend door hoofd RID. Deze processen zijn goed ingeregeld. Hiermee wordt voldaan aan de Wpg
32.1.c	Protocollering autorisaties	Autorisatieaanvragen worden gedurende 2 jaar bewaard en daarna digitaal gearchiveerd. Hiermee voldoet het autorisatiesysteem aan de vereisten van zorgvuldigheid en evenredigheid. Hiermee wordt voldaan aan de Wpg.
32.3 voor 32.1.c	Bewaren protocolgegevens autorisaties	Protocolgegevens worden conform de richtlijnen bewaard. Hiermee wordt voldaan aan de Wpg.
Art. 11, Geautomatiseerd vergelijken en in combinatie zoeken		
	• Hanteerbare interpretatie	De begrippen zijn slechts bij weinig geïnterviewden bekend. Interpretaties op landelijk niveau en binnen het korps zijn niet vastgelegd; dit bemoeilijkt uniforme toepassing. Hiermee wordt niet voldaan aan de Wpg.
	• Aangewezen functionarissen	De van de CIE, RID en de Infodesk voeren deze activiteiten uit en zijn aangewezen door hun leidinggevend. Hiermee wordt voldaan aan de Wpg.
11.4	Bevoegd gezag	In de voorfase van de keuze van onderzoeken wordt vaak ook aan een vorm van ICMEV gedaan. Het is niet helder hoe daarin moet worden gehandeld. Het verkrijgen van toestemming van het bevoegd gezag (OM) vindt bij ICMEV niet altijd plaats. Hiermee wordt deels voldaan aan de Wpg.
32.1.d en 32.1.h	Protocollering 11.1, 11.2, 11.4 en 11.5	Procedures voor protocollering van GV en ICMEV zijn niet aangetroffen. Het geautomatiseerd vergelijken van politiegegevens die worden verwerkt op grond van artikel 8, 9 of 10 met andere politiegegevens wordt uitgevoerd door de afdeling Analyse en Beheer, bijvoorbeeld bij een TGO. De afdeling Analyse en Beheer draagt ook zorg voor protocollering van de gegevens Hiermee wordt deels voldaan aan de Wpg.
32.3 voor 32.1.d en	Bewaren protocolgegevens	De afdeling Analyse en Beheer draagt ook zorg voor protocollering en bewaren van de protocolgegevens.

Norm	Aspect	Bevinding en oordeel
32.1.h	11.1, 11.2, 11.4 en 11.5	Hiermee wordt voldaan aan de Wpg.
Art. 14, Bewaartermijnen		
8.2 en 8.3	(8) van 1 tot 5 jaar	Er zijn in BVH geen beheersmaatregelen voor de bewaartermijnen. Er is in de nieuwe release een schoningsmodule voor BVH maar deze staat op verzoek van de voorzitter van de landelijk stuurgroep Wpg nog niet aan. Hiermee wordt niet voldaan aan de Wpg.
8.6	(8) verwijderen na 5 jaar	Er is geen proces opgesteld om politiegegevens in BVH te verwijderen. De gehanteerde applicaties bieden voor dit proces ook geen ondersteuning. Hiermee wordt niet voldaan aan de Wpg. Er heeft geen schoning plaatsgevonden op de politiegegevens in BPS. Er is sprake van politiegegevens die volgens de Wpg vernietigd hadden moeten zijn. BPS is thans alleen nog maar toegankelijk voor medewerkers van de Infodesk. Hiermee wordt niet voldaan aan de Wpg.
14.1 (8)	(8) vernietigen na 5 jaar verwijderd	Er is geen proces opgesteld om politiegegevens te vernietigen. De gehanteerde applicaties bieden voor dit proces geen ondersteuning. Politiegegevens worden niet vernietigd. Vanuit andere wetgeving (WSv, archiefwet) worden langere bewaartermijnen gehanteerd. Hiermee wordt niet voldaan aan de Wpg.
9.4	(9) verwijderen na OH plus ½ jaar	Er is geen proces opgesteld om politiegegevens te verwijderen. De gehanteerde applicaties bieden voor dit proces geen ondersteuning. Hiermee wordt niet voldaan aan de Wpg.
14.1 (9)	(9) vernietigen na 5 jaar verwijderd	Er is geen proces opgesteld om politiegegevens te verwijderen. De gehanteerde applicaties bieden voor dit proces geen ondersteuning. Politiegegevens worden niet vernietigd. Vanuit andere wetgeving (WSv, archiefwet) worden langere bewaartermijnen gehanteerd. Hiermee wordt niet voldaan aan de Wpg.
10.6	(10) verwijderen na 5 jaar geen subjectwaardige registratie	Het proceshandboek CIE omvat een hoofdstuk "verwijderen en bewaren van persoonsgegevens". Toezicht door CIE OvJ draagt bij aan naleven van deze bepaling. Hiermee wordt voldaan aan de Wpg
14.1 (10)	(10) vernietigen na 5 jaar verwijderd	Het proceshandboek CIE omvat een hoofdstuk "verwijderen en bewaren van persoonsgegevens". Toezicht door CIE OvJ draagt bij aan naleven van deze bepaling. De CIE blijkt wel gegevens te verwijderen maar niet te vernietigen. Vanuit andere wetgeving (WSv, archiefwet) worden langere bewaartermijnen gehanteerd. Hiermee wordt deels voldaan aan de Wpg.
14.3	Hernieuwde verwerking	Er is geen procedure voor hernieuwde verwerking van gegevens (Wpg art 14.3). Vanuit het korps is

Norm	Aspect	Bevinding en oordeel
		een concreet verzoek aan de privacyfunctionaris gedaan om hier naar te gaan kijken. De bevoegde functionarissen dragen zorgen voor verstrekking van gegevens bij hernieuwde verwerking. Tevens dient het OM dan toestemming te verlenen. De bevoegd functionaris heeft hierin een centrale rol. Niet in alle gevallen wordt de juiste procedure gevolgd. Hiermee wordt deels voldaan aan de Wpg.
32.1.e	Protocollering 14.3	In voorkomend geval worden deze aanvragen als een nieuwe aanvraag behandeld; deze wordt dan ook als zodanig geprotocolleerd. Hiermee wordt voldaan aan de Wpg.
32.3 voor 32.1.e	Bewaren protocolgegevens 14.3	Protocolgegevens worden bewaard. Hiermee wordt voldaan aan de Wpg.
12.2	(12) verwijderen na 4 maanden	Toezicht door CIE OvJ draagt bij aan naleven van deze bepaling. Hiermee wordt voldaan aan de Wpg.
12.6	(12) controleren en vernietigen	Toezicht door CIE OvJ draagt bij aan naleven van deze bepaling. Hiermee wordt voldaan aan de Wpg.
Art. 15, Ter beschikking stellen		
• Infodesk voor bevraging		Verzoeken om politiegegevens komen bij de front office van de Infodesk binnen. Artikel 8 informatie wordt gewoon ter beschikking gesteld. Alleen afwijkingen worden eerst aan het hoofd infodesk voorgelegd. De ter beschikking stellingen worden geprotocolleerd en de vastlegging bevindt zich in de outlookmap. Ter beschikking stellingen vinden altijd plaats via II zodat het tijdstip en aan wie de informatie is verstrekt vaststaat. De ontvanger moet bekend zijn binnen de politieorganisatie. Telefonische ter beschikking stellingen vinden niet plaats. Hiermee wordt voldaan aan de Wpg.
• Codering		Wanneer de Infodesk informatie ter beschikking stelt waarvoor de toestemming van een bevoegd functionaris nodig is dan wordt het feit dat deze toestemming is verleend II, waarin de informatie ter beschikking wordt gesteld, vermeld. Er wordt niet gewerkt met een aparte codering. Hiermee wordt voldaan aan de Wpg.
• Aanwijzing Bevoegd Functionaris		Bevoegd functionarissen zijn aangewezen. De aanwijzing is vastgelegd in een regionaal besluit. Bij ter beschikking stelling van informatie op basis van artikel 9 en 10 wordt toestemming gevraagd van de eigenaren van de informatie. De (assistent-)teamchefs zijn als bevoegd functionaris uiteindelijk verantwoordelijk voor het ter beschikking van III politiegegevens.

