COLLEGE BESCHERMING PERSOONSGEGEVENS

POLITIE INFODESK

Onderzoek naar de inrichting van de politie infodesk en de waarborgen voor de bescherming van persoonsgegevens

Onderzoeksrapport

INHOUD

COLLEGE BESCHERMING PERSOONSGEGEVENS

Politie infodesk

Onderzoek naar de inrichting van de politie infodesk en de waarborgen voor de bescherming van persoonsgegevens

Onderzoeksrapport

College bescherming persoonsgegevens - oktober 2008

SAMENVATTING

De praktijk van steeds ruimere toegang van de infodesks van de politiekorpsen tot afgeschermde politie-informatie is onder de op 1 januari 2008 in werking getreden Wet politiegegevens bestendigd en uitgebreid. In de aanloop naar de nieuwe wet heeft het College bescherming persoonsgegevens (CBP) onderzoek gedaan naar het functioneren van de infodesk en naar de waarborgen die de infodesk biedt voor de bescherming van persoonsgegevens.

De infodesk vormt een continu beschikbaar en herkenbaar loket binnen de politieregio, dat op verzoek snel en zorgvuldig operationele informatie aan gelegitimeerde functionarissen uit de daartoe beschikbare bronnen verstrekt, dan wel op basis van inzicht in informatie beheerders, gebruikers en aanvragers van informatie bij elkaar brengt. Daarnaast verstrekt de infodesk operationele informatie ten behoeve van strategische en tactische besluitvorming.

In de tot 1 januari 2008 geldende Wet politieregisters (Wpolr) kwam de functie van de infodesk niet voor. De Memorie van Toelichting bij de Wet politiegegevens (Wpg), die de Wpolr per die datum heeft vervangen, onderkent de functie van de infodesk wel expliciet.
De in de oude situatie al bestaande tendens om ter verhoging van de effectiviteit de toegang van de infodesk tot afgeschermde politie-informatie steeds verder uit te breiden, is in de nieuwe wet uitdrukkelijk mogelijk gemaakt. In de Wpg zijn de toegangsmogelijkheden van de infodesk tot gegevens in specifieke onderzoeken ten opzichte van de praktijk onder de oude wet toegenomen.

Op grond van artikel 35 Wpg ziet het College bescherming persoonsgegevens (CBP) toe op de verwerking van politiegegevens. Het onderzoek waarvan dit rapport verslag doet, is er op gericht zicht te krijgen op het functioneren van de infodesk in de regionale politiekorpsen en naar de wijze waarop de wettelijke waarborgen voor de bescherming van persoonsgegevens worden gegarandeerd. Zowel de situatie onder de in 2007 vigerende Wpolr als die onder de huidige Wpg is onderzocht.
Het onderzoek heeft in twee fasen plaatsgevonden. De eerste fase betrof het verkrijgen van informatie op basis van schriftelijke vragen aan de vijfentwintig regionale politiekorpsen. De tweede fase van het onderzoek bestond uit het bezoeken van drie politieregio's.

Inrichting

De wijze waarop de infodesk is georganiseerd, verschilt sterk per regio. Bijna alle korpsen (21) melden dat er een administratieve beschrijving van de infodesk aanwezig is.
De functies van de infodeskmedewerkers zijn in alle regio's vastgelegd in formele functieomschrijvingen.

Waarborgen

De Wpg verplicht de verantwoordelijke, de korpsbeheerder, zorg te dragen voor het kwaliteitsniveau en de deskundigheid van zijn medewerkers. Dit geldt als een van de waarborgen voor het zorgvuldig gebruik van de ruimere bevoegdheden die de Wpg biedt voor de verwerking van persoonsgegevens. Het onderzoek wijst uit dat er wat betreft de kwaliteitseisen die aan de medewerkers van de infodesk worden gesteld, sprake is van grote verscheidenheid tussen de regio's.

Een andere waarborg is gelegen in het autorisatiebeleid. Bijna alle regio's (24) verklaren een autorisatiesysteem te hanteren. De aard van het systeem en wie formeel en functioneel de autorisaties verstrekt is per korps anders geregeld.
Met het oog op de controleerbaarheid van de handelingen dient elk korps te voorzien in een logging van de bevragingen. In het bijzonder bij de toegang tot de bijzondere registers dient dat systematisch plaats te vinden. De bevragingen door infodeskmedewerkers van de

diverse registers worden in de meeste regio's (20) gelogd. Zes regio's melden dat de handelingen van de infodeskmedewerkers waarbij gegevens uit het bijzondere register worden geraadpleegd, niet worden gelogd. De regio's die nog niet stelselmatig loggen zullen dit onder de nieuwe wet, waarin het loggen een wettelijke verplichting is, wel moeten gaan doen. De meeste (16) van de regio's waar reeds logging plaatsvindt, controleren de loggings niet structureel. De Wpg schrijft controle op de logging door middel van audits voor.

Privacyfunctionaris, Functionaris gegevensbescherming en audits

Zeven van de 25 korpsen melden geen privacyfunctionaris of functionaris gegevensbescherming te hebben. In de overige korpsen is de inrichting van de functies uiteenlopend ingevuld. De Wpg bepaalt dat de privacyfunctionaris een overzicht van de autorisaties bijhoudt. De korpsen dienen hun autorisatiebeleid daarop aan te passen. Het merendeel van de regio's (15) verklaart thans geen audits te laten uitvoeren. Met de invoering van de Wpg is het laten uitvoeren van een audit verplicht.

Conclusie

Ter compensatie van de mogelijkheid van ruimere gegevensverstrekkingen binnen en door de regio's die door de Wpg is geïntroduceerd, zijn in de nieuwe wet waarborgen opgenomen. Veruit de meeste politieregio's bleken ten tijde van het onderzoek niet toegerust te zijn voor de situatie na 1 januari 2008 en hadden geen volledig beeld van de aard van de wijzigingen die doorgevoerd zouden moeten worden om deze waarborgen te effectueren. Tevens verklaren zij niet voornemens te zijn om wijzigingen als gevolg van de inwerkingtreding van de Wpg door te voeren. Deze betreffen met name de voorgeschreven kwaliteitseisen van infodeskmedewerkers, het autorisatiebeleid, de controle op de logging door middel van audits en tot slot de rol van de privacyfunctionaris binnen de regio. Hierdoor wordt niet voldaan aan de eisen die de Wpg stelt aan een zorgvuldige gegevensverwerking. Het CBP acht dit uitermate zorgwekkend.

Het CBP is toezichthouder op de verwerking van persoonsgegevens op grond van de Wet politiegegevens. Het CBP wijst erop dat naleving van de wet en zorgvuldige omgang met gevoelige persoonsgegevens vereisen dat de leemten die door dit onderzoek aan het licht zijn gekomen, worden opgevuld.

INLEIDING

Opsporingsambtenaren kunnen met informatieverzoeken terecht bij de infodesk van hun korps. De infodesk heeft zowel binnen het eigen korps als door middel van contacten bij andere korpsen toegang tot verschillende politiegegevens. Om de effectiviteit van de infodesks te vergroten is de tendens ontstaan om de toegang tot afgeschermde politie-informatie steeds verder uit te breiden. Deze mogelijkheid is met de inwerkingtreding van de Wet politiegegevens per 1 januari 2008 verder toegenomen. Het College bescherming persoonsgegevens heeft in de aanloop naar de nieuwe wet een onderzoek uitgevoerd naar het functioneren van de infodesk in de politieregio's en naar de wijze waarop de wettelijke waarborgen voor de bescherming van persoonsgegevens worden gegarandeerd.

De Wet politieregisters (Wpolr) is per 1 januari 2008 vervangen door de Wet politiegegevens (Wpg). De Memorie van Toelichting op de Wpg[1] opent met de zin: *'De samenleving verlangt van de politie dat deze op doelmatige en doeltreffende wijze zorg draagt voor de handhaving van de rechtsorde. Voorwaarde voor een goede taakuitvoering door de politie is dat de daarvoor noodzakelijke gegevens kunnen worden vastgelegd en op een efficiënte en effectieve wijze kunnen worden verwerkt. Meer dan ooit drijft het werk van de politie immers op het verwerken en veredelen van informatie. (…) waar aan de ene kant uitdrukkelijk is gekozen voor verruiming van de wettelijke mogelijkheden tot opslag, gebruik en verstrekking van persoonsgegevens door de politie voorziet het wetsvoorstel aan de andere kant in de nodige waarborgen voor de burger tegen ongerechtvaardigde inbreuken op zijn persoonlijke levenssfeer.'*

De infodesk

De infodesk wordt gedefinieerd[2] als een 'continue beschikbare eenheid ten behoeve van het opsporingsproces, die als een herkenbaar loket binnen de politieregio op verzoek snel, zo volledig en zorgvuldig mogelijk operationele informatie aan gelegitimeerde functionarissen uit daartoe beschikbare bronnen verstrekt, dan wel makelt. Deze eenheid verstrekt tevens operationele informatie ten behoeve van strategische en tactische besluitvorming.'

Om de effectiviteit van de infodesks te vergroten, is in de praktijk de toegang van de infodesk tot afgeschermde politie-informatie steeds verder uitgebreid. In de Memorie van Toelichting bij de Wpg wordt de functie van de infodesk, die in de Wpolr niet voorkwam, uitdrukkelijk onderkend.[3]

De toegangsmogelijkheden van de infodesk tot gegevens in specifieke onderzoeken zijn onder de Wpg toegenomen. De gegevens die onder de Wpolr werden verwerkt in tijdelijke registers worden onder de Wpg verwerkt ten behoeve van onderzoek in verband met de handhaving van de rechtsorde in een bepaald geval (ook te noemen: onderzoeksverwerking, of tijdelijke verwerking). Onder de Wpolr was de mogelijkheid om infodeskmedewerkers te autoriseren voor het tijdelijk register beperkt tot gegevens betreffende verdachten. Onder de Wpg kunnen infodeskmedewerkers geautoriseerd worden om alle gegevens in tijdelijke verwerkingen in een geautomatiseerde vergelijking te betrekken. Daarbij is wel een nieuwe beperking om de hoek komen kijken: zoekacties in onderzoeksgegevens mogen in beginsel alleen plaatsvinden ten behoeve van andere specifieke onderzoeken.

Onder de Wpolr was het mogelijk om infodeskmedewerkers te autoriseren voor het register zware criminaliteit voor zover het gegevens omtrent verdachten en betrokkenen betrof. Infodeskmedewerkers konden voor gegevens betreffende contacten alleen worden geautoriseerd indien en voor zover dezen tevens als verdachte waren aan te merken. Onder de Wpg kunnen infodeskmedewerkers geautoriseerd worden

---

[1] Kamerstukken II 2005-2006, 30327, nr. 3, p.1

[2] Regeling Regionale Infodesk. In 2001 vastgesteld door de Raad van Hoofdcommissarissen (zie Bijlage 3).

[3] Kamerstukken II 2005-2006, 30 327, nr. 3, p. 27, 41 en 53.

tot alle zwarecriminaliteitgegevens in het kader van projectvoorbereiding en het opstellen van operationele misdaadanalyses.

