‘Autoriseren: zo doen we dat hier!’

(visie op een landelijk autorisatiemodel voor de Nederlandse Politie)

Expertgroep Autorisatiemodel Nederlandse Politie
Opgesteld in opdracht van RKC / Portefeuillehouder Intelligence

Juli 2011

Inhoudsopgave

1. Inleiding **2**
1.1 Opdracht 3
1.2 Probleemdefiniëring 4
1.3 Aanpak en werkwijze 5
1.4 Rol Openbaar Ministerie 6
2. Het Autorisatiemodel **7**
2.1 Uitgangspunten 7
2.1.1 Algemeen 7
2.1.2 Scope 8
2.1.3 Fundamenten ordening 8
2.2 Model m.b.t. eigen verwerkingen 9
2.2.1 Inleiding 9
2.2.2 Plaatje 10
2.3 Model m.b.t. raadplegen 11
2.3.1 Inleiding 11
2.3.2 Raadplegen art. 8 gegevens 12
2.3.3 Raadplegen art. 9 gegevens 14
2.3.4 Raadplegen art. 10 gegevens 15
2.3.5 Raadplegen art. 13 gegevens 17
2.3.6 Totaaloverzicht autorisatiemodel 18
2.3.7 Art. 12 (besloten deel) 19
2.3.8 Plaatje art. 12 20
3. Randvoorwaarden **22**
3.1 Vanuit organisatie en beheer / minimaliseren afbreukrisico 22
3.1.1 Autorisatiebeleid 22
3.1.2 Opleiding en certificering: de informatiecompetente politiemedewerker 22
3.1.3 Controle en toezicht: Landelijke Autorisatieautoriteit 22
3.2 Vanuit ICT 23
3.2.1 Goede rubricering gegevens 23
3.2.2 Landelijk beheer van autorisaties 23
3.2.3 Logging 24
4. Consequenties bij implementatie **25**
4.1 Betekenis voor Organisatie 25
4.2 Betekenis voor ICT 27
5. Beslispunten **28**

Bijlage: Globale ICT impactanalyse **29**
Bijlage: Overzicht geraadpleegde deskundigen in 2e ronde **32**

1. Inleiding

Binnen de politie spelen gegevens en informatie een zeer belangrijke rol. Er is echter nog geen gemeenschappelijke landelijke visie en gezamenlijk beleefde urgentie met betrekking tot eenduidig delen van politie informatie vanuit professionaliteit en vakmanschap.

De Inspectie Openbare Orde en Veiligheid[1] concludeerde in 2010 niet voor niets dat landelijke eenduidigheid, inzicht, transparantie én toezicht met betrekking tot het delen van politie informatie en een landelijk autorisatiebeleid essentiële voorwaarden zijn op weg naar een informatiecultuur en - professionaliteit, dat uitgaat van het 'delen, tenzij' principe.

Ervaring leert dat de realisatie van deze ambitie een taai en weerbarstig proces is. De praktijk laat zien dat niet alle korpsen op landelijk niveau (eenduidig) politie informatie delen. Enerzijds vanwege technische redenen en anderzijds vanwege culturele- en professionele perspectieven waarbij het delen van informatie wordt vermeden.

In het land zijn wel verschillende los van elkaar staande initiatieven in gang gezet om tot een beter eigen regionaal autorisatie beleid, -beheer en -management te komen, rekening houdend met WPG eisen. Bijna elke politieregio is hierin wel actief. Kenmerkend is echter dat de initiatieven zich vooral op 'eigen' regionaal niveau afspelen. Er is nog steeds sprake van versnippering en nauwelijks van een gezamenlijke visie en strategie. Een ander kenmerk is dat deze initiatieven vooral voortborduren op bestaande professionele perspectieven en veelal zijn gebaseerd op applicatiegericht denken. De focus van de initiatieven ligt in het 'Hier en Nu' en is vooral gericht op het verbeteren en beheersen van het bestaande. De initiatieven zijn nog onvoldoende gericht op vernieuwing en het realiseren van vereenvoudiging vanuit een landelijk perspectief.
Wat ontbreekt is landelijke regie op dit vlak. Er is geen landelijk punt waar deze initiatieven en perspectieven bij elkaar komen om tot een fundamentele verandering en vernieuwing te komen.

Het resultaat van al deze versnipperde initiatieven brengt ook de vtsPN in een haast onmogelijke positie om adequate ondersteuning te kunnen realiseren. De complexiteit en versnippering is zodanig toegenomen dat landelijke eenduidigheid, inzicht, transparantie en vooral autorisatiebeheer en -management een haast onmogelijk opgave aan het worden is.

Kortom, er is veel positieve professionele energie, kracht en potentie maar er is nog geen gezamenlijkheid, nog geen landelijke regie en nog geen gezamenlijke visie met betrekking tot informatiedeling vanuit professionaliteit en vakmanschap.
En dat is fundamenteel om een eenduidige en transparante informatiedeling bij de Nederlandse politie te kunnen realiseren.

Vanuit deze urgentie en visie is door de portefeuillehouder Intelligence van de RKC, dhr. P.J. Aalbersberg na afstemming in de Raad van Korpschefs begin dit jaar het initiatief genomen om vanuit 'blauwe' professionaliteit en vakmanschap samen met het OM één landelijke visie te realiseren en strategische uitgangspunten te definiëren voor eenduidige en transparante informatiedeling bij de Nederlandse politie. Uitgangspunt is daarbij om op korte termijn landelijk een betekenisvolle stap voorwaarts te maken en een hefboom te realiseren voor verdere integrale vernieuwing en ontwikkeling.

[1] "Onderzoek Samenwerkingsafspraken politie 2008" (2010): Inspectie Openbare Orde en Veiligheid, Ministerie van Binnenlandse Zaken en Koninkrijksrelaties.

1.1 Opdracht

Door de opdrachtgever is daartoe de volgende opdracht met leidende principes geformuleerd:

Ontwikkel één landelijk autorisatiemodel voor de Nederlandse politie zodanig dat:

1. de complexiteit van het bestaande autorisatiemodel / -proces dusdanig wordt teruggebracht dat het aantal niveaus of perspectieven voor autorisatie zo min mogelijk is waarbij versimpeling en vereenvoudiging leidt tot minder procedures en protocollen (bureaucratie en administratieve lasten) zonder de kwaliteit van de informatieverstrekking aan te tasten;
2. de toedeling van autorisaties aan de voorkant van het proces op basis van *'het slot op de voordeur',* wordt vervangen door *'het delen, tenzij'* principe;
3. de toedeling van autorisaties zodanig plaatsvindt dat beleidsvorming, uitvoering en toezicht plaatsvindt onder eindverantwoordelijkheid van een nader te bepalen Autorisatieautoriteit voor de Nederlandse politie. Zonder administratieve lastenverzwaring zal monitoring, beheer en control mogelijk moeten zijn;
4. maximaal gebruikt wordt gemaakt van de bestaande wettelijke kaders zoals de Wet Politiegegevens; de Wet bescherming persoonsgegevens en in het verlengde daarvan relevante regelingen en besluiten, zoals de CIE regeling en zo nodig voorstellen voor wijziging gedaan;
5. voor medewerkers de gewenste verandering inzichtelijk en begrijpelijk wordt gemaakt.

Besteed bij de ontwikkeling van dit autorisatiemodel aandacht aan de volgende aspecten en doe daarin voorstellen met betrekking tot:

- strategische uitgangspunten voor ontwikkeling, implementatie en uitvoering van het nieuwe landelijke autorisatiemodel;
- een eerste betekenis voor ICT voor wat betreft uitvoering, kosten en architectuur;
- een eerste betekenis voor organisatie, processen en professionaliteit van medewerkers;
- eventuele aanpassing van bestaande regelgeving.

Als leidende principes voor ontwikkeling zijn gedefinieerd:

- '*By the book*': uitgaan van de maximale ruimte die de wet biedt. Oftewel:
  - Redeneer vanuit professionele ambities en vakmanschap binnen de WPG in plaats vanuit bestaande systemen, bedrijfsoriëntatie of -verstarring;
  - Redeneer vanuit vertrouwen en professionaliteit in plaats vanuit angst of misbruik.
- '*Delen, tenzij'* principe: binnen de kaders van de WPG moet informatie worden 'gedeeld, tenzij'. Informatie niet delen is plichtsverzuim.

1.2 Probleemdefiniëring

Het ontbreken van een eenduidige landelijke informatiedeling kent een veelheid aan problemen in een complex landschap. Door de expertgroep is een inventarisatie en analyse gemaakt van problemen die zich in dit verband in het Hier en Nu aandienen. Kenmerkend hierbij is dat de diversiteit aan vraagstukken betrekking heeft op zowel technische, bestuurlijke als culturele vraagstukken rondom koers en beleid van informatiedeling als rondom organisatie- (taken, besturing en samenwerking) en personeelsaspecten (deskundigheid, autonomie en houding) met betrekking tot informatiedeling.

Onderstaand overzicht illustreert deze veelheid aan problemen maar laat ook zien dat de kern van het probleem van informatiedeling niet enkel een technisch en juridisch vraagstuk betreft maar vooral te maken heeft met een cultuur waarin gebrek aan onderling vertrouwen van informatiedeling centraal staat. Een cultuur die kan ontstaan door de bestaande complexiteit, onoverzichtelijkheid alsmede het ontbreken van een landelijke visie op autorisatiebeleid.

Door de expertgroep is de kern van het vraagstuk en het doel dat met het landelijke autorisatiemodel wordt nagestreefd als volgt gedefinieerd.

Probleem: versnippering, diversiteit en gebrek aan eenduidigheid in autorisaties in politieregio's leiden tot een onoverzichtelijk, foutgevoelig, risicovol, complex en onbeheersbaar systeem van informatiedeling met een gebrek aan vertrouwen in informatiedelen als gevolg.

Doel: vergroten en verbeteren van informatiedeling bij de Nederlandse politie vanuit visie, professionaliteit en vertrouwen zodanig dat er sprake is van:

- één opzet en werkwijze van informatiedeling bij de Nederlandse politie;
- minder procedures en protocollen;
- maximaal drie niveaus

Oplossing: realiseren van één autorisatiemodel voor de gehele Nederlandse politie als hefboom voor een integrale verandering en vernieuwing van informatiedeling bij de Nederlandse politie. Daarmee is dit model en de achterliggende visie op informatiedeling een stap op weg naar deze professionele ambitie.