Norm	Aspect	Bevinding en oordeel
		functionaris. Hiermee wordt voldaan aan de Wpg.
	• Opleiding Bevoegd Functionaris	De (assistent-)teamchefs hebben als bevoegd functionaris ook gehad toegespitst op de rol van bevoegd functionaris. Verder hebben zij in t Hiermee wordt voldaan aan de Wpg
15.2	Weigeringgronden	Infodesk vervult hierin een toetsingsfunctie Hiermee wordt voldaan aan de Wpg
Art. 16 t/m 24, Verstrekking		
	• Verstrekkingenwijzer (landelijk)	De verstrekkingen wijzer is bekend Hiermee wordt voldaan aan de Wpg.
	• Proces voor convenanten	Momenteel wordt een onderzoek uitgevoerd naar convenanten als vervolg op een onderzoek dat in 2009 is uitgevoerd. Hierbij wordt een heel erg verschillend beeld waargenomen. Grote convenanten zijn doorgaans op orde, maar de kleinere convenanten veelal niet. Er is geen grip op volledigheid. Als er nieuwe convenanten worden gemaakt, wordt de Wpg (besluit art 20) bij het opstellen van deze convenanten direct meegenomen. Centraal beheer is gewenst. Voor zover aanwezig, zijn convenanten getoetst op Wpg aspecten, eventueel aangepast. Hiermee wordt deels voldaan aan de Wpg.
	• Proces voor Art. 20 Besluiten	Als er nieuwe convenanten worden gemaakt wordt de Wpg (besluit art 20) bij het opstellen van deze convenanten direct meegenomen. Wijzigingen in reeds bestaande convenanten worden in een addendum toegevoegd aan het convenant. Hiermee wordt voldaan aan de Wpg.
	• Verstrekkingenschema (regio)	Er wordt een verstrekkingentabel gehanteerd waarin staat vermeld welke stukken aan welke organisaties verstrekt mogen worden. Hiermee wordt voldaan aan de Wpg.
	• Proces voor geautomatiseerde verstrekking	Vanuit IJsselland is er een viertal automatische verstrekkingen: 1. 2. 3. 4. Er wordt een overzicht van automatische verstrekkingen in Excel bijgehouden. Hiermee wordt voldaan aan de Wpg.
7.2	Geheimhouding	De geheimhoudingsplicht wordt door Infodesk bij verstrekkingen meegenomen. Ontvangers van politiegegevens wordt gewezen op het feit dat de geheimhoudingsplicht niet mag worden geschonden. Die mededeling is ook op de

Norm	Aspect	Bevinding en oordeel
		verstrekkingenrapportage vermeld. Hiermee wordt voldaan aan de Wpg.
32.1.f	Protocollering verstrekking	Bij de verstrekkingen uit BVH worden niet of nauwelijks gebruikt. Het wordt enerzijds in de praktijk als niet werkbaar ervaren en anderzijds speelt onbekendheid van de diender met deze procedure. Medewerkers "Blauw" zijn niet op de hoogte van de Wpg. Zij verstrekken informatie maar protocolleren dit niet. Het is achteraf niet te achterhalen op welke wijze politiegegevens aan externen zijn verstrekt. Verstrekkingen worden in het Veiligheidshuis niet altijd geprotocolleerd. Er wordt altijd benadrukt dat men zorgvuldig met gegevens om moet gaan. De verstrekte informatie worden bewaard. Hiermee wordt deels voldaan aan de Wpg.
32.3 voor 32.1.f	Bewaren protocolgegevens verstrekking	Voor zover verstrekkingen worden geprotocolleerd worden de gedane mutaties in BVH en BVO door Infodesk bewaard. Alle verstrekkingen worden tevens in : bewaard. De mails met verstrekte informatie worden in het Veiligheidshuis bewaard. Hiermee wordt voldaan aan de Wpg.
• Toezicht door leidinggevenden op verstrekkingen en protocollering		Het hoofd Infodesk houdt toezicht op de verstrekkingen en protocollering. Hiermee wordt voldaan aan de Wpg.
Art. 25 t/m 31, Rechten van de betrokkene		
25.1	Verzoek om kennisneming	Hiervoor is een eigen, niet de landelijke, procedure aanwezig. De procedure Rechten betrokkenen is vastgesteld en goedgekeurd. Er wordt niet heel veel gebruik van gemaakt. De privacyfunctionaris is daarmee belast. Tot nu toe is de bestuurlijk voorgeschreven afhandelingstermijn gehaald. Hiermee wordt voldaan aan de Wpg.
28.1 t/m 28.3	Correctie	Nog niet voorgekomen.
Art. 32, Protocolplicht (32.1.c, d, e, f en h behandeld bij thema's)		
9.2 en 32.1.a	Protocollering doel onderzoek	De MRO's worden geprotocolleerd onder verantwoordelijkheid van de teamleiders en bewaard door de bevoegd functionaris. Hiermee wordt voldaan aan de Wpg.
32.3 voor 32.1.a	Bewaren protocolgegevens doel onderzoek	De bevoegd functionaris heeft de protocolleringsgegevens beschikbaar. Hiermee wordt deels voldaan aan de Wpg.
13.4 en 32.1.b	Protocollering Art. 13 gegevensverzameling en	Gegevens worden in voorkomend geval vastgelegd door de Infodesk. Hiermee wordt voldaan aan de Wpg.

III

II

II

Norm	Aspect		Bevinding en oordeel
32.3 voor 32.1.b	Bewaren protocolgegevens Art. 13 gegevensverzameling en		De protocolgegevens worden bewaard conform de richtlijnen. Hiermee wordt deels voldaan aan de Wpg.
32.1.g	Protocollering onrechtmatige handeling		Er is een procedure incidentenregistratie. Incidenten worden gemeld bij de directie. Deze worden of zelf afgehandeld door de directie dan wel voorgelegd aan de directie met verzoek tot het nemen van een besluit. Jaarlijks wordt een managementrapportage beveiligingsincidenten annex onrechtmatige handelingen vastgesteld. Hiermee wordt voldaan aan de Wpg.
32.3 voor 32.1.g	Bewaren protocolgegevens onrechtmatige handeling		De incidentmeldingen worden alle bewaard bij de IBF. Hiermee wordt voldaan aan de Wpg.
Art. 33, Audits			
RPAP 3.1	Interne audit-functie		Binnen IJsselland is een interne audit functie ingericht. Hiermee wordt voldaan aan de Wpg.
RPAP 3.4	Interne audit-plan		Een auditplan wordt momenteel opgesteld. Hiermee wordt deels voldaan aan de Wpg.
RPAP 3.6	Interne audit-rapport		Er is een audit onderzoek uitgevoerd. Hiermee wordt voldaan aan de Wpg.
Art. 34, Privacyfunctionaris			
34.1 en 34.4	Benoemd en gemeld		Formeel aangesteld door KC en aangemeld bij CBP Hiermee wordt voldaan aan de Wpg.
34.2	Overzicht over protocollering		De privacyfunctionaris heeft de protocolleringsgegevens niet of nauwelijks beschikbaar en vult de toezichthoudende taak nog maar beperkt uit. Hiermee wordt niet voldaan aan de Wpg.
34.3	Jaarverslag		Over 2010 is geen jaarverslag opgesteld. De privacyfunctionaris vult de toezichthoudende taak nog maar beperkt uit. Hiermee wordt niet voldaan aan de Wpg.
Optioneel Art. 36, Functionaris Gegevensbescherming			
36.1 en 36.2	Benoemd		FGB komt als functie niet voor
Wbp 63.3	Gemeld		FGB komt als functie niet voor
Wbp 64.1 t/m 64.4	Toezichthoudende rol		FGB komt als functie niet voor