Protocolplicht en privacyaudits onder de Wpg

In de Wpg is de protocolplicht ingevoerd[4], waaronder de verplichting om een overzicht bij te houden met de toekenning van de verstrekte autorisaties. Tevens is in de wet aan de korpsen opgedragen om periodiek privacyaudits uit te (laten) voeren[5]. Een afschrift van de controleresultaten van de privacyaudits dient aan het CBP te worden gezonden. Het CBP ziet toe op de verwerking van politiegegevens. Het CBP heeft de mogelijkheid om op basis van de Wpg bestuurlijke boetes op te leggen indien de protocolplicht niet wordt nagekomen (art. 35, eerste lid jo. art. 32 Wpg).

Het onderzoek

Het onderzoek waarvan in dit rapport verslag wordt gedaan, is er op gericht met het oog op (ten tijde van het onderzoek nog aanstaande) inwerkingtreding van de Wpg zicht te krijgen op het functioneren van de infodesk in het algemeen. Hoe is de infodesk ingericht en welke waarborgen voor de bescherming van persoonsgegevens biedt de infodesk daarbij?

Het onderzoek heeft in twee fasen plaatsgevonden. De eerste fase betrof het verkrijgen van informatie bij de vijfentwintig politieregio's op basis van schriftelijke vragen. De tweede fase van het onderzoek bestond uit het bezoeken van drie politieregio's. Het onderzoek vond van juni tot en met november 2007 plaats. De werkwijze van het onderzoek wordt in Bijlage 1 meer uitgebreid beschreven.

---

[4] Artikel 32 Wpg.

[5] Artikel 33 Wpg.

1

NORMENKADER

De verwerking van gegevens in politieregisters gebeurde tot en met 31 december 2007 onder het regime van de Wet politieregisters (Wpolr) en het Besluit politieregisters (Bpolr). Dit onderzoek richt zich bij de beoordeling van de bevindingen omtrent de Regionale infodesks bij de regionale politiekorpsen op de opvolger van de Wpolr, de Wet politiegegevens (Wpg). In dit hoofdstuk worden beide wetten nader toegelicht.

In algemenere zin geldt voor het beheer en de informatiebeveiliging de Politiewet 1993 en op basis daarvan het Besluit beheer regionale politiekorpsen. Artikel 3a van dat Besluit bepaalt dat de korpsbeheerder zorg draagt voor deugdelijke informatiebeveiliging, hetgeen omvat het treffen en onderhouden van een samenhangend pakket van maatregelen ter waarborging van de beschikbaarheid, integriteit en exclusiviteit van de informatiesystemen, onverminderd het bepaalde bij de Wet politieregisters en de Wet bescherming persoonsgegevens.

In artikel 2 van de Politiewet 1993 is de taak van de politie vastgelegd. Voor de goede uitvoering van de politietaak is het van essentieel belang dat op een efficiënte wijze bruikbare en juiste informatie wordt uitgewisseld tussen de verschillende korpsen en dienstonderdelen die zich bezighouden met de uitvoering van de politietaak, in het bijzonder het opsporingsproces, maar ook ter ondersteuning van strategische en tactische besluitvorming op basis van operationele informatie.
Een uniforme werkwijze voor de regionale infodesks is neergelegd in de Regeling Regionale Infodesk. Deze geldt als uitgangspunt. In de regeling is ook het takenpakket beschreven voor de regionale infodesk. De regeling is vastgesteld onder de verantwoordelijkheid van de Raad van Hoofdcommissarissen.

Wet politieregisters
De Wpolr ging uit van het registerbegrip (artikel 1, eerste lid onder c Wpolr).
De wet concentreerde zich op het opnemen van gegevens in politieregisters en het verstrekken van gegevens uit politieregisters.
Een politieregister werd ingevolge artikel 4 Wpolr aangelegd en aangehouden voor een bepaald doel en voor zover dit noodzakelijk was voor de goede uitvoering van de politietaak (zoals omschreven in artikel 2 Politiewet 1993). Voor ieder register moest een reglement worden opgesteld (artikel 9 Wpolr e.v.). Kern van het reglement was de omschrijving van het doel van het register.

Voor een politieregister was eindverantwoordelijk de beheerder in de zin van de Wpolr, tevens de verantwoordelijke in de zin van de Wet bescherming persoonsgegevens (Wbp). Bij de regionale politiekorpsen was dat de korpsbeheerder, zijnde de burgemeester van de grootste gemeente in de politieregio (artikel 1, eerste lid onder f Wpolr). Deze diende een registerbeheerder aan te stellen die de verantwoordelijkheid voor het register kreeg gedelegeerd. Deze kon op zijn beurt weer iemand met de dagelijkse leiding van het register belasten.

Artikel 7 Wpolr bepaalde dat de beheerder zorg droeg voor de juiste werking van het register. De beheerder droeg ook zorg voor de nodige voorzieningen van technische en organisatorische aard ter beveiliging van het register tegen verlies of aantasting van de gegevens en tegen onbevoegde kennisneming, wijziging of verstrekking daarvan.

De beheerder, de registerbeheerder en degene die was belast met de dagelijkse leiding hadden voor het vervullen van hun respectieve rollen toegang tot de gegevens in het betreffende register. Zij konden gegevens verstrekken uit het register overeenkomstig het verstrekkingenregime dat in de Wpolr was vastgelegd. De Wpolr kende de mogelijkheid gegevens rechtstreeks langs geautomatiseerde weg te verstrekken. Hiervoor was ingevolge artikel 17 Bpolr een schriftelijke autorisatie van de beheerder vereist. Het wettelijk vastgelegde verstrekkingenregime kon niet door een autorisatie worden doorbroken.

Het gesloten verstrekkingenregime van de Wpolr bestreek zowel de verstrekkingen uit een politieregister binnen de politie (interne verstrekkingen) als aan derden (externe verstrekkingen). Voor interne verstrekkingen gold het uitgangspunt dat uit een politieregister gegevens konden worden verstrekt aan ambtenaren van politie en ander politiepersoneel dat was aangesteld ter uitvoering van de politietaak, indien dat noodzakelijk was voor een goede uitvoering van de politietaak: de zogenaamde *'free flow of information'*, zij het dat daarvoor wel het *'need to know'*-principe gold. *'Nice to know'* was onvoldoende grond voor verstrekking.

Het reglement regelde ingevolge artikel 10,vierde lid Wpolr ook de verstrekking van gegevens uit het register, daaronder begrepen de rechtstreekse toegang met het oog op de raadpleging van persoonsgegevens. Een reglement kon het wettelijk verankerde verstrekkingenregime niet verruimen maar wel inperken.

Bij wijze van controlemechanisme voorzag artikel 19 Wpolr in een protocolplicht. In het Bpolr, de artikelen 16 tot en met 18, was deze nader uitgewerkt ten aanzien van een verstrekking rechtstreeks langs geautomatiseerde weg en niet rechtstreeks langs geautomatiseerde weg.

Ook kende de Wpolr de Functionaris voor de Gegevensbescherming als intern onafhankelijk toezichthouder: artikel 27 Wpolr bepaalde dat de artikelen 60 tot en met 64 Wbp daarop van overeenkomstige toepassing waren. Daarnaast kenden politiekorpsen de functie van privacyfunctionaris. Deze had echter geen wettelijke en onafhankelijke status en functioneerde vooral als adviseur van de beheerder.

Bijzondere politieregisters

De Wpolr maakte onderscheid tussen gewone politieregisters en bijzondere politieregisters. Onder bijzondere politieregisters werden begrepen de tijdelijke registers, de registers zware criminaliteit en de voorlopige registers. Paragraaf 3a Wpolr had betrekking op de bijzondere registers.

Voor bepaalde registers kon een afwijkend verstrekkingenregime gelden. Dat had zijn oorsprong ofwel in de regeling van het betreffende bijzondere register in de Wpolr ofwel in het reglement dat voor het register was vastgesteld.

De Wpolr bepaalde dat gegevens uit een tijdelijk register slechts mochten worden verstrekt overeenkomstig het doel van het register. Alleen als het opsporingsonderzoek waarvoor het register was aangelegd verstrekking vereiste, mocht derhalve verstrekking plaatsvinden.
Hieruit volgde dat alleen leden van het onderzoeksteam geautoriseerd mochten worden.
Een uitzondering op deze hoofdregel betroffen de gegevens over verdachten waarvoor *'free flow of information'* gold. Bovendien mochten gegevens, ook die over onverdachte personen, worden verstrekt ten behoeve van opneming in het register zware criminaliteit.
De eerste uitzondering maakte rechtstreekse toegang van de infodesk tot gegevens omtrent verdachten in tijdelijke registers mogelijk. Voorwaarde daarvoor was wel dat in het betreffende tijdelijk register onderscheid werd gemaakt tussen gegevens omtrent verdachten en andere gegevens.

De Wpolr bepaalde dat in het register zware criminaliteit (zwacriregister) gegevens konden worden opgenomen omtrent verdachten, betrokkenen en contacten van verdachten respectievelijk betrokkenen.
Voor gegevens omtrent verdachten en betrokkenen gold intern de *'free flow of information'*. Hierbij verdient aantekening dat gegevens omtrent betrokkenen, voor zover zij niet als verdachte konden worden aangemerkt, niet langer dan vier maanden in een gewoon politieregister mochten worden opgeslagen.
Ten aanzien van gegevens omtrent contacten bevatte de wet de hoofdregel dat deze alleen mochten worden verstrekt ten behoeve van opneming in een ander bijzonder politieregister, zoals een tijdelijk register. Een uitzondering hierop bestond als het

contact aangemerkt kon worden als verdachte, in welk geval de *'free flow of information'* gold.
De infodesk kon op grond hiervan worden geautoriseerd tot gegevens in het register zware criminaliteit omtrent verdachten en betrokkenen. Ten aanzien van contacten kon de infodesk slechts worden geautoriseerd tot gegevens omtrent contacten die als verdachte aangemerkt konden worden.

Op grond van de Wpolr konden medewerkers van de infodesk dus worden geautoriseerd tot gegevens omtrent verdachten en betrokkenen in het zwacriregister.
De mogelijkheid om infodeskmedewerkers te autoriseren tot gegevens in een tijdelijk register en tot gegevens omtrent contacten in een zwacriregister waren beperkt tot gegevens over geregistreerden die konden worden aangemerkt als verdachte.