1.3 Aanpak en werkwijze

Voor de realisatie van de opdracht is een ad hoc expertgroep samengesteld met mensen uit verschillende perspectieven van Politie en OM, waarbij de volgende rollen en vertegenwoordigingen zijn onderscheiden:

- een ZwaCri leidinggevende op strategisch / tactisch niveau
- een Intelligence leidinggevende op strategisch / tactisch niveau
- een Hoofd Regionale Informatie Organisatie of Regionaal Informatie Coördinator
- een Districtschef of van soortgelijk niveau
- deskundigheid over de WPG en relevante regelingen
- deskundigheid vanuit Businessarchitectuur van de vtsPN
- deskundigheid op het bestaande autorisatiemodel
- deskundigheid vanuit het Programma Intelligence
- deskundigheid vanuit de CIE en OM

Leden expertgroep	Organisatie
5.1.2.e , 5.1.2.e en 5.1.2.e	Programma Intelligence / SP2
5.1.2.e , 5.1.2.e recherche chef	KLPD / DNR
5.1.2.e , 5.1.2.e Informatie	Regiopolitie Utrecht
5.1.2.e , 5.1.2.e en 5.1.2.e	Regiopolitie ZHZ
5.1.2.e , autorisatie deskundige	vtsPN
5.1.2.e , enterprise architect	vtsPN
5.1.2.e , informatiemanagement	KLPD / IPOL
5.1.2.e , Officier van Justitie	OM / CIE Den Haag
5.1.2.e , Officier van Justitie	OM / CIE Amsterdam
5.1.2.e , Officier van Justitie	OM / Landelijk Parket
5.1.2.e , veranderkundige: procesregie en -begeleiding	KLPD / SP3
5.1.2.e , Business consultant en scribent	vtsPN

In verschillende expertbijeenkomsten is een conceptvoorstel op hoofdlijnen ontwikkeld. Dit concept is gepresenteerd en getoetst bij een vertegenwoordiging van de RKC (P.J. Aalbersberg), SBGI (P. Zorko) en OM (F. Westerbeke). Daarna is het concept voorstel besproken en getoetst bij een 'tweede kring van deskundigen' uit het veld[2]. Bij alle sessies zijn de discussies gevoerd aan de hand van voorbeelden uit de praktijk.

De uitkomsten van alle bijeenkomsten zijn door de expertgroep verder uitgediept en hebben geleid tot dit definitieve voorstel. Gedurende dit proces is voortdurend informatie verstrekt aan vertegenwoordigers van de LCIO en uit de domeinen WPG en Autorisatiemanagement en -beheer, om hen op die manier in het proces van ontwikkeling in de expertgroep mee te nemen.

[2] In de bijlage is een overzicht opgenomen van deze deskundigen.

1.4 Rol Openbaar Ministerie

Het Openbaar Ministerie (OM) is een belangrijke partner in het hele traject: van het bepalen van de visie tot het met het implementeren van de visie (& alle stappen daar tussenin). Niet alleen omdat het OM bepaalde wettelijke verantwoordelijkheden heeft[3] (zoals bij het verlenen van autorisaties aan categorieën van personen m.b.t. informanten, themaverwerking ernstige misdrijven en zwacri-verwerkingen; instemming met bepaalde doelafwijkende verwerkingen; het beschikbaarstellen van de bepaalde gegevens binnen de politieorganisatie en aan derden; aanwijzen van embargo-onderzoeken), maar ook omdat implementatie van het model een verandering zal vergen en teweegbrengen bij de Politie én bij het OM.

[3] Zie o.a. art. 6 WPG; art 2:6 Besluit Politiegegevens; Aanwijzing PG Wet politiegegevens (2008A017)

2. Het Autorisatiemodel

2.1 Uitgangspunten

2.1.1 Algemeen

- het model regelt de autorisaties voor circa 95% van het politiewerk (er zullen 'specials' zijn die niet in dit model passen, denk aan bijv. tolken, gedragsdeskundigen, functioneel beheerders)[4];
- het model moet haalbaar en realistisch zijn binnen de huidige praktijk, dus geen utopisch model;
- het model moet eenvoudig en transparant zijn;
- het autorisatiemodel gaat uit van het 'landelijk delen, tenzij' principe. Landelijk informatie delen 'by the book' (rechtmatigheid) is het uitgangspunt;
- het is belangrijk dat er een evenwicht is tussen informatiedelen aan de ene kant, en het voorkomen van afbreukrisico aan de andere kant;
- het model gaat uit van de professionaliteit van medewerkers: de deur met toegang tot gegevens wordt niet bij voorbaat dichtgezet uit eventuele angst voor verkeerd gebruik[5]. Het model heeft dus een belangrijke gedragscomponent;
- het model gaat uit van gegevensgericht denken (en niet van applicatiegericht denken). Met andere woorden: het gaat om gegevens waar je wel of niet voor wordt geautoriseerd; niet om applicaties waar je wel of niet bij mag. De WPG heeft het niet voor niets over politie*gegevens;*
- de autorisaties zijn rol gebaseerd. Het verlenen van autorisaties gebeurt dus niet op personen maar op basis van rollen. Een politiemedewerker krijgt op basis van de feitelijke werkzaamheden één of meerdere autorisatierollen toegekend. Aan die rol(len) zit(ten) een reeks van bevoegdheden vast;
- de toegang tot systemen wordt verleend op basis van gebleken 'noodzakelijkheid';

[4] Dat betekent niet dat er voor deze 'specials' niets geregeld wordt. Ook voor dergelijke autorisaties moet autorisatiebeleid worden vastgelegd.

[5] Dit vereist wel een set (beheers)maatregelen zodat het risico van verkeerd gebruik van informatie wordt geminimaliseerd. Denk bijv. aan certificering medewerkers, inregelen van (proactieve) controle en toezicht (zie verder hoofdstuk 3).

2.1.2 Scope

- het gaat om een model voor de Nederlandse politie en dus primair om het ter beschikking stellen van informatie binnen de politie, KMar en de BOD-en. Verstrekking van informatie buiten de politie (o.a. met ketenpartners maar ook internationaal) ligt buiten scope van de opdracht[6];
- het autorisatiemodel is van toepassing op *politiegegevens[7]:* niet alleen op de politiegegevens die in systemen worden vastgelegd, maar ook op de politiegegevens op netwerkschijven;
- het autorisatiemodel is niet van toepassing op gegevens die niet onder de WPG vallen (zoals beleidsstukken, opsporingsmethodieken, werkprocessen etc.);
- het model gaat niet over toegang tot en gebruik van de informatie die de RID verwerkt onder het regime van de Wet Inlichtingen en veiligheidsdiensten (WIV).

2.1.3 Fundamenten ordening

Het autorisatiemodel heeft een aantal fundamenten:

a) In de eerste plaats de WPG (en bijbehorende Besluit Politiegegevens): op 1 januari 2008 is de Wet politiegegevens in werking getreden. De WPG geeft regels om juist en zorgvuldig met politiegegevens om te gaan en onevenredige inbreuk op de persoonlijke levenssfeer van burgers door de politie te voorkomen. De wet geeft echter ruime mogelijkheden om informatie landelijk te delen[8]. In het autorisatiemodel wordt maximaal gebruik gemaakt van de mogelijkheden die de WPG biedt.
Twee belangrijke mogelijkheden die de Wet in dat kader biedt zijn:
   - het gebruiken van **afhandelingscodes[9]**: gegevens kunnen worden voorzien van een afhandelingscode. Die afhandelingscode bepaalt dan in hoeverre de gegevens door anderen (die op het eerste gezicht niet bij de informatie zouden mogen) toch benaderbaar zijn en gebruikt mogen worden. In § 2.3 wordt dit nader toegelicht.
   - het gebruiken van **super-users[10]**: dit zijn medewerkers die zijn belast met de coördinatie van informatie en die vanuit die rol uitgebreide toegang tot informatie mogen hebben. Zij vervullen een belangrijke rol bij het bewaren van het evenwicht tussen het delen van informatie en het eventuele afbreukrisico. Zij moeten kunnen inschatten wanneer iets wel of niet noodzakelijk is voor de politietaak. Er worden daarom extra eisen gesteld aan de kennis en kunde van deze medewerkers: ze moeten zijn opgeleid in de informatieprocessen van de politie, relevante wet- en regelgeving, en methoden en technieken van informatieanalyse (zie verder § 3.1).

b) Een ander belangrijk fundament is het Landelijk Functiehuis Nederlandse Politie (LFNP). Bij de implementatie van het autorisatiemodel is het, gezien het toedelen van autorisaties aan medewerkers, van groot belang dat er aansluiting is met (de functies en rollen van) het LFNP en het personeelssysteem waarin e.e.a. wordt geregistreerd.

---

[6] Dit dient in een 2e fase te worden meegenomen.

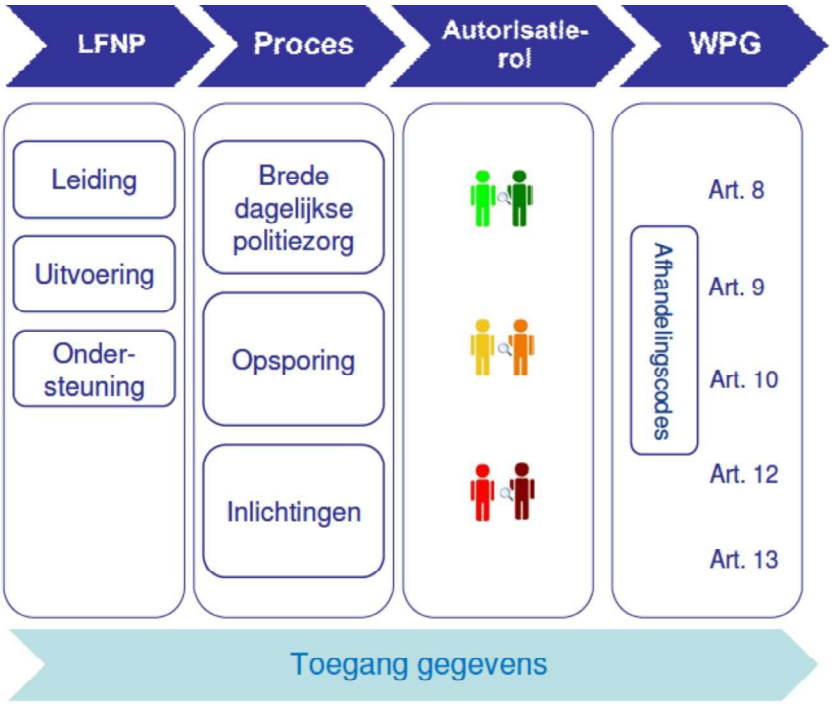
[7] Politiegegevens zijn tot personen herleidbare gegevens die in het belang van de politietaak worden vastgelegd.

[8] Het beginsel van evenredigheid is hierbij leidend: naarmate de verwerking van politiegegevens gerichter is dient de bescherming daarvan toe te nemen.

[9] Zie art. 2:10 t/m 2:13 Besluit politiegegevens.

[10] Zie art. 11 WPG.

c) Verder bepaalt het procesdomein waarbinnen iemand werkzaam is (brede dagelijkse politiezorg; opsporing; inlichtingen) de autorisatie.



