



Ministerie van Veiligheid en Justitie

Audit Wpg politie Utrecht

Rapport

Datum
Status

10 januari 2012
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
M wpg@minvenj.nl

Projectnaam

Audit Wet Politiegegevens

Ons kenmerk

DDS/5719701/11

Auteur

Inhoud

Colofon 3

1 Assurance Verklaring 7

2 Samenvatting 9

3 Inleiding 20

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

4 Bevindingen 23

- 4.1 Inleiding 23
- 4.2 Verantwoordelijke (artikel 1.f) 24
- 4.3 Kwaliteitsaspecten van politiegegevens (artikel 3 en 4) 24
- 4.4 Gevoelige gegevens (artikel 5) 29
- 4.5 Autorisatie (artikel 6) 29
- 4.6 Geautomatiseerd Vergelijken (GV)/In Combinatie Met Elkaar Verwerken (ICMEV)(artikel 11) 32
- 4.7 Bewaartermijnen (artikel 14) 34
- 4.8 Ter beschikking stellen (artikel 15) 37
- 4.9 Verstrekken (artikel 16/24) 39
- 4.10 Rechten van betrokkenen (artikel 25/28) 42
- 4.11 Protocolplicht (artikel 32) 44
- 4.12 Audits (artikel 33) 46
- 4.13 Privacyfunctionaris (artikel 34) 46
- 4.14 Functionaris Gegevensbescherming (artikel 36) 47

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 juni en december 2011 is een privacy audit uitgevoerd bij het korps Utrecht.

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 Utrecht.

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

Den Haag, 10 januari 2012

De Directeur van de Departementale Auditdienst

I

2 Samenvatting

Het korps Utrecht heeft een aantal zaken in opzet opgepakt, zoals een convenanten databank en een interne audit functie. De korpsleiding toont hiermee en met andere initiërende activiteiten haar aandacht aan voor de Wpg.

Niettemin voldoet het door ons beschouwde stelsel van maatregelen nog niet in opzet, bestaan en werking aan de vereisten van de Wpg.

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

Criteria:

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

Norm	Aspect	Bevinding en oordeel
Artikel 1.f, Verantwoordelijke		
1.f	Mandaatbesluit	Er is een mandaatbesluit Wet politiegegevens politie Utrecht waarin de korpsbeheerder zijn mandaat verleent aan de onderscheiden functionarissen/functiegroepen van de politie Utrecht. Hiermee wordt voldaan aan de Wpg.
Artikel 3 en 4, Kwaliteitsaspecten van politiegegevens		
8.1 en 9.1	Onderscheid onderzoek Dagelijkse Politietask (8) versus Bepaald geval (9)	Op Intranet is de 'Beslisboom Wet Politiegegevens' beschikbaar, op basis waarvan kan worden nagegaan onder welk artikel de betreffende politiegegevens dienen te worden verwerkt en onder welk regime een onderzoek valt. Medewerkers zijn door middel van presentaties, e-Learning en workshops geïnformeerd over de criteria voor het onderscheid tussen artikel 8 en artikel 9 gegevensverwerkingen. Hiermee wordt voldaan aan de Wpg.
3.1 t/m 3.3 (8) 4.1 (8)	Noodzakelijkheid (8) Doelbinding Rechtmatigheid Juistheid Volledigheid	Het korps Utrecht gebruikt TrueBlue voor bewaking van de kwaliteit van een aantal velden in BVH. Binnen het korps zijn alle wijkteams en wijkchefs door middel van een presentatie over de Wpg opgeleid. Medewerkers worden op basis van de handreiking verstrekkings en op basis van de werkinstructies BVH en HKS gewezen op de kwaliteitsaspecten. Tevens vindt een kwaliteitscontrole plaats door de medewerkers van de unit gegevensbeheer BVH van de afdeling informatiebeheer. Blauw geeft aan dat er voor leidinggevendenden Wpg-bijeenkomsten zijn georganiseerd maar dat de medewerkers op straat nog te weinig Wpg kennis hebben. De documentatie op intranet wordt beperkt

			geraadpleegd. Hiermee wordt deels voldaan aan de Wpg.
3.1 t/m 3.4 (9) 4.1 (9)	Noodzakelijkheid (9) Doelbinding Rechtmatigheid Herkomst en wijze van verkrijging Juistheid Nauwkeurig Volledigheid		Het rechteproces bevat waarborgen voor de kwaliteitsaspecten van artikel 9 gegevens. De PDCA-cyclus sluit via het OM en de rechter. Binnen artikel 9 verwerkingen bieden de regels van Strafvordering een extra waarborg voor dit vereiste. Voor het opsporingsproces zijn geen procesbeschrijvingen opgesteld. Wel hebben medewerkers toegang tot de beslissboom Wpg en meldingsformulieren artikel 9. Hierin zijn de kwaliteitsaspecten slechts beperkt opgenomen. Het niveau van Wpg kennis is bij de districts-rechercheurs nog beperkt. Dit heeft er nog niet toe geleid dat er zaken stuk zijn gelopen op de Wpg. Hiermee wordt deels voldaan aan de Wpg.
3.4 (10 en 12) 4.1 (10 en 12)	Noodzakelijkheid (10 en 12) Doelbinding Rechtmatigheid Herkomst en wijze van verkrijging Juistheid Nauwkeurig Volledigheid		Bij de CIE en RID zijn de kwaliteitscriteria in verband met de aard van het werk ingeregeld conform Wpg. Bij de CIE gebeurt dit volgens het landelijk proceshandboek CIE en de toezichthoudende rol van de CIE-OvJ. Het proceshandboek is Wpg proof. De aard van het werk van de RID brengt met zich mee dat bij het vastleggen van informatie veel aandacht is voor het voldoen aan de kwaliteitseisen. De CIE-OvJ van het OM is verantwoordelijk voor het voldoen van de CIE aan deze kwaliteitseisen. Hiermee wordt voldaan aan de Wpg.
4.3	Beveiliging		De landelijke informatiesystemen zijn nog niet Wpg-proof. Binnen het korps is een quickscan op de regionale applicaties uitgevoerd. Hierbij is onderzocht of ze Wpg compliant zijn. Het merendeel van de applicaties is niet Wpg compliant. Politiegegevens worden ook op persoonlijke en afdelingsmappen opgeslagen. Het is niet mogelijk om na te gaan of er politiegegevens op persoonlijke mappen staan. CIE- en RID-informatie is binnen het korps voldoende beveiligd. Een beperkt aantal mensen heeft toegang tot deze locatie. Hiermee wordt niet voldaan aan de Wpg.
Artikel 5, gevoelige gegevens			
	• Gevoelige gegevens		Gevoelige gegevens worden slechts incidenteel verwerkt in aanvulling op de verwerking van andere politiegegevens en voor zover dit voor het doel van de verwerking onvermijdelijk is, conform het gestelde in artikel 5 Wpg. Er is geen procesbeschrijving hoe om te gaan met gevoelige gegevens. Hiermee wordt deels voldaan aan de Wpg.
Artikel 6, Autorisatie			

III

• Korpsautorisatiematrix		Het korps Utrecht heeft een autorisatiebeleid opgesteld waarin is beschreven hoe autorisatiematrices dienen te worden opgesteld. Het korps heeft met het opstellen van autorisatiematrices besloten te wachten tot de oplevering van het Landelijk Autorisatiemodel. Hiermee kan worden aangesloten bij een landelijke standaard en wordt het beheer centraal bij vtsPN geregeld. De verantwoordelijkheid voor autorisaties op groepsschijven is bij de desbetreffende afdelingen belegd. Hiermee wordt niet voldaan aan de Wpg.
• Aanvraagproces		Er zijn chefs (MT-leden) aangewezen die autorisaties afgeven en intrekken. Autorisaties worden verstrekt op een 'need-to-know' basis. Het autorisatieaanvraagproces is gedocumenteerd. Voor het aanvragen van autorisaties op de centrale mappen is een aanvraagformulier dat leidinggevenden gebruiken om bij vtsPN autorisaties aan te vragen. VtsPN toetst de aanvraagformulieren Hiermee wordt voldaan aan de Wpg.
• Wijziging en verwijdering		Een eenduidige procesbeschrijving ter borging van het intrekken van autorisaties bij functiewijziging of afronding van de werkzaamheden ontbreekt. Controle door leidinggevenden op uitgegeven autorisaties vindt slechts voor een beperkt aantal systemen plaats. Bij uitdiensttreding worden de autorisaties van betrokkene verwijderd op grond van het ontslagbesluit. Daarmee is onmiddellijk de toegang tot de kantooromgeving geblokkeerd, zodat vanuit deze omgeving geen toegang meer mogelijk is tot regionale of landelijke applicaties en tot schijven en mappen. Hiermee wordt deels voldaan aan de Wpg.
• Autorisatiebeheer CIE, RID		Bij de CIE en RID vindt een strak autorisatiebeheer plaats dat consequent wordt uitgevoerd. Autorisaties worden toegekend en ingetrokken door het hoofd van de betreffende eenheid, bij de CIE conform het door de OvJ goedgekeurde autorisatiebeleid. Door het hoofd van de RID zijn drie medewerkers aangewezen die conform zijn opdracht autorisaties kunnen realiseren en verwijderen. Dit is niet vastgelegd. Slechts de technische kant van het aanmaken en verwijderen van een autorisatie is beschreven. Hiermee wordt voldaan aan de Wpg.
32.1.c	Protocollering autorisaties	Functioneel beheer protocollert autorisaties. Inzake BVH vindt protocollering in de applicatie plaats. Voor BVO wordt het door functioneel beheer opgeslagen. Er is geen centraal autorisatieoverzicht.

V

			De privacyfunctionaris heeft inzicht bij welke functioneel beheerders of medewerkers een overzicht verkrijgbaar is van de actuele autorisaties. Hiermee wordt deels voldaan aan de Wpg.
32.3 voor 32.1.c	Bewaren protocolgegevens autorisaties		De logging in BVH heeft geen einddatum. De logging tenminste wordt bewaard tot na de eerstvolgende audit. Hiermee wordt voldaan aan de Wpg.
Artikel 11, Geautomatiseerd vergelijken en in combinatie zoeken			
	Hanteerbare interpretatie		Het korps heeft voor geautomatiseerd vergelijken en in combinatie zoeken definities opgesteld: - Onder geautomatiseerd vergelijken wordt verstaan het vergelijken van een concreet zoekgegeven (bijvoorbeeld een volledig kenteken, volledige personalia, concreet adres) met geregistreerde politiegegevens, waarbij het resultaat van de vergelijking relevante hits oplevert. - Onder in combinatie verwerken wordt verstaan het vergelijken met meerdere, soms onvolledige, zoekgegevens (bijv. een onvolledig kenteken, merk en kleur van een motorvoertuig) met geregistreerde politiegegevens, waarbij het resultaat ook niet-relevante hits bevat die wel worden uitgerechercheerd teneinde de relevantie vast te stellen of uit te sluiten. Deze manier van zoeken impliceert een grotere inbreuk op de persoonlijke levenssfeer van – soms grote aantallen – personen. Uit de interviews blijkt dat de medewerkers nog onvoldoende op de hoogte zijn van de gehanteerde interpretaties van het korps. Hiermee wordt deels voldaan aan de Wpg.
	Aangewezen functionarissen		De artikel 11 zoekslagen worden slechts uitgevoerd door hoofdzakelijk de medewerkers van de Regionale Infodesk en door informatiecoördinatoren uitgevoerd. De bevoegdheden uit artikel 11 Wpg (geautomatiseerd vergelijken en in combinatie verwerken) en de toedeling van deze bevoegdheden naar functies zijn vastgelegd in een matrix. Hiermee wordt voldaan aan de Wpg.
11.4	Bevoegd gezag		Het verkrijgen van een opdracht tot in combinatie verwerken o.g.v. artikel 11.4 is (nog) niet in een procesbeschrijving vastgelegd. Wel staat in de matrix met betrekking tot artikel 11 dat het bevoegd gezag betrokken dient te zijn. De CIE OvJ geeft aan dat het bevoegd gezag dient te worden benaderd alvorens een artikel 11.4 zoekslag wordt uitgevoerd. Hiermee wordt deels voldaan aan de Wpg.
32.1.d	Protocollering 11.1, 11.2, 11.4 en 11.5		Er wordt in de meeste systemen die worden gebruikt voor artikel 11 zoekslagen, gelogd (<i>BlueView</i> , <i>BVO</i> , <i>HKS</i>). De medewerkers van de afdeling