Daarnaast is op de verwerking van zwacrigegevens de CIE-Regeling (Stcr. 12 oktober 2000, nr. 198) van toepassing. In artikel 4 van die Regeling zijn de werkzaamheden van de Criminele Inlichtingen Eenheid beschreven, waaronder ook het analyseren van criminele inlichtingen en het verstrekken van criminele inlichtingen overeenkomstig de daartoe vastgestelde modelreglementen. In de toelichting op dit artikel staat onder meer het volgende: *'Het modelreglement voor het register zware criminaliteit gaat uit van het beginsel van vrije verstrekking binnen de politieorganisatie; verstrekking van gegevens kan alleen dan achterwege worden gelaten indien de goede uitvoering van de politietaak zich daartegen verzet (vgl. artikel 13a, derde lid Wpolr). Dit betekent ook dat aan nieuwe functionaliteiten binnen de politiekorpsen zoals de infodesks ruime medewerking moet worden verleend, met dien verstande dat informatieverstrekking vanuit de criminele inlichtingen eenheid niet rechtstreeks langs geautomatiseerde weg kan plaatsvinden, omdat daarmee de toetsing of de goede uitvoering van de politietaak aan de verstrekking in de weg staat, zou komen te vervallen.'*

Wet politiegegevens (Wpg)

De Wet politiegegevens (Wpg) verlaat het registerbegrip en gaat uit van het verwerken van politiegegevens. De verantwoordelijke voor die verwerking bij de regionale politiekorpsen is ingevolge artikel 1, onder f Wpg de korpsbeheerder.

Eén van de uitgangspunten van de Wpg is dat politiegegevens alleen mogen worden verwerkt voor de doelen waarvoor ze zijn verkregen, behalve als de wet uitdrukkelijk in doelafwijkende bepalingen voorziet (artikel 3, derde lid Wpg). De wet bepaalt daartoe bij de verschillende doeleinden van verwerking of de daarvoor verwerkte politiegegevens, en zo ja ten behoeve van welke andere doeleinden de betreffende politiegegevens ter beschikking kunnen worden gesteld. Ook doorbreekt de wet de doelbinding door te voorzien in de geautomatiseerde vergelijking en het in combinatie met elkaar verwerken van politiegegevens die voor verschillende doeleinden worden verwerkt, zoals bepaald in artikel 11 Wpg. Het geautomatiseerd vergelijken houdt in dat een verzameling van gegevens wordt bevraagd aan de hand van gegevens uit een andere verwerking.

Een ander uitgangspunt van de Wpg is het autorisatievereiste, neergelegd in artikel 6 Wpg en nader uitgewerkt in het Bpg: de Wpg en het Bpg bepalen wie geautoriseerd kunnen worden tot het verwerken en het geautomatiseerd vergelijken van gegevens. De verantwoordelijke dient de politiefunctionarissen te autoriseren tot die verwerkingen van politiegegevens die zij nodig hebben voor het uitvoeren van de aan hen opgedragen onderdelen van de politietaak.

In het Bpg worden niet alleen categorieën te autoriseren personen aangewezen, maar ook deskundigheidseisen gesteld. Autorisaties zijn daarmee de spil in de bescherming van politiegegevens; het autorisatiebeleid maakt deel uit van het beveiligingsbeleid. In de nieuwe wet heeft de verantwoordelijke de verplichting ervoor zorg te dragen dat de infodeskmedewerkers voldoen aan eindtermen betreffende kennis en vaardigheden op het gebied van het informatieproces binnen de politie, de verschillende vormen van verwerking van politiegegevens en de wet- en regelgeving over de verwerking van politiegegevens (artikel 2:7 Bpg). Deze kwaliteitseisen worden gekoppeld aan de te verlenen autorisaties.

Welke gegevens door welke politiefunctionarissen mogen worden verwerkt krijgt vervolgens vorm door de combinatie van doelbinding en de daarop geformuleerde uitzonderingen en het stelsel van autorisaties dat de verantwoordelijke binnen de gegeven grenzen dient vorm te geven. De privacyfunctionaris, die binnen iedere regio aangesteld moet zijn ingevolge artikel 34 Wpg, krijgt onder meer de taak om een overzicht bij te houden van de verleende autorisaties.
De privacyfunctionaris is, hoewel hij geen formele bevoegdheden had onder de Wpolr, wel al in de meeste regio's aanwezig. De privacyfunctionaris krijgt in de Wpg de taak namens de verantwoordelijke toe te zien op de verwerking van gegevens, waaronder het bijhouden van een lijst met autorisaties en het adviseren van de verantwoordelijke over de naleving van de wet.

In de Wpg is tevens de protocolplicht opgenomen. Niet alleen verstrekkingen van politiegegevens, maar ook aanwijzingen dat gegevens onrechtmatig verwerkt worden, moeten schriftelijk worden bijgehouden. Dit geldt ook voor de toekenning van autorisaties. In het Bpg wordt de wijze waarop moet worden gelogd nader uiteengezet.

In de Wpg is voorzien in drie vormen van intern toezicht: het periodiek laten uitvoeren van privacyaudits ter controle op de naleving van de wet (artikel 33 Wpg), het toezicht door de functionaris gegevensbescherming (artikel 36 Wpg) en de verplichting een privacyfunctionaris aan te wijzen (artikel 34 Wpg). De wetgever heeft het van belang geacht passende waarborgen te creëren *'teneinde zorg te dragen dat de door het wetsvoorstel voorgestelde grenzen in de praktijk niet worden overschreden'*[6]. Bovendien is in de MvT (idem) opgemerkt dat *'wil men tot een evenwichtig verwerkingsbeleid van politiegegevens komen en dit adequaat implementeren en onderhouden, dan zal dat een belangrijke plaats in de managementcyclus moeten innemen.'* De auditverplichting bestond niet onder de Wpolr.

Onder het nieuwe regime is in het Bpg bij de invulling van de voorwaarden voor bepaalde autorisaties uitdrukkelijk het bestaan van een functionaliteit als die van de infodesk onderkend.

Paragraaf 2 van de Wpg heeft betrekking op de interne verwerking van politiegegevens, de onderlinge uitwisseling van politiegegevens daaronder begrepen. Voor ieder doel is uit deze paragraaf een intern verstrekkingenregime af te leiden. Het eerdere tijdelijke register en het register zware criminaliteit zijn onder de Wpg overgegaan in sterk met deze registers corresponderende verwerkingen, te weten de verwerking van politiegegevens ten behoeve van onderzoek in verband met de handhaving van de rechtsorde in een bepaald geval (artikel 9 Wpg, vergelijkbaar met de tijdelijke registers onder de Wpolr), respectievelijk de verwerking van politiegegevens met het oog op het verkrijgen van inzicht in de betrokkenheid van personen bij zware criminaliteit (artikel 10, eerste lid, onder a Wpg, vergelijkbaar met de vroegere registers zware criminaliteit).

Het Bpg staat toe dat de verantwoordelijke aan infodeskmedewerkers een autorisatie verleent om tijdelijke verwerkingen te betrekken in geautomatiseerde vergelijkingen van politiegegevens. Dergelijke zoekacties in onderzoeksgegevens mogen door infodeskmedewerkers in beginsel alleen worden uitgevoerd aan de hand van gegevens

---

[6] Memorie van Toelichting, Kamerstukken II 2005-2006, 30 327, nr. 3, p. 89

[7] Staatsblad 2007, 550, p. 35

uit en ook slechts ten behoeve van andere tijdelijke verwerkingen.
Alleen in voorkomende gevallen, waarmee blijkens de nota van toelichting[7] in dit geval wordt bedoeld: als er personele capaciteitsproblemen zijn bij de criminele inlichtingen eenheid (CIE), mogen infodeskmedewerkers ook worden geautoriseerd tijdelijke verwerkingen te bevragen aan de hand van zwacrigegevens ten behoeve van een zwacriverwerking.
Uit de omstandigheid dat deze functionele autorisatie voor het geautomatiseerd vergelijken van gegevens met tijdelijke verwerkingen aan de infodesk kunnen worden toegekend kan afgeleid worden dat in beginsel aan infodeskmedewerkers niet een doelgebonden autorisatie voor een tijdelijke verwerking kan worden verleend. Infodeskmedewerkers kunnen dus geautoriseerd worden tot gegevens in tijdelijke verwerkingen ten behoeve van de uitwisseling daarvan met andere tijdelijke verwerkingen.

Het Bpg staat toe dat de verantwoordelijke aan infodeskmedewerkers in voorkomende gevallen een autorisatie verleent om zwacrigegevens te verwerken.
Met voorkomende gevallen wordt blijkens de nota van toelichting[8] in dit verband bedoeld: ten behoeve van het voorbereiden van projecten of het opstellen van strategische of operationele misdaadanalyses.
Het Bpg staat bovendien toe dat de verantwoordelijke aan infodeskmedewerkers in voorkomende gevallen een autorisatie verleent voor het geautomatiseerd vergelijken van een zwacriverwerking aan de hand van (andere) zwacrigegevens, gegevens uit een themaverwerking, dan wel gegevens uit een RID-verwerking. Met voorkomende gevallen wordt in dit verband weer bedoeld situaties waarin om redenen van personele capaciteit bij de CIE uitbreiding van de kring van geautoriseerden is vereist.
Hieruit volgt dat infodeskmedewerkers onder de Wpg in voorkomende gevallen geautoriseerd kunnen worden tot zwacrigegevens, namelijk voor operationele misdaadanalyses en in het kader van de voorbereiding van projecten.

---

[8] Staatsblad 2007, 550, p. 39

2

BEVINDINGEN

2.1 Inrichting en werkwijze regionale infodesks

Positionering

De positionering van de politie infodesk verschilt sterk per korps. In elf korpsen vormt de infodesk een onderdeel van een informatie-eenheid. In zeven korpsen is de infodesk een onderdeel van het Regionaal Informatie Knooppunt (RIK). Andere korpsen hebben de infodesk ergens anders ondergebracht, bijvoorbeeld onder de afdeling Regionale Recherche.
Wanneer naar de positionering van de infodesk ten opzichte van de Criminele Inlichtingen Eenheid (CIE) wordt gekeken, blijkt dat de meeste korpsen (13) ervoor hebben gekozen om de infodesk onder te brengen in dezelfde eenheid als de CIE.
In drie gevallen hebben de CIE en de infodesk ook dezelfde leidinggevende.

Organisatie

De organisatorische inrichting verschilt per korps. Bij dertien van de vijfentwintig ondervraagde korpsen is sprake van een centrale en een decentrale infodesk. In dat geval heeft de infodesk meerdere locaties. Zes korpsen hebben uitsluitend een centrale infodesk waar de informatieverzoeken van het gehele korps binnenkomen. Van de andere regio's is uit de antwoorden op de vragenlijst niet op te maken of zij met alleen een centrale of ook met decentrale infodesks werken.
In antwoord op de vraag naar de manier waarop de informatieverzoeken worden verwerkt, geven dertien van de vijfentwintig korpsen aan met een aparte front- en backoffice te werken.
In enkele regio's worden externe klanten direct bediend door het backoffice.
Eén regio kiest er voor om externe klanten juist specifiek via het frontoffice te bedienen. De meeste regio's rekenen andere infodesks, het Openbaar Ministerie (OM), de Koninklijke Marechaussee (KMar) en dergelijke tot hun externe klanten.
De intake gebeurt doorgaans op dezelfde wijze.
Ook de drie bezochte korpsen hebben de infodesk verschillend ingericht. Twee infodesks melden in het frontoffice te werken met een centrale intake. Vragen komen doorgaans centraal binnen en worden door een senior medewerker uitgezet bij de medewerkers die de verzoeken backoffice afhandelen. Het derde bezochte korps kent geen scheiding tussen front- en backoffice.