III

3 Inleiding

3.1 Algemeen

In opdracht van de landelijke stuurgroep Wpg, waarin de Directeur-Generaal Politie en het KBB zijn vertegenwoordigd, heeft de DAD van het ministerie van VenJ een privacy audit uitgevoerd bij het korps IJsselland zoals de Korpsbeheerders deze, uit hoofde van de Wpg, twee jaar na inwerkingtreding van de wet dienen te laten uitvoeren (Wpg artikel 33 lid 1).

De opdracht is beschreven in het document 'Plan van aanpak Audit Wet Politiegegevens' d.d. 08-09-2011 met kenmerk DAD/DDS/2011/5706209. De audit is uitgevoerd bij het korps IJsselland in de maanden augustus en september 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 (Art. 33:1). 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.

3.3 Doelstelling, aard en scope van de opdracht

Deze privacy audit heeft tot doel op systematische wijze te toetsen of aan de bepalingen van de Wpg op adequate wijze uitvoering is gegeven ten aanzien van de in de wet genoemde verwerkingen bij het korps IJsselland.

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 maart 2011, van maatregelen en procedures, waarmee het korps IJsselland beoogt te voldoen aan de beheersdoelstellingen die bij of krachtens de Wpg gelden.

Binnen deze audit richten wij ons (conform de artikelen van de Wpg) op de volgende thema's:

- Noodzakelijkheid, rechtmatigheid en doelbinding (artikel 3)
- Juistheid, volledigheid en beveiliging politiegegevens (artikel 4)
- Gevoelige gegevens (artikel 5)
- Autorisaties (artikel 6)
- Geautomatiseerd vergelijken en in combinatie verwerken (artikel 11)
- Bewaartermijnen (artikel 14)
- Ter beschikking stellen van politiegegevens (artikel 15)
- Verstrekkingen (artikel 16 t/m 24)
- Rechten van betrokkenen (artikel 25 t/m 31)
- Protocolplicht (artikel 32)
- Audits (artikel 33)
- Privacyfunctionaris (artikel 34)
- Functionaris gegevensbescherming (artikel 36)

Deze audit richt zich op de opzet, het bestaan en waar mogelijk, de werking van de implementatie van de Wpg per korps. Pas wanneer wij, tijdens het uitvoeren van de audit bij een korps, hebben geconstateerd dat de opzet en het bestaan aan de daaraan te stellen eisen voldoen voeren wij aanvullende werkzaamheden uit om de werking vast te stellen.

3.4 Afbakening

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

De audit is gericht op bovengenoemde objecten en aspecten voor zover onder verantwoordelijkheid van het politiekorps IJsselland. Dit betekent dat wij geen onderzoek hebben verricht naar door de vtsPN aan het korps IJsselland geleverde faciliteiten, voor zover de verantwoordelijkheid daarvoor is belegd bij de vtsPN of bij anderen dan het korps IJsselland.

3.5 Normenkader

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

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

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

3.6 Beperkingen voor de privacy audit

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

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

3.7 Onderzoeksmethoden en werkwijze

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

Het onderzoek is uitgevoerd door het houden van interviews onder medewerkers en leidinggevenden van het politiekorps IJsselland en het Openbaar Ministerie, deelwaarnemingen in de procesbeschrijvingen en andersoortige documentatie en deelwaarnemingen in informatiesystemen.

Wij hebben onze werkzaamheden uitgevoerd in de periode november 2011.

Het conceptrapport met bevindingen is op 9 december 2011 besproken met de korpschef van het korps IJsselland; met de korpsbeheerder is het rapport procedureel afgedaan.

Het eindrapport is met inachtneming van het ontvangen commentaar vastgesteld.

3.8 Doelgroep van het rapport

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

Wij voeren deze audit uit in opdracht van de stuurgroep waarin het KBB is vertegenwoordigd.

De stuurgroep wordt voorgezeten door drs. J.J.M. Stikvoort.

mr. A.F. Gaastra neemt namens DG Politie deel aan de stuurgroep.

drs. H.M.F. Bruls neemt namens het KBB deel aan de stuurgroep.

De specifieke doelgroep waarvoor het rapport is bestemd bestaat uit:

- onze opdrachtgever zoals bovengenoemd;
- de korpsbeheerder, H.J. Meijer;
- de korpschef voor deze de directeur Opsporing mr. I
- de Hoofd Officier van Justitie mr. W. Tomesen;
- de privacyfunctionaris van het korps IJsselland, I
- de voorzitter van het College Bescherming Persoonsgegevens.

Het rapport mag uitsluitend met toestemming van de korpsbeheerder dan wel de korpschef van korps IJsselland 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

Binnen het regiokorps IJsselland is men in de loop van 2009 begonnen aan de implementatie van de Wpg waardoor de implementatie onder grote tijdsdruk is uitgevoerd. De directie heeft toen ingezet op project Wpg I. Uitgangspunt hierbij was de inventarisatie van de meest cruciale activiteiten die het regiokorps uitvoert. De activiteiten zijn geclusterd opgenomen in een overzicht tevens voortgangsrapportage Wpg implementatie. Voor de realisatie daarvan is een projectorganisatie in het leven geroepen bestaande uit een stuurgroep implementatie Wpg IJsselland onder aansturing van de plv korpschef met daaraan verbonden deelprojecten gestuurd door deelprojectleiders. Project Wpg I is gerealiseerd begin 2010.

Uit de interviews is gebleken dat borging en naleving van de Wpg nog niet is ingebed in de management control cyclus. Uit onze interviews komt naar voren dat men zich binnen het korps hiervan bewust is en dat dit wordt aangepakt in het project verbetering Wpg II.

Op basis van de interne audit is door de korpsleiding op 1 februari 2011 een zevental aandachtspunten naar voren gekomen; onder meer worden genoemd:

- Verhoging van het kennisniveau van de medewerkers van de WPG en de toepassing daarvan.
- Het actualiseren van de autorisatiematrix en het mede verstrekken van autorisatie op basis van de rollen in de matrix.
- Het aanpassen van de convenanten aan de Wpg eisen.