			Informatiecoördinatie (DIK's, RIK, TIO en TMSI) verzorgen de vastlegging van verstrekking of ter beschikking stelling van de resultaten van hun zoekslagen in BVO, in de module 09Infodesk. Protocolgegevens met betrekking tot GV/ICMEV-verwerkingen worden echter niet structureel vastgelegd. De privacyfunctionaris heeft toegang tot de vastlegging. Hiermee wordt deels voldaan aan de Wpg.
32.3 voor 32.1.d	Bewaren protocolgegevens 11.1, 11.2, 11.4 en 11.5		Een artikel 11 Wpg zoekactie dient te worden geregistreerd in de BVO-Infodeskmodule. Protocolgegevens met betrekking tot GV/ICMEV-verwerkingen worden echter niet structureel vastgelegd. De bewaarde protocolgegevens worden ten minste bewaard tot na de audit volgend op het moment van vastlegging. Hiermee wordt deels voldaan aan de Wpg.
Artikel 14, Bewaartermijnen			
8.2 en 8.3	(8) van 1 tot 5 jaar		BVH ondersteunt niet de levensloop van Politiegegevens. Het schoningsscript in BVH 1.2.2 staat voorlopig nog niet aan. Het korps is in afwachting van het landelijk standpunt om dit script aan te zetten. Er zijn geen maatregelen getroffen om de bewaartermijnen van informatie in de mappenstructuur conform de Wpg na te leven. Het korps is voornemens om in het voorjaar van 2012 de ordening en schoning van de schijven en mappen ter hand te nemen. Hiermee wordt niet voldaan aan de Wpg.
8.6	(8) verwijderen na 5 jaar		De regels voor de verwijdering van oude artikel 8 gegevens zijn moeilijk uitvoerbaar omdat het handmatig moet gebeuren. Binnen het korps zal in 2012 een project voor schoning van politiegegevens worden gestart. Voor BVH is verwijdering nog niet aan de orde omdat deze applicatie ruim twee jaar geleden in gebruik is genomen. In verband met de uitfasering van BPS is de toegang tot deze applicatie zeer beperkt. Er is een werkinstructie waarin de procedures voor verwijdering uit BPS staan beschreven. Hiermee wordt deels voldaan aan de Wpg.
14.1 (8)	(8) vernietigen na 5 jaar verwijderd		Er zijn geen maatregelen genomen om de vernietiging van politiegegevens te borgen. Tevens is geen inzicht in de informatie die is opgeslagen op de persoonlijke schijven en groepsschijven. Hier is ook geen beleid voor opgesteld. Hiermee wordt niet voldaan aan de Wpg
9.4	(9) verwijderen na OH plus ½ jaar		Het opschonen van artikel 9 onderzoeken gebeurt nog onvoldoende. Hierbij is de ketensamenwerking en specifiek de overdracht van informatie over

			afgesloten zaken van OM naar de politie een aandachtspunt. Het OM Utrecht is bezig om hierover duidelijkheid te verschaffen, maar dit blijkt lastig. Hiermee wordt niet voldaan aan de Wpg.
14.1 (9)	(9) vernietigen na 5 jaar verwijderd		Doordat politiegegevens niet worden verwijderd is het niet mogelijk om vijf jaar na dato de gegevens te vernietigen. Het korps is hiervoor mede afhankelijk van de terugkoppeling van het OM. Hiermee wordt niet voldaan aan de Wpg.
10.6	(10) verwijderen na 5 jaar geen subjectwaardige registratie		De CIE en de RID hebben een schoningsprocedure opgesteld. De bewaringscriteria voor controle op noodzaak is omschreven in de documentatie. Er vinden halfjaarlijkse controles plaats om er zorg voor te dragen dat politiegegevens tijdig worden verwijderd. Hiermee wordt voldaan aan de Wpg.
14.1 (10)	(10) vernietigen na 5 jaar verwijderd		Vanuit de CIE worden periodieke controles uitgevoerd waarbij ook naar de bewaartermijnen wordt gekeken. Hiermee wordt voldaan aan de Wpg.
14.3	Hernieuwde verwerking		Het korps heeft nog geen invulling gegeven aan een procedure voor het hernieuwd verwerken van politiegegevens. Hiermee wordt niet voldaan aan de Wpg.
32.1.e	Protocollering 14.3		Er is geen afzonderlijke vastlegging en geen overzicht beschikbaar. De herkomst van gegevens die worden gebruikt voor hernieuwde verwerking wordt in het artikel 9 proces-verbaal vastgelegd. Dit is geen vastlegging conform artikel 6:4 Besluit politiegegevens. Hiermee wordt niet voldaan aan de Wpg.
32.3 voor 32.1.e	Bewaren protocolgegevens 14.3		Er is geen proces voor hernieuwde verwerking. Generiek voor protocolleringen geldt: Protocolgegevens worden voor ten hoogste 4 jaar en tenminste tot na de eerstvolgende audit na het moment van vastlegging, bewaard. De vastlegging is echter niet conform Wpg. Hiermee wordt niet voldaan aan de Wpg.
12.2	(12) verwerken tot 4 maanden		Artikel 12 politiegegevens worden voor een periode van maximaal vier maanden na de datum van de eerste verwerking ter beschikking gesteld. Hier wordt door de teamleiders CIE en de CIE-OVJ op toegezien. Hiermee wordt voldaan aan de Wpg.
12.6	(12) controleren en vernietigen		De CIE en het RID zien toe op het tijdig schonen van politiegegevens in het informant register. Dit wordt halfjaarlijks gecontroleerd. Hiermee wordt voldaan aan de Wpg.
Artikel 15, Ter beschikking stellen			
• Infodesk voor bevraging			Het beschikbaar stellen van informatie verloopt veelal via de Districtelijk Informatie Knooppunt (DIK), Regionaal Informatie Knooppunt (RIK) en de afdeling Team Monitoring en Signalering Informatie (TMSI). Bij artikel 9 gegevens wordt verwezen naar

		de bevoegd functionaris, er wordt in principe geen artikel 9 informatie ter beschikking gesteld. Vanuit het korps wordt naar het stroomschema voor verstrekkingen verwezen met betrekking tot de te volgen procedures. Tevens is er sprake van informatie op persoonlijke en groepsschijven. De Infodesken hebben hier geen toegang toe waardoor zij deze informatie niet ter beschikking kunnen stellen. Hierdoor wordt informatie niet ter beschikking gesteld aan personen die dit behoeven conform artikel 15 Wpg. In de infodeskmodule is niet altijd duidelijk wie welke politiegegevens ter beschikking stelt. Hiermee wordt deels voldaan aan de Wpg.
	• Codering	Codering wordt gebruikt voor artikel 9 onderzoeken die in BVO/Summ-It worden verwerkt. Dit wordt bereikt door te kiezen voor een bepaald autorisatieniveau waarop de informatie wordt weggezet en daarmee wordt de mate van afscherming en toegang bepaald. Door middel van codering worden ook embargo-onderzoeken afgeschermd en wordt de export naar BlueView bepaald. Hiermee wordt voldaan aan de Wpg.
	• Aanwijzing bevoegde functionaris	Bevoegde functionarissen zijn op basis van functie aangewezen. Dit is vastgelegd in een door de verantwoordelijke ondertekend en gepubliceerd aanwijzingsbesluit. In dit besluit zijn de taken en bevoegdheden van de bevoegd functionaris gedocumenteerd. Hiermee wordt voldaan aan de Wpg.
	• Opleiding bevoegde functionaris	Leidinggevend (onderzoekersleiders) van de recherche-onderdelen zijn gedurende een eendaags seminar opgeleid tot onder andere bevoegde functionaris. Tevens hebben ze een handleiding ontvangen met daarin een omschrijving van de rol en taken van de bevoegde functionaris. In zowel de training als de handleiding zijn de begrippen doelbinding, doelafwijking en proportionaliteit benoemd als beoordelingscriteria. Het korps heeft nog geen proces om te borgen dat nieuwe bevoegde functionarissen worden opgeleid. Het korps heeft de politieacademie verzocht om het onderwerp "bevoegde functionaris" op te nemen in de "leergangen tactisch en operationeel leiding geven" (OLL en TLL). Hiermee wordt deels voldaan aan de Wpg.
15.2	Weigeringsgronden	Tijdens de opleiding zijn de leidinggevend ingelicht over de verplichting tot het intern ter beschikking stellen en de wettelijke weigeringsgronden. In de werkinstructie voor bevoegde functionarissen zijn de weigeringsgronden niet expliciet genoemd. Wel wordt er naar artikel 2:13 Bpg verwezen.

		Hiermee wordt deels voldaan aan de Wpg.
Artikel 16 t/m 24, Verstrekking		
• Verstrekkingenwijzer (landelijk)		De landelijke verstrekkingenwijzer is beschikbaar op alle informatieknooppunten en wijkteams. Tevens staat de verstrekkingenwijzer op Intranet en is daar voor een ieder te raadplegen. Hiermee wordt voldaan aan de Wpg.
• Proces voor convenanten		Er is een proces voor de totstandkoming van convenanten. Hierin staat onder andere beschreven wie convenanten mogen opstellen en waar op gelet dient te worden. Nieuwe convenanten dienen vóór ondertekening ter toetsing aan de privacyfunctionaris te worden voorgelegd. Bestaande convenanten worden in het voorjaar van 2012 geïnventariseerd, aan de Wpg-eisen aangepast en op intranet geplaatst. De korpsleiding heeft deze werkwijze goedgekeurd. Na een nog nader te bepalen datum zijn alleen die convenanten geldig die aan de Wpg zijn aangepast en die op intranet zijn geplaatst. Hiermee wordt deels voldaan aan de Wpg
• Proces voor Artikel 20 Besluiten		Zie "Proces voor Artikel 20 Besluiten". Binnen het korps is een voorbeeldbesluit (conform artikel 20 lid 2 Wpg) en een modelconvenant opgesteld. In het artikel 20-besluit is de geheimhoudingsplicht opgenomen. Hiermee wordt deels voldaan aan de Wpg.
• Verstrekkingenschema (regio)		Het korps Utrecht heeft geen overzicht van alle partijen aan wie lokaal mag worden verstrekt op basis van opgestelde convenanten en artikel 20 Wpg besluiten. Er is een handleiding verstrekkingen waarin staat aangegeven hoe het verstrekkingenproces is ingericht, zoals wie mag verstrekken en hoe de verstrekkingen moeten worden geprotocolleerd. De handleiding is op intranet gepubliceerd. Aan de uitvoerende eenheden is een poster beschikbaar gesteld met een beslisboom/stroomschema waar de verstrekkinggrondslagen eenvoudig zijn te raadplegen. Hiermee wordt deels voldaan aan de Wpg.
• Proces voor geautomatiseerde verstrekking		Binnen het korps Utrecht is er geen proces voor geautomatiseerde verstrekkingen. Aanvragen lopen via de CIO of de proceseigenaar Informatie. Politiegegevens worden aan het CJIB en Slachtofferhulp verstrekt. Deze twee partijen zijn toegestaan op basis van de landelijke verstrekkingenwijzer. De automatische verstrekking beperkt zich tot artikel 8 gegevens. Er wordt vanuit BVH, PSH-Transactie Module automatisch verstrekt. Door middel van logging is achteraf te bepalen over welke personen op een geautomatiseerde wijze politiegegevens zijn verstrekt. Deze gegevens zijn