2.2 Model m.b.t. eigen verwerkingen

2.2.1 Inleiding

Zoals gezegd is het autorisatiemodel rol gebaseerd. De autorisatierollen zijn ontleend aan de WPG. De drie basisrollen in het autorisatiemodel zijn:

Medewerker Dagelijkse politietaak. Deze rol is gebaseerd op art. 8 van de WPG. Art. 8 regelt dat politiegegevens mogen worden verwerkt ten behoeve van de dagelijkse politietaak. Het gaat met andere woorden om het basispolitiewerk zoals surveillance, afhandeling verkeersproblematiek, opnemen van aangiften e.d.. In de huidige situatie zouden bijv. functies als wijkagent, surveillant noodhulp, centralist deze rol krijgen. Kijkend naar het LFNP zullen vrijwel alle functies in de categorieën Leiding en Uitvoering minimaal deze rol krijgen.

Medewerker Rechtsorde. Deze rol is gebaseerd op art. 9 van de WPG. Art. 9 regelt de verwerking van politiegegevens voor een onderzoek in verband met de handhaving van de rechtsorde in een bepaald geval. Meestal zal het hierbij gaan om een rechercheonderzoek, maar het kan ook een openbare orde onderzoek betreffen. In de huidige situatie zou bijv. een rechercheur deze rol krijgen, maar ook iedereen die het recherche-onderzoek ondersteunt zoals leden van het AT en OT en forensisch rechercheurs.

Medewerker CIE/RID/Thema. Deze rol is gebaseerd op art. 10 en 12 van de WPG. Art. 10 gaat over de gerichte en omvangrijke verwerking van politiegegevens met het oog op het verkrijgen van inzicht in de betrokkenheid van personen bij bepaalde

ernstige bedreigingen van de rechtsorde. Er wordt met andere woorden een informatiepositie opgebouwd. De opgebouwde informatiepositie kan vervolgens aanleiding geven voor een operationeel opsporingsonderzoek.
Art. 12 van de WPG gaat over informanten, infiltranten en beschermde getuigen. Deze rol zal zijn toegewezen aan de leden van de eenheden CIE en RID, maar ook aan de chefs in de lijn boven deze eenheden zoals de korpschef[11].

De rol bepaalt onder andere onder welk WPG regime de medewerkers hun eigen gegevens mogen/moeten verwerken:

- een medewerker dagelijkse politietaak mag zijn eigen gegevens verwerken onder het art. 8 regime van de WPG (in de huidige situatie betekent dit dat hij o.a. in BVH mag verwerken[12]);
- een medewerker rechtsorde kan, afhankelijk van het doel van de verwerking, in art. 8 of art. 9 regime (bijv. BVO) verwerken;
- en een medewerker CIE mag verwerken onder art. 10 of art. 12 regime (als het gaat om bruto-verslagen of informantengegevens).

2.2.2 Plaatje

Voor eigen verwerkingen ziet het autorisatiemodel er als volgt uit:

Eigen verwerkingen		Medewerker dagelijkse politietaak	Medewerker rechtsorde	Medewerker CIE/RID/Thema
Dagelijkse politietaak	**Art. 8 WPG**	√	√	
Onderzoek bepaald geval	**Art. 9 WPG**		√	
Inzicht dreiging rechtsorde	**Art. 10 WPG**			√
Informanten, infiltranten, beschermde getuigen	**Art. 12 WPG**			√

[11] Dit betekent overigens niet dat de korpschef daarmee toegang tot betreffende ICT systemen krijgt. De daadwerkelijke toegang tot ICT systemen is immers gebaseerd op 'noodzakelijkheid'.

[12] In de huidige praktijk wordt van gegevens in BVH gemakshalve aangenomen dat ze artikel 8 zijn. Dit is eigenlijk onjuist omdat er ook artikel 9 gegevens in verwerkt worden.

2.3 Model m.b.t. raadplegen

2.3.1 Inleiding

Naast het verwerken van eigen informatie is het noodzakelijk dat medewerkers ook informatie van anderen kunnen raadplegen.

Er zijn een aantal zaken van belang bij dit onderdeel van het model:

a) Er zijn twee vormen van raadplegen:

- **Hit/no hit zoeken**: dit is zoeken door middel van een beperkte zoeksleutel/vaste kenmerken (zoals op naam, kenosleutel, postcode of kenteken).
  Als er een treffer is, dan mag men de bijbehorende gegevens zien.

- **Vrij doorzoeken**: dit is het doorzoeken van grote hoeveelheden politie-gegevens met uitgebreide zoeksleutels en het leggen van complexe verbanden (bijv. naam begint met een J, heeft blond haar, rijdt een BMW). Bij deze manier van zoeken is de inbreuk op de persoonlijke levenssfeer groter dan bij het hit/no hit raadplegen. Deze manier van zoeken is dan ook niet voor iedereen weggelegd en zal met name bij zogenaamde super-users zijn belegd (zie verder onder b). Overigens, wie vrij mag doorzoeken, mag ook hit/no hit zoeken.

b) De Wet biedt ruimte om gebruik te maken van **super-users.** Dit zijn medewerkers die zijn belast met de coördinatie van informatie en die daarom uitgebreide toegang tot informatie mogen hebben.

Aan het autorisatiemodel zijn de volgende (super-user) rollen toegevoegd waarbij ook uitgegaan is van drie autorisatieniveaus:

Informatiecoördinator Dagelijkse Politietaak. Deze super-user mag bij gegevens uit het art. 8 regime van de WPG (in de huidige situatie zouden bijv. medewerkers op districtelijke informatieknooppunten en centralisten deze rol krijgen).

Informatiecoördinator Rechtsorde. Deze super-user mag bij gegevens uit de art. 8 en 9 regimes van de WPG (in de huidige situatie zou bijv. een infodeskmedewerker of een tactisch analist deze rol kunnen krijgen). Deze informatiecoördinator mag bij meer gegevens dan de informatiecoördinator Dagelijkse Politietaak.

Informatiecoördinator CIE/RID/Thema. Deze super-user mag bij gegevens uit art. 8, 9 en 10 regimes van de WPG (in de huidige situatie zou bijv. een lid van de eenheid CIE/RID of een CIE-analist deze rol kunnen krijgen).

c) De Wet biedt ruimte om gebruik te maken van **afhandelingscodes**: gegevens die worden verwerkt onder het regime van art. 9 of 10 van de WPG kunnen worden voorzien van een afhandelingscode. Die afhandelingscode bepaalt dan in hoeverre de gegevens door anderen (die op het eerste gezicht niet bij de informatie zouden mogen) toch benaderbaar zijn en gebruikt mogen worden.

De bevoegd functionaris / teamleider geeft daarmee vooraf toestemming voor een bepaalde vorm van gebruik.

Aan het autorisatiemodel zijn de volgende afhandelingscodes toegevoegd, waarbij ook uitgegaan is van drie niveaus:

Bruikbaar (groen): deze gegevens zijn direct operationeel bruikbaar (in een proces verbaal bijvoorbeeld)

For Intelligence Only (oranje): deze gegevens zijn niet direct operationeel bruikbaar, maar kunnen wel gebruikt worden voor analysedoeleinden. De gegevens kunnen niet gebruikt worden voor bewijsvoering of voor verantwoording buiten de politie/KMar/BOD-en. Ze kunnen ook niet gedeeld worden met personen en instanties buiten het politiedomein. Om deze gegevens operationeel te kunnen gebruiken is toestemming van de bevoegd functionaris nodig.

Embargo (Rood): deze gegevens worden niet getoond aan degene die raadpleegt, maar de bevoegd functionaris[13] krijgt een signaal dat iemand naar die informatie heeft gezocht. Het betreft bijvoorbeeld gegevens uit strafrechtelijke onderzoeken door Interne Zaken/Rijksrecherche of embargo onderzoeken.

De afhandelingscodes zullen nader worden toegelicht in §2.3.4 (m.b.t. art. 9 regime) en §2.3.5 (m.b.t. art. 10 regime).

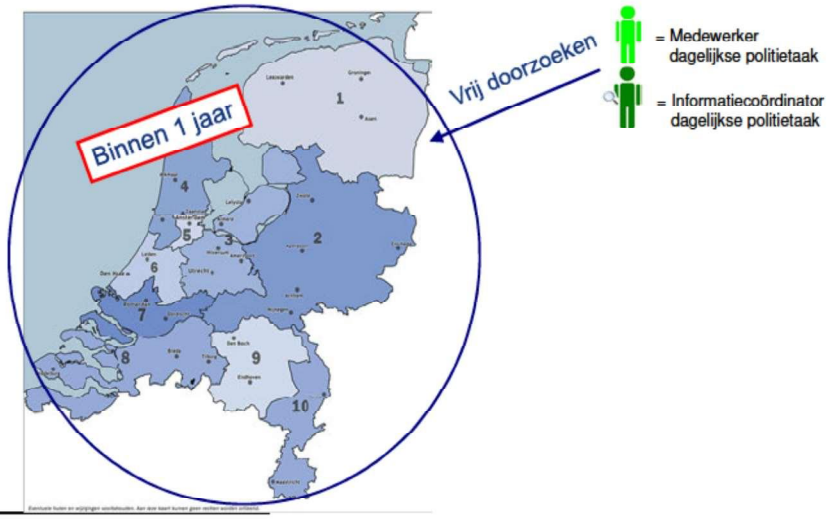
d) Voor de rollen in het autorisatiemodel geldt 'Wie het meerdere mag, mag ook het mindere'.

2.3.2 Raadplegen art. 8 gegevens

Art. 8 van de WPG gaat over de dagelijkse politietaak. Het betreft met andere woorden het basispolitiewerk (surveillance, afhandeling verkeersproblematiek, verlenen van hulp, opnemen van aangiften e.d.).