4.1.2 Bekendheid met de Wpg binnen de organisatie

In de interne audit en uit onze gesprekken is naar voren gekomen dat de kennis van de Wpg nog niet bij iedereen voldoende aanwezig is. Hierdoor is men zich in het dagelijkse werk ook niet altijd bewust wat de Wpg inhoudt en welke mogelijkheden het biedt. Daarbij gaat het vooral om het verbeteren van het kennisniveau van de medewerkers. Het moet beklijven dat de kennis van de Wpg niet gebrach
niet gebracht wat ervan werd verwacht. Het gaat toch primair om gedrag en attitude. Het komend half jaar 2012 worden er activiteiten gepland voor de doelgroep; maar ook t

Door de korpsleiding is ruimte gecreëerd om hieraan tijd te besteden.

4.1.3 Wpg en de praktijk

In 2009 is er een monitoringslag geweest bij de implementatie van de Wpg. IJsselland had nogal wat bevindingen. De directie heeft onmiddellijk ingezet op project Wpg I, gerealiseerd begin 2010. Er is een achttal deelprojecten benoemd en men heeft in een half jaar de Wpg op de rails gezet. Ook het landelijk project was inmiddels gestart. Gedateerd 25 oktober 2011 is inmiddels versie 0.6 van de voortgang van het project Implementatie WPG-2 (2011) verschenen. In het vierde kwartaal 2010 is er een interne audit uitgevoerd en de resultaten zijn neergelegd in het rapport Pré-Audit Wet Politiegegevens van 8 december 2010, versie 0.2. De interne audit had tot resultaat een 7 tal aandachtspunten. Samen met het achtste aandachtspunt protocollering is april 2011 gestart met het project Wpg II. Men is hier nog steeds druk mee doende.

Gesteld kan worden dat het korps IJsselland momenteel met een veelheid aan activiteiten actief bezig is om aan de implementatie van de Wpg gestalte te geven. Helaas moet worden geconstateerd dat de bestaffing van de verbeterorganisatie summier is bedeed. De aangewezen projectleider doet deze taak erbij naast zijn eigenlijke werk; de tijd die hij kan aanwenden ten behoeve van het project is beperkt. Voorts is ook de vervulling van de functie van Privacyfunctionaris problematisch. Momenteel is er een kandidaat aangetrokken die op basis van 1 dag in de week deze functie invulling geeft. In diverse interviews is gebleken dat het nauwelijks beschikbaar zijn van de privacyfunctionaris door een aantal medewerkers als een groot gemis wordt ervaren. In aanmerking genomen dat deze twee functies als sleutelfunctionarissen voor een goede inbedding van de Wpg in politiekorps IJsselland zijn aan te merken, moet thans gesproken worden van ernstig belemmerende factoren in de implementatie van de Wpg.

4.2 Verantwoordelijke (artikel 1.f)

Mandaatbesluit

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.

In oktober 2009 is een mandaatbesluit Korpsbeheerder-Korpschef opgesteld waarin verantwoordelijkheden voor de Wpg bij de korpschef zijn belegd. In de ondermandaatbesluiten van dezelfde datum worden deze verantwoordelijkheden door de korpschef bij proceseigenaren belegd.

Met betrekking tot de werking van de mandatering is uit de interne audit gebleken dat er in de praktijk nog niet altijd uitvoering wordt gegeven aan de toebedeelde verantwoordelijkheden.

4.3 Kwaliteitsaspecten van politiegegevens (art 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 (art 3) en volledigheid, juistheid en beveiliging (art 4).

4.3.2 Bevindingen

Het voldoen aan de bepalingen van deze artikelen is een aangelegenheid waarin bijna alle geledingen van de politie zijn betrokken. Niettemin is in het bijzonder van belang dat het zwaartepunt van het voldoen aan deze criteria ligt bij de eerste vastlegging van gegevens.

Voor wat betreft het onderscheid in de onderzoeken op het gebied van de dagelijkse politie taak (Wpg art 8) en die van onderzoeken naar een bepaald geval (Wpg art 9) kan het volgende worden vermeld. Voor artikel 9 onderzoeken wordt een zaak aangemaakt in BVO door middel van het MRO formulier.

Echter ook in BVH zijn art 9 onderzoeken vastgelegd. Eenvoudige onderzoeken (de zogenaamde 6 uur onderzoeken) worden sowieso alleen in BVH vastgelegd. Zaken beginnen veelal als een art 8 registratie en groeien dan uit naar een art 9 onderzoek. Overheveling naar BVO vindt niet altijd plaats. In dat geval is sturing door het OM niet altijd gewaarborgd. Met het OM is afgesproken dat een dossier alleen wordt aangenomen wanneer het een BVO-nummer heeft. Dit nummer wordt automatisch gegenereerd, wanneer een zaak in BVO wordt aangemaakt. Dat betekent echter niet dat het dossier volledig is, daar dan nog veel informatie in de BVH kan staan. Met betrekking tot politiegegevens kan het OM vaak geen duidelijk onderscheid maken tussen art. 8 en 9 politiegegevens. Beide soorten worden in BVH opgeslagen. Binnen de politie zijn geen vuistregels opgesteld om het onderscheid te bepalen.

Met betrekking tot artikel 8 informatie *'verwerken van politiegegevens ten behoeve van de dagelijkse politiepraktijk, zoals surveilleren, advisering over preventie, afhandelingen van de verkeersproblematiek, eenvoudig recherchewerk, verlenen van hulp en handhaven van wetten en regels'* zijn geen procesbeschrijvingen aangetroffen waarin is opgenomen op welke wijze de zorg voor het voldoen aan de criteria voor deze informatie dient plaats te vinden. Dat wil niet zeggen dat er iets niet goed gaat. Algemene procesbeschrijvingen met betrekking tot art 8 en 9 onderzoeken zijn er wel.

Aandacht voor kwaliteitscriteria van informatie wordt vooral gegeven in de basisteams en is een lijnverantwoordelijkheid. Er wordt op gestuurd door de assistent team chefs; die controleren de informatie op kwaliteitscriteria. Verder vindt er in BVH een controle plaats op personalia met behulp van GBA. Voorts vindt er in het systeem een beperkte check plaats op juistheid en volledigheid. Tot slot komt de Afdeling analyse en beheer in actie bij geconstateerde onjuistheden; zij hanteert hiervoor h en geeft opdracht tot corrigeren.

In artikel 9 Wpg wordt gesproken over het *'gericht verwerken van politiegegevens ten behoeve van een onderzoek met het oog op de handhaving van de rechtsorde in een bepaald geval'*. Hiervoor zijn geen procesbeschrijvingen aangetroffen waarin is opgenomen op welke wijze de zorg voor het voldoen aan de criteria voor deze gegevens dient plaats te vinden.

Een aantal kwaliteitsaspecten wordt bij de start van het (opsporings)onderzoek, met het invullen van standaardformulieren, geborgd. Middels de MRO wordt onder andere het doel van het onderzoek vermeld. Een punt hierbij is dat recherche werk vaak zijn oorsprong/start vindt in het dagelijks politiewerk. Initieel is er dan met betrekking tot de vergaarde informatie nog geen sprake van doelbinding. Wanneer dagelijks politiewerk (art 8) opsporingswerk wordt (art 9), moet de zaak in BVO worden aangemaakt en moeten gegevens vanuit BVH naar BVO worden getransporteerd. Technisch vormt dit een probleem. Het overzetten dient derhalve nog handmatig te gebeuren. Door deze arbeidsintensieve handeling komt het voor dat een opsporingsonderzoek in BVH wordt afgerond.