Organisatorische integratie

De vijfentwintig korpsen is gevraagd of ze een vorm hanteren van (organisatorische) integratie van de informatiefuncties, bijvoorbeeld of de verschillende afdelingen zoals de CIE, infodesk en misdaadanalyse zijn samengevoegd in een centrale informatieafdeling. In achttien regio's is geen sprake van integratie van de informatiefuncties. Zes korpsen verklaren dat dat wel het geval is; soms is sprake van volledige ontschotting. Van één korps is niet bekend of het een vorm van organisatorische integratie hanteert.

Administratie

De korpsen is gevraagd of zij de organisatorische invulling van de infodesk ook hebben beschreven in een administratieve organisatie. Bijna alle korpsen (21) beantwoorden die vraag positief. Vier korpsen verklaarden dat de infodesk niet is beschreven in een administratieve organisatie.
Tien korpsen melden dat er bij de infodesk geen specifieke werkprocedure is voor het verwerken van gegevens die zijn opgenomen in tijdelijke en zwacriregisters.
Van de vijftien korpsen die melden wel een specifieke werkprocedure te hebben, hebben negen korpsen die werkprocedure echter niet kunnen overleggen.
Als werkprocedure noemen zes korpsen de CIE-regeling. Eén korps meldt dat het hele proces met betrekking tot de toegang tot bijzondere registers onder de CIE valt.
Driekwart van de korpsen heeft ook de taken van de infodesk beschreven. Bij de overige korpsen zijn de taken niet duidelijk beschreven.

De ondervraagde korpsen hanteren verschillende benamingen voor de functies binnen de infodesks. Alle korpsen geven aan dat de functies zijn beschreven.
De functie-eisen die door de korpsen worden gesteld aan infodeskmedewerkers lopen erg uiteen.
Bij de bezoeken aan de drie korpsen is door de infodesks aangegeven dat procedures en afspraken niet altijd formeel zijn vastgesteld. Als redenen hiervoor worden de vele veranderingen en ontwikkelingen genoemd, die tegelijkertijd werden en worden doorgevoerd, zoals de overgang naar het nieuwe Blue View[9] en de invoering van de Wpg.

Bovenregionale samenwerking

Uit de vragenlijsten en de interviews bleek dat sommige politiekorpsen streven naar het opzetten van bovenregionale diensten, bijvoorbeeld op het gebied van informatiebeveiliging en bescherming van persoonsgegevens. Zo worden ook bij de voorbereidingen van de invoering van de Wpg afspraken gemaakt over het inrichten van bovenregionale samenwerkingsverbanden, bijvoorbeeld voor de invulling van de functies van de functionaris gegevensbescherming en de privacyfunctionaris: sommige korpsen willen samen één functionaris gegevensbescherming aanstellen.
De wet voorziet echter niet in de mogelijkheid dat meerdere korpsen één functionaris gegevensbescherming aanstellen. Ook zijn er plannen om de invoering van de nieuwe wet vorm te geven als een bovenregionaal project.
Twee van de drie bezochte infodesks gaven te kennen dat er, in meerdere of mindere mate, wordt gewerkt aan bovenregionale samenwerking. Bij alle drie de bezochte korpsen waren projecten gestart om de implementatie voor te bereiden of zouden op korte termijn worden gestart. De gesprekspartners gaven echter aan dat de implementatie van de Wpg niet tijdig gereed zou zijn en evenmin eenvoudig te realiseren.
Geen van de drie bezochte korpsen gaf aan per 1 januari 2008 gereed te zijn voor de implementatie van de Wpg. Als één van de problemen werd genoemd dat het moeilijk was om tijdig medewerkers op te leiden voor de Wpg. Men gaf aan dat het zeer problematisch is om tijdig relevante cursussen te kunnen volgen bij de politieacademie.

2.2 Waarborgen

Beveiligingsmaatregelen

Van de vijfentwintig korpsen geven er vierentwintig aan dat voor de infodesk specifieke, technische beveiligingsmaatregelen zijn getroffen. Vaak wordt verwezen naar fysieke afsluiting van de ruimte, speciale elektronische passen en autorisaties.
Dertien korpsen melden dat de beveiligingsmaatregelen ook zijn beschreven.
Zestien korpsen verklaren dat de beveiligingsmaatregelen deel uitmaken van een breder informatiebeveiligingsbeleid.

Functiescheiding

Negen regio’s melden een beschrijving te hebben van een functiescheiding tussen de diverse functionarissen zoals de beschikkende, administrerende en uitvoerende taken binnen de inrichting van de infodesk. Slechts vijf korpsen echter hebben die beschrijving ook kunnen overleggen. De zestien andere korpsen verklaren geen beschreven functiescheiding te hebben.
Vijftien korpsen geven aan controle uit te oefenen op de functiescheiding, door de chef, door het hoofd of door de leidinggevende.
Eén van de drie bezochte korpsen werkt met functiescheiding tussen verschillende infodeskmedewerkers. De scheiding vertaalt zich daar onder meer in verschillende autorisatieniveaus van infodeskmedewerkers. Bij de twee andere bezochte korpsen hebben infodeskmedewerkers in beginsel dezelfde autorisatieniveaus en worden zij

---

[9] Blue View is een centrale databank met zoekmachine waarin de regiokorpsen al hun geregistreerde informatie zoals informatie over aangiftes, verhoren, processen-verbaal en opsporing, kunnen delen.

ook geacht alle werkzaamheden te verrichten. Wel worden bepaalde medewerkers in voorkomende gevallen speciaal geautoriseerd voor bepaalde lopende onderzoeken.

Kwaliteitseisen

Op de vraag of er voor infodeskmedewerkers periodiek voorlichting of scholing plaatsvindt, antwoorden achttien korpsen bevestigend. Drie van deze achttien korpsen geven daarbij aan dat het gaat om (bij)scholing in de vorm van een werkoverleg. Ten aanzien van de waarborgen die gelden voor het raadplegen van tijdelijke en zwacriregisters verklaren zes van de bevraagde korpsen dat er voor het verkrijgen van toegang tot de registers geen extra eisen aan de infodeskmedewerkers worden gesteld. Vier regio's verwijzen naar een opleiding die gelijk is aan die van een CIE-medewerker.

Verschillende korpsen (7) melden nog in het ongewisse te verkeren over de implicaties die de nieuwe wet zal hebben op de te stellen kwaliteitseisen.

Het opleidingsniveau van de infodesksmedewerkers bij de drie bezochte korpsen verschilt. Twee korpsen stellen geen nadere speciale opleidingseisen aan medewerkers, een andere wel. Twee van de drie bezochte korpsen geven expliciet aan dat het opleidingsniveau van de medewerkers zal moeten toenemen, vanwege de overgang naar het nieuwe Blue View en de implementatie van de Wpg. In dit verband heeft men het over het volgen van cursussen bij de politieacademie.

Een van de bezochte infodesks deelt mede dat het moeilijk is om de benodigde cursussen de komende tijd te kunnen volgen bij de politieacademie: er zou daar onvoldoende ruimte zijn om in de behoefte van korpsen te kunnen voorzien. Eén van de korpsen die meent extra opleiding nodig te hebben, stelt dat dit in de vorm van een project binnen het korps de hoogste prioriteit krijgt.

In één van de bezochte infodesks zijn alle infodeskmedewerkers bijzonder opsporingsambtenaar, bij een ander korps is slechts een derde van de infodeskmedewerkers bijzonder opsporingsambtenaar.

Autorisaties

Bijna alle regio's (24) zeggen te werken met een systeem van autorisaties. Men verklaart te werken met autorisaties om te voorkomen dat onbevoegden toegang krijgen tot de (bijzondere) politieregisters. In de meeste gevallen neemt de leidinggevende de beslissing om een medewerker te autoriseren tot een bepaald niveau. Autorisaties kunnen vast aan functies worden verbonden. Eén van de bezochte infodesks gaf aan dat de autorisaties afhankelijk zijn van het opleidingsniveau van de functionaris. Formeel worden de autorisaties ter fiattering voorgelegd aan een hoger niveau (welke functionaris dat is, verschilt per korps). De autorisaties worden gerealiseerd door de applicatiebeheerder. Vaak is dat de ICT Service Coöperatie Politie, Justitie en Veiligheid (ISC; inmiddels de voorziening tot samenwerking (vts) Politie Nederland). In de meeste gevallen wordt de lijst van autorisaties bijgehouden door de technische afdeling (applicatiebeheerders).

Op de vraag welke rol de privacyfunctionaris speelt in het systeem van autorisaties, verklaarden zeven korpsen expliciet dat de privacyfunctionarissen geen rol vervullen bij de autorisaties. Bij de andere korpsen worden verschillende taken rondom de autorisatieverlening door de privacyfunctionarissen uitgevoerd. Zo melden twee korpsen dat de privacyfunctionaris de lijst van autorisaties beheert of bewaart.

Niet in alle regio's hebben infodeskmedewerkers toegang tot tijdelijke en zwacriregisters. Bij de meeste regio's (21) is dit echter wel het geval. Uit de antwoorden is niet af te leiden of deze toegang wat betreft het zwacriregister betrekking heeft op verdachten of/en betrokkenen en wat betreft het tijdelijke register op verdachten.

De controle op de autorisaties door de bezochte korpsen verschilt. Het ene korps doet dat maandelijks op basis van een actuele autorisatielijst, de twee andere korpsen doen het één keer per jaar.

Een van de bezochte korpsen meldt met ISC al jaren te werken aan een Service Level Agreement (SLA). Deze overeenkomst is echter nog niet gesloten. De oorzaak daar-

van zou liggen in de bovenregionale samenwerking: de betreffende korpsen werken met verschillende softwarepakketten waardoor elk korps verantwoordelijk is voor zijn eigen data. De andere twee infodesks geven aan dat er wel sprake is van SLA's.
De drie bezochte korpsen werken met bevragingen omtrent gevoelige informatie, zoals CIE-informatie, zwacriregisters en tijdelijke registers op basis van een hit/no hit-werkwijze. Dat betekent dat infodeskmedewerkers veelal wel de betreffende registers kunnen raadplegen, maar alleen zien of er een hit is of niet. Voor nadere informatie moeten zij zich vervolgens richten tot de betreffende geautoriseerde functionarissen en eenheid.
De nieuwe versie van Blue View (voor onder meer het raadplegen van afgesloten mutaties in het Herkenningsdienstsysteem (HKS) en het Bedrijfsprocessensysteem (BPS)) kent een beperkt aantal autorisaties. Dat vindt men veelal een goede zaak. De infodesks geven aan graag controle en regie te voeren op het bevragen en verstrekken van informatie. Een van de bezochte korpsen deelt mee dat het beperktere aantal autorisaties zorg draagt voor een goede monitoring van de wijze waarop medewerkers gebruik maken van de toegekende autorisaties. Alleen die medewerkers moeten geautoriseerd zijn die er ook daadwerkelijk gebruik van moeten maken; het aantal autorisaties is immers beperkt.