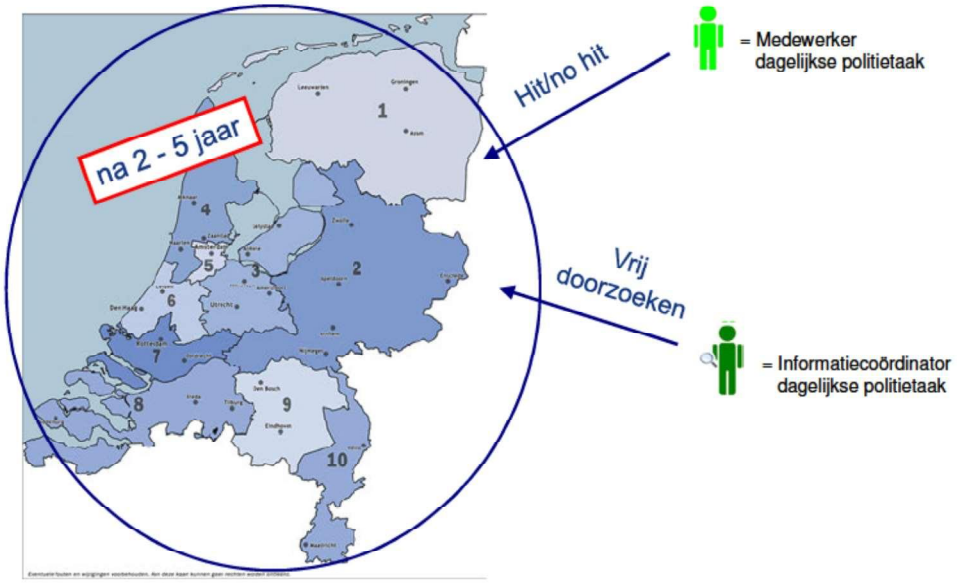
Kernpunten bij het raadplegen van art. 8 gegevens zijn:

- Binnen het 1e jaar (van de vastlegging) mag 'iedereen' vrij zoeken in die gegevens

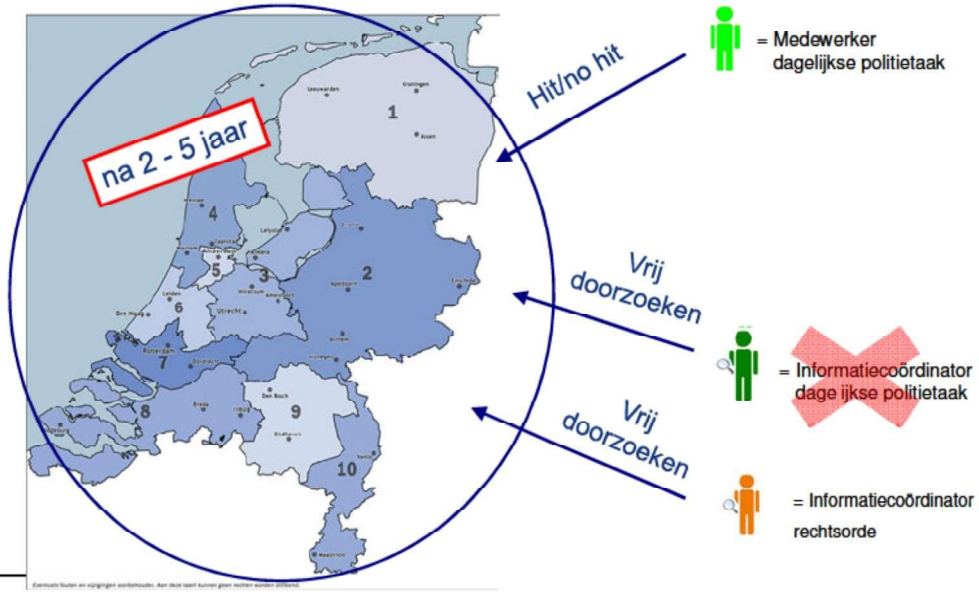


[13] Teamleider van een onderzoek of zijn plaatsvervanger.

- Van het 2e tot en met het 5e jaar mag de medewerker Dagelijkse politietaak de gegevens slechts nog hit/no hit raadplegen. De informatiecoördinatoren mogen wel vrij zoeken.



- De rol Informatiecoördinator Dagelijkse politietaak wordt op termijn uitgefaseerd. In de visie van de expertgroep zijn er over 5 jaar alleen nog informatie-coördinatoren die vanuit een totaalperspectief kijken: informatie-coördinatoren die gedegen en volledig zijn opgeleid om vanuit welke vraag dan ook te kunnen zoeken en te kunnen beoordelen óf en zo ja op welke wijze gegevens kunnen worden ontsloten.
  Met andere woorden: in de toekomst zijn er alleen nog maar 'Informatiecoördinatoren rechtsorde'[14].



[14] Dit heeft impact voor de inrichting van de (informatie) organisatie en zal nader moeten worden uitgewerkt.

- Er komt geen 'beslotenheid' meer voor in art. 8. Het is niet wenselijk om gegevens af te schermen in het art. 8 regime. Indien bepaalde 'gevoelige' gegevens moet worden afgeschermd moeten die gegevens worden verwerkt onder het art. 9 regime.

2.3.3 Raadplegen art. 9 gegevens

Art. 9 van de WPG gaat over de verwerking van politiegegevens voor een onderzoek in verband met de handhaving van de rechtsorde in een bepaald geval.

Momenteel kan een rechercheur alleen bij de gegevens uit zijn eigen onderzoek en kan alleen een informatiecoördinator (bijv. tactisch analist) bij gegevens uit andere onderzoeken.

De wet – en het autorisatiemodel – bieden echter meer ruimte. Kernpunten daarbij zijn:

- **Programmatische rechercheren:** Art. 9 heeft betrekking op een 'gericht onderzoek bepaald geval'. Een programma met een bepaald doel (bijv. georganiseerde hennepteelt) kan daar ook onder worden geschaard. Binnen zo'n programma (en de verschillende deelonderzoeken) hebben de medewerkers dan dus 'breed' toegang tot alle gegevens uit het programma;

- **Gebruik afhandelingscodes:** In art. 9 wordt op de volgende manier gebruik gemaakt van de afhandelingscodes:

  Bruikbaar (groen): alle gegevens die niet zijn verkregen via Bijzondere Opsporingsbevoegdheid (BOB) zijn direct operationeel bruikbaar. Hiermee krijgen twee rollen ruimere toegang tot art. 9 gegevens dan ze nu hebben, namelijk: de medewerker Rechtsorde (bijv. rechercheur) en de Informatiecoördinator Dagelijkse politietaak. Zij mogen deze gegevens op basis van hit/no hit raadplegen.

  For Intelligence Only (oranje): gegevens die zijn verkregen met BOB middelen zijn in eerste instantie For Intelligence Only. Ze kunnen pas operationeel gebruikt worden

als de Officier van Justitie daar toestemming voor heeft gegeven. De Informatiecoördinator Rechtsorde mag vrij zoeken in deze gegevens[15].

Embargo (Rood): (een treffer op) embargo informatie wordt niet getoond aan degene die raadpleegt. Wel krijgt de bevoegd functionaris een signaal dat iemand naar die informatie heeft gezocht.

2.3.4 Raadplegen art. 10 gegevens

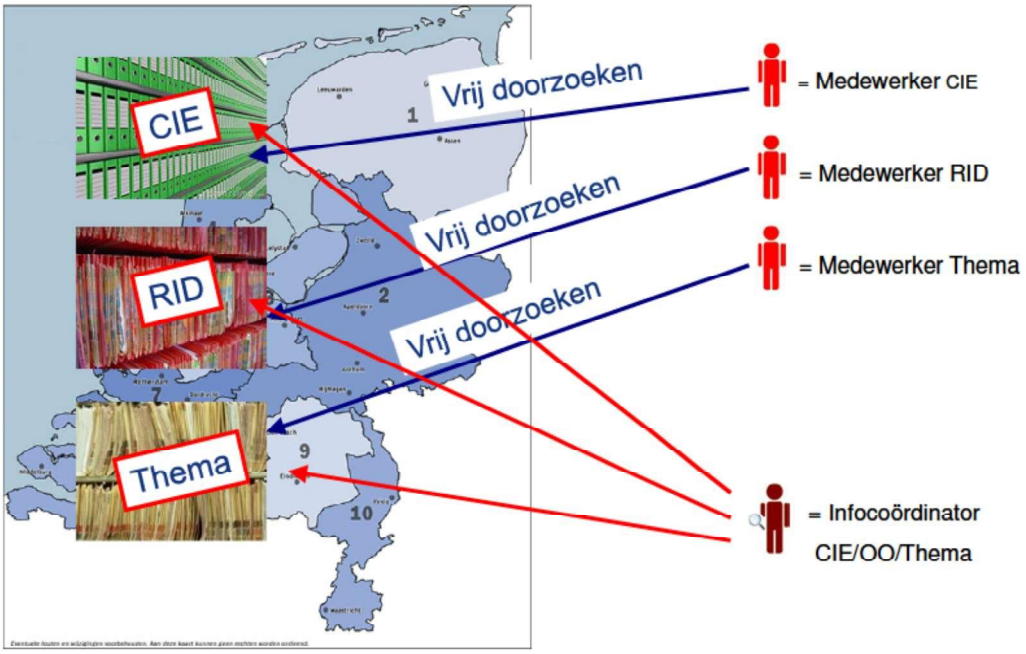
Art. 10 van de WPG gaat over de gerichte en omvangrijke verwerking van politiegegevens met het oog op het verkrijgen van inzicht in de betrokkenheid van personen bij bepaalde ernstige bedreigingen van de rechtsorde (CIE, RID en themagegevens). Er wordt met andere woorden een informatiepositie opgebouwd.
Kernpunten bij het raadplegen van art. 10 gegevens zijn:

- Medewerkers CIE/RID/Thema mogen alleen bij gegevens van hun eigen eenheid: dus een medewerker CIE mag bij CIE info, een medewerker RID bij RID info en een medewerker Thema bij Thema info;
- Aangezien het nu drie functioneel van elkaar gescheiden gebieden zijn, kan dit een risico opleveren bij operaties. Om dit in de toekomst te voorkomen stelt de expertgroep voor om een (limitatief aantal) informatiecoördinatoren CIE/RID/Thema de mogelijkheid te geven dwars door de CIE/RID/Thema gegevens te zoeken[16]. De

[15] Met OM moet nader worden uitgewerkt wanneer gegevens als 'oranje' worden geclassificeerd en wat er wel/niet met die gegevens mag.

[16] Momenteel bestaat deze rol nog niet en wordt alleen dwars door de gegevens gezocht als de Officier van Justitie daar een opdracht voor heeft gegeven (art. 11 lid 4 WPG). Met de nu voorgestelde rol heb je als politie zelf in de hand wanneer je doorzicht wilt creëren.

wet biedt deze ruimte[17]. De rol zal bij iemand uit de CIE of RID eenheid worden belegd[18];



- Bij art. 10 wordt op de volgende manier gebruik gemaakt van de afhandelingscodes:

  Bruikbaar (groen): de volgende gegevens zullen als bruikbaar worden geclassificeerd: verstrekte CIE pv's, subject-/persoonsgegevens die door de CIE ter beschikking worden gesteld, rest- en zijtakinfo. Hiermee krijgen de medewerker Rechtsorde (bijv. rechercheur) en de Informatie-coördinator Rechtsorde toegang tot deze gegevens.

  For Intelligence Only (oranje): dit betreft bijvoorbeeld gegevens van informanten die nog geverifieerd moet worden. In de CIE praktijk zal nader moeten worden uitgewerkt wanneer gegevens als Oranje worden geclassificeerd.

  Embargo (Rood): dit betreft bijvoorbeeld gegevens van informanten met zware beperking voor gebruik (waar informant of lopende inlichtingentrajecten op stuk kunnen lopen), politiek gevoelige gegevens of gegevens in verband met ambtelijke corruptie. Zie ook afhandelingscodes 00 en 300 uit de CIE regeling. Embargo

[17] Wel geeft de wet aan dat toestemming van het hoofd van de eenheid nodig is. Dit zal landelijk ingeregeld moeten worden om te voorkomen dat hoofden van een eenheid deze bevoegdheid tegenhouden.

