

4.5.2**Bevindingen**

Het handboek autorisatie dat in 2004 is opgesteld is door de komst van de Wpg herzien. Het handboek bevat een duidelijke procesbeschrijving. Regio Noord- en Oost-Gelderland heeft een administratief systeem waarin de autorisaties worden vastgelegd en beheerd. Deze applicatie autoriseert medewerkers op basis van een autorisatiematrix. In de matrix zijn standaard relaties vastgelegd tussen enerzijds functies, organisatieonderdelen en taakaccenten en anderzijds gebruikersrollen of autorisatieniveaus op applicatie en gegevensbronnen. Wijzigingen in autorisaties worden alleen doorgevoerd na schriftelijke toestemming van een leidinggevende. De functies waaraan de autorisaties zijn gekoppeld komen uit het personeelsinformatiesysteem Beaufort. Een voorwaarde voor de juistheid en volledigheid van de autorisaties is dat Beaufort volledige en juiste gegevens moet bevatten van de medewerkers van het korps, inclusief inhuurkrachten en stagiairs. Met het oog hierop is gedateerd 23-8-2011 een procesbeschrijving opgesteld. Belangrijk hierbij is de tijdigheid van aanpassingen in het systeem. Beaufort moet altijd up-to-date zijn. Tweemaal per jaar dienen de systeemeigenaren een controle uit te voeren op de toegekende autorisaties en de resultaten hiervan te rapporteren aan de privacyfunctionaris. Uit de gesprekken is naar voren gekomen dat dit nog niet overal heeft plaatsgevonden. De accreditatie voor toegang tot bepaalde gegevens in de administratie van het autorisatiebeheer wordt geprotocolleerd. Hiermee voldoet het autorisatiesysteem aan de vereisten van zorgvuldigheid en evenredigheid.

III

Protocolgegevens worden conform de richtlijnen bewaard.

4.5.3**Verbeterpunten**

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

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

4.6.1**Norm**

Voor het onderzoek kunnen politiegegevens die voor dat onderzoek zijn verwerkt, geautomatiseerd worden vergeleken met andere politiegegevens (GV) die worden verwerkt op grond van artikel 8 of 9 teneinde vast te stellen of verbanden bestaan tussen de betreffende gegevens. De gerelateerde gegevens kunnen, na instemming van de daartoe bevoegde functionaris, zijnde de leider van het betreffende onderzoek of zijn plaatsvervanger, voor dat onderzoek verder worden verwerkt. Indien politiegegevens in combinatie met elkaar worden verwerkt (ICMEV), worden van die verwerking nader genoemde gegevens vastgelegd (protocolplicht).

4.6.2**Bevindingen**

Deze activiteit wordt met name uitgevoerd door algemene analisten bij de divisie Informatie & Intelligence, alsmede door specifieke analisten bij de CIE en RID. Zij dragen ook zorg voor protocollering van de gegevens en de teamchefs zien toe op toepassing en bewaring. Vragen naar de opzet van de verwerking van politiegegevens conform deze richtlijnen worden in het algemeen met grote

omzichtigheid tegemoet getreden. Het is een onderwerp dat slechts bij weinig geïnterviewden bekend lijkt. Waar bekendheid met deze begrippen uit de Wpg aanwezig is, is direct de vraag aan de orde waar de grenzen van GV en ICMEV liggen en op welke wijze daarmee dan in de praktijk moet worden omgegaan. Het verkrijgen van toestemming van het bevoegd gezag (OM) vindt bij ICMEV niet altijd plaats.

Het geautomatiseerd vergelijken van politiegegevens die worden verwerkt op grond van artikel 8, 9 of 10 met andere politiegegevens wordt uitgevoerd door de info coördinatoren van divisie I&I, bijvoorbeeld bij een TGO. Zij dragen ook zorg voor protocollering van de gegevens.

4.6.3

Verbeterpunten

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

4.7 Bewaartermijnen (art 14)

4.7.1

Norm

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

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

4.7.2

Bevindingen

De landelijke systemen zoals BPS, BVH en BVO zijn niet voorzien van beheersmaatregelen op het gebied van termijnen voor verwijderen en vernietigen van politiegegevens. Het is in BVH en BPS niet mogelijk informatie na bijvoorbeeld 1 jaar achter een schot te plaatsen zodat deze informatie niet meer kan worden geraadpleegd. Ook vinden er geen handmatige verwijderingen plaats. In de nieuwe release van BVH zou dit wel tot de mogelijkheden behoren; deze release wordt volgens planning in week 43 bij Noord- en Oost-Gelderland ingevoerd. In BVO worden registraties gesloten en dan worden de autorisaties op nul gezet zodat men niet meer bij de informatie kan. Er is hier echter geen sprake van vernietiging. Er is met betrekking tot artikel 8 en 9 Wpg geen procedure aangetroffen voor de omgang met bewaartermijnen en vernietiging van politiegegevens. Nader onderzoek naar het Wpg proof zijn van BVH en BVO is noodzakelijk.