Logging

Twintig korpsen melden dat de handelingen (bevragingen van de diverse registers/bestanden) van de infodeskmedewerkers worden gelogd. De meeste van deze korpsen (16) controleren de logs niet structureel. Zij gebruiken de logs alleen naar aanleiding van incidenten.
Zes van de ondervraagde korpsen melden dat handelingen van de infodeskmedewerkers waarbij gegevens worden geraadpleegd uit het bijzondere register, niet worden gelogd. Hierbij verklaarde één korps wel te loggen voor de algemene registers en niet voor het bijzondere register.
De drie bezochte infodesks leggen alle binnenkomende informatievragen, veelal handmatig, vast. Dat geldt ook voor de verstrekkingen. Op de verstrekking staat in principe de naam van de infodeskmedewerker die de informatie heeft verstrekt. Deels worden die verstrekkingen automatisch gelogd, deels handmatig. Bij één regio wordt HKS bijvoorbeeld automatisch gelogd en BPS alleen naar aanleiding van een signaal en dan alleen na toestemming van het plaatsvervangend hoofd sturingsinformatie.
Bij geen van de drie bezochte infodesks is sprake van een structurele controle op logs. Controle vindt alleen plaats als er een signaal is dat er iets niet in de haak zou zijn.

2.3 Privacyfunctionaris, Functionaris gegevensbescherming en audits

Privacyfunctionaris en Functionaris gegevensbescherming

Zeven van de vijfentwintig korpsen hebben geen privacyfunctionaris (PF) of functionaris gegevensbescherming (FG). Zij melden dat de werkzaamheden die horen bij die functies zijn ondergebracht bij andere functionarissen. Van de korpsen die mededelen wel een privacyfunctionaris of functionaris gegevensbescherming te hebben (18), is bij acht korpsen de functie van privacyfunctionaris gecombineerd met een andere functie.
De PF's/FG's hebben geen vaste plaats binnen de inrichting van de korpsen. Zo valt de PF/FG bij zeven korpsen onder een integriteitsunit en bij drie andere korpsen direct onder het Stafbureau.
Iets meer dan de helft van de regio's (13) verklaart te beschikken over een functieomschrijving voor de privacyfunctionaris.
Zeventien korpsen melden dat de taak van de privacyfunctionaris voor het overgrote deel bestaat uit advisering. Bij vier andere bevraagde korpsen behoren ook controlerende taken tot de functie.

De drie bezochte korpsen zien de privacyfunctionaris vooral als adviseur. In beperkte en verschillende mate hebben zij ook een controlerende rol, bijvoorbeeld bij gegevensverstrekkingen aan burgers, verstrekkingen uit BPS ouder dan vijf jaar of bij controle op logs. Ook bij de voorbereiding van de implementatie van de Wpg is de privacyfunctionaris betrokken. Een medewerker van één van de drie bezochte infodesks deelt mee dat de privacyfunctionaris dichtbij de werkvloer staat en makkelijk te bereiken is, terwijl bij een ander korps de privacyfunctionaris een beperktere (advies)rol heeft, meer op afstand. Bij het derde bezochte korps is er bij incidenten contact met de privacyfunctionaris.

Audit

Vijftien korpsen melden dat de beheersmaatregelen niet door middel van een audit worden gecontroleerd. Zeven korpsen zeggen dat een controle of audit binnen het eigen korps wordt uitgevoerd. Bij vier van de zeven speelt de privacyfunctionaris daarbij een rol. Twee korpsen zijn door de Inspectie Openbare Orde en Veiligheid (IOOV) geaudit. Eén korps verklaart door een particulier auditbureau te zijn onderzocht.

Wpg

Geen enkele van de ondervraagde korpsen heeft concrete plannen om de functie van privacyfunctionaris bij de invoering van de nieuwe wet een andere invulling te geven. Uit de antwoorden die de korpsen geven is een tendens te zien gericht op meer samenwerking met andere korpsen. Men denkt dan aan het samenvoegen van de werkzaamheden binnen verschillende buurregio’s. Daarbij blijkt ook duidelijk dat nog wordt gewacht op een ‘vertaling’ van de nieuwe wet naar de politieorganisatie.

3

BEOORDELING EN CONCLUSIE

3.1 Inrichting en werkwijze regionale infodesks

Organisatie

De organisatie van de infodesk verschilt sterk per regio. Er is meer eenduidigheid betreffende de aard en bediening van de interne en externe klanten.

Administratie

Bijna alle korpsen (21) melden dat er een administratieve beschrijving van de organisatie van de infodesk aanwezig is. De diverse functies en specialismen die in de infodesk van de verschillende korpsen vertegenwoordigd zijn, zijn in alle regio's neergelegd in een formele functieomschrijving.

Het CBP kan geen oordeel vellen over de organisatorische en administratieve organisatie van de infodesk buiten de situatie dat deze invloed heeft op de verwerking van gegevens. Het is evenwel van belang te constateren dat het leeuwendeel van de regio's meldt geen van beide aan te passen in het licht van de nieuwe wet, terwijl daarin wel specifieke eisen aan de organisatie worden gesteld.

3.2 Waarborgen

Functiescheiding

Negen regio's verklaren over een beschrijving van de functiescheiding tussen de diverse functionarissen te beschikken. Zestien regio's hebben geen beschrijving. Vijftien regio's melden controle uit te oefenen op de functiescheiding. De controle gebeurt door de chef, door het hoofd of door de leidinggevende.
De regio's gaan niet eenduidig om met de functiescheiding als waarborg voor een zorgvuldige gegevensverwerking. Het autorisatiebeleid per regio is hiervoor echter de wettelijke graadmeter, samen met de in het Bpg neergelegde kwaliteitseisen.

Kwaliteitseisen

Wat betreft de kwaliteitseisen die aan infodeskmedewerkers worden gesteld, merkt het CBP op dat op dit vlak een grote verscheidenheid tussen de regio's bestaat.
Ook de kwaliteitseisen die voor de toegang tot bijzondere registers gelden worden door de ondervraagde regio's verschillend ingevuld. Dit is opmerkelijk omdat de Regeling Regionale Infodesk, waarvan het merendeel van de regio's heeft aangegeven dat deze geïmplementeerd is, hierover wel duidelijkheid geeft.
De Wpg verplicht de verantwoordelijke zorg te dragen voor het kwaliteitsniveau en deskundigheid van zijn medewerkers. Dit geldt als één van de waarborgen, naast het systeem van autorisaties, voor het zorgvuldig gebruik van de ruimere bevoegdheden die de Wpg biedt voor de verwerking van persoonsgegevens. De minimum eindtermen met betrekking tot kennis en vaardigheden kunnen bij ministeriële regeling worden vastgesteld. Voor infodeskmedewerkers gelden deze kwaliteitseisen ook, hoewel voor het verwerken van gegevens voor de uitvoering van de dagelijkse politietaak, het verwerken van gegevens voor een onderzoek in een bepaald geval en het verwerken van gegevens voor de ondersteunende taken geen specifieke deskundigheidseisen worden gesteld (toelichting bij het Besluit politiegegevens, p. 23). Dat betekent dat in ieder geval voor de zwacriverwerking deze eisen wel worden gesteld.
Drie van de achttien korpsen die mededelen dat er periodiek voorlichting of scholing plaatsvindt, melden daarbij dat het gaat om scholing in de vorm van een werkoverleg. Naar het oordeel van het CBP is een periodiek werkoverleg niet hetgeen wordt bedoeld met opleiding en het op peil houden van de kennis van de wet en regelgeving. Dat een aantal regio's dit wel onder periodieke voorlichting of scholing verstaat, baart het CBP zorgen. Zeker omdat dezelfde regio's niet voornemens zijn om in het licht van de nieuwe wet de kwaliteitseisen aan te passen.

Autorisaties

Wat betreft het autorisatiebeleid geven bijna alle regio's (24) aan een autorisatiesysteem te hanteren. De aard van het systeem en wie formeel en functioneel de autorisaties verstrekt zijn echter door de regio's allesbehalve eenduidig aangegeven. Volgens het Besluit politieregisters was het de beheerder die de autorisatie verleende. Dit was feitelijk door de beheerder gedelegeerd. Onder de Wpg is het de verantwoordelijke die het systeem van autorisaties onderhoudt en de autorisaties verstrekt. Het is vervolgens de privacyfunctionaris die feitelijk de autorisaties dient bij te houden. Zeven van de vijfentwintig regio's melden expliciet dat de privacyfunctionaris geen rol vervult bij de autorisaties. Bij de andere regio's voeren de privacyfunctionarissen verschillende taken rondom de autorisatieverlening uit.

De regio's dienen in het licht van de Wpg op dit gebied hun autorisatiebeleid aan te passen. De autorisaties zullen moeten worden gewijzigd: in beginsel kan onder de Wpg immers aan infodeskmedewerkers geen doelgebonden autorisatie voor een tijdelijke verwerking worden verleend, maar wel een functionele autorisatie tot gegevens in tijdelijke verwerkingen ten behoeve van de uitwisseling daarvan met andere tijdelijke verwerkingen. Het is bovendien mogelijk dat infodeskmedewerkers onder de Wpg geautoriseerd worden voor toegang tot zwacrigegevens, bijvoorbeeld voor operationele misdaadanalyses en in het kader van de voorbereiding van projecten.

Het is duidelijk geworden dat de regio's geen eenduidig beleid op dit gebied voeren. Niet in alle regio's hebben infodeskmedewerkers toegang tot tijdelijke en zwacriregisters. Bij de meeste regio's (21) is dit echter wel het geval. Uit de antwoorden is niet af te leiden of deze toegang betrekking heeft op verdachten of/en betrokkenen (wat betreft het zwacriregister) en verdachten (wat betreft het tijdelijke register). Onder de Wpolr werd de rechtstreekse toegang langs geautomatiseerde weg tot zwacrigegevens niet wenselijk geacht in verband met de toetsing van de weigeringgronden voor de verstrekking van gegevens.

Logging

De bevragingen door infodeskmedewerkers van de diverse registers worden in de meeste regio's (20) gelogd. Met het oog op de controleerbaarheid van de handelingen dient elk korps te voorzien in een logging van de bevragingen. In het bijzonder bij de toegang tot de bijzondere registers zou dat systematisch moeten plaatsvinden. Zes regio's geven aan dat de handelingen van de infodeskmedewerkers waarbij gegevens uit tijdelijke en zwacriregisters worden geraadpleegd, niet worden gelogd. Dit acht het CBP zorgelijk.

De logs worden in de meeste regio's niet structureel gecontroleerd. Een dergelijke controle is echter wel belangrijk. In de Wpolr was niet bepaald dat de controle moest plaatsvinden in de vorm van een audit. In de Wpg is dit wel voorgeschreven. Op dit punt zullen de regio's maatregelen moeten nemen. Onder de nieuwe wetgeving is het loggen een verplichting die volgt uit de wet en nader is uitgewerkt in het besluit. De regio's die nog niet stelselmatig en eenduidig logden, zullen hun beleid in het licht van de nieuwe wet moeten aanpassen.