[18] Een Thema eenheid is door wetgever weliswaar opgenomen in art. 10 en heeft daardoor uitgebreide bevoegdheden (vergelijkbaar met CIE/RID eenheid), maar ze mogen geen informanten runnen. Daardoor is het niet wenselijk dat een medewerker Thema deze bevoegdheid krijgt om dwars door de CIE/RID/Thema gegevens te zoeken.

informatie wordt niet getoond aan degene die raadpleegt. Wel krijgt de bevoegd functionaris een signaal dat iemand naar die informatie heeft gezocht.

Deze afhandelingscodes komen overigens niet één op één overeen met de afhandelingscodes uit de CIE-regeling. Met het OM zal dit nader moeten worden uitgewerkt en of/op welke wijze deze afhandelingscodes de afhandelingscodes uit de CIE regeling kunnen vervangen en/of de CIE regeling in dit verband dient te worden aangepast[19]. Het vereist in ieder geval professionaliteit aan beide kanten: zowel bij het classificeren van gegevens als bij het gebruiken van de informatie.

2.3.5 Raadplegen art. 13 gegevens

Art. 13 van de WPG gaat over de verdere verwerking van politiegegevens voor ondersteunende taken. Het zijn gegevens die in eerste instantie in een art. 8, 9 of 10 verwerking zijn opgenomen, maar die structureel relevant kunnen zijn ter ondersteuning van de politietaak. De WPG regelt níet wie toegang mag hebben tot art. 13 gegevens. Wel bepaalt de wet dat voor art. 13 gegevensverzamelingen (zoals bijv. HKS, HAVANK, LORS, OPS, FCM) een protocol moet worden opgesteld waarin onder andere wordt vastgelegd wie geautoriseerd is voor die gegevens.

Kernpunten voor het Autorisatiemodel zijn:

- De expertgroep stelt voor om de toegang tot de art. 13 gegevensverzamelingen in lijn met het Autorisatiemodel in te richten. Daartoe zal voor elke art. 13 gegevensverzameling moeten worden nagegaan voor wie de gegevens speciaal bedoeld zijn: is dat voor ondersteuning van de dagelijkse politietaak (art 8), onderzoek bepaald geval (art. 9) of art. 10. Vervolgens kan in het verlengde daarvan het Autorisatiemodel worden toegepast.
- Om er voor te zorgen dat protocollen in overeenstemming met het Autorisatiemodel zijn opgesteld, is het denkbaar dat zo'n protocol pas kan worden vastgesteld als een (toekomstige) toetsende instantie er naar heeft gekeken en heeft goedgekeurd[20].

[19] Een mogelijk voordeel van het gebruik van deze afhandelingscodes is dat je aan de afhandelingscode/-kleur niet kunt zien dat het gaat om afscherming van een informant.

[20] Zie Autorisatieautoriteit in Hoofdstuk 3

2.3.6 Totaaloverzicht autorisatiemodel

Al met al ziet het autorisatiemodel voor raadplegen er als volgt uit:

Raadplegen			Medewerker dagelijkse politietaak	Informatiecoördinator dagelijkse politietaak	Medewerker rechtsorde	Informatiecoördinator rechtsorde	Medewerker CIE/RID/Thema	Informatiecoördinator CIE/RID/Thema
Dagelijkse politietaak	Art. 8 WPG	Binnen 1 jaar	√	√	√	√	√	√
		2- 5 jaar	hit/no hit	√	hit/no hit	√	√	√
Onderzoek bepaald geval	Art. 9 WPG	Eigen onderzoek			√	√	√	√
		Afhandelcode Bruikbaar		hit/no hit	hit/no hit	√	√	√
		Afhandelcode For Intell Only				√	√	√
		Afhandelcode Embargo	Signaal naar bevoegd funct.	Signaal naar bevoegd funct.	Signaal naar bevoegd funct.	Signaal naar bevoegd funct.	Signaal naar bevoegd funct.	Signaal naar bevoegd funct.
Inzicht dreiging rechtsorde	Art. 10 WPG	Alle verwerkingen					√	√
		Afhandelcode Bruikbaar			hit/no hit	√	√	√
		Afhandelcode For Intell. Only Hit/no hit				hit/no hit	√	√
		Afhandelcode Embargo	Signaal naar bevoegd funct.	Signaal naar bevoegd funct.	Signaal naar bevoegd funct.	Signaal naar bevoegd funct.	Signaal naar bevoegd funct.	Signaal naar bevoegd funct.
Onder-steunende taken	Art. 13 WPG	'Art. 8' basis	hit/no hit	√	hit/no hit	√	√	√
		'Art. 9' basis			hit/no hit	√	√	√

√ = Vrij doorzoeken: dit is het doorzoeken van grote hoeveelheden politie-gegevens met uitgebreide zoeksleutels en het leggen van complexe verbanden. Wie vrij mag doorzoeken, mag ook hit/no hit zoeken.

Hit/no hit = Hit/no hit zoeken: zoeken door middel van een beperkte zoeksleutel/vaste kenmerken (zoals op naam, kenosleutel, postcode of kenteken).

Signaal = Deze gegevens worden niet getoond aan degene die raadpleegt, maar de bevoegd functionaris krijgt een signaal dat iemand naar die informatie heeft gezocht.

Zo'n signaalfunctie vindt overigens niet alleen plaats als iemand in embargo gegevens zoekt, maar ook bij groene en oranje gegevens[21]. Deze 'signaalfunctie' is om meerdere redenen gewenst:
- het levert een positieve bijdrage aan vertrouwen en cultuur (dat goed met informatie wordt omgegaan);
- er gaat een preventieve werking van uit (medewerker weet dat zichtbaar is dat hij/zij naar bepaalde gegevens heeft gezocht);

[21] Nadere uitwerking van de signaalfunctie en in hoeverre/op welke manier dit in ICT kan worden gebouwd moet nog plaatsvinden. Zie verder Bijlage 'Globale ICT Impactanalyse'.

- het levert bevoegd functionaris ook nuttige informatie op (wellicht dat ‘raadpleger’ ook nuttige informatie voor hem heeft);
- stimuleert onderlinge afstemming en coördinatie.

2.3.7 Art. 12 (besloten deel)

Er is echter ook nog een ‘besloten’, niet algemeen inzichtelijk deel van het autorisatiemodel. Dit betreft art.12 van de WPG en gaat over de verwerking van gegevens over informanten, infiltranten en beschermde getuigen.
Voor dit deel van het autorisatiemodel worden de volgende rollen toegevoegd:

Chef CIE/RID (ook bijv. de korpschef en RIO chef zullen deze rol krijgen)

Informatiecoördinator Veiligheid (is een nieuwe rol vanuit oogpunt veiligheid en beheer; is nu nog nergens belegd)

Medewerker Infiltratie, beschermde getuige

2.3.8 Plaatje art. 12

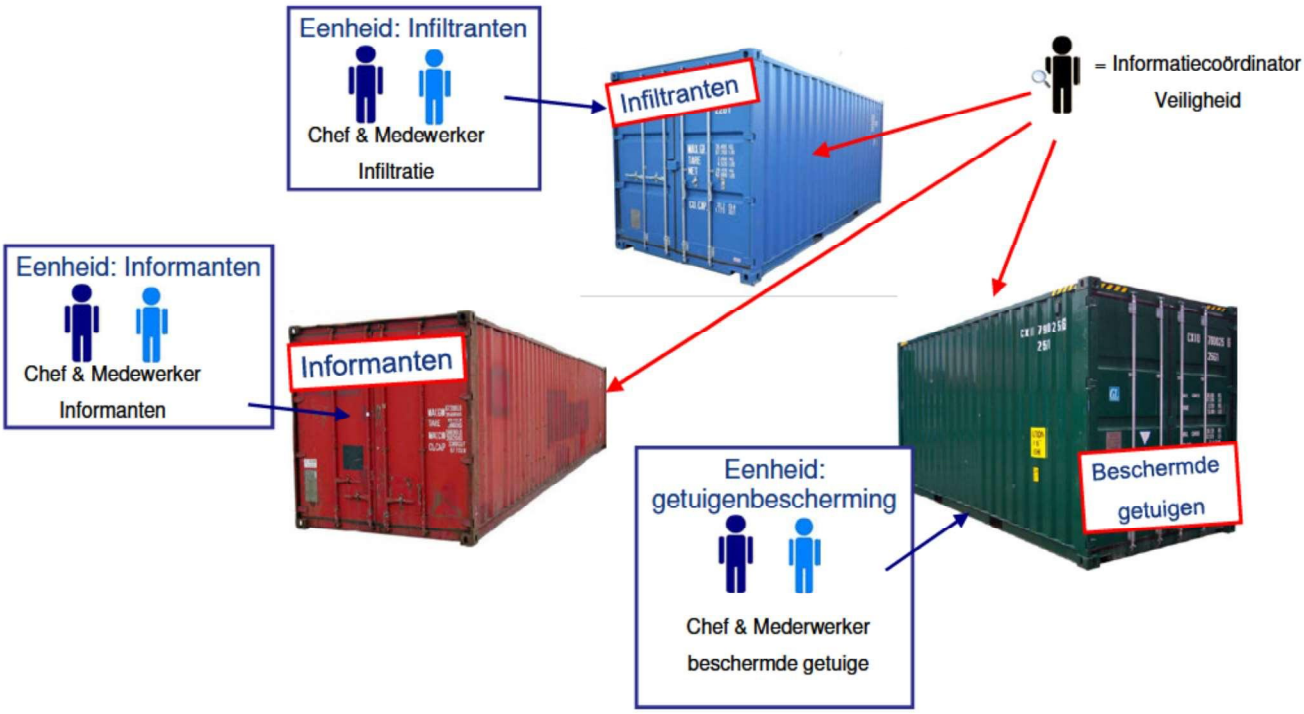
Het autorisatiemodel voor art. 12 ziet er als volgt uit:

	Raadplegen		CIE RID		CIE RID		
			Medewerker CIE/RID	Informatiecoördinator CIE/RID/Thema	Chef CIE/RID	Informatiecoördinator Veiligheid	Medewerker infiltratie, beschermde getuige
Dagelijkse politietaak	Art. 8 WPG	Binnen 1 jaar	√	√	√	√	
		2- 5 jaar	√	√	√	√	
Onderzoek bepaald geval	Art. 9 WPG	Eigen onderzoek	√	√	√	√	
		Afhandelcode Bruikbaar	√	√	√	√	
		Afhandelcode For Intell Only	√	√	√	√	
		Afhandelcode Embargo	Signaal naar bevoegd funct.	Signaal naar bevoegd funct.	Signaal naar bevoegd funct.	Signaal naar bevoegd funct.	
Inzicht dreiging rechtsorde	Art. 10 WPG	Alle onderzoeken	√	√	√	√	
		Afhandelcode Bruikbaar	√	√	√	√	
		Afhandelcode For Intell. Only	√	√	√	√	
		Afhandelcode Embargo	Signaal naar bevoegd funct.	Signaal naar bevoegd funct.	Signaal naar bevoegd funct.	Signaal naar bevoegd funct.	
Onder-steunende taken	Art. 13 WPG	'Art. 8' basis	√	√	√	√	
		'Art. 9' basis	√	√	√	√	
Informanten, infiltranten, beschermde getuigen	**Art. 12 WPG**	**Algem. gegevens (eigen eenheid)**	√	√	√	√	√
		Identificerende gegevens			√		

Kernpunten bij het raadplegen van art. 12 gegevens zijn:

- De leden van een eenheid mogen alleen bij gegevens van hun eigen eenheid: dus de eenheid getuigenbescherming mag alleen bij getuigenbescherming, de eenheid infiltranten mag alleen bij infiltranten en de eenheid informanten alleen bij informanten;
- Het zou goed zijn een rol Informatiecoördinator Veiligheid te creëren die vanuit beheer en veiligheid oogpunt alle gegevens kan overzien om te voorkomen dat

operaties gaan botsen. Deze rol zou slechts bij een enkeling moeten worden belegd[22];



- Art. 12 kent geen afhandelingscodes;
- Alleen de Chef CIE/RID mag bij identificerende gegevens.