			voor de privacyfunctionaris opvraagbaar. Hierdoor wordt deels voldaan aan de Wpg.
7.2	Geheimhouding		De geheimhoudingsplicht wordt expliciet vermeld in het modelbesluit, het voorbeeldconvenant en de standaard Wpg-bijlage voor bestaande convenanten. Medewerkers van de informatieknooppunten gebruiken een disclaimer waarin de geheimhoudingsplicht staat vermeld, deze wordt standaard met verstrekte gegevens meegestuurd. Hiermee wordt voldaan aan de Wpg.
32.1.f	Protocollering verstrekking		De op Intranet beschikbare 'Handleiding verstrekkingen' stelt dat verstrekkingen dienen te worden vastgelegd middels I90 formulieren of BVO verstrekkingenmutaties en beschrijft welke gegevens hierbij dienen te worden vastgelegd. In de praktijk wordt er ook via standaardbrieven en formulieren geprotocolleerd. Door de verschillende wijzen van protocollering kan het achteraf lastig zijn om te achterhalen wie wat heeft verstrekt. De privacyfunctionaris heeft een overzicht van alle verstrekkingen in BVH. Uit dit overzicht blijkt dat een aantal meldingen geen verstrekkingen zijn, maar wel als zodanig worden vastgelegd. Dit duidt op gebrekkige kennis van verstrekkingen. Het risico bestaat dat niet alle verstrekkingen juist zijn geborgd. Verstrekkingen worden niet structureel vastgelegd in de Infodeskmodule. Hierdoor wordt niet aan de protocolplicht voldaan. Hiermee wordt deels voldaan aan de Wpg.
32.3 voor 32.1.f	Bewaren protocolgegevens verstrekking		Verstrekkingen die zijn geprotocolleerd, worden bewaard in BVH dan wel BVO tot na het moment van plaatsvinden van de eerstvolgende audit. Hiermee wordt voldaan aan de Wpg.
• Toezicht door leidinggevend op verstrekkingen en protocollering			Het korps heeft geen proces voor het toezicht houden op de verstrekkingen en de daarbij behorende protocollering. Hiermee wordt niet voldaan aan de Wpg.
Artikel 25 t/m 31, Rechten van de betrokkene			
25.1	Verzoek om kennisneming		Inzageverzoeken worden binnen de daarvoor gestelde termijn afgehandeld door Bureau politiegegevens. Een verdaging wordt beperkt tot een periode van vier weken, tenzij de betrokkene niet tijdig reageert op een aanvullend verzoek om de vereiste identiteitsvaststelling te kunnen waarborgen. Er is geen proces gedocumenteerd voor de afhandeling van inzageverzoeken. Het korps Utrecht heeft een concept procedure opgesteld maar deze dient nog te worden bijgewerkt. Hiermee wordt deels voldaan aan de Wpg.
28.1 t/m 28.3 + 30.1	Correctie		Zie "Verzoek om kennisneming". 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		Het doel van artikel 9 Wpg onderzoeken wordt vastgelegd in de aanvragen voor een BVO-registratie. Bij het starten van een onderzoek wordt een Melding Recherche Onderzoek (MRO) verstuurd naar de landelijke verwijsindex VROS, onder beheer van KLPD. Deze doelen worden door leidinggevend en of de bevoegd functionarissen getoetst. De herkomst en wijze van verkrijging van informatie wordt vastgelegd in BVO als onderdeel van het onderzoeksproces. Hiermee wordt voldaan aan de Wpg.
32.3 voor 32.1.a	Bewaren protocolgegevens doel onderzoek		De MRO wordt bewaard in VROS. De protocolgegevens worden tenminste bewaard tot na de eerstvolgende audit, of zolang het onderzoek nog niet beëindigd is. Hiermee wordt voldaan aan de Wpg.
13.4 en 32.1.b	Protocollering Artikel 13 gegevensverzameling en		Ten aanzien van artikel 13 gegevensverzamelingen zijn schriftelijke vastleggingen gemaakt van de in de wet en het besluit vermelde aspecten. Voor de aanmelding van nieuwe artikel 13 gegevensverzamelingen is geen procedure vastgelegd. Er dienen nog protocollen voor geïdentificeerde systemen te worden opgesteld. In het geval van een vijftal applicaties is een uitzondering gemaakt, omdat onduidelijkheid over de vastlegging tot problemen zou kunnen leiden. Met betrekking tot deze vijftal applicaties zijn wel protocollen opgesteld conform de Wpg. De privacyfunctionaris heeft toegang tot een overzicht van artikel 13 gegevensverzamelingen en de bijbehorende protocollen. Hiermee wordt deels voldaan aan de Wpg.
32.3 voor 32.1.b	Bewaren protocolgegevens Artikel 13 gegevensverzameling en		De reglementen worden door de privacyfunctionaris bewaard, zo lang de verwerking loopt. Het korps wil deze reglementen in de toekomst via Intranet toegankelijk maken voor medewerkers, maar dit is mede afhankelijk van de ontwikkelingen landelijke politie. Hiermee wordt voldaan aan de Wpg.
32.1.g	Protocollering onrechtmatige handeling		Op vermoedens van onrechtmatige handelingen wordt vanuit het korps geacteerd. De informatiebeveiligingsfunctionaris voert deze onderzoeken uit. De procedure voor het afhandelen van onrechtmatige verwerkingen is in een protocol vastgelegd. Onrechtmatige handelingen worden door de Informatie Beveiligings Functionaris (IBF) in het incidentenregister geprotocolleerd. Hiermee wordt voldaan aan de Wpg.

32.3 voor 32.1.g	Bewaren protocolgegevens onrechtmatige handeling		Generiek voor protocolleringen geldt: Protocolgegevens worden voor ten hoogste 4 jaar en tenminste tot na de eerstvolgende audit na het moment van vastlegging, bewaard. Hiermee wordt voldaan aan de Wpg.
32.2	Gemeenschappelijke verwerking		Het korps Utrecht heeft geen gemeenschappelijke verwerkingen.
Artikel 33, Audits			
RPAP 3.1	Interne audit-functie		Het korps heeft een interne Wpg auditor aangesteld. De taken van de interne auditor zullen bestaan uit het opstellen van de planning en het auditplan, het uitvoeren en coördineren van de feitelijke audit en het opstellen van de audit-rapportage. De vanuit de RPAP voorgeschreven jaarlijkse audit heeft niet plaatsgevonden. Hiermee wordt deels voldaan aan de Wpg.
RPAP 3.4	Interne audit-plan		Er is geen vaktechnisch verantwoord en meerjarig intern Wpg audit-plan. Voor 2012 heeft het korps de intentie om naar aanleiding van de externe audit-rapportage over 2011 en het aangekondigde nieuwe normenkader een auditplan op te stellen. Hiermee wordt niet voldaan aan de Wpg.
RPAP 3.6	Interne audit-rapport		Er is geen intern Wpg audit-rapport. Hiermee wordt niet voldaan aan de Wpg.
Artikel 34, Privacyfunctionaris			
34.1 en 34.4	Benoemd en gemeld		De privacyfunctionaris is formeel benoemd en aangemeld bij het CBP. Hiermee wordt voldaan aan de Wpg.
34.2	Overzicht over protocollering		De privacyfunctionaris heeft toegang tot de aanwezige protocollering en kan hier steekproeven op nemen. In 2011 vervult de privacyfunctionaris echter nog hoofdzakelijk een adviserende functie. Door de vele werkzaamheden wordt nog zeer beperkt invulling gegeven aan de toezichthoudende rol zoals beschreven in de Wpg. Hiermee wordt voldaan aan de Wpg.
34.3	Jaarverslag		Door de vele werkzaamheden wordt onvoldoende invulling gegeven aan de toezichthoudende rol. Hiermee wordt niet voldaan aan de Wpg.
Optioneel Artikel 36, Functionaris Gegevensbescherming			
36.1 en 36.2	Benoemd		Niet van toepassing. Er is geen functionaris gegevensbescherming benoemd.
Wbp 63.3	Gemeld		Niet van toepassing.
Wbp 64.1 t/m 64.4	Toezichthoudende rol		Niet van toepassing.

I

II

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 Utrecht 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 Utrecht in 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

Doelstelling

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

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

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

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 leidinggevend van het korps Utrecht en het Openbaar Ministerie, deelwaarnemingen in de procesbeschrijvingen en andersoortige documentatie en deelwaarnemingen in informatiesystemen.

Wij hebben onze werkzaamheden uitgevoerd in de periode maart tot en met december 2011.

Het eindrapport is met inachtneming van het ontvangen commentaar vastgesteld.

3.8 Doelgroep van het rapport

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

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

De stuurgroep wordt voorgezeten door drs. J.J.M. Stikvoort.
mr. A.F. Gaastra neemt namens DG Politie deel aan de stuurgroep.
drs. H.M.F. Bruls neemt namens het KBB deel aan de stuurgroep.

De specifieke doelgroep waarvoor het rapport is bestemd bestaat uit:

- Onze opdrachtgever zoals bovengenoemd.
- De korpsbeheerder mr. A. Wolfsen.
- De waarnemend korpschef drs. M.H.C. Barendse.
- De Hoofd Officier van Justitie mr. dr. J.R. Bac.
- De privacyfunctionaris
- De voorzitter van het College Bescherming Persoonsgegevens.

I

Het rapport mag uitsluitend met toestemming van de korpsbeheerder dan wel de korpschef van korps Utrecht aan derden ter beschikking worden gesteld.

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

4 Bevindingen

4.1 Inleiding

De nieuwe Wet Politiegegevens (Wpg), die op 1 januari 2008 in werking is getreden, biedt meer armslag voor het gebruik van persoonsgegevens, voorziet in mogelijkheden om gegevens, die voor een bepaald doel zijn verwerkt, te gebruiken voor andere doelen en biedt meer mogelijkheden voor verstrekking van politiegegevens aan personen en instanties buiten de politiesector. Daarnaast voorziet de nieuwe wet in waarborgen voor de burger tegen ongerechtvaardigde inbreuken op diens persoonlijke levenssfeer.

4.1.1 *Regie en doorzettingsmacht voor de Wpg implementatie*

Het korps Utrecht heeft om de Wpg te implementeren een regionaal project 'Implementatie Wet Politiegegevens' in het leven geroepen. Het project draagt zorg voor de implementatie van de Wpg in de politieregio Utrecht.

Het project heeft een Program Initiatie Document (PID) "090522 PID Wpg versie 1.0" opgesteld met daarin de aanpak, beschikbare capaciteit, doelen en risico's van de implementatie van de Wpg.

Algehele aandachtspunten die bij de audit binnen Politie Utrecht naar voren zijn gekomen zijn:

- Op de werkvloer is behoefte aan protocollering, werkinstructies, stroomschema's etc. waarin de regelgeving van de Wpg concreet en helder wordt beschreven. Dit biedt de medewerkers handvatten bij het uitvoeren van zijn dagelijkse werkzaamheden conform de Wpg.
- De informatie die wordt aangehouden op de groepsschijven en persoonlijke schijven die binnen het korps middels de kantoorautomatisering wordt gebruikt voldoet niet aan de Wpg-vereisten. Wij adviseren het korps om de inrichting van de mappenstructuur te herzien conform de Wpg.
- De privacyfunctionaris zit voornamelijk nog in de adviesrol en komt onvoldoende toe aan de toezichthoudende taak. Wij adviseren om het taakaccent van de privacyfunctionaris te verschuiven naar de controlerende rol.
- Het proces voor het autoriseren van medewerkers, muteren en verwijderen van autorisaties op de informatiesystemen is nog voor verbetering vatbaar.
- Het invullen van een structurele belegging van de interne auditfunctie, inclusief het opstellen van een auditplan voor 2012.

4.1.2 *Bekendheid met de Wpg binnen de organisatie*

Politie Utrecht heeft door middel van opleiding, e-Learning en presentaties de medewerkers opgeleid. In de praktijk is naar voren gekomen dat in sommige gevallen de Wpg kennis nog onvoldoende is en men een opfriscursus op prijs zou stellen.

4.1.3 *Wpg en de praktijk*

Ten tijde van de implementatie van de Wpg was er bij "Blauw" veel onduidelijkheid over wat je wel of niet mag verstrekken. Het idee leefde dat je helemaal niks aan derden mag verstrekken. Gedurende de auditperiode is dit beeld veranderd en is

geconstateerd dat het binnen het korps steeds duidelijker wordt wat voor politiegegevens verstrekt mogen worden.

4.2 Verantwoordelijke (artikel 1.f)

Mandaatbesluit

4.2.1 Norm

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

4.2.2 Bevindingen

Er is een mandaatbesluit Wet politiegegevens politie Utrecht waarin de korpsbeheerder zijn mandaat verleent aan de onderscheiden functionarissen/functiegroepen van de politie Utrecht.

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

Onderscheid artikel 8 en 9

Voor het onderscheid tussen artikel 8 en 9 gegevensverwerking is de 'Beslisboom Wet Politiegegevens' opgesteld. Op basis waarvan kan worden nagegaan onder welk artikel de betreffende politiegegevens verwerkt dienen te worden en onder welk regime een onderzoek valt. Dit document is voor medewerkers op intranet beschikbaar gesteld.

Medewerkers zijn door middel van presentaties, e-Learning en workshops geïnformeerd over de criteria voor het onderscheid tussen artikel 8 en artikel 9 gegevensverwerkingen.