Gegevens die in de kantoorautomatisering zijn opgeslagen vallen helemaal buiten beeld. Controle op de bewaartermijnen en vernietiging vindt hierop niet plaats. Er is geen totaaloverzicht van wat er in die omgeving is opgeslagen. De outlook-mailboxen vereisen hier bijzondere aandacht, verzonden mails, met bijvoorbeeld verstrekkingen, worden waarschijnlijk niet geschoond. Uit de gesprekken is wel naar voren gekomen dat de kennis van de bewaartermijnen en vernietiging vaak wel aanwezig is.

In het handboek CIE en RID (artikel 10 Wpg) is wel aandacht geschonken aan deze onderwerpen. In de interne audit zijn deze documenten inhoudelijk beoordeeld en aangegeven is dat het handboek CIE onvoldoende waarborgen bevat voor het

naleven van wettelijke bepalingen op het gebied van verwijderen, bewaren en vernietigen van politiegegevens.

Binnen de recherche is aangegeven dat bij het kopiëren van gegevens van digitale gegevensdragers, zoals smartphones en tablets, de gegevens na gebruik niet worden vernietigd. Alle in beslag genomen gegevensdragers worden na de beslissing van de officier van Justitie teruggegeven. Het Openbaar Ministerie geeft vaak geen signaal als een onderzoek tot een onherroepelijk vonnis heeft geleid. Hierdoor ontstaan overvolle kasten en schijven. Alleen uit ruimtebesparende motieven wordt een enkele keer gegevens verwijderd of vernietigd.

De bevoegde functionarissen dragen zorgen voor verstrekking van gegevens bij hernieuwde verwerking. Tevens dient het OM dan toestemming te verlenen. De bevoegd functionaris heeft hierin een centrale rol. Niet in alle gevallen wordt de juiste procedure gevolgd. Het handboek bevoegd functionaris dient hierin de weg te wijzen.

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

4.7.3

Verbeterpunten

- Voer controle uit op de gegevens in de kantoorautomatisering.
- Houd beheersmaatregelen voor verwijdering en vernietiging in de systemen BVH en BVO landelijk op de agenda.
- Pas het handboek CIE aan op het gebied van wettelijke bepalingen voor verwijderen, bewaren en vernietigen van politiegegevens.
- Ontwerp een procedure waarin gebruikte gegevens afkomstig van in beslag genomen gegevensdragers na gebruik kunnen worden vernietigd.

4.8 Ter beschikking stellen (art 15)

4.8.1

Norm

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

4.8.2

Bevindingen

Bij het ter beschikking stellen van politiegegevens wordt gebruik gemaakt van een standaard formulier. Deze formulieren worden verstuurd naar de Infodesk bij Divisie I&I, die ze verder afhandelt. Het werkproces van de Infodesk is beschreven. Aangegeven is dat in de praktijk nog niet alles via I&I verloopt en dat nog veel formulieren terecht komen bij de privacyfunctionaris. De CIE en de RID zijn beide strikt in het vastleggen van het ter beschikking stellen van gegevens. Bij de CIE is een extra waarborg dat de CIE-OvJ toezicht houdt. Wanneer de Infodesk informatie ter beschikking stelt c.q. verstrekt waarvoor de toestemming van een Bevoegd Functionaris nodig is dan wordt het feit dat deze toestemming is verleend in de mail, waarin de informatie ter beschikking wordt gesteld, vermeld. Er wordt niet gewerkt met een aparte codering. Het verstrekken van dit soort informatie gebeurt (vrijwel) niet.

4.8.3

Verbeterpunten

- Stimuleer centrale afhandeling van het ter beschikking stellen van politiegegevens door de Infodesk.

- Zorg voor bewustwording en kennis over het proces van ter beschikking stellen door de Infodesk, medewerkers moeten automatisch de Infodesk kunnen vinden in plaats van de privacyfunctionaris.