[22] Denk bijv. aan bronafschermingszaken van Ipol. De verdere uitwerking moet nog worden vormgegeven.

3. Randvoorwaarden

Er zijn diverse randvoorwaarden aan dit model en deze visie verbonden. Voordat dit autorisatiemodel volledig in de praktijk kan worden gebracht moeten deze randvoorwaarden worden ingevuld. Niet alleen om het risico van verkeerd gebruik van informatie te minimaliseren, maar ook om het autorisatiemodel in de organisatie en de ICT in te kunnen regelen.

3.1 Vanuit organisatie en beheer / minimaliseren afbreukrisico

Er is een set (beheers)maatregelen nodig om het afbreukrisico van verkeerd gebruik van gegevens te minimaliseren. De invulling van de volgende randvoorwaarden is noodzakelijk.

3.1.1 Autorisatiebeleid

Bij een autorisatiemodel hoort ook een autorisatiebeleid waarin het gehele proces wordt beschreven dat er voor zorgt dat medewerkers de juiste (toegangs)rechten hebben.
Het beschrijft niet alleen welke (autorisatie)rol bij welke gegevens mag, maar ook:

- wie welke taken, verantwoordelijkheden en bevoegdheden heeft in het proces van autorisatietoekenning;
- op welke manier het toekennen, wijzigen en intrekken van autorisaties plaatsvindt;
- welke (autorisatie)rollen onverenigbaar zijn met elkaar;
- welke deskundigheidseisen worden gesteld aan autorisaties;
- etc.

3.1.2 Opleiding en certificering: de informatiecompetente politiemedewerker

Eén van de uitgangspunten van het model is dat het uit gaat van de professionaliteit van medewerkers: de deur met toegang tot gegevens wordt niet bij voorbaat dichtgezet uit eventuele angst voor verkeerd gebruik.
Dit betekent dat het van cruciaal belang is dat er eisen gesteld worden aan medewerkers voordat ze geautoriseerd worden om met politiegegevens te kunnen werken. Een belangrijke eis is dat politiemedewerkers goed opgeleid zijn in het gebruiken van informatie[23].
Voorwaarde voor het verkrijgen van een bepaalde autorisatierol is het succesvol afronden van de daarvoor vereiste opleiding. In het algemeen geldt: naarmate de toegang tot informatie ruimer is, zijn de opleidings- en screeningseisen zwaarder.

Hierbij kan een vergelijking worden gemaakt met andere bevoegdheden van politiemedewerkers: wapen dragende ambtenaren moeten gecertificeerd zijn en regelmatig getraind en getoetst worden voordat ze geweldsmiddelen mogen gebruiken. Als de schiettoets niet gehaald wordt, dan gaat er geen vuurwapen mee de straat op. Eenzelfde eis moet gaan gelden voor de bevoegdheid om informatie te gebruiken: zonder aantoonbare en getoetste competentie geen toegang tot informatie.

3.1.3 Controle en toezicht: Landelijke Autorisatieautoriteit

Maar met een autorisatiebeleid en opleiding en certificering van medewerkers zijn we er niet. Er is ook (pro)actief controle en toezicht nodig:
- op juiste toepassing van het autorisatie regime en -beleid (bijv. wie zijn geautoriseerd en is dat legitiem?);
- op integriteit van het omgaan met de informatie (maakt de geautoriseerde op de juiste manier gebruik van zijn autorisatie?). Dit kan gerealiseerd worden door o.a. het gautomatiseerd monitoren van toegang tot en zoekgedrag op informatie en met een

[23] Andere eisen hebben betrekking op screening, benodigde competenties e.d

geautomatiseerde signaleringsfunctie/alertering[24]. Dit stelt eisen aan de ICT: deze zal monitor-, controle- en alerteringfunctionaliteit moeten bieden.

De expertgroep stelt voor dat er een Landelijke Autorisatieautoriteit Nederlandse Politie komt. Hierin zullen Politie en OM zijn vertegenwoordigd.
Deze autoriteit zal onder andere (pro)actief toezicht en controle uitoefenen op de rechtmatige toepassing van het autorisatiemodel en de toegang tot en het gebruik van informatie. Verder onderhoudt de Autorisatieautoriteit het autorisatiemodel en bijbehorend –beleid (idem voor de 'specials'), is het de goedkeurende instantie voor nieuw benodigde autorisatie rollen, art. 13 protocollen etc.

3.2 Vanuit ICT

De ICT zal er voor moeten zorgen dat de juiste informatie toegankelijk is voor de juiste personen/rollen. De invulling van de volgende randvoorwaarden is bepalend voor het slagen hiervan.

3.2.1 Goede rubricering gegevens

Om te kunnen autoriseren is het noodzakelijk dat gegevens goed worden gerubriceerd: van de vastgelegde gegevens moet duidelijk zijn in welk WPG-regime ze vallen en welke afhandelingscode erop van toepassing is.
Alleen op die manier kan ingeregeld worden dat een autorisatierol toegang krijgt tot de juiste gegevens[25]. Dit vereist dat zwaar wordt ingezet op goede invoer/gegevensbeheer.
Daarnaast is het belangrijk dat gestuurd wordt op wélke gegevens wáár worden weggeschreven: indien er applicaties zijn waarin gegevens behoren te worden vastgelegd, dan moet dáárin worden geregistreerd en niet in Word/Excel.

3.2.2 Landelijk beheer van autorisaties

Momenteel is het beheer van autorisaties versnipperd, regionaal verschillend, chaotisch, vindt veelal handmatig plaats en er is geen landelijke sturing op. Om deze problemen op te lossen (en de korpsbeheerders aan hun verantwoordelijkheid te kunnen laten voldoen om een systeem van autorisaties te onderhouden dat voldoet aan de vereisten van zorgvuldigheid en evenredigheid) is het noodzakelijk dat:

- de registratie van medewerkers en dienstverbanden uniform, eenduidig en actueel is. Autorisaties komen bij voorkeur geautomatiseerd via het personeelssysteem tot stand. Zodra daar een functie, rol of taak wordt toegekend, gewijzigd of ingetrokken zal dit automatisch tot een autorisatiewijziging leiden. Dit vereist een goede, tijdige registratie van medewerkers, dienstverbanden, opleidingen etc. op een centrale plaats, op landelijk niveau. Het personeelssysteem moet het Single-point-of-Truth zijn rond de status van de medewerker. Bovendien moet een gebruiker een uniek landelijk personeelsnummer hebben.
- er een landelijk autorisatiebeheersysteem komt waarin autorisaties centraal worden vastgelegd en decentraal kunnen worden beheerd. Dit autorisatiebeheersysteem moet geautomatiseerd signalen van het HRM systeem kunnen verwerken (zoals uitdiensttreding en schorsing).

[24] Bijvoorbeeld bij afwijkend zoekgedrag. Maar ook door bijvoorbeeld een signaal naar de 'bevoegd functionaris' te sturen dat iemand heeft gezocht in onderzoeksgegevens.
[25] Momenteel gebeurt dat op basis van 'applicaties': BVH gegevens worden als art. 8 WPG gerubriceerd en BVO gegevens als art. 9 WPG. In het echt is het niet zo zwart/wit: BVH bevat niet alleen art 8 WPG gegevens en BVO niet alleen art. 9 WPG gegevens.

3.2.3 Logging

Alle relevante verwerkingen moeten gelogd worden. Dat heeft niet specifiek met het autorisatiemodel te maken. De WPG eist van zichzelf al voldoende transparantie.
Hiervoor lopen op dit moment al projecten[26] binnen de vtsPN. Van belang is dat hierin de voor toezicht en controle benodigde functionaliteiten worden meegenomen (ten behoeve van bijv. monitoring en alertering).

[26] Project BVI Logging en Rapportage server

4. Consequenties bij implementatie

In dit hoofdstuk worden de eerste consequenties voor de Organisatie en ICT op hoofdlijnen beschreven.
Maar het is goed te realiseren dat de implementatie van dit autorisatiemodel (en de daaraan verbonden uitgangspunten en visie op informatiedeling) niet alleen gevolgen heeft voor de organisatie en de techniek van informatiedeling.
De implementatie van het autorisatiemodel beoogt ook een hefboom te zijn voor het teweeg brengen van veranderingen in cultuur, werkwijzen, processen, professionaliteit, deskundigheid, techniek en organisatie (taken en bevoegdheden) bij landelijke informatiedeling. Vooral de cultuur en professionaliteit van informatiedeling en de daaraan verbonden professionele opvattingen en overtuigingen zijn volgens de expertgroep essentiële *'triggers for change'*.

Aanbevolen wordt om in een Business Case verder uit te werken welke consequenties de implementatie van dit autorisatiemodel heeft voor de organisatie, ICT en de overige hiervoor genoemde aspecten. Ook de gevolgen die dit heeft voor de verander- en ontwikkelstrategie en de concretisering van een en ander naar een 'roadmap' moet daarin worden uitgewerkt.

4.1 Betekenis voor Organisatie

Implementatie van dit autorisatiemodel heeft gevolgen op verschillende terreinen:

- Het heeft gevolgen voor de wijze waarop taken, bevoegdheden en besluitvorming met betrekking tot informatiedeling in de (informatie) organisatie zijn en/of worden verankerd.