3.3 Privacyfunctionaris, Functionaris gegevensbescherming en audits

Privacyfunctionaris en Functionaris gegevensbescherming

De verantwoordelijke voor de verwerking van politiegegevens onder de Wpg, de korpsbeheerder, heeft een wettelijke verplichting een privacyfunctionaris aan te stellen. Deze privacyfunctionaris heeft met de inwerkingtreding van de Wpg een expliciete rol gekregen bij de controle op en voorlichting over de verwerking van persoonsgegevens, bijvoorbeeld op het gebied van de te verlenen autorisaties. Deze rol blijkt veelal niet uit de door de regio's gegeven antwoorden. Geconstateerd kan worden dat de regio's vaak niet het voornemen hebben om de rol van de privacyfunctionaris te veranderen. Zij geven merendeels ook aan nog geen zicht te hebben op de gevolgen van de inwerkingtreding van de nieuwe wet voor de organisatie in de praktijk.

Audits
Het merendeel van de regio's verklaart thans geen audits uit te (laten) voeren. Met de invoering van de Wpg is dat wel een verplichting geworden. Geen enkele regio heeft aangegeven de technische beheersomgeving bij de inwerkingtreding van de nieuwe wet te wijzigen. Het CBP acht dit een zeer verontrustend punt.

3.4 Algemene conclusie

Hoewel er grote verschillen bestaan tussen de politieregio's, staat wel vast dat veruit de meeste regio's ten tijde van het onderzoek geen volledig beeld hadden van de aard van de wijzigingen die doorgevoerd zouden moeten worden na de inwerkingtreding van de Wpg. Ook bleek dat deze regio's niet voornemens waren om wijzigingen door te voeren. Dit betrof met name de voorgeschreven kwaliteitseisen van infodeskmedewerkers, het autorisatiebeleid, de controle op de logging door middel van audits en tot slot de rol van de privacyfunctionaris binnen de regio.

Al deze elementen betreffen leemten in de waarborgen die in de Wpg zijn gecreëerd ter compensatie voor het ruimere verstrekkingenbeleid binnen en door de regio's. Dat de regio's op deze punten niet toegerust waren voor de situatie na 1 januari 2008 en de eisen die de Wpg stelt aan een zorgvuldige gegevensverwerking, is uitermate zorgwekkend.

BIJLAGEN

Bijlage 1

HET ONDERZOEK

Onderwerp en reikwijdte van het onderzoek

Object van onderzoek is de gegevensverwerking binnen de infodesks van de verschillende politieregio's.
Het onderzoek richt zich enerzijds op het verkrijgen van een algemeen beeld van de invulling van de infodesk bij de politiekorpsen. Anderzijds zijn de waarborgen onderzocht voor die onderdelen van de infodesk die het meest kwetsbaar zijn.
Het onderzoek is beperkt tot de opsporingsfunctionaliteit van de infodesk en de tijdelijke en zwacriregisters. Tevens is alleen de regionale functie van de infodesk onderzocht.

Doel van het onderzoek

Het onderzoek is er op gericht zicht te krijgen op het functioneren van de infodesk in het algemeen: hoe is de infodesk ingericht en welke waarborgen voor de bescherming van persoonsgegevens biedt de infodesk daarbij? Onderzocht is de situatie zoals die bestond onder de Wpolr, met een blik op de kort daarna in werking tredende Wpg.

Onderzoeksvragen

De onderzoeksvragen zijn:
1. Hoe hebben de verschillende korpsen vorm gegeven aan de infodesk?
2. Wat zijn de waarborgen voor de bescherming van persoonsgegevens (o.a. autorisaties, logging, audits, opleiding, afscherming eigen bestanden) bij de opsporingsfunctionaliteit van de infodesk wanneer men het tijdelijke en zwacriregister voor regionale activiteiten raadpleegt?

De onderzoeksvragen zijn onderzoektechnisch ingedeeld in vier aandachtsgebieden.
De infodesk is onderverdeeld in:
- een organisatorische beschrijving (Organigram);
- een administratieve beschrijving (Administratieve Organisatie; AO);
- een personele beschrijving (Functiebeschrijving, kwaliteitseisen);
- een technische beschrijving (Technische waarborgen).

Daarnaast zijn de verschillende korpsen bevraagd over plannen in relatie tot de implementatie van de Wpg en over (de rol van) de privacyfunctionaris/functionaris voor de gegevensbescherming.

Werkwijze

Het onderzoek heeft in twee fasen plaatsgevonden. De eerste fase betrof het verkrijgen van informatie bij 25 politieregio's op basis van schriftelijke vragen.
Het Korps Landelijke Politiediensten is niet aangeschreven omdat dit naast reguliere taken ook andere taken heeft, zoals op het gebied van verkeer, en hierbij ook gebruik maakt van andere registers dan de regionale politiekorpsen. De tweede fase van het onderzoek bestond uit het bezoeken van drie regiokantoren, waarbij interviews zijn afgenomen.

Eerste fase van het onderzoek

De Inspectie Openbare Orde en Veiligheid (IOOV) heeft in maart 2005 het rapport *Landelijke coördinatie en uitwisseling van politie-informatie* aan de Tweede Kamer aangeboden. In dat rapport zijn onder andere bevindingen opgenomen over de politie infodesk. Omdat een deel van het onderzoek bruikbaar was voor het CBP en het CBP ook de lastendruk voor de politieregio's wilde beperken, heeft het CBP de Inspectie verzocht medewerking te verlenen aan het onderzoek door de onderzoekers inzage te geven in een deel van de antwoorden die in het kader van het IOOV-onderzoek waren gegeven. De Inspectie heeft vervolgens toestemming gegeven om dat deel van de antwoorden beschikbaar te stellen die betrekking hadden op de infodesk. De regio's zijn afzonderlijk gevraagd om na te gaan of de antwoorden (nog) correct waren en deze zo mogelijk te actualiseren.

Tweede fase van het onderzoek

Resultaten van een schriftelijk uitgevoerd onderzoek dienen met enige terughoudendheid te worden geïnterpreteerd. Antwoorden gegeven op een vragenlijst geven een niet getoetst beeld van de dagelijkse praktijk. Voor het verkrijgen van een vollediger beeld hebben onderzoekers van het CBP in oktober en november 2007 drie regio's bezocht. Zij hebben daarbij gesproken met het hoofd van de infodesk, een medewerk(st)er van de infodesk en een informatiebeveiligingsfunctionaris. Tijdens die interviews is een vollediger beeld verkregen van de werkzaamheden, met name die op de 'werkvloer'. Van de interviews zijn verslagen gemaakt die zijn afgestemd met de regio's. De bevindingen van die bezoeken zijn in dit rapport verwerkt.

Bijlage 2

BEVOEGDHEID CBP

Het CBP ziet toe op de verwerking van politiegegevens overeenkomstig het bij en krachtens de Wet politiegegevens bepaalde (artikel 35 Wpg).

De Algemene wet bestuursrecht (Awb) is van toepassing op het CBP. De Awb definieert een toezichthouder als een persoon, bij of krachtens wettelijk voorschrift belast met het houden van toezicht op de naleving van het bepaalde bij of krachtens enig wettelijk voorschrift.

Het CBP is zijn ambtshalve onderzoek gestart op grond van artikel 35 Wpg j° 60 Wbp. Op grond van artikel 5:16 Awb is een toezichthouder bevoegd om inlichtingen te vorderen. Artikel 5:20 Awb bepaalt dat een ieder verplicht is aan een toezichthouder binnen de door hem gestelde redelijke termijn alle medewerking te verlenen die deze redelijkerwijs kan vorderen bij de uitoefening van zijn bevoegdheden.

Bijlage 3

REGELING REGIONALE INFODESK

Artikel 1

In deze regeling wordt verstaan onder:
regionale infodesk: een continue beschikbare eenheid ten behoeve van het opsporingsproces, die als een herkenbaar loket binnen de politieregio op verzoek snel, zo volledig en zorgvuldig mogelijk operationele informatie aan gelegitimeerde functionarissen verstrekt uit daartoe beschikbare bronnen, dan wel makelt. Deze eenheid verstrekt tevens operationele informatie ten behoeve van strategische en tactische besluitvorming;

beheerder: de beheerder, bedoeld in artikel 1, eerste lid, onder f, van de Wet politieregisters;

registratiesysteem: het regionaal aangewezen systeem waarin het verzamelproces voorafgaand aan de verstrekking wordt vastgelegd;

verstrekken: het bekend maken of ter beschikking stellen van informatie uit ter beschikking staande (geautomatiseerde) bronnen;

makelen: het op basis van inzicht in informatie beheerders en gebruikers van informatie bij elkaar brengen dan wel beheerders van informatie op de hoogte stellen van de informatiebehoefte van de gebruiker;

operationele informatie: alle informatie die uit de beschikbare bronnen kan worden gebruikt in de opsporing;

gelegitimeerde functionarissen: zij die op grond van artikel 1 van de Wet politieregisters gerechtigd zijn om informatie te ontvangen;

Artikel 2

De Regionale Infodesk ondersteunt het verzamelproces van de opsporing door het verstrekken of makelen van informatie uit algemene politieregisters en open bronnen. Ten aanzien van informatie uit tijdelijke registers en bijzondere politieregisters beperkt de bevoegdheid van de Regionale Infodesk zich tot het raadplegen teneinde te kunnen makelen.

Toelichting artikel 2
De Regionale Infodesk is verantwoordelijk voor het verstrekken en makelen van zo volledig mogelijke informatie. De Regionale Infodesk is intern (regionaal) en extern (bovenregionaal) gericht. Intern betekent dit dat collega's uit de eigen regio een beroep doen op de Regionale Infodesk bij hun verzamelproces van operationele informatie. De Regionale Infodesk heeft daarvoor kennis van en toegang tot diverse systemen en is goed op de hoogte van actuele zaken en ontwikkelingen (het zgn. overzicht). Extern betekent het dat ook andere opsporingsambtenaren en/of -instanties de Regionale Infodesk om ondersteuning kunnen vragen bij het verzamelen van operationele informatie.

De Regionale Infodesk heeft een specifieke verantwoordelijkheid om op aangewezen aandachtsgebieden van criminaliteit bij te dragen aan bovenregionaal overzicht. Een en ander laat onverlet dat ambtenaren met een taakaccent op hun aandachtsgebied rechtstreeks informatie kunnen uitwisselen.

Uit de verantwoordelijkheid tot verstrekken en makelen van informatie vloeit de bevoegdheid voort om informatie uit algemene politieregisters en open bronnen te verstrekken. Tevens is de Regionale Infodesk bevoegd het tijdelijke register (afhankelijk van de aard), het ZwaCri register en het voorlopig register (de laatste twee op subjectniveau) te raadplegen teneinde te kunnen makelen. De Regionale Infodesk heeft geen toegang tot beheersregisters (onder andere het informantenregister van de CIE).

Artikel 3
Het verzamelproces voorafgaand aan het verstrekken van informatie wordt vastgelegd in een registratiesysteem.