De juistheid en volledigheid van informatie wordt niet automatisch in het systeem gecontroleerd. De privacyfunctionaris heeft geen overzicht van meldingen en sluitingen van onderzoeken. Medewerkers verzamelen veelal zoveel mogelijk informatie voor het onderzoek maar houden zich hierbij doorgaans niet bezig met de aspecten ter zake dienend en niet bovenmatig. Er is ook geen middel voor handen om de rechtmatigheid van gegevens te toetsen.

Voor wat betreft de herkomst en wijze van verkrijging van informatie (Wpg art 3.4) geldt een analoge situatie als boven gemeld. Ook hiervoor zijn geen specifieke procedurebeschrijvingen en werkinstructies.

Artikel 10 'verwerken van politiegegevens met het oog op het verkrijgen van inzicht in de betrokkenheid van personen bij bepaalde ernstige bedreigingen van de rechtsorde' en artikel 12 informatie 'verwerken van politiegegevens met het oog op controle op en het beheer van een informant alsmede de beoordeling en verantwoording van het gebruik van informantgegevens' wordt vooral verwerkt bij de CIE en de RID. Hier wordt aan de kwaliteitsaspecten, vanwege de bijzondere aard van hun taken, specifiek aandacht besteed. Daarbij is in de opzet voldaan aan deze criteria. Bij de CIE vanwege de toezichthoudende rol van het OM (de CIE OvJ) en het landelijk gebruik van het proceshandboek, regeling CIE en instructie CIE OvJ. De teamchef van de CIE controleert alle inkomende informatie op de kwaliteitsaspecten. Ook de RID maakt gebruik van een proceshandboek specifiek voor het regiokorps. De ruimtes van de CIE en de RID zijn

De Infodesk behandelt de aanvragen voor ter beschikking stellen en verstrekkingen. Zij krijgen de aanvragen binnen via een vaststaand format waar nadrukkelijk naar het doel gevraagd wordt. Voor de medewerkers van de Infodesk zijn procesbeschrijvingen beschikbaar.

Voor het aspect beveiliging van informatie (Wpg art 4.3) is van belang dat ook

Deze worden ook

Het

heeft wel tot gevolg dat schoning en bewaring niet is gewaarborgd en dat het delen van gegevens, een doelstelling van de Wpg, niet gerealiseerd kan worden. Momenteel wordt gewerkt aan de installatie

Daarop dient dan alle politie informatie te worden geplaatst die niet in BVH en BVO kan worden verwerkt.

4.3.3 Verbeterpunten

- Stel procesbeschrijvingen op voor art. 8 en art. 9 informatie om de kwaliteitsaspecten te kunnen toetsen.
- Beperk de vastleggingen van politiegegevens in de kantoorautomatisering.

4.4 Gevoelige gegevens (artikel 5)

4.4.1 Norm

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

4.4.2 Bevindingen

Er zijn geen procesbeschrijvingen aangetroffen waarin is opgenomen op welke wijze de zorg voor het voldoen aan de criteria voor de verwerking van gevoelige gegevens dient plaats te vinden. Uit de interviews is gebleken dat een aantal geïnterviewden niet op de hoogte is van het feit dat gevoelige gegevens alleen opgeslagen mogen worden indien er een noodzaak voor is. Niettemin geeft men aan en blijkt ook uit de interne audit dat gegevens over afkomst, ras, godsdienst of seksuele- of politieke voorkeur zelden worden geregistreerd. Slechts een beperkt deel doet dit op regelmatige basis. Een bijkomend aspect bij deze gegevens is dat deze veelal niet actief worden verzameld, maar daar waar zij gevonden worden, worden die meegenomen zonder dat er een onderscheid is in de verwerking.

4.4.3 Verbeterpunten

Draag zorg voor implementatie van procedures/instructies voor de verwerking van gevoelige gegevens.

4.5 Autorisatie (art 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 dient de verantwoordelijke zorg te dragen voor een schriftelijke vastlegging van de toekenning van autorisaties (protocolplicht).

4.5.2 Bevindingen

De bestaande autorisatie matrix bij IJsselland dateert van 10 januari 2006 en is na vaststelling niet meer geactualiseerd. De matrix bevat bijvoorbeeld functies die niet meer binnen de organisatie voorkomen en later toegevoegde functies komen op deze lijst niet voor. De matrix wordt inmiddels ook gebruikt voor toetsing van aangevraagde en afgegeven autorisaties. Voor het autorisatieproces zou gebruik worden gemaakt van een zogenaamde autorisatie server (ABS). Die is echter landelijk op "hold" gezet en niet geïmplementeerd.

Het afgelopen jaar is veel in het werk gesteld om het autorisatie proces op orde te krijgen. Nu is er een Handboek autorisatie politie dat officieel op 6 oktober 2009 is vastgesteld door de korpsleiding. Men krijgt pas een autorisatie als diverse procedures zijn doorlopen. Verder is er een autorisatiebeheerder aangesteld binnen de afdeling analyse en beheer, die ook verantwoordelijk is voor beheer en schoning.

Wijzigingen in autorisaties worden alleen doorgevoerd na schriftelijke toestemming van een leidinggevende. De functies waaraan de autorisaties zijn gekoppeld, komen uit t
beheerder
-aadpleegd. Op basis van signaleringslijsten zijn de in- en uitdiensttredingen zichtbaar en worden autorisaties aangepast. Een voorwaarde

voor de juistheid en volledigheid van de autorisaties is dat 'rolledige en juiste gegevens moet bevatten van de medewerkers van het korps, inclusief inhuurkrachten en stagiairs. Belangrijk hierbij is de tijdigheid van aanpassingen in het systeem. Het proces om autorisaties te verwijderen of aan te passen als gevolg van uitdiensttreding of functiewijziging is in opzet inmiddels verbeterd. Bij de autorisatiebeheerder worden alle mutaties ingeleverd en getoetst.

II

Gebruikelijk is dat proceseigenaren periodiek een controle uitvoeren op de toegekende autorisaties en de resultaten hiervan rapporteren aan de privacyfunctionaris. Uit de gesprekken is naar voren gekomen dat dit niet heeft plaatsgevonden. Vanuit het korps worden verder geen autorisatieoverzichten opgevraagd om de toebedeelde autorisaties te controleren. Wel vindt er jaarlijks een accountantscontrole plaats waarbij op basis van steekproeven wordt gecontroleerd of het autorisatieproces wordt gevolgd. Ook door de privacyfunctionaris wordt nauwelijks controle op de autorisaties uitgevoerd en worden geen rapportages opgeleverd. Inmiddels worden de wekelijks door VtsPN aangeleverde mutatie overzichten door de autorisatiebeheerder gecontroleerd. Afwijkingen worden doorgenomen met de IBF.

In de interne audit is voorts vastgesteld dat het autorisatieproces in de huidige situatie niet op gelijke wijze wordt uitgevoerd waardoor een centraal overzicht en controle op verleende autorisaties wordt bemoeilijkt.

Ook tussentijds vindt geen controles plaats op afwijkingen. Alleen op het moment dat een mutatie bekend is en in ieder geval maandelijks aan de hand van een uit afkomstige lijst van "medewerkers-uit-dienst" worden autorisaties aangepast dan wel beëindigd. Tot slot is het intranet autorisatieformulier aangepast; daarom behoeft voor een aantal applicaties niet meer op andere wijze autorisatie te worden aangevraagd.

Autorisatieaanvragen worden gedurende 2 jaar bewaard en daarna Hiermee voldoet het autorisatiesysteem aan de vereisten van zorgvuldigheid en evenredigheid.