4.9 Verstrekken (art 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

Verstrekkingen verlopen bij het regiokorps via de Infodesk bij divisie I&I. Voor zover verstrekkingen onder afgesloten convenanten vallen, wordt een verstrekkingen tabel gehanteerd waarin staat vermeld welke stukken aan welke organisaties verstrekt mogen worden. Alle verstrekkingen gaan via de (beveiligde) mail en worden in de computer in een gezamenlijke bak bewaard (Outlook). De verstrekkingen worden gemuteerd in BVH en BVO zodat steeds duidelijk is wat er verstrekt is.

Van de overige verstrekkingen moet een vastlegging worden gemaakt zoals een I90 formulier bij een BVH verstrekking of een vastlegging in het werkjournaal bij verstrekkingen afkomstig uit BVO of andere politie systemen. Aangegeven is dat deze aantallen vastleggingen niet in evenwicht zijn met de feitelijk gedane verstrekkingen.

De RID levert de verstrekkingenrapporten bij de Infodesk aan per mail. Aandachtspunt hierbij is dat de verstrekkingenrapporten in de verzonden items van de mailbox blijven staan. Als schoning achterwege blijft, dreigt het risico van overschrijding van de bewaartermijnen.

Voor de structurele verstrekkingen aan samenwerkingsverbanden is er onderscheid te maken in algemene en Wpg convenanten. Voor het traceren van convenanten is er een oproep geweest aan de districtscheffs om deze aan te leveren aan de privacyfunctionaris. In eerste instantie kwam hierop weinig respons. De convenanten die zijn aangeleverd, zijn getoetst op de Wpg en waar nodig aangepast en op intranet geplaatst. Inmiddels weten de mensen de privacyfunctionaris te vinden als het om dit onderwerp gaat. Convenanten worden momenteel beheerd door de privacyfunctionaris. Vanwege deze ontstaansgeschiedenis bestaat er momenteel nog geen zekerheid over de volledigheid van de convenanten. Er is (nog) geen procesbeschrijving hoe nieuwe convenanten tot stand komen, maar daar wordt door Sturingsondersteuning aan gewerkt. Ook is een beleidsmedewerker opgeleid om hulp te bieden bij het WPG proof maken van oude en nieuw te maken convenanten. Als er nieuwe convenanten worden gemaakt, wordt de Wpg (besluit art 20) bij het opstellen van deze convenanten direct meegenomen. Wijzigingen in reeds bestaande convenanten worden in een addendum toegevoegd aan het convenant.

Voor wat betreft de geautomatiseerde verstrekkingen wordt er dagelijks een programma (query) gedraaid over BVH. Op basis van dit programma wordt dagelijks één bestand gemaaild naar slachtofferhulp met voor hun relevante informatie. Het korps heeft hiermee inzicht in de geautomatiseerde verstrekkingen en de inhoud daarvan.

In NOG neemt de politie deel aan 3 casusoverleggen in het kader van het Veiligheidshuis (Jeugd, Veelplegers en Huiselijke Geweld). De samenwerking is gebaseerd op de raamregeling Samenwerkingsovereenkomst NOG Veiligerhuis (met

privacy reglement, waarin de informatieverstrekking wordt geregeld). Door de voorzitter van de casusoverleggen (een hoofdinspecteur van politie) wordt onderscheid gemaakt in de verstrekking van informatie aan opsporingsambtenaren en hulpverleners. Schriftelijk krijgen opsporings-ambtenaren NAW gegevens en overige relevante informatie; hulpverleners krijgen alleen NAW gegevens. De aanwezigheid van partners (opsporingsambtenaren en hulpverleners) bij de casusoverleggen geschiedt conform de samenwerkingsovereenkomst - hulpverleners dus ook aanwezig. Mondeling gaat er dus wel e.e.a. over tafel. M.a.w. toezicht binnen het Veiligheidshuis is wel geregeld, maar er ligt ingevolge de Wpg nog wel een knelpunt.

4.9.3 *Verbeterpunten*

- Zorg voor beheersmaatregelen die gericht zijn op een volledige registratie van verstrekkingen door middel van I90 formulieren en andere vastleggingen.
- Controleer of verzonden verstrekkingen in de mailbox RID en Infodesk tijdig worden geschoond.
- Zorg voor een adequaat en centraal beheer van convenanten.

4.10 Rechten van betrokkenen (art 25/28)

4.10.1 *Norm*

De verantwoordelijke deelt een ieder op diens schriftelijk verzoek binnen zes weken mede of, en zo ja welke, deze persoon betreffende politiegegevens zijn vastgelegd.