Gedurende de projectperiode zijn alle wijkteams bezocht en hebben ze een presentatie over de Wpg gehad, waaronder met betrekking tot de kwaliteitsaspecten van artikel 8 en 9 Wpg. Daarnaast is aan alle wijkchefs een presentatie verzorgd bij de uitreiking van de stroomschema's verstrekkingen.

Uit de interviews komt het beeld naar voren dat de gegeven opleiding met betrekking tot de Wpg voor de medewerkers niet tot het gewenste resultaat heeft geleid. Medewerkers hebben nog te weinig kennis van de Wpg. Bovendien wordt het op intranet beschikbare Wpg materiaal beperkt geraadpleegd. Om dit te verbeteren is vanuit Blauw ook een eigen fysieke map met Wpg materiaal ingelicht.

Er wordt uitsluitend van de beschreven werkwijze afgeweken indien daartoe aanleiding bestaat in verband met de bewaartermijn of het belang van afscherming van de gegevens. De medewerkers van het Bureau politiegegevens controleren steekproefsgewijs op de verwerkingsgrondslag.

Feiten worden vastgelegd in BVH met een bepaald doel, Tachtig procent van het vastgelegde werk vindt plaats in BVH. Winkeldiefstal en mishandeling wordt ook

geregistreerd in BVH. Alleen echte opsporing, zoals zware zaken is BVO. Op moment van tappen, zwaardere middelen ga je naar BVO. Meeste informatie is artikel 8 Wpg.

Het komt voor dat er soms artikel 9 informatie in BVH wordt opgenomen. Een verklaring voor het opnemen van artikel 9 informatie in BVH kan zijn dat medewerkers informatie willen verwerken, maar niet geautoriseerd zijn om in BVO te werken. Een tweede verklaring is dat ze niet geschoold zijn om in BVO te werken en daarom BVH gebruiken omdat ze dat systeem wel kennen. Ten slotte komt het ook voor dat medewerkers wel geschoold zijn in het werken met BVO maar er nooit wat mee hebben gedaan en zo niet weten hoe gewerkt moet worden in het BVO.

Kwaliteitscriteria artikel 8

Noodzakelijkheid

Door middel van communicatie, opleiding en handleidingen op intranet is het Blauw gewezen op de vastlegging van informatie indien wordt voldaan aan de noodzakelijkheidseis. In incidentele gevallen, wanneer een vraag aan de helpdesk Wpg wordt gesteld, wordt op de noodzaak voor vastlegging gewezen.

Doelbinding

Artikel 8 gegevens zijn breed raadpleegbaar en worden gebruikt conform het gestelde in artikel 15 Wpg.

Rechtmatigheid

De rechtmatigheid wordt deels geborgd door het politieproces waarbij vergaarde informatie wordt getoetst op rechtmatigheid in de vorm van een rechtszaak. Het korps heeft geen andere maatregelen geïmplementeerd met betrekking tot de rechtmatigheid.

Juistheid & volledigheid

De volledigheid en juistheid van gegevens wordt enigszins geborgd door de verplichte invulvelden van BVH. De medewerkers van de unit Gegevensbeheer BVH van de afdeling Informatiebeheer controleren op de juistheid en integriteit van de ingevoerde gegevens voor artikel 8 Wpg informatie.

Het korps maakt gebruik van TrueBlue voor achteraf controle op ingevoerde gegevens in BVH. De controle wordt uitgevoerd door functioneel beheerders en medewerkers van de afdeling Informatiebeheer. Verder zijn er werkinstructies BVH die op intranet raadpleegbaar zijn en werkinstructies HKS, die via een vtsPN-pagina raadpleegbaar zijn.

BVH dwingt de gebruikers om de verplichte velden in te vullen. BVH kent een aantal geautomatiseerde invoercontroles, waarmee de volledigheid van ingevoerde gegevens wordt geborgd.

Toezien op correct systeemgebruik en zo nodig begeleiden van nieuwe kerninstructeurs/gebruikers gebeurt door de functioneel beheerder. Hierbij wordt toegezien op juistheid, betrouwbaarheid en nauwkeurigheid van de door de applicatie gehanteerde gegevensverzamelingen (tabellen) en deze actueel houden.

Kwaliteitscriteria artikel 9

Het researchproces bevat waarborgen voor de kwaliteitsaspecten van artikel 9 gegevens. De PDCA-cyclus sluit via het OM en de rechter.

De Wpg speelt in de dagelijkse praktijk echter maar een beperkte rol binnen de districtsrecherche. Onderzoeksteams toetsen niet of voldaan wordt aan de Wpg bij gebruik van informatiebronnen. Medewerkers gebruiken bij het oplossen van zaken alle beschikbare informatie. Ze vinden het belangrijker dat een zaak wordt opgelost en/of te kunnen beoordelen of personen, de maatschappij of medewerkers van de politie gevaar lopen, dan dat aan de wettelijke bepalingen van de Wpg wordt voldaan.

Vanuit de korps- en teamleiding wordt weinig direct gestuurd op toepassing van de Wpg. Het bureau Politiegegevens (met de coördinator Wpg en de privacyfunctionaris) is ook vrij onzichtbaar.

Binnen de districtsrecherche is het binnen de werkprocessen voldoen aan de Wpg niet overal geborgd via protocollen. Meer in het algemeen bestaat er binnen de districtsrecherche ook bij andere processen behoefte aan procedures. Dit geldt dan met name voor het schonen en bewaren van bestanden.

De meeste medewerkers van de districtsrecherche hebben niet veel kennis van de Wpg. De kennis van de Wpg is bij medewerkers van het district beperkt. Daarnaast wordt er ook niet veel expliciet met de wet gewerkt. Hierdoor treden verschillen in interpretaties niet veel naar de voorgrond.

Noodzakelijkheid

Door middel van communicatie, opleiding en handleidingen op intranet is het Blauw gewezen op het noodzakelijkheidsvereiste bij de vastlegging van informatie. In incidentele gevallen, wanneer een vraag aan de helpdesk Wpg wordt gesteld wordt op de noodzaak van een doelbinding voor vastlegging gewezen. Binnen artikel 9 verwerkingen bieden de regels van Strafvordering een extra waarborg voor dit vereiste.

Doelbinding

Het doel van artikel 9 Wpg-onderzoeken wordt vastgelegd in de aanvragen voor een BVO-registratie. In deze aanvraag dient onder andere het doel van het onderzoek, de leider van het onderzoek, het categorie delict en de bevoegde functionaris te worden vermeld. Hiermee wordt het mogelijk de doelbinding van een onderzoek te toetsen.

De onderzoeksleiders toetsen de gegevens en verifiëren of de vastleggingen een doelbinding hebben met het onderzoek. De infodeskmedewerker of de bevoegde functionaris die een informatieverzoek in behandeling neemt, controleert de doelbinding van het informatieverzoek.

In de procedurebeschrijving is een toets op de doelbinding echter niet beschreven.

Rechtmatigheid

De herkomst en wijze van verkrijging van informatie wordt vastgelegd in BVO als onderdeel van het onderzoeksproces. Door de inrichting van het politieproces wordt impliciet voldaan aan dit aspect van de Wpg. In het algemeen geldt dat bij artikel 9 en 10 verwerkingen de rechtmatigheid wordt getoetst door de onderzoeksleider, de informatiecoördinator en de zaaksofficier van justitie.

De rechtmatigheid wordt daarnaast geborgd door de het politieproces waarbij vergaarde informatie wordt getoetst op rechtmatigheid in de vorm van een rechtszaak. De regels van Strafvordering bieden een extra waarborg voor dit

vereiste. Het korps heeft geen andere maatregelen geïmplementeerd met betrekking tot de rechtmatigheid.

Juistheid en Nauwkeurigheid

De juistheid van informatie wordt impliciet gecontroleerd door het onderzoeksproces. Het is de rechercheurs er alles aan gelegen om te werken met juiste informatie om te voorkomen dat zaken worden geseponeerd.

Volledigheid

Bij BVO ligt het accent op de kwaliteit van gegevens zoals startmutatie en einddatum. Het verwijderen van gegevens wordt in BVO gelogd.

Niet altijd worden alle artikel 9 gegevens in BVO of BVH verwerkt, omdat deze systemen door medewerkers als te ingewikkeld worden beschouwd. Het komt soms voor dat een deel van de gegevens op afdelingsschijven of in mappen wordt geplaatst.

De teamleider, de tactisch coördinator, de informatiecoördinator en de proces-verbaalcoördinator voeren interne controles uit op de kwaliteit van artikel 9 politiegegevens. Daarnaast vindt periodiek controle plaats door de zaaksofficier van justitie in het wekelijks overleg van de vaste kern leidinggevend (VKL).

Oncontroleerbaarheid vastleggingen

Medewerkers zetten steeds meer informatie niet meer in BVO omdat het makkelijker is om MS Word te gebruiken. Dit zorgt er helaas voor dat gegevens niet toegankelijk zijn voor collega's. Daardoor worden deze gegevens ook niet ter beschikking gesteld.

Artikel 10 en 12 CIE en RID

De aard van het werk van de RID brengt met zich mee dat bij het vastleggen van informatie veel aandacht is voor het voldoen aan de kwaliteitseisen. De CIE maakt gebruik van het landelijk proceshandboek CIE. Bovendien stelde eerdere wetgeving ongeveer dezelfde eisen aan het vergaren, bewaren en bewerken van informatie als dat de Wpg nu doet. De CIE-officier van het OM is verantwoordelijk voor het voldoen aan deze kwaliteitseisen.

De CIE-OvJ draagt zorg voor een deugdelijke vastlegging van de gegevens over informanten. Om aan deze verantwoordelijkheid gestalte te kunnen geven, geeft hij aanwijzingen omtrent en voert hij controle uit op de rechtmatige verkrijging en verwerking van de gegevens, waaronder de juistheid, de volledigheid, het gebruik alsmede de vernietiging van de gegevens.

Er is een inventarisatie van alle applicaties waarbij Wpg aspecten een rol spelen. Deze zijn onderverdeeld naar de verschillende artikelen.

Beveiliging

Tijdens de audit is opgemerkt dat een koppeling tussen de systemen BVO en BVH ontbreekt. Dit brengt een noodzaak tot handmatig overzetten van gegevens met zich mee. Dit handmatig overzetten is mensenwerk met de onder andere de volgende risico's:

- Bij het handmatig overzetten kunnen er fouten ontstaan.
- Als het overzetten niet gebeurt, kunnen door te vroege schoning in BVH gegevens niet meer worden gebruikt.
- Met BlueView kan nog niet gelabelde artikel 9 informatie als artikel 8 informatie in BVH worden geraadpleegd. Dit kan leiden tot onrechtmatig gebruik.

De systemen BVH en BVO sluiten niet op elkaar aan. In theorie staat in BVH slechts artikel 8 Wpg informatie en in BVO slechts artikel 9 Wpg informatie. BVH wordt gebruikt als formulierensysteem. Informatie welke moet worden omgezet van BVH naar BVO moet handmatig worden overgezet. Het korps Utrecht heeft geen aanvullende maatregelen genomen om dit te borgen.

Kantoorautomatisering

Binnen de politie Utrecht is de kantoorautomatisering (schijven en mappen) nog niet Wpg-proof. Binnen het korps bestaat ook geen mogelijkheid om te controleren of de persoonlijke schijven en mappen van politiemedewerkers politiegegevens bevatten.

Alle medewerkers van het korps worden geïnstrueerd geen gebruik te maken van kantoorautomatisering bij het registreren, verwerken of verstrekken van politiegegevens. Risico's die het korps loopt doen zich met name voor rond schoning en bewaartermijnen. Risico's op lekken en verstrekken worden klein ingeschat.

Medewerkers van het korps maken relatief nog veel gebruik van kantoorautomatisering bij het vastleggen van gegevens die onder de Wpg vallen. De verklaring hiervoor is tweeledig. Enerzijds ervaren agenten de systemen, die de primaire processen ondersteunen, niet als gebruiksvriendelijk. Anderzijds komt het ook voor dat medewerkers het nut niet erkennen van het gebruik van de formele systemen.

Het komt voor dat politiegegevens worden opslagen binnen de kantoorautomatisering. In dat geval worden ook gegevens dubbel opgeslagen (zowel in de daarvoor bestemde applicaties als op de persoonlijke en/of afdelingsschijf); waarmee zicht op bewaartermijn, delen en reguleren rechtmatige toegang lastig blijkt te zijn.

In BVO wordt gebruik gemaakt van de automatische logging die dit systeem biedt. Met deze loggingsgegevens is inzichtelijk wie welke informatie invoert of bewerkt.