II

Autorisaties voor medewerkers van de CIE en RID worden toegekend door het hoofd van de CIE respectievelijk RID. De CIE OvJ heeft de autorisaties bij de CIE goedgekeurd.

Protocolgegevens worden conform de richtlijnen bewaard.

4.5.3 *Verbeterpunten*

- Zorg voor een procedure waarin personeelsmutaties adequaat worden verwerkt, zodat wijzigingen in de autorisaties direct kunnen worden opgepakt.
- Zorg voor een structurele controle van de toegekende autorisaties.

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

4.6.1 *Norm*

Voor het onderzoek kunnen politiegegevens die voor dat onderzoek zijn verwerkt, geautomatiseerd worden vergeleken met andere politiegegevens (GV) 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 (ICMEV), worden van die verwerking nader genoemde gegevens vastgelegd (protocolplicht).

4.6.2

Bevindingen

Deze activiteit wordt met name uitgevoerd door , team Analyse en Beheer, alsmede door bij de CIE en RID. Vragen naar de opzet van de verwerking van politiegegevens conform deze richtlijnen worden in het algemeen met grote omzichtigheid tegemoet getreden. Het is een onderwerp dat slechts bij weinig geïnterviewden bekend lijkt. Waar bekendheid met deze begrippen uit de Wpg aanwezig is, is direct de vraag aan de orde waar de grenzen van GV en ICMEV liggen en op welke wijze daarmee dan in de praktijk moet worden omgegaan. Dit onderwerp is nu nog niet goed geregeld en is zeker een aandachtspunt. Door het toebedelen van een prominente rol aan Analyse en Beheer voor informatie buiten de CIE en de RID is het wel meer beheersbaar geworden. Definities zijn nog in onderzoek en dat geldt ook voor de protocollering van deze verwerkingen alsmede de bewaring ervan. Met de privacyfunctionaris wordt hierover gepraat.

III

Geautomatiseerd vergelijken gaat altijd in opdracht van de teamleider, die bevoegd functionaris is. In de voorfase van de keuze van onderzoeken wordt vaak ook aan een vorm van ICMEV gedaan. De Wpg is niet helder hoe daarin moet worden gehandeld. Het verkrijgen van toestemming van het bevoegd gezag (OM) vindt bij ICMEV niet altijd plaats.

Het geautomatiseerd vergelijken van politiegegevens die worden verwerkt op grond van artikel 8, 9 of 10 met andere politiegegevens wordt uitgevoerd door de afdeling Analyse en Beheer, bijvoorbeeld bij een TGO. Zij dragen ook zorg voor protocollering van de gegevens.

4.6.3

Verbeterpunten

- Stel procesbeschrijvingen op waarin is aangegeven hoe bij GV en ICMEV moet worden gehandeld.
- Ontwikkel casuïstiek voor het geautomatiseerd vergelijken en in combinatie met elkaar verwerken van politiegegevens.

4.7

Bewaartermijnen (art 14)

4.7.1

Norm

Politiegegevens worden vernietigd zodra zij niet langer noodzakelijk zijn voor de uitvoering van de dagelijkse politietaken (art 8) en worden in ieder geval uiterlijk vijf jaar na de datum van eerste verwerking verwijderd.

Politiegegevens die niet langer noodzakelijk zijn voor het doel van het onderzoek, worden verwijderd, of worden gedurende een periode van maximaal een half jaar verwerkt teneinde te bezien of zij aanleiding geven tot een nieuw onderzoek als bedoeld in artikel 9 of een nieuwe verwerking als bedoeld in artikel 10, en na verloop van deze termijn worden verwijderd.

4.7.2

Bevindingen

De landelijke systemen zoals BPS, BVH en BVO zijn niet voorzien van beheersmaatregelen op het gebied van termijnen voor het automatisch verwijderen en vernietigen van politiegegevens. Het is in BVH en BPS niet mogelijk informatie na 1 jaar achter een schot te plaatsen zodat deze informatie niet meer kan worden geraadpleegd. Onlangs is voor BVH een nieuwe release opgeleverd die automatische schoning zou moeten ondersteunen. Het advies van de landelijk projectleider Wpg is echter om deze release niet toe te passen vanwege de kennelijk ongewenste effecten die dit oproept. Dat is bij IJsselland dan ook niet gebeurd.

De schoning van BVH conform de Wpg regels (1/5/5 jaar BVH en 5/5 jaar BVO) is bij IJsselland dan ook niet op orde. Procedures voor het handmatig schonen en vernietigen van politiegegevens conform de bewaartermijnen artikel 8 en 9 Wpg Wpg zijn bij IJsselland niet aanwezig. Iedere executieve kan in BVH tot 5 jaar terug informatie opvragen. Mede om te voorkomen dat informatie zou worden verwijderd waarvan dat niet de bedoeling is, wordt er op de landelijke systemen geen schoning toegepast.

In BVO worden registraties gesloten €

Gezien de ingebruikname zal verwijdering na 5 jaar op zijn vroegst in 2013 plaatsvinden.

Er is hier echter geen sprake van vernietiging.

De teamleiders moeten de zaak bij de functioneel beheerder afmelden. De functioneel beheerder heeft vanuit zijn functie een signalerende rol, maar uiteindelijk is de naleving van de bewaartermijnen niet de verantwoordelijkheid van de functioneel beheerder. Het is ook via maandelijkse management/ rapportages te zien of er mutaties in een zaak hebben plaatsgevonden. Bij het ontbreken van mutaties worden vragen gesteld en op de bewaartermijnen gewezen.

Het politievstelsel BPS is alleen nog toegankelijk voor

Er heeft geen

schoning plaatsgevonden op de politiegegevens in BPS. Er is sprake van politiegegevens die volgens de Wpg vernietigd hadden moeten zijn. Op het moment dat een medewerker toegang wil tot deze gegevens is hiervoor toestemming van het bevoegd gezag vereist. De privacyfunctionaris heeft in dit proces een controlerende rol.

Er is geen procedure voor hernieuwde verwerking van gegevens (Wpg art 14.3). Vanuit het korps is een concreet verzoek aan de privacyfunctionaris gedaan om hier naar te gaan kijken. Bij hernieuwde verwerking heeft de bevoegd functionaris van dat onderzoek een rol. De bevoegd functionaris zal dan samen met het Openbaar Ministerie bekijken of de informatie opnieuw zal worden geopend voor hernieuwde verwerking. Het OM dient dan toestemming te verlenen. Het is dan ook aan de bevoegd functionaris die in eerste aanleg toetst of er voldoende aanleiding is voor hernieuwde verwerking. Dit heeft zich in de afgelopen 3 jaar 3 keer voorgedaan.

Gegevens die in de kantoorautomatisering zijn opgeslagen vallen buiten beeld. Controle op de bewaartermijnen en vernietiging vindt hierop niet plaats. Er is geen totaaloverzicht van wat er in die omgeving is opgeslagen.

verstrekkingen, worden waarschijnlijk niet gescand. Uit de gesprekken is wel naar voren gekomen dat de kennis van de bewaartermijnen en vernietiging vaak wel aanwezig is. Op het gebruik van is onvoldoende grip. Omdat BVO manco's kent wordt er door de verwerker informatie

Eigenlijk zou de informatie vervolgens moeten worden gehaald. Dit heeft alles te maken met gedrag. Je kunt hier alleen grip op krijgen door steekproeven uit te voeren. Een dergelijk steekproef is wel eens uitgevoerd door de interne auditor.

In het handboek CIE en RID (artikel 10 Wpg) is wel aandacht geschonken aan deze onderwerpen.