  De ambitie om op termijn geen informatie-coördinatoren *'dagelijkse politietaak'* meer te hebben en om de informatiecoördinator *'rechtsorde'* als 'draaischijf' te organiseren in de inrichting van de informatie-organisatie, is hierin van grote betekenis. Niet alleen voor wat betreft de 'dagelijkse politietaak' in de gebiedsgebonden teams en de meldkamers, maar ook in de bestrijding van de criminaliteit. De positie en rol van de informatiecoördinator in de verschillende benoemde procesdomeinen heeft impact voor de inrichting van de (informatie) organisatie. De keuze voor de wijze waarop de informatieorganisatie wordt ingericht in het nieuwe Nationale politiebestel, om de werkprocessen vanuit informatie coördinatie te ondersteunen, is hierin essentieel;

  De balans die het autorisatiemodel zoekt tussen informatiedeling enerzijds en afbreukrisico anderzijds heeft ook gevolgen voor de omvang en plaats van de informatiecoördinatoren en/of de informatieorganisatie. Uitgangspunt is dat de rollen van informatiecoördinatie dicht tegen het primaire proces van de dagelijkse politietaak en opsporing aan dienen te worden georganiseerd om effectief te kunnen zijn. Dit heeft o.a. gevolg voor de wijze waarop de rol van informatiecoördinator wordt georganiseerd in bijvoorbeeld rechercheteams, teams voor de dagelijkse politietaak maar ook o.a. binnen meldkamers en multidisciplinaire realtime 'command en control' eenheden;

- Het autorisatiemodel en de visie daarachter impliceren dat de vertaling van functies vanuit het LFNP naar autorisatierollen meer is dan een instrumentele conversie. Deze vertaling dient plaats te vinden binnen de visie en context van informatiedeling, zoals die binnen dit autorisatiemodel is beschreven. Zo ontstaat landelijk vanuit functies eenduidigheid in toedeling en gebruik van rollen. De implementatie van dit autorisatiemodel heeft daarmee direct impact op een landelijke implementatie van het

LFNP en een toekenning van rollen aan functies. De wijze waarop dit dient te worden vormgegeven moet in genoemde Business Case nader worden uitgewerkt. Hierin dient expliciet aandacht te worden besteed aan de landelijk relatie en verbinding tussen het autorisatieproces en het HRM proces;

- Het thema Veiligheid, in relatie tot de functionele domeinen bij artikel 10 en 12, verdient specifieke aandacht voor wat betreft organisatie, werkwijze en benodigde rollen hierin. De praktijk van de afgelopen jaren heeft laten zien dat hierin nog een omissie zit met betrekking tot informatiecoördinatie en organisatie. Dit verdient nog nadere uitwerking binnen genoemde Business Case;

- Realisatie van het autorisatiemodel heeft ook gevolgen voor werkwijze en processen van informatievastlegging en informatiedeling. De keuze voor een driedeling van classificatie van gegevens in **groen**, **oranje** en **rood** heeft hierin gevolgen. Dit zal in een Business Case en met een strategie van verandering nader moeten worden uitgewerkt. Hierbij dient in ieder geval ingegaan te worden op:
  - de keuze om met betrekking tot artikel 8 geen classificatie toe te passen;
  - de keuze om bepaalde politie-gegevens in artikel 9 en 10 op voorhand als bruikbaar te classificeren en de gevolgen daarvan voor werkprocessen en afspraken;
  - de keuze om deze driedeling van classificatie ook van toepassing te laten zijn op de classificaties die de CIE-regeling hanteert. Met het OM en de CIE zal nader onderzocht moeten worden hoe en op welke wijze dit gestalte kan worden gegeven en/of de CIE regeling in deze kan worden aangepast;
  - de wijze waarop het programmatisch rechercheren landelijk vorm wordt gegeven en de betekenis daarvan voor taken, bevoegdheden en processen van informatiedeling;
  - de werkwijze met betrekking tot rest- en zijtakinformatie.

- Voorts heeft implementatie van dit autorisatiemodel tot gevolg dat op landelijk niveau binnen het nieuwe bestel een Autorisatieautoriteit moet worden ingericht. Met als taak landelijke eenduidigheid, inzicht, transparantie én toezicht met betrekking tot het eenduidig delen van politie-informatie conform het landelijke autorisatiebeleid te realiseren;

- Realisatie van een eenduidige en transparante informatiedeling bij de Nederlandse politie stelt nieuwe eisen aan de organisatie van opleiding van medewerkers en heeft gevolgen voor de benodigde inspanningen vanuit de Business hierin. Zoals in hoofdstuk 3.1 reeds is vermeld is professionalising en certificering van medewerkers een essentiële voorwaarde om genoemde ambities en deskundigheid te realiseren. Voor het OM is dit een cruciale voorwaarde om akkoord te gaan met dit autorisatiemodel. Deze ambitie stelt nieuwe eisen aan organisatie en opzet van opleiding aan de Politieacademie. In de Business Case dienen de consequenties van professionalisering en certificering nader te worden onderzocht. Niet alleen voor wat betreft de organisatie van de opleidingen maar ook voor wat betreft toekomstige inspanning en kosten voor de organisatie om dit te realiseren;

- Realisatie van dit autorisatiemodel brengt ook veranderingen met zich mee voor de organisatie van autorisatiebeheer en autorisatiemanagement. De huidige landelijke versnippering hierin dient tot een landelijk autorisatiebeheer en -management te transformeren. Dit is een essentiële voorwaarde om de ambities in dit voorstel te realiseren.

4.2 Betekenis voor ICT

De implementatie van dit landelijke autorisatiemodel zal voor de ICT impact hebben op de volgende terreinen:

- zoals aangegeven in het vorige hoofdstuk is het noodzakelijk dat gegevens goed worden gerubriceerd: van de vastgelegde gegevens moet duidelijk zijn in welk WPG-regime ze vallen en welke afhandelingscode erop van toepassing is. Dit zal grote impact hebben op de huidige applicaties waarin politiegegevens worden vastgelegd. Omdat de impact groot is zal een selectie gemaakt moeten worden welke applicaties in aanmerking komen voor ombouw;
- ook de applicaties met raadpleegfunctionaliteit moeten worden aangepast conform het Autorisatiemodel. Dit heeft gevolgen voor systemen die specifiek gericht zijn op raadplegen (BVI, BlueView, BVI IB en allerlei analysetools), maar ook op systemen die primair bedoeld zijn voor vastlegging (daarin wordt ook geraadpleegd ten behoeve van het vinden van een zaak die verder verwerkt wordt);
- er moet een goede registratie zijn van medewerkers, dienstverbanden en permissies. Deze moet landelijk uniform en eenduidig zijn en op een centrale plaats vastgelegd op landelijk niveau. Met andere woorden, dit stelt eisen aan een landelijke HRM voorziening (en vereist bijvoorbeeld landelijke personeelsnummers);
- er moet een landelijk autorisatiebeheersysteem komen waarin autorisaties centraal worden vastgelegd en decentraal kunnen worden beheerd. Dit autorisatiebeheer-systeem moet geautomatiseerd signalen van het HRM systeem kunnen verwerken (zoals uitdiensttreding en schorsing);
- om technisch toegepast te kunnen worden moet het model vertaald worden naar zogenaamde objecttypen (klassen) en attributen (eigenschappen) in de Gegevensarchitectuur[27]. Daarnaast moeten te implementeren maatregelen (bijv. de signaal/alerteringsfunctie) uit het model in zogenaamde use cases beschreven worden. Hiermee wordt in detail duidelijk wat de ICT moet gaan leveren;
- de toezicht en controle op het autorisatiemodel stellen eisen aan de logging van verwerkingen op informatie en het inzien daarvan.

In de Bijlage 'Globale ICT impactanalyse van een nieuw Landelijk Autorisatie Model' is meer te lezen over genoemde consequenties.
Al met al geeft deze globale impactanalyse een eerste idee van wat de ICT gevolgen zijn. Om een en ander preciezer en gekwantificeerd te bepalen is vervolgonderzoek nodig.

[27] Betreft het Politie Gegevens Model (PGM) en Canonical Domain Model (CDM). Het huidige gegevensmodel is nog gedeeltelijk gebaseerd op het BVO Autorisatiemodel, gecombineerd met WPG elementen. Er is een relatief kleine aanpassing nodig.

5. Beslispunten

1. Stel de visie en strategische uitgangspunten voor eenduidige en transparante informatiedeling bij de Nederlandse politie vast als basis voor verdere uitwerking in een businesscase;

2. Geef de Portefeuillehouder Intelligence uit de RKC de opdracht om in afstemming met de LCIO en het Openbaar Ministerie op basis van deze (als basis) vastgestelde visie en uitgangspunten een businesscase te ontwikkelen, die in ieder geval verder ingaat op de in deze notitie nog nader uit te werken onderdelen (inclusief de positie van BOD en KMar in dit traject);

3. Geef de Portefeuillehouder Intelligence uit de RKC de opdracht om in afstemming met de LCIO en het Openbaar Minsterie in het verlengde van de businesscase de veranderstrategie te ontwikkelen voor de implementatie van eenduidige en transparante informatiedeling bij de Nederlandse politie;

4. Realiseer de businesscase en het voorstel voor de veranderstrategie uiterlijk 1 december 2011, opdat deze voorstellen door de kwartiermaker van de nationale politie kunnen worden meegenomen in de implementatie van de Nationale Politie.

Bijlage: Globale ICT impactanalyse

Vanuit politiewerk zijn meerdere gegevensverwerkingen te onderkennen die door implementatie van een nieuw Landelijk Autorisatie Model (LAM) zullen worden geraakt. Hierbij moet oa. gedacht worden aan: invoeren, opnieuw verwerken, zoeken, signaleren dat er gegevens zijn en signaleren dat er naar gegevens is gezocht enzovoort. Naast deze primaire gegevensverwerkingen moet het logisch en functioneel model in de bedrijfsarchitectuur worden aangepast om autorisatie correct te kunnen vastleggen. In de volgende alinea's zal nader worden ingegaan op deze onderwerpen evenals de organisatorische consequenties bezien vanuit het ICT perspectief.

a. Het Landelijk Autorisatie Model

Het model wordt in eerste instantie in een beschrijvende vorm opgeleverd. Om technisch toegepast te kunnen worden moet het model vertaald worden naar zogenaamde objecttypen (klassen) en attributen (eigenschappen) in de Gegevensarchitectuur[28]. Het huidige gegevensmodel is nog gedeeltelijk gebaseerd op het BVO Autorisatiemodel, gecombineerd met WPG elementen. Er is een relatief kleine aanpassing nodig *(eventueel verwijderen autorisatieniveau, eventueel verwijderen oude afhandelingscode, beschrijven en opnemen van nieuwe afhandelingscode en opnemen van effectief te gebruiken wetsartikel voor artikel 13 gegevens)* om deze up-to-date te brengen. Daarnaast moeten te implementeren maatregelen uit het model in zogenaamde use cases beschreven worden. Hiermee wordt zeer specifiek bepaald wat opmerkingen in het model in het echt betekenen.

b. Classificeren van gegevens

Zowel de medewerker die nieuwe gegevens invoert alsook de medewerker die gegevens hergebruikt moeten informatie classificeren zodat de bevoegd functionaris kan beoordelen of de juiste autorisaties zijn aangebracht. Dit zal grote impact hebben op de huidige systemen omdat dit nu verschillend is geïmplementeerd of zelfs onmogelijk is. Alle systemen aanpassen zal een majeure operatie zijn, het is daarom verstandig om samen met SP3 een selectie te maken van systemen die moeten worden aangepast. Uit te faseren systemen dienen om die reden niet meegnomen te worden, nieuw te bouwen systemen moet direct aan de eisen van het LAM voldoen. Dit resulteert in een lijst applicaties en een bijbehorende planning. Opgemerkt moet worden dat in het kader van Huis op Orde en het Continuïteitsspoor bijna alle applicaties bevroren worden, aanpassen is dan een groot probleem.