Regionale applicaties

Er is een inventarisatie beschikbaar van alle (regionale) applicaties welke in gebruik zijn bij het korps Utrecht. De applicaties zijn ingedeeld naar het regime van de Wpg waaronder de informatie in de betreffende applicatie valt. Een deel van de applicaties is niet Wpg compliant.

CIE- en RID-informatie is binnen het korps voldoende beveiligd.

III

4.3.3

Verbeterpunten

Als verbeterpunten zijn te noemen:

- Opstellen van procedures, richtlijnen voor het inrichten van een mappenstructuur die voldoet aan de vereisten vanuit de Wpg.
- Controle op de bewaartermijnen van de aangehouden informatie binnen mappenstructuur.
- Het aanbieden van praktische handreikingen voor toetsing op de in artikel 3 en 4 genoemde kwaliteitscriteria van de politiegegevens.
- Organiseer de toezichtstaak op de kwaliteitscriteria van politiegegevens.

4.4 Gevoelige gegevens (artikel 5)

4.4.1 Norm

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

4.4.2 Bevindingen

De gevoelige gegevens worden slechts incidenteel verwerkt in aanvulling op de verwerking van andere politiegegevens en voor zover dit voor het doel van de verwerking onvermijdelijk is, conform het gestelde in artikel 5 Wpg.

Uit de gedurende de audit aangedragen informatie is niet gebleken dat het korps gevoelige gegevens vastlegt wanneer dat niet onvermijdelijk is. Bij bepaalde verwerkingen wordt toegelicht waarom het vastleggen van gevoelige gegevens noodzakelijk en onvermijdelijk is. Tijdens alle presentaties en workshops aangaande de Wpg is expliciet de aandacht op gevestigd op het omgaan met gevoelige gegevens. Bij vragen of casussen waarop advies wordt gevraagd en waarbij sprake is van het gebruik van gevoelige gegevens, wordt dit wel specifiek toegelicht.

4.5 Autorisatie (artikel 6)

4.5.1 Norm

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

4.5.2 Bevindingen

Autorisatiematrix

Het korps Utrecht heeft een autorisatiebeleid opgesteld waarin is beschreven hoe autorisatiematrices dienen te worden opgesteld. Echter heeft het korps het beleid nog niet vertaald in een autorisatiematrix.

De autorisatiematrix dient volgens het korpsbeleid te worden beheerd door de divisiechef Informatie in diens rol als proceseigenaar informatie. In ieder geval jaarlijks zal de divisiechef van de afdeling Informatie een advies over noodzakelijke wijzigingen in de autorisatiematrix aan de proceseigenaren vragen. De privacyfunctionaris en de informatiebeveiligingsfunctionaris zullen de wijzigingen toetsen op de vigerende wet- en regelgeving. Specifieke autorisaties zullen alleen worden gewijzigd in overleg met het OM. De standaardwijze waarop autorisaties worden vertaald naar rechten binnen informatiesystemen wordt beheerd door het hoofd van de afdeling Informatiemanagement. Wijzigingen in de standaardeffectuering zullen altijd in overleg met de divisiechef Informatie worden genomen.

Op korpsniveau blijkt in de praktijk geen autorisatiebeheer plaats te vinden. Autorisaties worden verstrekt op een 'need-to-know' basis. Een proces ter borging van het intrekken van autorisaties bij functiewijziging of afronding van de werkzaamheden ontbreekt.

Autorisatieprocedure

De bevoegdheid tot het verstrekken van standaardautorisaties aan medewerkers is gemandateerd aan MT-leden van het betreffende korpsonderdeel. Daarbij wordt getoetst aan de voorwaarden die aan de autorisatie zijn gesteld. De goedgekeurde aanvraag (opdracht) wordt ter effectuering aan de Servicedesk vtsPN gestuurd.

V

De verantwoordelijkheid voor autorisaties op groepsschijven is bij de desbetreffende afdelingen belegd.

Tijdelijke autorisaties

Autorisaties voor een bepaalde tijd worden door de lijn aangevraagd onder vermelding van een doelbinding. De proceseigenaar Informatie adviseert hierover. De goedgekeurde aanvraag (opdracht) wordt ter effectuering aan de Servicedesk vtsPN gestuurd.

Autorisatieprofielen worden gezien als gereedschap bij het op de juiste wijze uitvoeren van de bedrijfsprocessen en daarmee als een onlosmakelijk onderdeel daarvan. De verantwoordelijkheid voor het definiëren en beschrijven van de autorisatieprofielen, ligt daarmee bij de proceseigenaren.

Goedkeuring beleid

Het bovenstaand autorisatiebeleid is integraal vastgesteld en middels een oplegnotitie ter goedkeuring aan de stuurgroep voorgelegd. Het korps Utrecht heeft een implementatievoorstel opgesteld om de autorisatiematrix, de hulpmiddelen en het autorisatieproces te borgen.

De autorisaties worden verstrekt op een 'need-to-know' basis waarbij noodzaak tot uitbreiding van autorisaties dient te worden aangetoond. Het korps is in afwachting van de oplevering van het landelijk autorisatiemodel. Hiermee kan worden aangesloten bij een landelijke standaard en wordt het beheer centraal bij vtsPN geregeld.

Voor het aanvragen van autorisaties op de centrale mappen is een aanvraagformulier wat leidinggevend gebruiken om bij vtsPN autorisaties aan te vragen. VtsPN toetst de aanvraagformulieren op de handtekening van de gemandateerde, dit dient een MT-lid te zijn. Zie het document "Mandaatprocedure Autorisaties Definitief".

BVO

Voor autorisaties in BVO is een bovenregionaal autorisatiemodel ontwikkeld door vtsPN. Dit model is een aanzet voor de inrichting binnen het korps.

Autorisaties worden verleend volgens het landelijk autorisatiemodel BVO. De toegang wordt via een autorisatieformulier aangevraagd bij het vtsPN door de teamleider en door een gemandateerde ondertekend. Functioneel beheer maakt vervolgens de autorisatie aan conform het BVO-autorisatieniveau. Functioneel beheer controleert of de betrokkene de juiste opleiding voor aangevraagd autorisatieniveau heeft gevolgd. Handelingen in de BVO worden voor iedere BVO gebruiker gelogd en is via vtsPN opvraagbaar.

Conform de in verzorgingsgebied (VG) Midden geldende werkafspraken, wordt functioneel beheer BVO toegevoegd bij ieder operationeel onderzoek.

III

Wanneer iemand buiten het VG-Midden autorisatie tot een applicatie/menu vraagt dan gaat dit via de privacyfunctionaris van zijn korps en via de privacyfunctionaris van het verzorgingsgebied. Functioneel beheer dient in een dergelijk geval een opleidingscertificaat te mailen.

Wijzigen en verwijderen

Het korps heeft geen proces voor schoning en verwijdering van autorisaties. Tevens vindt geen periodieke controle plaats op tijdige uitvoering van mutaties. Voor een deel van de systemen worden autorisatieoverzichten voorgelegd aan de verantwoordelijke chef. Een voorbeeld hiervan zijn de BlueView autorisaties.

Het korps maakt geen gebruik van geautomatiseerde updates van autorisaties waardoor het handmatig aanpassen van autorisaties noodzakelijk is wanneer zich interne verschuivingen voordoen of dienstverbanden eindigen.

Bij het verlaten van het korps geeft de applicatie Beaufort hiervan melding en wordt deze melding door functioneel beheer verwerkt, dat wil zeggen dat de accounts op 'disabled' gezet worden.

Het wijzigen van het bereik van een verstrekte autorisatie, wordt aangevraagd door de lijn en na toetsing aan de voorwaarden, toegewezen door een MT-lid. Niet bekend is welke voorwaarden hiervoor zijn vastgesteld. Het wijzigen van de manier waarop een autorisatie is geëffectueerd, wordt na vaststelling door de korpsleiding, opgedragen aan de Chief Information Officer.

Controle door leidinggevend op uitgegeven autorisaties vindt voor een beperkt aantal systemen plaats. Bij uitdiensttreding worden de autorisaties van betrokkene ingetrokken op grond van het ontslagbesluit. Daarmee is onmiddellijk de toegang tot de kantooromgeving geblokkeerd, zodat vanuit deze omgeving geen toegang meer mogelijk is tot regionale of landelijke applicaties, en tot schijven en mappen. De opdracht tot intrekken, wordt ter effectuering aan de Servicedesk vtsPN gestuurd.

Een besluit tot schorsing van een autorisatie wordt in de lijn genomen. De opdracht voor schorsing wordt aan de afdeling Regie (Informatiemanagement) gestuurd ter effectuering.

De vertaling van het beleid naar een eenduidig proces moet nog verder worden uitgewerkt. Door het ontbreken van een nadere uitwerking van het autorisatieproces is men afhankelijk van de professionaliteit van de individuen. Het risico dat hiermee gepaard gaat is dat de kennis niet expliciet is gemaakt en daarmee niet is geborgd. Bovendien bestaat het risico dat autorisatieverzoeken niet uniform worden afgehandeld.

VtsPN signaleert dat gebruikers gedurende een half jaar niet zijn ingelogd. In dat geval geeft functioneel beheer aan dat de gebruiker een opfriscursus moet volgen waarna het account door functioneel beheer weer wordt gereactiveerd.

Autorisaties Veiligheidshuis

Rond autorisaties bij systemen in het Veiligheidshuis spelen verschillende issues:

- Er vindt geen geautomatiseerde update van autorisaties plaats en is handmatige update nodig, wat risico's met zich meebrengt.
- De toegang tot de systemen geschiedt via justitienet, waarmee de centraal georganiseerde waarborgen gelden.

- Deelnemers van justitiële casusoverleggen krijgen slechts informatie in COOS te zien waarvoor ze geautoriseerd zijn.

Digitale recherche

De digitale rechercheurs krijgen in principe de informatie die ze nodig hebben voor de uitvoering van hun dagelijkse politietaak. De afwegingen van een onderzoeksleider om autorisaties toe te kennen worden, voor zover bekend, niet getoetst.

Wijkpolitie

Het verkrijgen van autorisaties is ingeregeld middels een standaardformulier voor het aanvragen van accounts. Deze autorisatieverzoeken worden ingediend bij de Servicedesk voor landelijke applicaties. Er is geen gestructureerd proces voor het intrekken van autorisaties. Een MT-lid keurt voor de wijkpolitie de autorisaties en laat deze waar nodig intrekken.

Procedure CIE en RID

Bij de CIE en RID vindt een strak autorisatiebeheer plaats dat consequent wordt uitgevoerd. Autorisaties worden toegekend en ingetrokken door het hoofd van de betreffende eenheid, bij de CIE conform het door de OvJ goedgekeurde autorisatiebeleid.

Door het hoofd van de RID zijn drie medewerkers aangewezen die in zijn opdracht autorisaties kunnen realiseren en verwijderen. Het proces is niet vastgelegd. De technische kant van het aanmaken en verwijderen van een autorisatie is wel beschreven.

Protocollering autorisaties

Aanvragen en wijzigingen worden in BVH gelogd en zijn naar de persoon terug te herleiden. Voor BVO geldt dat dit wordt bijgehouden door de functioneel beheerders. BVH heeft voor deze vastlegging geen einddatum. De logging tenminste wordt bewaard tot na de eerstvolgende audit.

De privacyfunctionaris heeft inzicht bij welke functioneel beheerders of medewerkers een overzicht verkrijgbaar is van de actuele autorisaties. De privacyfunctionaris heeft echter geen inzicht in de CIE en RID autorisatieprocessen zoals vereist conform artikel 32.1 sub c Wpg.

4.5.3

Verbeterpunten

Als verbeterpunten zijn te noemen:

- Het in gebruik nemen van een tool en/of een proces om autorisaties in een geautomatiseerde vorm vast te leggen en te beheren.
- Een eenduidige procesbeschrijving ter borging van het intrekken van autorisaties bij functiewijziging of afronding van de werkzaamheden vaststellen.

4.6

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

4.6.1

Norm

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

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

4.6.2

Bevindingen

De Regionale Infodesk en Informatiecoördinatoren zijn de aangewezen functionarissen voor artikel 11 zoekslagen. Tevens wordt gesteld dat geen logging plaatsvindt van artikel 11 zoekslagen omdat dit technisch niet mogelijk zou zijn.