4.10.2 *Bevindingen*

Er is een landelijke handreiking rechten betrokkenen opgesteld. Deze is gebruikt in het project Implementatie Wpg binnen regiokorps Noord- en Oost-Gelderland. Het implementatie team van de Wpg heeft procedures beschreven en formulieren ontwikkeld ter ondersteuning van het proces rechten van de betrokkene. Er is een stroomschema opgesteld op basis van de Landelijke handreiking. In de eindrapportage van dit project heeft de implementatie van het artikel de status AF gekregen. Echter uit de interne audit blijkt dat de procedures uit de landelijke handreiking niet specifiek zijn gemaakt en ook niet zijn afgestemd op de administratieve organisatie van het korps.

4.10.3 *Verbeterpunt*

- Maak de landelijke handreiking specifiek en stem deze af op de administratieve organisatie van het korps.

4.11 Protocolplicht (art 32)

4.11.1 *Norm*

De verantwoordelijke draagt zorg voor de schriftelijke vastlegging van:

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

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

4.11.2 *Bevindingen*

Volgens het privacyjaarverslag 2009-2010 heeft de privacyfunctionaris een overzicht van alle protocolgegevens. Dit is nodig om de toezichhoudende en adviserende taak uit te voeren. De privacyfunctionaris houdt van een aantal protocol verplichtingen overzichten bij.

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

4.12 Audits (art 33)

4.12.1 *Norm*

Bij regeling van Onze Ministers kan bepaald worden dat ter voorbereiding op de controle, bedoeld in het eerste lid, interne audits plaatsvinden en kunnen regels worden gesteld over de wijze waarop deze audits worden verricht.

4.12.2 *Bevindingen*

Binnen het korps Noord- en Oost-Gelderland is in de periode maart tot en met juni 2011 een interne audit uitgevoerd, die als verdienstelijk kan worden gekwalificeerd en heel praktisch is gericht op het zicht krijgen op bestaande knelpunten in de uitvoering van de Wpg. De audit is uitgevoerd in opdracht van de korpschef na goedkeuring van het opgestelde plan van aanpak. Het interne auditteam bestaat uit 5 medewerkers van de afdeling Sturingsondersteuning en de Divisie Informatie & Intelligence. Zij hebben een training gevolgd op het gebied van auditing en de Wpg. In de interne audit is niet naar alle artikelen van de Wpg gekeken. Op basis van een risicoanalyse zijn de artikelen bepaald. Men is nu bezig een auditplanning voor de komende jaren op te stellen, waarbij er jaarlijks een audit plaats vindt. Na vier jaar zijn op deze wijze alle artikelen van de Wpg aan bod gekomen.

4.12.3 *Verbeterpunten*

- Houd bij de interne meerjaren auditplanning rekening met de opvolging van de aanbevelingen uit de voorgaande audits.
- Zorg voor een structurele borging van de interne auditfunctie. Borg hierbij ook de vaktechnische kennis, bijvoorbeeld door het aanbieden van een interne audit opleiding.

4.13 Privacy functionaris (art 34)

4.13.1 *Norm*

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

4.13.2 *Bevindingen*

De privacyfunctionaris is formeel aangesteld door de korpschef en aangemeld bij het CBP. De privacyfunctionaris voert o.a. de volgende taken uit:

- Een overzicht bijhouden van de toekenning van artikel 6 autorisaties; de autorisatieverzoeken van lijnchefs voor hun medewerkers, waarop zij het fiat moet geven.

- Een overzicht bijhouden van de meldingen/sluitingen van onderzoeken ex artikel 9, daarbij wordt met name het doel getoetst.
- Een overzicht bijhouden van de gegevens krachtens artikel 13 Wpg m.b.t. ondersteunende taken).
- Een overzicht bijhouden van de gegevens krachtens artikel 25 Wpg i.v.m. art.4 BPG (= recht van betrokkenen).
- Een overzicht bijhouden van incidentele verstrekkingen.
- Een privacyjaarverslag opstellen.
- Wpg- en de Wob-verzoeken zijn bij de privacy functionaris belegd.

Het uitvoeren van de toezichthoudende taak van de privacyfunctionaris krijgt om informatie. Tijd om daadwerkelijk toezichthoudende activiteiten uit te voeren in het veld is er daardoor niet.

De functiebeschrijving van de privacyfunctionaris was gericht op de Wet Politierregisters. In het nieuwe functiehuis wordt wel gesproken over de aanstelling conform artikel 34 Wpg, maar over de inhoud van het werk wordt niets vermeld.

4.13.3

Verbeterpunten

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

4.14 Functionaris Gegevensbescherming (art 36)

Het korps Noord- en Oost-Gelderland heeft geen functionaris Gegevensbescherming.