Voorbeeld BVH: Op dit moment wordt van gegevens die in BVH worden vastgelegd aangenomen dat ze artikel 8 zijn. Dit is onjuist omdat er ook artikel 9 gegevens verwerkt worden. Daarnaast zijn er afschermingsniveau's in BVH om gegevens voor anderen af te schermen. Deze niveaus worden bij het implementeren van de WPG gebruikt om gegevens die niet meer ingezien mogen worden af te schermen. Die afschermingsniveaus bestaan in de WPG niet. Als deze zaken afscherming behoeven dan vallen ze onder artikel 9. Een oplossing zou kunnen zijn procedureel af te regelen dat alle artikel 9 zaken niet meer in BVH maar in BVO worden verwerkt. De impact daarvan (overzetten van zaken tussen systemen als het gewicht wijzigt, opleiden handhaving gebruikers in BVO, toegenomen performance eisen aan BVO, gebruikers-onvriendelijkheid etcetera) is zo groot dat hiervoor nooit gekozen mag worden. In plaats daarvan is een oplossing nodig waardoor binnen BVH aangegeven kan worden wat het betreffende artikel is. Voor de gebruiker zal dit slechts een vinkje (artikel 8 of 9) zijn. Het systeem kan de gebruiker helpen door default artikel 8 aan te bieden en bij aangiften die een misdrijf betreffen artikel 9 voor te stellen. Uiteindelijk blijft het de verantwoordelijkheid van de BVH gebruiker het juiste artikel te selecteren.

[28] PGM – Politie Gegevens Model, een logisch model in UML en het CDM - Canonical Domain Model, een technisch model in XML Schema.

c. Het beheer van autorisaties

Uitgangspunt en randvoorwaarde voor implementatie van LAM is een goede registratie van medewerkers, dienstverbanden en permissies, die uniform en eenduidig zijn en op een centrale plaats vastgelegd op landelijk niveau. De medewerker moet vervolgens via een juiste identificatie uniek gemaakt worden en die functionaliteiten aangeboden worden die zijn rol vereisen. Dit leidt tot een vereiste voor een landelijke HRM voorziening en landelijke personeelsnummers. Hierbinnen moet actueel duidelijk zijn wie welke functies uitvoert en welke certificaten cq opleidingen heeft behaald. Vastlegging gebeurt op basis van formele besluiten. Dit wordt dan de basis voor een serieuze en controleerbare autorisatie. Er ligt mogelijk een kans aan te sluiten bij de ontwikkelingen binnen de Nationale Politie.
Naast en gekoppeld aan deze HRM registratie is er een nationale autorisatieregistratie noodzakelijk. De vele losse oplossingen nu leiden tot ondoorzichtigheid, oncontroleerbaarheid, gebrek aan actualiteit en fouten cq incidenten. Aan deze voorziening moeten de volgende eisen gesteld worden:

1. Een gekochte voorziening die werkt op basis van marktconforme, open standaards
2. Geschikt om autorisatiebeheer centraal vast te leggen en decentraal te beheren. Immers, de lijnchef deelt autorisatie toe
3. Geschikt om geautomatiseerd signalen van het HRM systeem te verwerken, zoals uitdiensttreding en schorsing
4. Hoogste bruikbaarheid, beschikbaarheid en continuïteit

d. De toepassing van Landelijk Autorisatie Model

Uitgaande van goede vastlegging bij eerste gegevensverwerking en bij hergebruik van gegevens moet de raadpleegfunctionaliteit worden aangepast conform het LAM. Dit heeft gevolgen voor systemen die specifiek gericht zijn op raadplegen (BVI, BlueView, BVI IB en allerlei analysetools).

Voorbeeld BVI BlueView: Als de aanleverende systemen de gegevens op de nieuwe manier aanleveren zijn na een volledig nieuwe aanlevering en een volledig opnieuw opbouwen van de database (een majeur conversietraject) alle ingrediënten aanwezig om volgens het model te werken. Toch zijn er nog verdere aanpassingen nodig. De vastlegging moet omgebouwd worden van de autorisatieniveau's naar de nieuwe afhandelingscodes (wetsartikelen zijn al aanwezig). De gewijzigde regels moeten geïmplementeerd worden, met name een tweede type hit-no-hit en de signalen komen nog niet voor. Het aanpassen van de autorisatiestructuur lijkt minder werk te zijn omdat deze ooit al op basis van de WPG (toen in wording) opgezet is.

Niet vergeten mag worden dat ook binnen systemen veel geraadpleegd wordt ten behoeve van het vinden van een zaak die verder verwerkt wordt dan wel het lokaal hergebruiken van gegevens. Zo kan elke BVH gebruiker ook in de eigen BVH raadplegen. Ook hierin zijn wijzigingen nodig. Denk bijvoorbeeld aan lichte onderzoeken die in BVH gevoerd worden. Deze krijgen artikel 9 toegewezen. Dit betekent dat binnen die BVH de overige handhavinggebruikers deze gegevens niet meer mogen vinden, alleen de bewerkers zelf.

Voorbeeld signaleringsfunctie: Dit is snel opgeschreven maar levert een ICT'er veel vraagtekens op. Wie de eigenaar van gegevens is leggen we nu vaak en straks altijd vast bij de gegevens. Dat is dus makkelijk te achterhalen. Maar wat voor signaal moet daarheen (hoe ziet het eruit en welke gegevens staan erop)? Een eigenaar is vaak een organisatie(onderdeel). Hoe adresseer je die? Via welk kanaal (een telefoontje, een email, een sms, een schermpje dat opent in je applicatie, een workflow opdracht, een portaalfunctie) volgt het signaal? Moet gecontroleerd worden wat ermee gedaan wordt? Moeten de signalen bewaard blijven? Hoe lang? Wie mag ernaar kijken? Hoe ga je om met de vertrouwelijkheid van de gestelde vraag? Stel dat iemand in een ZwaCri onderzoek een vraag stelt betreffende een persoon. Dan mag de zaakleider van een gewoon onderzoek daar zeker geen signaal van hebben. Immers, de vraag verraadt de betrokkenheid en inzicht in de gestelde vragen geeft veel kansen op stapeling.

e. Loggen

Het delen van gegevens is niet vanzelfsprekend, integendeel. Aangegeven werd dat het delen van gegevens makkelijker wordt indien vervolgens transparant is wie welke gegevens bevraagd cq verwerkt heeft. Daartoe werden twee smaken benoemd.
Allereerst moeten alle relevante verwerkingen gelogd worden. Dat heeft echter niet specifiek iets met het autorisatiemodel te maken. De WPG eist van zichzelf al voldoende transparantie. Hiervoor lopen er op dit moment al projecten[29] die gewoon door moeten gaan.
Daarnaast spreekt de wet over een signaal naar de eigenaar en ook geven de deskundigen aan dat in zijn algemeenheid een signaal naar de eigenaar als zijn/haar gegevens geraakt cq verwerkt worden het vertrouwen en daarmee de bereidwilligheid te delen zou vergroten. Er zijn verschillende modellen mogelijk om een signaalfunctie te realiseren. De eerste mogelijkheid is dit in alle systemen op te lossen. Dit is zeer complex en ingrijpend omdat alle systemen aangepast moeten worden. De betere mogelijkheid is dit signaal te koppelen aan de BVI Informatiedienst Logging. Daar komen immers alle logregels bij elkaar en kan op één plaats zo'n signaalfunctie komen. Dat kan ook weer op twee manieren. De eerste manier geeft bevoegde medewerkers de mogelijkheid in te zien welke eigen gegevens bevraagd cq verwerkt zijn. Dit is redelijk makkelijk te doen en betekent een middelgrote scope uitbreiding op het huidige project. Een andere oplossing kan zijn dat de BVI Informatiedienst Logging zelf actief signalen doorstuurt naar geïnteresseerden. Dit moet gezien worden als een grote scope uitbreiding.

f. Advies vervolgonderzoeken

Bovenstaande geeft een eerste idee van wat de ICT gevolgen zijn. Om een en ander preciezer en gekwantificeerd te bepalen is vervolgonderzoek nodig. Aan de hand van de uitkomsten wordt het mogelijk een fasering en roadmap te maken. Dit zijn de onderzoekspunten:

1. Maak een inhoudelijke inventarisatie van lopende en te starten project en ontwikkelingen waarvan de inhoud deze impactanalyse raakt. Wie is allemaal waar mee bezig?
2. Onderzoek welke bronapplicaties in aanmerking komen voor aangepaste vastlegging en bepaal per applicatie de impact. Bezie ook per bronapplicatie de "interne" raadplegingen.
3. Onderzoek de bronnen die nu nog niet ontsloten worden maar die wel van groot belang zijn.
4. Onderzoek welke raadpleegapplicaties in aanmerking komen voor aangepaste raadpleging en bepaal per applicatie de impact.
5. Bepaal de impact van een landelijk HRM systeem
6. Bepaal de impact van een landelijk autorisatiebeheersysteem
7. Bepaal de impact van het gevraagde op de BVI Informatiedienst Logging

[29] Project BVI Logging en Rapportage server

Bijlage: Overzicht geraadpleegde deskundigen in 2e ronde

Deskundige	Organisatie
5.1.2.e [redacted]	KLPD
5.1.2.e [redacted]	Regiopolitie Amsterdam
5.1.2.e [redacted]	Regiopolitie Amsterdam
5.1.2.e [redacted]	BRNON IJsselland
5.1.2.e [redacted]	vtsPN
5.1.2.e [redacted]	Regiopolitie Amsterdam (CIE chef)
5.1.2.e [redacted]	Politieacademie (opleiding & certificering)
5.1.2.e [redacted]	Regiopolitie Twente / PLIC

Bijlage: Overzicht geraadpleegde klankbordgroep in 3e ronde

Klankbordgroep	Organisatie
5.1.2.e [redacted]	OM
5.1.2.e [redacted]	OM
5.1.2.e [redacted]	OM
5.1.2.e [redacted]	WPG
5.1.2.e [redacted]	WPG
5.1.2.e [redacted]	WPG
5.1.2.e [redacted]	WPG
5.1.2.e [redacted]	WPG