Het korps Utrecht hanteert de volgende interpretaties:

- Onder geautomatiseerd vergelijken wordt verstaan; het vergelijken van een concreet zoekgegeven (bijvoorbeeld een volledig kenteken, volledige personalia, concreet adres) met geregistreeerde politiegegevens, waarbij het resultaat van de vergelijking relevante hits oplevert.
- Onder in combinatie verwerken wordt verstaan; het vergelijken met meerdere, soms onvolledige, zoekgegevens (bijvoorbeeld een onvolledig kenteken, merk en kleur van een motorvoertuig) met geregistreeerde politiegegevens, waarbij het resultaat ook niet-relevante hits bevat die wel worden uitgerechercheerd teneinde de relevantie vast te stellen of uit te sluiten. Deze manier van zoeken impliceert een grotere inbreuk op de persoonlijke levenssfeer van – soms grote aantallen – personen.

De artikel 11 zoekslagen worden slechts uitgevoerd door de medewerkers van de Regionale Infodesk, de informatiecoördinatoren en analisten. Deze functies zijn formeel belegd.

Uit de gevoerde interviews blijkt het echter niet altijd duidelijk te zijn wat gecombineerd verwerken inhoudt. Bovendien bestaat onduidelijkheid over het verschil tussen 'geautomatiseerd vergelijken' en 'in combinatie met elkaar verwerken'. Men geeft aan dat de wet verschillend wordt geïnterpreteerd door juristen binnen en buiten de politie.

Aangewezen functionarissen

Het korps heeft de bevoegdheden ten opzichte van artikel 11 Wpg schematisch als volgt in beeld gebracht:

Verwerking	Wpg/Bpg grondslag	Primair Bevoegd	Secundair bevoegd
Geautomatiseerd vergelijken	Artikel 8.2	Ambtenaren van politie met een art. 8 autorisatie	
In combinatie verwerken	Artikel 8.3 en 2:1	Informatie Coördinatie en Analyse	
Geautomatiseerd vergelijken	Artikel 11.1 en 2:2 lid 1	Informatie Coördinatie en Analyse	Politieambtenaren belast met de verwerking van artikel 10 gegevens
Geautomatiseerd vergelijken	Artikel 11.2 en 2:2 lid 2	Politieambtenaren belast met de verwerking van artikel 10 gegevens	Informatie Coördinatie en Analyse
In combinatie verwerken	Artikel 11.4 en 2:2 lid 2	Politieambtenaren belast met de verwerking van	Voor CIE-werkzaamheden aangewezen

		artikel 10 gegevens	medewerkers van de afdelingen Analyse en Informatie Coördinatie
Verdere verwerking van 8, 9 en 10 gegevens t.b.v. ondersteuning vd politietaak	Artikel 13.3 en 2:8 onder c	Politieambtenaren die werkzaam zijn bij een eenheid die met de uitvoering van deze taak is belast. (zie Bpg 2:8 c)	Medewerkers van de afdeling Informatie Coördinatie (TMSI en TIO)

Bevoegd gezag

Op het moment dat gegevens in combinatie worden verwerkt is het bevoegd gezag hierbij betrokken. De bevoegd functionarissen dienen in het geval het politiegegevens uit een opsporingsonderzoek betreft hun instemmingstaak uit te voeren in nauw overleg met de zaakofficier van justitie. De CIE-OvJ is het bevoegde gezag in het geval van CIE artikel 11.4 gegevensverwerkingen.

De OvJ verleent zijn instemming mondeling dan wel schriftelijk. Indien de officier zich in de verdere verwerking van politiegegevens, gelet op de belangen van het (strafrechtelijk) onderzoek, niet kan vinden dan deelt hij dit zo spoedig mogelijk mondeling dan wel schriftelijk mede aan de betreffende bevoegde functionaris.

Protocollering artikel 11.1, 11.2, 11.4 en 11.5

Er wordt in de meeste systemen die worden gebruikt voor GV/ICMEV worden gelogd, dit zijn bijvoorbeeld BlueView, BVO en HKS. De medewerkers van de afdeling Informatiecoördinatie (DIK's, RIK, TIO en TMSI) verzorgen de vastlegging van verstrekking of terbeschikkingstelling van de resultaten van hun zoekslagen in BVO

Protocolgegevens met betrekking tot GV/ICMEV-verwerkingen worden echter niet structureel vastgelegd.

Alleen de vastlegging van verstrekkingen is voor de privacyfunctionaris opvraagbaar, maar niet de vastlegging van de zoekvraag en de daarop gegenereerde hits.

4.6.3**Verbeterpunten**

Als verbeterpunten zijn te noemen:

- Het hanteren en naar de medewerkers communiceren van praktische richtsnoeren om de onduidelijkheid met betrekking tot de betekenis van artikel 11 zoekslagen weg te nemen.
- Borg het structureel vastleggen van de artikel 11 zoekslagen.

4.7**Bewaartermijnen (artikel 14)****4.7.1****Norm**

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

verwerking als bedoeld in artikel 10, en na verloop van deze termijn worden verwijderd.

4.7.2 *Bevindingen*

Oude informatie uit BPS wordt handmatig benaderd, BPS kent geen schotten. Per 1 december 2011 is BPS door vtsPN uitgefaseerd en kunnen slechts bepaalde functionarissen nog bij de gegevens.

Doordat de landelijke systemen niet voorzien in een schoningsmechaniek heeft het korps Utrecht zelf een schoningsbeleid opgesteld en wordt handmatig geschoond. Door de grootte van de databases is dit arbeidsintensief. Tevens wisselt informatie van regime, waardoor schoning wordt bemoeilijkt. Het korps heeft een project ingericht voor het schonen van de regionale applicaties. Gedurende deze audit was het project (genaamd Project Schoning) nog niet gestart.

Het korps heeft geen zicht op de informatie die is opgeslagen op de persoonlijke schijven, waardoor hier mogelijk informatie op staat die de bewaartermijnen van de Wpg overschrijden. Het gebruik van de mappen is enigszins beperkt door de autorisatiestructuur binnen de Kantoorautomatisering. Men moet zijn gemachtigd om nieuwe mappen aan te kunnen maken op bepaalde schijven. Alle medewerkers van het korps worden geïnstrueerd geen gebruik te maken van kantoorautomatisering bij het registreren, verwerken of verstrekken van politiegegevens.

De verantwoordelijkheid voor verwijdering van artikel 8 Wpg gegevens na 5 jaar is belegd, maar niet formeel gedocumenteerd. Ook het proces van verwijdering is niet expliciet gemaakt.

Papieren documenten

Over het algemeen wordt papier in gesloten containers gedaan en opgehaald door een gespecialiseerd bedrijf dat voor vernietiging zorgdraagt. Vertrouwelijke gegevens worden versnipperd en worden door hetzelfde bedrijf opgehaald.

Helmcamera's

Het gebruik van helmcamera's en de omgang met de vastgelegde informatie is gevestigd, inclusief de bewaartermijn van het beeldmateriaal en onder welke voorwaarden het beeldmateriaal mag worden gebruikt.

Artikel 8 van 1 tot 5 jaar

Voor de Wpg-compliance van landelijke applicaties is er een sterke afhankelijkheid van vtsPN. BVH ondersteunt niet de levensloop van Politiegegevens. Gegevens ouder dan één jaar na eerste vastlegging in BVH worden niet achter schot gezet. Het schoningsscript in BVH 1.2.2 staat voorlopig nog niet aan in afwachting van landelijk standpunt om dit script aan te zetten. Er leven echter nog vraagpunten over hoe één en ander geïnterpreteerd moet worden. Ook is er nog onduidelijkheid omtrent de praktische uitwerking van het schoningsscript.

Er zijn geen maatregelen getroffen om de bewaartermijnen van informatie in de mappenstructuur conform de Wpg na te leven. In het voorjaar van 2012 is het korps voornemens de ordening en schoning van de schijven en mappen ter hand te nemen.

Artikel 8 verwijderen na 5 jaar

Artikel 8 gegevens worden (nog) niet verwijderd na 5 jaar. Voor BVH is dit nog niet aan de orde omdat deze applicatie ruim twee jaar geleden in gebruik is genomen. In

verband met de uitfasering van BPS is de toegang tot deze applicatie zeer beperkt. Zie het document "Werkinstructie raadplegen en wijzigen in BPS".

In het voorjaar van 2012 is het korps voornemens de ordening en schoning van de schijven en mappen ter hand te nemen.

Artikel 8 vernietigen na 5 jaar verwijderd

Het korps Utrecht heeft geen maatregelen genomen om de vernietiging van politiegegevens te borgen. Tevens is geen inzicht in de informatie die is opgeslagen op de persoonlijke schijven en groepsschijven. Hier is ook geen beleid voor opgesteld.

Verwijderen na OH-moment

Het opschonen van artikel 9 onderzoeken gebeurt nog onvoldoende. Hierbij is de overdracht van informatie over afgesloten zaken van OM naar de politie een aandachtspunt.

Hierbij dient te worden aangetekend dat geen structurele terugkoppeling van de OvJ wordt ontvangen zodat het OH-moment onduidelijk blijft. Er zijn echter geen compenserende maatregelen getroffen om aan de Wpg te voldoen. Er wordt aangegeven dat de interactie met het OM moeizaam is, bijvoorbeeld wanneer informatie door het OM dient te worden vrijgegeven en dit niet gebeurt. Het korps kan de betreffende informatie in dat geval niet schonen.

Het OM Utrecht is bezig om met betrekking tot de afloopberichten duidelijkheid omtrent het OH-moment te verschaffen, maar dit blijkt lastig en lijkt weinig prioriteit te hebben. Ook is er vanuit het landelijk project contact met het landelijk parket (en/of College van PG's) op dit onderwerp.

Artikel 9 vernietigen na 5 jaar verwijderd

Doordat het juiste moment waarop verwijderd moet worden niet bekend is, kan niet 5 jaar na verwijdering worden vernietigd.

Medewerkers blijken onderzoeksbestanden (bijvoorbeeld uitwerking van verhoren) veelal in hun persoonlijke map op te slaan waardoor de informatie op een ongestructureerde wijze op de schijf komen te staan. Zo kunnen gegevens van grote rechercheonderzoeken 10 jaar in persoonlijke mappen staan in plaats van in de juiste onderzoeksmap.

In district Utrecht Stad worde Artikel 9 gegevens ook in fysieke dossiers bewaard in de kelder van het bureau. Enkele medewerkers hebben toegang tot dit archief. Op welke wijze autorisaties hiervoor worden verleend is onduidelijk. Deze dossiers dienen nog te worden geschoond.

Artikel 10 en 12 Wpg

Artikel 10 gegevens vallen onder de verantwoordelijkheid van de CIE en RID. Hiertoe is een schoningsproces opgesteld, waarin wordt aangegeven dat halfjaarlijkse controles plaatsvinden. Tevens is het verwijderings- en vernietigingsproces hierin beschreven.

Het RIDS wordt tweemaal per jaar geschoond door de kwaliteitsfunctionaris. Toezicht hierop is niet belegd.

Artikel 10 en 12 Wpg gegevens vallen onder de verantwoordelijkheid van de CIE en RID. Hiertoe is een schoningsproces opgesteld, waarin wordt aangegeven dat

halfjaarlijkse controles plaatsvinden. Tevens is het verwijderings- en vernietigingsproces hierin beschreven.

De CIE en het RID zien toe op de bewaartermijnen en de halfjaarlijkse controle van politiegegevens in het informantenregister en werken dit bij. De procedures hiervoor zijn beschreven.

In het journaal van het openbare orde register wordt verantwoord dat schoning heeft plaatsgevonden.

Hernieuwde verwerking

Het korps heeft nog geen invulling gegeven aan een procedure voor het hernieuwd verwerken van politiegegevens.

Protocollering hernieuwde verwerking

De herkomst van gegevens die worden gebruikt voor hernieuwde verwerking wordt in het artikel 9 proces-verbaal vastgelegd. Er is geen afzonderlijke vastlegging conform artikel 6:4 Besluit politiegegevens jo. artikel 32 lid 1 sub e Wpg. Derhalve worden deze gegevens ook niet bewaard en is daarvan geen overzicht beschikbaar.

Verder verwerken na vier maanden

De teamleiders CIE en de CIE-OvJ zien toe op de maximale periode van 4 maanden dat politiegegevens omtrent informanten, na dato van de eerste verwerking, ter beschikking worden gesteld voor verdere verwerking.

Gegevens worden in de meeste gevallen hernieuwd verwerkt na toestemming van de OvJ. Een procesbeschrijving hiervan is niet beschikbaar.