Toelichting artikel 3
De Regionale Infodesk is verantwoordelijk voor het verzamelproces (volledigheid van geraadpleegde systemen) op basis waarvan informatie wordt verstrekt. Dit verzamelproces wordt vastgelegd in een registratiesysteem. De informatie in het registratiesysteem kan alleen worden gebruikt om te makelen. Verstrekkingen vallen onder het regime van het geraadpleegde systeem.

Een politieregio kan ervoor kiezen om verzamelprocessen die leiden tot het makelen van informatie, eveneens vast te leggen in een registratiesysteem.

De Regionale Infodesk is niet verantwoordelijk voor de kwaliteit van de informatie die uit systemen wordt verstrekt, tenzij redelijkerwijs had kunnen worden voorzien dat de informatie qua betrouwbaarheid en bruikbaarheid twijfelachtig is.
De Regionale Infodesk is wel kwalitatief verantwoordelijk voor de begeleiding bij verstrekkingen uit open bronnen.

De Regionale Infodesk is verantwoordelijk voor het zoeken naar en toegankelijk maken van andere c.q. nieuwe (open) bronnen. De Regionale Infodesk dient daartoe ontwikkelingen te volgen en toegang te verkrijgen tot bronnen, die de opsporing kunnen ondersteunen.

Artikel 4
De Regionale Infodesk verricht in ieder geval de volgende werkzaamheden:

a. verzamelen van informatie;
b. veredelen van informatie;
c. registreren van het verzamelproces;
d. opstellen van overzichten;
e. verstrekken van informatie;
f. makelen van informatie;
g. verstrekken van informatie buiten de regio;
h. ontsluiten en bevorderen gebruik van nieuwe bronnen.

Toelichting artikel 4

a Verzamelen van informatie
De Regionale Infodesk heeft de taak ten aanzien van een informatieverzoek de relevante informatie te verzamelen door middel van het raadplegen van relevante en beschikbare bronnen. Ten bate van het regionaal overzicht heeft de Regionale Infodesk volledig toegang tot basisregisters en –systemen van aangrenzende regio’s. Indien een medewerker relevante informatie uit de basisregisters van aangrenzende regio’s vindt wordt dit via een informatieverzoek bij de andere regio aangevraagd.

b Veredelen van informatie
De Regionale Infodesk heeft als taak ten aanzien van een informatieverzoek combinaties te leggen tussen informatie uit verschillende bronnen, inclusief de daaruit volgende logische informatiebehoeften.

c Registreren van het verzamelproces
Teneinde verantwoording te kunnen afleggen over het verzamelproces vindt registratie van het verzamelproces plaats. Transparantie in de opsporing brengt met zich mee dat de Regionale Infodesk inzicht kan bieden in de wijze waarop de Regionale Infodesk aan de verstrekte informatie is gekomen ter onderbouwing van de verstrekte informatie.

d Opstellen van overzichten
Binnen de Regionale Infodesk worden overzichten opgesteld ter ondersteuning van andere disciplines binnen de politieregio. De informatie verandert niet wezenlijk van inhoud en aard. Het maken van strategische, tactische of operationele analyses behoort nadrukkelijk niet tot het takenpakket van de Regionale Infodesk. Operationele en strategische analisten worden uiteraard in hun proces van informatieverzameling ondersteund door de Regionale Infodesk en werken dus wel nauw samen met de Regionale Infodesk.

e Verstrekken van informatie
De primaire taak van de Regionale Infodesk is het ondersteunen van de opsporing met relevante informatie. De Regionale Infodesk verstrekt daartoe zowel binnen de regio als daarbuiten informatie ten behoeve van strategische, tactische en operationele processen. Deze informatie komt uit algemene politieregisters en open bronnen. Verstrekking vindt plaats onder het regime van de bron waar de informatie in is opgenomen. Hierbij vindt advisering plaats over de betrouwbaarheid en de veiligheid van de bron en de toepassingsmogelijkheden van de verkregen informatie.

f Makelen van informatie
Op basis van inzicht in informatie kan de Regionale Infodesk beheerders en gebruikers van informatie bij elkaar brengen, dan wel de beheerder op de hoogte stellen van de informatiebehoefte van de gebruiker/verzoeker. Bij informatie uit de tijdelijke registers en de Bijzondere Politieregisters beperkt de taak van de Regionale Infodesk zich tot het makelen.

g Verstrekken van informatie buiten de regio
Het is de taak van de Regionale Infodesk om informatie ten aanzien van de benoemde criminaliteitsvelden regionaal aan te leveren in de daartoe aangewezen systemen om bij te dragen aan het landelijk beeld over een specifiek criminaliteitsveld. Het is denkbaar dat de Regionale Infodesk een aantal criminaliteitsvelden zelfstandig volgt en vastlegt indien het informatiebeheer ten aanzien van deze criminaliteitsvelden niet beter gewaarborgd is op regionaal niveau. Overigens verstrekt de Regionale Infodesk ook operationele informatie aan ontvangstgerechtigden buiten de eigen politieregio.

h Ontsluiten en bevorderen gebruik (nieuwe) bronnen
De Regionale Infodesk heeft de taak nieuwe bronnen voor het opsporingsproces aan te boren en aanbevelingen te doen over bronnen die de opsporingsambtenaar zelfstandig moet kunnen bevragen.

Artikel 5

De Regionale Infodesk verstrekt en makelt volgens een landelijk gestandaardiseerde werkwijze.

Toelichting artikel 5
De Regionale Infodesk verstrekt of makelt indien daartoe een verzoek wordt ingediend. Dit verzoek is nodig om de informatiebehoefte van de gebruiker te kunnen benoemen. Ten aanzien van speerpunten van beleid en dergelijke, hoeft echter niet telkens opnieuw een verzoek te worden ingediend, maar zal de Regionale Infodesk volgens gemaakte afspraken informatie verstrekken.

De medewerker Regionale Infodesk toetst de vraagstelling van de gebruiker van informatie aan de beginselen van proportionaliteit en subsidiariteit en doet dit in overleg met de gebruiker. Verstrekkingen vinden slechts plaats binnen de bepalingen van de Wet op de Politieregisters en relevante privacywetgeving.

De Regionale Infodesk laat de beantwoording van informatieverzoeken geschieden door middel van vooraf vastgestelde verzamelprotocollen waarin de te bevragen bronnen zijn vastgelegd. Daartoe dienen landelijk gestandaardiseerde verzamelprotocollen, informatieproducten en werkprocessen te worden ontwikkeld. Door de korpsen worden reeds processen gestandaardiseerd volgens de OMP. Tevens dient te worden aangegeven over welke informatiebronnen de Regionale Infodesk minimaal dient te beschikken.

De medewerker Regionale Infodesk registreert elk verzamelproces dat leidt tot informatieverstrekking in een regionaal daarvoor aangewezen systeem en legt daarbij vast:
- Identiteit en functie aanvrager;
- Identiteit en functie behandelaar;
- Vraagstelling;
- Geraadpleegde bronnen inclusief datum en tijd van bevraging;
- De verstrekte informatie;
- Eventuele condities omtrent het gebruik van informatie.

Het verstrekken c.q. makelen gebeurt in principe mondeling. Indien verstrekte informatie wordt gebruikt als bewijs in een opsporingsonderzoek, wordt deze door middel van een proces verbaal verstrekt. Op verzoek van de gebruiker kan informatie schriftelijk worden verstrekt.

Artikel 6
De Regionale Infodesk heeft toegang tot de algemene Politieregisters en tijdelijke registers2. Met betrekking tot de bijzondere politieregisters (het ZwaCri- en voorlopig register) heeft de Regionale infodesk toegang op subjectniveau. De Regionale Infodesk heeft geen toegang tot het informantenregister.

Toelichting artikel 6
De wetgever heeft in de privacywetgeving een onderscheid aangebracht tussen de Bijzondere Politieregisters en de overige politieregisters. Het bijzondere karakter van de informatie in de Bijzondere Politieregisters speelt hierbij een centrale rol.

In het tijdelijke register wordt informatie opgeslagen voor een bepaald geval, de zogenaamde onderzoeksregisters. In deze registers mag zeer ruim informatie, die noodzakelijk is voor het te onderzoeken geval, worden opgenomen. Daartegenover staat dat het gebruik van de informatie beperkt is, teneinde de privacy van de burger voldoende te kunnen waarborgen.

In het register zware criminaliteit en het voorlopig register mag zeer ruim informatie worden opgenomen van personen ten aanzien van wie een redelijk vermoeden van betrokkenheid bij benoemde misdrijven kan worden vastgesteld. Binnen deze kaders kan de politie dossiers aanleggen van personen die zich bezighouden met de zware en georganiseerde criminaliteit zonder dat er een onderzoek tegen hen loopt. Binnen deze dossiers is opname mogelijk van onbevestigde / zachte informatie uit tijdelijke registers, van informanten en uit de overige politieregisters. De wetgever heeft aangegeven, dat voor de verstrekking van deze informatie een kwalitatieve toetsing noodzakelijk is. Het beheer is mede om die reden opgedragen aan de CIE.

Rekening houdende met bovenstaande en gelet op de taakopdracht van de Regionale Infodesk is het noodzakelijk, dat de medewerkers van de Regionale Infodesk volledig toegang hebben tot het tijdelijk register en beperkt (op subjectniveau) tot het ZwaCri-

en het voorlopig register. De directe toegang tot het tijdelijke register is noodzakelijk om vanuit een integraal overzicht aan informatie de juiste ondersteuning in de opsporing te kunnen bieden. De Regionale Infodesk heeft echter geen bevoegdheid om informatie uit de tijdelijke - en Bijzondere Politieregisters te verstrekken.
De Regionale Infodesk oefent hier uitsluitend de makelaarsrol uit.

Gelet op het afbreukrisico van de informatie binnen de Bijzondere Politieregisters dient aan een beperkt aantal medewerkers van de Regionale Infodesk een autorisatie te worden verleend.

Artikel 7

Ter ondersteuning van het regionale informatie(verzamel)-proces van de opsporing werken de verschillende Regionale Infodesken en de Infodesk van het KLPD met elkaar samen. Regionale Infodesken nemen geen verzoeken om informatie in ontvangst vanuit andere politiekorpsen, anders dan door tussenkomst van de Regionale Infodesk van het betreffende korps.

Toelichting artikel 7

In het informatie (verzamel)proces van de diverse regionale politieonderdelen bestaan bilaterale informatiestromen met andere politieregio's. Deze zijn veelal gericht op specifieke expertisenetwerken (fraude, CIE, e.d.) of op basis van samenwerking in bijvoorbeeld grensgebieden of in onderzoeken. Deze informatieprocessen dienen normaal plaats te kunnen vinden en kunnen gerangschikt worden onder informatie-uitwisseling / verzoeken in de primaire werkprocessen.

Informatieverzoeken met een andere dan hierboven genoemde informatiebehoefte worden binnen de regio aan de Regionale Infodesk gesteld. Is er hierbij behoefte aan informatie uit andere politieregio's dan doet de eigen Regionale Infodesk de intake. De Regionale Infodesk beoordeelt dan in overleg met de opsporingsambtenaar of het zinvol is om direct contact tussen ambtenaar en Regionale Infodesk van de andere regio te leggen. Een Regionale Infodesk neemt dus geen informatieverzoek van andere regio's in behandeling, dan door tussenkomst van een Regionale Infodesk.