Hierdoor wordt niet volledig voldaan aan de eisen die de Wpg stelt aan bewaartermijnen en vernietiging.

4.7.3 *Verbeterpunten*

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

4.8 **Ter beschikking stellen (art 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*

Verzoeken om politiegegevens komen bij de front office van de Infodesk binnen. Gaat het om interne verzoeken dan is het een ter beschikking stelling is het een extern verzoek dan betreft het een verstrekking. Indien de vragende organisatie niet bekend is dan volgt eerst overleg met het hoofd Infodesk.

Artikel 8 informatie wordt gewoon verstrekt. Alleen afwijkingen worden eerst aan het hoofd infodesk voorgelegd. De ter beschikking stellingen worden geprotocolleerd verstrekt en de vastlegging bevindt zich in (). Ter beschikking stellingen vinden altijd plaats via () zodat het tijdstip en aan wie de informatie is verstrekt vaststaat. De ontvanger moet bekend zijn binnen de politieorganisatie. Telefonische ter beschikking stellingen vinden niet plaats. II

De () wordt gebruikt voor het ter beschikking stellen van politiegegevens. Functioneel beheer maakt zelf geen overzichten maar autoriseert wel medewerkers om dit zelf te doen. Afhankelijk van de functie krijgt een medewerker een autorisatieniveau. Op basis van deze niveaus kunnen bepaalde overzichten worden gecreëerd. () echter niet Wpg compliant. Een handig persoon kan met behulp van () operationele informatie ouder dan vijf jaar extraheren. Tevens is gebleken dat besloten registraties uit BVH via () inzichtelijk kunnen worden gemaakt, bijvoorbeeld zedenzaken.

Doordat geautoriseerde medewerkers zelf overzichten maken heeft functioneel beheer geen zicht op welke politiegegevens inzichtelijk worden gemaakt en met welke doeleinden. II

Aangegeven is dat () op korte termijn WPG proof wordt gemaakt. () kunnen dan alleen nog informatie zien tot 1 jaar oud. Informatie ouder dan 1 jaar is niet meer toegankelijk.

Bij ter beschikking stelling van informatie op basis van artikel 9 en 10 wordt toestemming gevraagd van de eigenaren van de informatie. De (assistent-)teamchefs zijn als bevoegd functionaris uiteindelijk verantwoordelijk voor het ter beschikking van politiegegevens. Zij hebben ook een opleiding Wpg gehad toegespitst op de rol van bevoegd functionaris. De teamleiding protocolleert het dan in BVH of BVO door middel van mutatiecodes. Pas na de toestemming van het hoofd Infodesk en vanuit de functie als Bevoegd Functionaris wordt de informatie vrijgegeven voor verzending.

Wanneer vragen of twijfels zijn over het ter beschikking stellen, worden deze voorgelegd aan de privacyfunctionaris. Voor het ter beschikking stellen van politiegegevens is er een (). Dit is een applicatie die over een aantal II

politie organisatie. Daarna is niet duidelijk waar die informatie blijft. In principe ligt de verantwoordelijkheid echter bij de convenantpartners.

De RIEC werkwijze is schriftelijk uitgewerkt en altijd dient bij het verzoek om informatie het doel te worden vermeld. Verstrekkingen worden net als de ter beschikking stellingen verstrekt. Om te voorkomen dat de maximale opslagcapaciteit wordt bereikt worden ook in

II

De feitelijke verstrekking aan het RIEC doet de Infodesk; het RIEC is een regionale instelling waarin gemeenten, politie en ook bijvoorbeeld de FIOD samenwerken. Veelal gaat het om aanvragen van vergunningen bij de gemeente waarbij het noodzakelijk is om informatie van de politie te ontvangen over de aanvrager. Dit geldt uiteraard ook voor de FIOD als het om economische delicten gaat. De verstrekkingen vinden plaats via de contactpersoon bij het RIEC en vallen onder de convenanten; deze worden op zichzelf niet als echt helder en inzichtelijk gekwalificeerd.

CIE informatie

CIE informatie wordt over het algemeen niet gedeeld tenzij. In het geval dat mondeling informatie wordt verstrekt vindt protocollering plaats. De tekst van het PV wordt hierbij vastgelegd. Politiegegevens worden vrijelijk verstrekt aan opsporingsdiensten buiten de politie, bijvoorbeeld het FIOT.

II

Tevens wordt informatie verstrekt aan:

- Kamer van Koophandel, dit gebeurt alleen met toestemming van de CIE officier;
- CIOT;
- Ouwe aiD;
- Bijzondere opsporingsdiensten.

Voor verstrekking is toestemming nodig van de CIE officier. Er dient te worden vastgelegd waarom politiegegevens worden verstrekt, wat er wordt verstrekt, wanneer dit plaatsvond en wat er mee is gebeurd. Dit laatste punt blijkt in de praktijk soms moeilijk toetsbaar.

Aan interne teams wordt informatie via een proces verbaal verstrekt. Als er dan samenwerking plaatsvindt met andere partijen kan op basis van het PV informatie worden verstrekt.

Convenanten

Momenteel wordt een onderzoek uitgevoerd naar convenanten als vervolg op een onderzoek dat in 2009 is uitgevoerd. Hierbij wordt een heel erg verschillend beeld waargenomen. Grote convenanten zijn doorgaans op orde, maar aan de kleinere convenanten mankeert nogal het een en ander. Er is geen grip op volledigheid. Wat aangeleverd wordt, is in beheer genomen. Als er nieuwe convenanten worden gemaakt, wordt de Wpg (besluit art 20) bij het opstellen van deze convenanten direct meegenomen.

Het zwaarwegend algemeen belang is als grondslag voor verstrekking in de convenanten opgenomen. Andere elementen zoals doelbinding zijn wel verankerd in de organisatie al is de doelbinding bij de een beter verzorgd dan bij de ander.

Voor de geautomatiseerde verstrekkingen aan het ... hulp is geen apart convenant aanwezig. Periodiek wordt een programmaatje (query) gedraaid over BVH. Op basis hiervan wordt dagelijks informatie met relevante informatie.

III

De privacyfunctionaris gaat te zijner tijd sturen op de convenanten via centralisering. De privacyfunctionaris heeft een procesbeschrijving voor

convenanten opgesteld. Het model convenant en art. 20 besluit worden op korte termijn afgerond.

Veiligheidshuis

In het Veiligheidshuis vindt informatie verstrekking plaats op uiteenlopende gebieden als III
Voor het beheer en autorisatie is een externe partner ingehuurd. Het Veiligheidshuis is geen entiteit. Het Veiligheidshuis lift mee met convenanten die liggen onder andere thema's. Sommige partners komen vaak terug, en daarom wil het korps nu kijken of bepaalde zaken in convenanten ontbreken in deze overleggen.
Woningcorporaties zijn incidenteel betrokken bij de casus overleggen, maar daar ligt geen convenant onder. De reden is dat een bepaalde woningcorporatie misschien maar twee keer per jaar een casus heeft. Hierdoor is een convenant praktisch gezien niet werkbaar.

Veel verstrekkingen lopen via een contactpersoon regionaal die over de doelgroepen gaat, ook wel portefeuillehouders genoemd. Ook kan het voorkomen dat informatie in sommige gevallen rechtstreeks via de wijkagent gaat. Geheimhoudingsplicht wordt altijd benadrukt bij een verstrekking per mail. Een structurele verstrekking is bijvoorbeeld de informatiestroom die naar gemeente gaat. Er is een afspraak onder deze verstrekking, maar of dit een convenant is, is niet bekend.