4.7.3

Verbeterpunten

Als verbeterpunten zijn te noemen:

- Stel een procedure op voor het vernieuwd verwerken van gegevens conform artikel 14 lid 3 Wpg, buiten de CIE om.

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

Infodesk

Ter beschikking stellingen verlopen veelal via de DIK's, de afdeling Regionaal Informatie Knooppunt en de nieuwe afdeling TMSI (Team Monitoring en Signalering Informatie). In de Infodeskmodule blijkt niet altijd goed te worden vastgelegd welke informatie aan wie ter beschikking wordt gesteld.

Een procesbeschrijving aangaande het ter beschikking stellen is vastgelegd in de vorm van een stroomschema dat op intranet is gepubliceerd. Tevens is deze informatie beschikbaar op de bureaus. De DIK's maken gebruik van een protocol. In dit protocol is beschreven dat artikel 9 Wpg of artikel 10 Wpg politiegegevens

slechts ter beschikking worden gesteld na goedkeuring van de hiervoor bevoegde functionaris.

V

Ter beschikking stellen in relatie tot de persoonlijke schijven

Er is sprake van informatieopslag op de persoonlijke schijven (bijvoorbeeld bij recherche onderzoeken).

Doordat er informatieopslag op de persoonlijke schijven plaatsvindt, zijn deze gegevens veelal niet vindbaar door de betreffende Infodesk. Hierdoor wordt niet alle informatie gedeeld en kan niet worden geborgd dat alle relevante informatie ter beschikking wordt gesteld.

Dit geldt ook voor de districtsrecherche, waar informatie veelal in MS Word wordt opgebouwd om vervolgens in BVH of BVO te worden gezet. De districtsrecherche heeft vanwege de beperkingen in de basissystemen een eigen server met een mappenstructuur opgezet. Hierdoor wordt informatie niet ter beschikking gesteld aan personen die dit behoeven conform artikel 15 Wpg.

Voor het verwerken van BVO-bruto naar BVO-netto wordt de medewerker geautoriseerd door de teamleiding.

Bevoegde functionarissen

De bevoegde functionarissen zijn op basis van functie formeel aangewezen. Er is een door de verantwoordelijke ondertekend en gepubliceerd aanwijzingsbesluit.

De leidinggevenden van de recherche-onderdelen zijn opgeleid tijdens een eendaags seminar. Leidinggevenden binnen de dagelijkse politietaak zijn over hun rol als bevoegde functionaris volledig geïnformeerd door middel van een handleiding waarin de verantwoordelijkheden vanuit de Wpg zijn uiteengezet. In zowel de training als de handleiding zijn de begrippen doelbinding, doelafwijking en proportionaliteit benoemd als beoordelingscriteria.

Het korps heeft niet geborgd dat *nieuwe* bevoegde functionarissen worden opgeleid over de Wpg. Om dit te borgen is aan de politieacademie reeds geruime tijd geleden de vraag gesteld om het onderwerp "bevoegde functionaris" op te nemen in de "leergangen tactisch en operationeel leiding geven" (OLL en TLL).

De bevoegde functionarissen hebben verschillende documenten tot hun beschikking waarin de medewerkers op de kwaliteitsaspecten van de Wpg worden gewezen. Dat staat onder andere in de handreiking verstrekkingen, de checklist en modelformulieren artikel 20, de instructie met betrekking tot de rol van bevoegde

functionaris en documenten van het landelijk project die beschikbaar zijn op de projectpagina Wpg (intranet Utrecht).

Codering

Codering wordt gebruikt voor artikel 9 onderzoeken die in BVO/SUMM-IT worden verwerkt. Dit wordt bereikt door te kiezen voor een bepaald autorisatieniveau waarop de informatie wordt weggezet en daarmee wordt de mate van afscherming en toegang bepaald. Door middel van codering worden ook embargo-onderzoeken afgeschermd en wordt de export naar Blueview bepaald.

Weigeringsgronden

De bevoegde functionarissen zijn ingelicht over de verplichting tot het intern ter beschikking stellen en de wettelijke toegestane weigeringsgronden die van toepassing zijn. Dit maakt expliciet onderdeel uit van de training.

In de werkinstructie voor bevoegde functionarissen wordt verwezen naar het betreffende artikel 2:13 van het Besluit politiegegevens waarin deze wettelijk toegestane weigeringsgronden staan opgesomd.

4.8.3

Verbeterpunten

Als verbeterpunten zijn te noemen:

- Minimaliseer het opslaan van politiegegevens op de persoonlijke schijven.
- Borg dat nieuwe bevoegde functionarissen worden opgeleid over de Wpg.

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

Verstrekkingenwijzer (landelijk)

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

Hierdoor dient het korps andere maatregelen te hebben getroffen om aan te tonen de artikelen 16 t/m 24 binnen de processen is geborgd.

Om de werking conform de landelijke verstrekkingenwijzer aan te tonen dient een vastlegging aanwezig te zijn van de verstrekte informatie en ontvanger(s) van de informatie.

De landelijke verstrekkingenwijzer wordt gehanteerd door de medewerkers die betrokken zijn bij verstrekkingen. De verstrekkingenwijzer is beschikbaar op alle informatieknooppunten en bij de wijkteams. Tevens is de verstrekkingenwijzer gepubliceerd op Intranet en is daarmee voor eenieder te raadplegen.

CIE

De medewerkers van de CIE verstrekken niet zelf rechtstreeks aan derden. Dit loopt via de afdeling Informatiecoördinatie van de Divisie Informatie. Informatievragen vanuit het wijkteam voor HKS gaan via DIK of Meldkamer.

Proces voor convenanten

De originele convenanten worden opgeslagen bij het organisatieonderdeel dat het convenant is aangegaan. Een kopie van hetconvenant wordt door de privacyfunctionaris bewaard. Tevens is afgesproken dat convenanten op intranet worden geplaatst en daar raadpleegbaar zijn. In het voorjaar van 2012 moet dit worden gerealiseerd.

Aan de hand van de 'checklist convenanten voor structureel uitwisselen politiegegevens met derden' worden de convenanten opgesteld en getoetst. Als bijlage bij de checklist is een voorbeeldbesluit en een modelconvenant toegevoegd.

De verantwoordelijke dient volgens de checklist in overeenstemming met het bevoegde gezag een beslissing te nemen tot het verstrekken van politiegegevens aan personen of instanties binnen een samenwerkingsverband. De hiervoor gemandateerden zijn de korpschef, leden van de korpsleiding en de districts- en divisiechefs.

De checklist omvat verder de noodzakelijke gegevens welke conform artikel 20 tweede lid Wpg verplicht zijn in een artikel 20 besluit te vermelden. De afdeling die de structurele gegevensuitwisselingen verricht, stelt zelf het convenant op.

Wanneer het bevoegde gezag convenantpartner is wordt door deze mede ondertekend. Daarnaast worden bepaalde onderwerpen in de (lokale) driehoek besproken alvorens een convenant op te stellen en te tekenen.

De privacyfunctionaris is verantwoordelijk voor de toetsing op compliance aan de Wpg van artikel 20 besluiten.

Het korps Utrecht heeft een modelconvenant voor artikel 20 besluit opgesteld. Daarin zijn de criteria vanuit de Wpg opgenomen voor het opstellen van nieuwe artikel 20 besluiten.

Convenanten

Uit de gesprekken blijkt dat door de hoeveelheid convenanten het overzicht begint te verdwijnen. Hierdoor wordt onduidelijk welke convenanten er zijn, welke convenanten wanneer geldig zijn en daarmee op grond van welk convenant welke gegevens mogen worden verstrekt.

Het korps heeft diverse convenanten met ketenpartners als de Belastingdienst en gemeenten afgesloten om gegevensverstrekkingen te structureren. De convenanten gelden daarbij voor het doen van gegevensverstrekkingen rond een bepaald doel, zoals de bestrijding van voetbalvandalisme, illegale prostitutie, mensenhandel, woninginbraak of hennepcultuur. Het aantal afgesloten convenanten is door de jaren heen gegroeid. Voor veel nieuwe behoeften aan extra gegevensuitwisseling is een separaat convenant afgesloten.

Verstrekkingsschema (regio)

Vanaf voorjaar 2012 zullen de convenanten op intranet worden geplaatst en daar raadpleegbaar zijn. Het korps Utrecht heeft geen overzicht van alle partijen aan wie

lokaal mag worden verstrekt op basis van opgestelde convenanten en artikel 20 Wpg besluiten.

Voor incidentele verstrekkingen conform artikel 19 Wpg is het elke politieambtenaar en BOA (werkzaam binnen de politie Utrecht) toegestaan om informatie aan derden te verstrekken (voor zover dit hun taakvervulling betreft). Er is een handleiding verstrekkingen op intranet geplaatst, en aan de uitvoerende eenheden is een poster beschikbaar gesteld met een beslisboom/stroomschema waar de verstrekkinggrondslagen zijn te raadplegen.

Geautomatiseerde verstrekkingen

Er vinden bij korps Utrecht geautomatiseerde verstrekkingen plaats naar twee verschillende partijen, namelijk:

- CJIB, noodzakelijk voor het innen van boetes.
- Slachtofferhulp, noodzakelijk voor het behartigen van de belangen van slachtoffers van misdrijven of verkeersongevallen.

De automatische verstrekking beperkt zich in alle gevallen tot artikel 8 gegevens. Voor Slachtofferhulp wordt vanuit BVH ten aanzien van een bepaald aantal maatschappelijke klassen de noodzakelijke politiegegevens verstrekt. Tevens vindt er vanuit de PSH-Transactie Module automatische verstrekking plaats.

Aanvragen lopen via de CIO of de proceseigenaar Informatie. Het korps heeft echter geen schriftelijk proces met betrekking tot de geautomatiseerde verstrekkingen uitgewerkt. Door middel van logging is achteraf te bepalen over welke personen op een geautomatiseerde wijze politiegegevens zijn verstrekt. Deze logging vindt plaats binnen de applicaties BVH voor Slachtofferhulp en een rechtstreekse verbinding tussen de Centrale Verwerkingseenheid (CVE) van de politie Utrecht naar het CJIB. De loggegevens zijn voor de privacyfunctionaris opvraagbaar.

Het CJIB en Slachtofferhulp komen beide in de nationale verstrekkingenwijzer voor.

Geheimhouding

De geheimhoudingsplicht wordt expliciet vermeld in het modelbesluit, het voorbeeldconvenant en de standaard Wpg-bijlage voor bestaande convenanten.

De medewerkers van de informatieknooppunten gebruiken een disclaimer die standaard met verstrekte gegevens wordt meegestuurd:

Dit document en de eventuele bijlagen bevat(ten) mogelijk politiegegevens in de zin van de Wet politiegegevens. Deze gegevens zijn uitsluitend bestemd voor het doel waarvoor deze hier worden verstrekt. Verdere verwerking van deze gegevens is toegestaan, maar uitsluitend voor zover een wet daarin voorziet of een goede taakuitvoering dit noodzakelijk maakt. Voor elke andere handeling met deze gegevens geldt, ook nadat u deze hebt ontvangen, geheimhouding zoals bedoeld in artikel 7 van de Wet politiegegevens. Overtreding van deze geheimhoudingsbepaling is strafbaar gesteld in artikel 272 van het Wetboek van Strafrecht, waarvan lid 2 hier niet van toepassing is.

Protocollering verstrekking

De op Intranet beschikbare 'Handleiding verstrekkingen' stelt dat verstrekkingen dienen te worden vastgelegd middels I90-formulieren of BVO-verstrekkingen-mutaties en beschrijft welke gegevens hierbij dienen te worden vastgelegd.

De privacyfunctionaris heeft een overzicht opgevraagd van alle vastgelegde verstrekkingen in BVH (I90 en E62). Het blijkt dat onder deze code ook zaken worden geplaatst die geen verstrekkingen zijn. Dit duidt op gebrekkige kennis van verstrekkingen en brengt het risico met zich mee dat niet alle schriftelijke vastleggingen van verstrekkingen juist zijn geborgd. Tevens blijkt dat uit de vastgelegde verstrekkingen niet altijd goed is te herleiden welke informatie aan welke personen of instanties is verstrekt.

De vastleggingen worden bewaard in BVH dan wel BVO tot na de eerstvolgende audit na vastlegging. In de BVO-Infodeskmodule blijkt echter niet altijd goed terug te vinden welke gegevens verstrekt zijn en aan welke partijen.