Door deze lijn te volgen kunnen aan de informatieverzoeken kwaliteitseisen gesteld worden en standaards ontwikkeld worden, die een efficiënte en kwalitatieve behandeling van verzoeken waarborgen. Het gebruik van een standaardformulier is daarbij aan te bevelen. Na intake door de eigen Regionale Infodesk bestaat natuurlijk altijd de mogelijkheid om te makelen en een direct contact tot stand te brengen tussen de Regionale Infodesk van de andere regio en de eigen functionaris.

Artikel 8

De Regionale Infodesk verzamelt in samenwerking met het Informatie Knooppunt Politie van het KLPD informatie volgens vastgestelde informatiebehoefte op door het CBO benoemde criminaliteitsvelden ter voorbereiding op de bovenregionale criminaliteits-bestrijding door Boven Regionale Teams.

Toelichting artikel 8

In de bovenregionale samenwerking ter bestrijding van de middencriminaliteit heeft de Regionale Infodesk een specifieke rol toebedeeld gekregen. Samen met het Informatie Knooppunt Politie (IKP) bij het KLPD vormen zij het netwerk waarbinnen in eerste aanleg informatie wordt verzameld om inzicht te krijgen in een criminaliteitsveld. De analyse van deze verzamelde informatie wordt door het IKP uitgevoerd. Op basis van deze overzichtsanalyses kan in tweede aanleg aanvullende informatieverzameling plaatsvinden ter voorbereiding van een Bovenregionaal Recherche Team (BRT). De Regionale Infodesk fungeert hierin als actieve participant om regionale informatie te verzamelen en ten behoeve van overzicht en/of projectvoorbereiding aan te leveren.

De criminaliteitsvelden zijn benoemd door de Raad van Hoofdcommissarissen en worden periodiek door de Commissie Bovenregionale Opsporing (CBO) beoordeeld op relevantie. Zij kunnen in de tijd wisselen, afhankelijk van gestelde prioriteiten. De informatieverzameling vindt alleen plaats op basis van vastgestelde informatiebehoefte (= verzoek c.q. opdracht).

Artikel 9
De Regionale Infodesk fungeert tevens als loket voor de specifieke informatiebehoefte van hen die blijkens de wet Politieregisters bevoegd zijn politie-informatie te ontvangen.

Toelichting artikel 9
De in Wet en Besluit Politieregisters genoemde ontvangstgerechtigden van informatie uit politieregisters dienen hun informatieverzoeken in bij de politieregio's en het KLPD. Hierbij kan gedacht worden aan bijzondere opsporingsdiensten, sociaal rechercheurs, departementen, andere landen e.d. Het lijkt logisch om voor deze groep als loket op te treden. Bestaande bilaterale informatie-uitwisseling tussen specifieke politie-eenheden en ontvangstgerechtigden kunnen normaal hun doorgang vinden.

Artikel 10
Regionaal valt de Regionale Infodesk onder het hoofd van de (regionale) recherche-eenheid.

Toelichting artikel 10
Deze regeling beperkt zich tot de Regionale Infodesk binnen de politieorganisatie. Voor de samenwerking en informatie-uitwisseling verdient het aanbeveling dat de Bijzondere Opsporingsdiensten een Infodesk inrichten volgens de Regeling.

De Regionale Infodesk vervult landelijk en regionaal een centrale rol in de informatievoorziening van de politie, met name gericht op de opsporing. Deze informatievoorziening is op grond van het Besluit Beheer Regionale Politiekorpsen onderdeel van de recherchefunctie. Het is dan ook vanzelfsprekend dat de verantwoordelijkheid voor deze informatievoorziening en dus voor de Regionale Infodesk is opgedragen aan het hoofd van de (regionale) recherche-eenheid.

Indien er sprake is van decentralisatie binnen de regio, blijft het hoofd van de regionale recherche-eenheid verantwoordelijk voor de producten en de kwaliteit van de decentrale Infodesk, de zogenaamde procesverantwoordelijkheid. In de toekomst wordt dit een bredere verantwoordelijkheid voor de opsporing.

Artikel 11
De ambtenaar die deel uitmaakt van een Regionale Infodesk voldoet aan de kernopgaven, zoals die vastgesteld zijn door de LSOP programmaraad.
Het hoofd van de (regionale) recherche-eenheid draagt ervoor zorg dat de kennis en vaardigheden van de ambtenaren worden onderhouden op het niveau van de kermopgaven.

Toelichting artikel 11
Het doel van kwaliteitseisen is het opbouwen en behouden van deskundigheid binnen het korps voor het bevragen van de grote hoeveelheid (interne en externe) systemen in combinatie met wet- en regelgeving ten aanzien van de verstrekking en het gebruik van die informatie. De eindtermen worden door het LSOP in samenwerking met het Cito geformuleerd.

1 Binnen de Regionale Infodesk dienen de hieronder genoemde kwaliteitseisen te worden gerealiseerd. Deze kunnen worden vertaald naar deelgebieden en autorisaties, waarmee kwaliteitseisen aan individuele medewerkers kunnen worden gesteld.

Binnen de Regionale Infodesk dient aantoonbaar gedegen kennis aanwezig te zijn van:

- proces van opsporing en vervolging binnen politie en justitie;
- recherchewerk;
- relevante privacy- reglementen;
- Regeling CIE;
- Bijzondere Politieregisters;
- (bijzondere) opsporingsbevoegdheden;
- opbouw van databasestructuren.

2 Om kwaliteitseisen van een medewerker Regionale Infodesk vast te stellen, moet eerst worden bepaald wat de medewerker nu feitelijk moet kunnen. In essentie gaat het hierbij om het verstrekken en makelen van informatie uit open en gesloten bronnen. Hij moet daartoe:

- De informatiebehoefte van de gebruiker kunnen vertalen naar concrete vragen in bronnen;
- Inzicht hebben in de structuur van informatiebronnen c.q. de betrouwbaarheid en de relevantie van daarin opgeslagen informatie;
- Kennis hebben van bijbehorende reglementen voor het gebruik van informatie;
- Zicht hebben op de mogelijke consequenties van het verstrekken van informatie uit open en gesloten bronnen;
- Zich een beeld kunnen vormen over de wijze waarop de verstrekte informatie zal worden gebruikt.

Aan de individuele medewerker worden de volgende minimumeisen gesteld:

- Onbesproken gedrag (vertrouwensfunctie);
- Goede communicatieve vaardigheden;
- Analytisch denkvermogen;
- Status bijzonder of algemeen opsporingsambtenaar;
- Basisopleiding Informatievoorziening (BOIV).

Aan medewerkers die geautoriseerd worden om de Bijzondere Politieregisters te raadplegen, zullen hogere kwaliteitseisen worden gesteld. Zij moeten voldoen aan de eisen van de vervolgopleiding. Door middel van een certificaat voor bepaalde tijd dient de medewerker aan te tonen over de voor de functie vereiste kennis te beschikken.

Artikel 12

De vertrekken van de Regionale Infodesk waar Bijzondere Politieregisters worden geraadpleegd, zijn afsluitbaar en beveiligd. Tot deze vertrekken hebben slechts toegang ambtenaren die deel uitmaken van de Regionale Infodesk dan wel de CIE en personen die door deze ambtenaren worden begeleid.

In afwijking van het eerste lid, tweede volzin, kan de korpsbeheerder aan anderen toegang zonder begeleiding toestaan, indien het betreden van de vertrekken alleen kan plaatsvinden nadat identiteitsgegevens elektronisch zijn vastgelegd en de toegang noodzakelijk is vanuit de verantwoordelijkheid voor de ambtenaren van de Regionale Infodesk.

Bij afwezigheid van ambtenaren van de Regionale Infodesk zijn de vertrekken deugdelijk afgesloten.

Toelichting artikel 12
Aangezien de Regionale Infodesk Bijzondere Politieregisters op subjectniveau kan raadplegen, dienen de inrichtingseisen van de betreffende werkruimte minimaal dezelfde te zijn als die van de CIE. Tegelijkertijd is uit evaluaties gebleken, dat de Regionale Infodesk kwalitatief beter functioneert, indien de afdeling fysiek dicht bij de werkvloer wordt gehuisvest. Bovenstaande tekst is overgenomen uit de Regeling CIE, maar beperkt zich tot de vertrekken van de Regionale Infodesk waar de Bijzondere Politieregisters daadwerkelijk worden geraadpleegd.

Artikel 13
De beheerder draagt ervoor zorg dat onbevoegde kennisneming van criminele inlichtingen als bedoeld in artikel 1 onder e van de Regeling CIE niet kan plaatsvinden. In dat kader ziet de beheerder erop toe dat:

deze informatie niet door onbevoegden waarneembaar is;
deze informatie niet zonder toestemming wordt vermenigvuldigd of vernietigd dan wel uit de vertrekken bedoeld in het artikel hierboven, wordt meegenomen;
informatiedragers op afdoende wijze vernietigd kunnen worden;
toegang tot geautomatiseerde registers wordt beveiligd met een gebruikersnaam en periodiek wisselende wachtwoorden;
bij geautomatiseerd transport van criminele inlichtingen voldoende beveiligingsmaatregelen worden getroffen;
bij gebruik van een netwerksysteem voldoende beveiligingsmaatregelen zijn getroffen tegen het verloren gaan van de informatie en ter voorkoming van onbevoegde bevraging.

Toelichting artikel 13
Aangezien de Regionale Infodesk Bijzondere Politieregisters op subjectniveau kan raadplegen, dienen de inrichtingseisen van de betreffende werkruimte minimaal dezelfde te zijn als die van de CIE. Tegelijkertijd is uit evaluaties gebleken, dat de Regionale Infodesk kwalitatief beter functioneert, indien de afdeling fysiek dicht bij de werkvloer wordt gehuisvest. Bovenstaande tekst is overgenomen uit de Regeling CIE, maar beperkt zich tot de vertrekken van de Regionale Infodesk waar de Bijzondere Politieregisters daadwerkelijk worden geraadpleegd.

COLOFON

Politie infodesk
Onderzoek naar de inrichting van de politie infodesk en de waarborgen voor de bescherming van persoonsgegevens

College bescherming persoonsgegevens,
Den Haag, oktober 2008.
z 2007-00090

Het College bescherming persoonsgegevens (CBP) publiceert in zijn serie rapporten resultaten van onderzoek naar de stand van zaken bij bescherming van persoonsgegevens in organisaties en sectoren.

De rapporten zijn gebaseerd op onderzoeken uitgevoerd door, of in opdracht van het CBP. Door publicatie van deze rapporten vraagt het CBP aandacht voor feiten die de persoonlijke levenssfeer van de burger raken. Het CBP wil hiermee bewustwording en naleving van de normen voor de bescherming van persoonsgegevens bevorderen.

Postbus 93374
2509 AJ Den Haag
E-MAIL info@cbpweb.nl

www.cbpweb.nl
www.mijnprivacy.nl