Politiegegevens over personen in II
wordt vanuit de politie, via het veiligheidshuis geleverd aan de gemeente. In II staan NAW gegevens, geboortedatum en aantal meldingen. Dit is een redelijk structurele verstrekking.

Verstrekkingen worden niet altijd geprotocolleerd. Er wordt altijd benadrukt dat men zorgvuldig met gegevens om moet gaan. De mails met verstrekte informatie worden bewaard.

Bij het Veiligheidshuis is men niet bekend met de weigeringsgronden voor het verstrekken van informatie.

4.9.3

Verbeterpunten

- Zorg voor beheersmaatregelen die gericht zijn op een volledige registratie van verstrekkingen door middel III
en andere vastleggingen.
- Controleer of verzonden verstrekkingen III
en Infodesk tijdig worden geschoond.
- Zorg voor een adequaat en centraal beheer van convenanten.

4.10

Rechten van betrokkenen (art 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

Hiervoor is een eigen, niet de landelijk, procedure aanwezig. De procedure Rechten betrokkenen is vastgesteld en goedgekeurd. Er wordt niet heel veel gebruik van gemaakt. Per week druppelt een aantal aanvragen binnen. De privacyfunctionaris is daarmee belast. Er is inmiddels een achterstand ontstaan in de afhandeling van verzoeken recht op kennisneming en rechten betrokkenen. De achterstand loopt terug tot maart 2011. De projectleider Wpg heeft het aanspreekpunt in het RMT over de achterstand geïnformeerd. Er zouden maatregelen worden genomen om dit

probleem op te lossen. Tot nu toe is de bestuurlijk voorgeschreven afhandelings termijn gehaald.

De geïnterviewde beleidsmedewerker heeft uitgesproken nog niet te hebben meegemaakt dat gegevens na inzage van rechten van betrokkene gecorrigeerd moesten worden.

4.10.3 *Verbeterpunten*

- Tref maatregelen om de achterstand in afdoening verzoeken recht op kennisneming van betrokkenen af te doen.

4.11 **Protocolplicht (art 32)**

4.11.1 *Norm*

De verantwoordelijke draagt zorg voor de schriftelijke vastlegging van:

- de doelen van art. 9 onderzoeken;
- gegevens die op grond van ondersteunende taken worden vastgelegd (art. 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, ten minste tot de datum waarop de laatste controle (audit) is verricht.

4.11.2 *Bevindingen*

Er bestaat landelijk onduidelijkheid over de Wpg definities, dit maakt het protocolleren lastig. Met betrekking tot bovengenoemde schriftelijke vastleggingen is het volgende geconstateerd:

- De privacyfunctionaris heeft geen inzicht in de doelen van onderzoek art 9. Hij heeft ook geen inzicht in de aangemelde MRO's. II
functioneel beheerder.
- De Landelijke art. 13 protocollen zijn klaar, deze worden in het land uitgedragen en dienen voor elk korps te worden ingevuld en afgetekend te worden. Reglementen die in 13.1 staan zijn opgesteld. Controle op protocollering gebeurt nog niet.
- De verzoeken voor het toekennen van autorisaties (art 6) worden naar de privacyfunctionaris gestuurd ter kennisneming.
- Er vindt geen controle plaats met betrekking tot het in combinatie verwerken. De definities worden nog niet eenduidig binnen het korps gehanteerd.
- Geautomatiseerde vergelijking van gegevens met openbare bronnen is bij de privacyfunctionaris tot op heden nog niet gemeld; controle heeft dan ook niet plaatsgevonden.
- Zicht op het voorkomen van hernieuwde verwerking is bij de privacyfunctionaris op dit moment niet aanwezig.
- De privacyfunctionaris heeft nog geen informatie verstrekt met als reden dat de veiligheid van de staat in het gedrang was.
- Er is een procedure incidentenregistratie. Incidenten worden gemeld bij de

Deze worden of zelf afgehandeld door de dan wel voorgelegd aan de directie III

met verzoek tot het nemen van een besluit. Jaarlijks wordt een managementrapportage beveiligingsincidenten annex onrechtmatige handelingen vastgesteld.

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

4.12 Audits (art 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

Bij IJsselland heeft een interne auditfunctionaris met een stagiair en een medewerker van de afdeling Analyse en Beheer in het vierde kwartaal 2010 een audit Wpg uitgevoerd. Namens de verantwoordelijke, de korpsbeheerder, werd door de directeur Besturing en Ondersteuning opdracht gegeven tot de uitvoering van deze pré-audit. Doel hiervan was de beoordeling van de opzet en het bestaan van maatregelen en procedures die in de borging van de wettelijke eisen moeten voorzien en de werking van de getroffen maatregelen en procedures. De audit moest inzicht geven in de eigen sterke en zwakke punten. Tevens was de audit bedoeld als input voor de externe audit.

De audit bestond uit 3 delen.

- 1 Een geautomatiseerde vragenlijst ten behoeve van een actueel beeld op de toepassing van de Wpg.
 - 2 De toetsing van de uitvoering van de eerdere besluitvorming door IJS op het gebied van de Wpg met als centrale onderwerpen de toegangsautorisatie, de verstrekking en bewaring van gegevens.
 - 3 De actuele situatie rond ANPR in relatie tot onderzoek van het CBP.
- De audit heeft een actueel beeld opgeleverd op de toepassing van de Wpg binnen de politie IJsselland en er zijn waar relevant aanbevelingen gedaan.
- De uitkomsten van deze pré-audit zijn in de (externe) audit van de DAD van het ministerie van Veiligheid en Justitie betrokken.

Een auditplan voor in de toekomst uit te voeren audits hebben wij niet aangetroffen.

4.12.3 Verbeterpunten

- Geef in de interne meerjaren auditplanning een plaats aan de audit Wpg.
- Zorg voor een structurele borging van de interne auditfunctie op de Wpg.

4.13 Privacy functionaris (art 34)

4.13.1 Norm

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

4.13.2 *Bevindingen*

De privacyfunctionaris is formeel aangesteld door de Korpschef en aangemeld bij het CBP. Over 2010 is er geen jaarverslag opgesteld. Het ligt in het voornemen om dat over 2011 wel uit te brengen. De privacyfunctionaris voert o.a. de volgende taken uit:

- Het opleiden van medewerkers aan de hand van *III*
- Het behandelen van verzoeken tot verstrekking van politiegegevens;
- Ondersteuning bieden aan de projectleider Wpg.

Vanwege de beperkte inzetbaarheid van de privacyfunctionaris krijgt het uitvoeren van de toezichthoudende taak van de privacyfunctionaris momenteel niet tot nauwelijks invulling. Tijd om daadwerkelijk toezichthoudende activiteiten uit te voeren in het veld is er daardoor niet. Wel tracht de privacyfunctionaris waar mogelijk controle uit te oefenen, bijvoorbeeld door in de wandelgangen logging gegevens op te vragen. Op het moment dat medewerkers geen goed antwoord hebben of geen bewijsmateriaal kunnen overleggen verricht de privacyfunctionaris nader onderzoek.

4.13.3 *Verbeterpunten*

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

4.14 **Functionaris Gegevensbescherming (art 36)**

Die functie komt bij IJsselland niet voor. Taak elementen van die functie zijn nu gekoppeld aan de Interne Beveiligings Functie.