In 2011 zijn er 314 I90-formulieren ingevuld. Het korps geeft zelf aan dat het weinig is. Daarnaast worden wel veel verstrekkingen vastgelegd door middel van standaardbrieven/formulieren, zoals brief zorgmelding jongere (verstrekking aan Bureau Jeugdzorg) en een mededeling van verstrekking in een mutatie ('fomutra'). Het aantal van deze verstrekkingen bedroeg in 2011: 501. Hierbij dient wel in ogenschouw te worden genomen het feit dat de informatie-medewerkers hun verstrekkingen vastleggen in de BVO.

Toezicht door leidinggevenden op verstrekkingen en protocollering

Het toezicht door leidinggevenden op verstrekkingen vindt niet structureel plaats. Weliswaar is de toezichtsrol tijdens de bijeenkomsten met bijvoorbeeld de wijkchefs gecommuniceerd, maar de inschatting binnen het korps is dat weinig leidinggevenden zich hiermee bezig houden. Hier wordt ook nog niet op gestuurd en wordt er niet gecontroleerd door de privacyfunctionaris.

4.9.3 Verbeterpunten

Als verbeterpunten zijn te noemen:

- Stimuleer het gebruik van één centrale methode (bijv. I90-formulieren) om de gedane verstrekkingen vast te leggen.

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

Voor de afhandeling van inzageverzoeken is een Bureau politiegegevens ingericht. Binnen het korps is Bureau politiegegevens opgericht welke zich buigt over met name uitvoeringsvraagstukken rond de Wpg. Tevens houdt het bureau zich bezig met inzageverzoeken. Andere taken van het bureau rond de Wpg zijn:

- Afhandeling van inzage- en informatieverzoeken.
- Advisering rond verwijderingsverzoeken.
- Opleiding en vorming met betrekking tot de Wpg.
- Het geven van voorlichting over implicaties van de implementatie van de Wpg.
- Advisering rond verstrekkingen.

De inzageverzoeken worden binnen de daarvoor gestelde termijn afgehandeld door Bureau politiegegevens. Een verdaging wordt beperkt tot een periode van vier weken, tenzij de betrokkene niet tijdig reageert op een aanvullend verzoek om de vereiste identiteitsvaststelling te kunnen waarborgen.

Er is nog geen definitief proces opgesteld voor de afhandeling van inzageverzoeken. Het beschreven proces dat is aangeleverd bevindt zich in de conceptfase ('nog aan te passen') en kan aldus nog niet als definitief worden beschouwd.

Conceptprocedure

Een ieder kan *schriftelijk* verzoeken om kennisname van politiegegevens die over hem of haar worden vastgelegd bij de politie Utrecht. Het verzoek moet zo concreet mogelijk zijn. Richt het verzoek schriftelijk aan:

- Korpsbeheerder Politie Utrecht
- Bureau Politiegegevens
- Postbus 8300
- 3503 RH UTRECHT

Men kan het verzoek ook laten doen door de advocaat. Aan deze dient men een bijzondere machtiging te verlenen. Deze machtiging moet de advocaat met het verzoek meesturen. In het geval het om een minderjarige onder de 16 jaar of om een onder curatele gestelde gaat, moet de wettelijke vertegenwoordiger het verzoek doen.

Antwoord

Bureau politiegegevens stelt de identiteit van betrokkene deugdelijk vast. Bureau politiegegevens geeft in principe binnen zes weken antwoord op het verzoek. Verlenging van deze termijn met vier weken is in bijzondere gevallen mogelijk. Van dat uitstel krijgt de verzoeker schriftelijk bericht.

Afwijzing

De korpsbeheerder kan kennisneming afwijzen, in het belang van:

- De goede uitvoering van de politietaak.
- Gewichtige belangen van derden.
- De veiligheid van de staat.

Afwijzen kan geheel of gedeeltelijk en gebeurt schriftelijk naar de betrokkene.

Kennisnemen

In geval van toewijzing van het verzoek nodigt Bureau politiegegevens de verzoeker uit en stelt deze in de gelegenheid om kennis te nemen van zijn/haar gegevens.

Correcties

Degene die op grond van artikel 25 van de Wet politiegegevens kennis heeft kunnen nemen van zijn / haar gegevens kan verzoeken deze gegevens:

- Te verbeteren.
- Aan te vullen.
- Te verwijderen.
- Af te schermen.

Dat kan als deze gegevens feitelijk onjuist, onvolledig, niet ter zake dienend zijn of onwettig verwerkt. De verzoeker krijgt binnen vier weken na ontvangst schriftelijk bericht.

De korpsbeheerder kan het verzoek afwijzen en geeft daarbij aan om welke redenen dat is.

4.10.3 *Verbeterpunten*

Als verbeterpunten zijn te noemen:

- Completeer de inzage- en correctieprocedure en communiceer deze naar de personen die belast zijn met het afhandelen van de verzoeken van de betrokkenen.

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; en
- 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*

Protocollering doel onderzoek

Het doel van artikel 9 Wpg onderzoeken wordt vastgelegd in de aanvragen voor een BVO-registratie.

V

Bij het starten van een onderzoek wordt een Melding Recherche Onderzoek (MRO) verstuurd naar de landelijke verwijzindex VROS, onder beheer van KLPD.

De privacyfunctionaris geeft aan dat artikel 9 onderzoeken worden aangemeld en beschikbaar gesteld voor de privacyfunctionaris.

Bewaren protocolgegevens doel onderzoek

Men geeft aan dat alle artikel 9 onderzoeken die gemeld worden in een gezamenlijke map worden geplaatst waar zowel de BVO-beheerders als de privacyfunctionaris toegang tot hebben. De protocolgegevens worden ten minste bewaard tot na de eerstvolgende audit, of zolang het onderzoek nog niet beëindigd is.

Er is een overzicht van onderzoeken met doelmelding in BVO te vinden. Als het onderzoek niet in BVO wordt gedraaid, wordt de artikel 9 doelmelding door de privacyfunctionaris in de aanmeldingen map geplaatst. Districten werken niet in BVO omdat dit systeem veelal als te ingewikkeld beschouwd wordt.

Protocollering Artikel 13 gegevensverzamelingen

Er is een overzicht van alle informatiesystemen met bijbehorende wetsartikelen. Ten aanzien van artikel 13 gegevensverzamelingen zijn schriftelijke vastleggingen gemaakt van de in de wet en het besluit vermelde aspecten.

Het korps heeft geen proces ingericht voor de aanmelding van nieuwe artikel 13 gegevensverzamelingen. De privacyfunctionaris heeft toegang tot een overzicht van artikel 13 gegevensverzamelingen en de bijbehorende protocollen.

Een aanzet is aanwezig tot identificatie van alle applicaties waarbij de Wpg van toepassing is. Zo ook voor applicaties met een gekoppelde artikel 13 Wpg gegevensverzameling. Hieruit volgt echter nog niet welke acties zijn ondernomen ten aanzien van deze verzamelingen.

Korps Utrecht wacht met het grootste gedeelte geïdentificeerde artikel 13 applicaties de landelijke reglementen af. In het geval van een vijftal applicaties is een uitzondering gemaakt, omdat onduidelijkheid over de vastlegging tot problemen zou kunnen leiden. Met betrekking tot deze vijftal applicaties zijn wel protocollen opgesteld conform de Wpg.

Protocollering onrechtmatige handeling

De binnen het korps bekende beveiligingsincidenten (waaronder de categorie 'onrechtmatige Wpg-verwerking') worden geregistreerd in het incidentenregister. Dit register wordt gevoerd en onderhouden door de Informatie Beveiligings Functionaris (IBF) van het korps. Het incidentenregister maakt het onder andere mogelijk om overzichten te produceren van onrechtmatige verwerkingen ten behoeve van de toezichthoudende taak van de privacyfunctionaris.

In het incidentenregister, worden de volgende gegevens vastgelegd:

1. Datum en tijdstip van de melding.
2. Naam en onderdeel van de melder.
3. De categorie van het incident is: "onrechtmatige Wpg verwerking".
4. Omschrijving van de onrechtmatige Wpg verwerking.
5. De plaats, tijdstip en korpsonderdeel waar de onrechtmatige Wpg verwerking zich voordoet of heeft voorgedaan.
6. Deze registratie wordt aangevuld met de gegevens tijdens en na afhandeling van het incident, zoals:
 - a. De reeds genomen acties (om erger te voorkomen).
 - b. Degene aan wie is doorgemeld i.v.m. het oplossen van het incident.
 - c. Datum en tijdstip van deze doormelding.
 - d. Is de oorzaak - al dan niet tijdelijk - weggenomen.
 - e. Welke permanente acties worden genomen.
 - f. Datum en tijdstip van het herstel van de situatie.
 - g. Is er reden voor nadere evaluatie en zo ja, met wie?

De afhandeling van incidenten, waaronder onrechtmatige Wpg verwerkingen, is primair een lijnverantwoordelijkheid. De IBF maakt jaarlijks een rapportage naar aanleiding van het incidentenregister. Onderdeel hiervan zijn de registraties van onrechtmatige verwerkingen in het kader van de Wpg. Hierdoor ontstaat inzicht in de veiligheidssituatie per district, divisie of ander korpsonderdeel.

Gemeenschappelijke verwerking

Het korps Utrecht heeft geen gemeenschappelijke verwerkingen.

4.11.3 *Verbeterpunten*

Als verbeterpunten zijn te noemen:

- Stel de protocollen op voor de geïdentificeerde artikel 13 gegevensverzamelingen.

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*

Interne auditfunctie

De interne auditfunctie is niet structureel belegd. Het korps heeft wel een interne auditor aangesteld. De interne auditor heeft een Operational Auditing opleiding gevolgd.

De taken van de interne auditor zijn ondergebracht als taakaccent bij medewerkers van het regionaal bureau Beleid en Control. Eén van hen (gediplomeerd operational auditor) is verantwoordelijk voor de coördinatie en uitvoering van de interne auditing op de Wpg. De taken zullen bestaan uit het opstellen van de planning en het auditplan, het uitvoeren en coördineren van de feitelijke audit en het opstellen van de audit-rapportage.

Auditplan

Er is geen vaktechnisch verantwoord en meerjarig intern Wpg audit-plan. In het kader van de korpsaudit-cyclus is capaciteit ingepland om steeds delen van het korps te auditen. Dit geldt voor 2010 en 2011. Voor 2012 is in de planning rekening gehouden met de uitvoering van een interne audit. Het korps anticipeert op nieuwe ontwikkelingen, uitkomsten van verrichte audits en een aangekondigd nieuw normenkader.

Het korps heeft capaciteit ingepland om onderdelen van het korps te auditen. Het auditplan wordt opgesteld in afwachting van landelijke ontwikkelingen en uitkomsten van de externe audit.

Intern auditrapport

De jaarlijkse interne Wpg audit heeft niet plaatsgevonden.

4.12.3 *Verbeterpunten*

Als verbeterpunten zijn te noemen:

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

4.13 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*

Het korps Utrecht heeft een privacyfunctionaris aangewezen en aangemeld bij het College Bescherming Persoonsgegevens.

II

In het algemeen is er veel werk en daardoor wordt er niet geïnvesteerd op de toezichthoudende taak.

- De mailbox wordt dagelijks gevuld met vragen en is de privacyfunctionaris veel tijd kwijt aan het beantwoorden ervan. Daarnaast houdt de PF zich bezig met andere adviesvragen.
- Op dit moment is sprake van onvoldoende capaciteit om aan de wettelijke toezichtstaak vorm te geven. Ook aan het maken van een jaarverslag zoals voorgeschreven door de Wpg, is de privacyfunctionaris niet toegekomen.
- Bovendien heeft de privacyfunctionaris geen overzicht van de protocollering en niet inzicht in het geheel van de protocollering.

Activiteiten taken van de privacyfunctionaris zijn:

- De privacyfunctionaris geeft presentaties aan werkstudenten en wijkagenten over de Wpg. Tevens wordt voorlichting gegeven aan de wijkteamchefs.
- De privacyfunctionaris zit in meerdere overlegstructuren, waardoor op regionaal en landelijk niveau informatie-uitwisseling en kennisdeling plaatsvindt.
- De privacyfunctionaris denkt mee met het wijkteam bij het opstellen van een convenant. En vragen waarvan het team niet weet of ze die kunnen beantwoorden leggen ze voor aan de privacyfunctionaris.

4.13.3 *Verbeterpunten*

Als verbeterpunten zijn te noemen:

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

4.14 **Functionaris Gegevensbescherming (artikel 36)**

De optionele functionaris Gegevensbescherming bestaat niet als functie bij korps Utrecht.