# Gegevens burgers niet veilig bij politie

Onderzoek naar de audits Wet politiegegevens bij de politie

4 juli 2012

BITS OF FREEDOM
VERDEDIGT DIGITALE BURGERRECHTEN

De politie heeft ingrijpende bevoegdheden voor het verwerken van persoonsgegevens. Ook is daarin bepaald hoe zij met die gegevens moet omgaan. Elke vier jaar wordt gecontroleerd of ze zich aan die regels houdt. Bits of Freedom heeft de rapporten van eind vorig jaar opgevraagd. Het resultaat is diep triest. Geen enkel korps voldoet aan alle wettelijke regels. Persoonsgegevens zijn bij de politie dus lang niet altijd in veilige handen. Bits of Freedom eist dat de misstanden direct worden gecorrigeerd, de korpsen jaarlijks worden gecontroleerd, en een moratorium op uitbreiding van bevoegdheden wordt ingesteld.

# INHOUD



BITS OF FREEDOM
VERDEDIGT DIGITALE BURGERRECHTEN

Bits of Freedom komt op voor jouw vrijheid en privacy op internet. Deze grondrechten zijn onmisbaar voor je ontwikkeling, voor technologische innovatie en voor de rechtsstaat. Maar die vrijheid is niet vanzelfsprekend. Je gegevens worden opgeslagen en geanalyseerd. Je internet-verkeer wordt afgeknepen en geblokkeerd. Bits of Freedom zorgt ervoor dat jouw internet jouw zaak blijft.


Stichting Bits of Freedom
Postbus 10746
1001 ES Amsterdam

Contactpersoon: Rejo Zenger
rejo.zenger@bof.nl
+31 6 39 64 27 38

## 01. INTRODUCTIE

### Voorgeschiedenis

De politie heeft op grond van de Wet Politiegegevens (Wpg) uitgebreide bevoegdheden voor het verzamelen, bewaren, gebruiken en verstrekken aan derden van persoonsgegevens, ook van mensen die niet als verdachte zijn aangemerkt.[1] Eén van de voorwaarden is dat de politie zichzelf elke vier jaar controleert.[2] Ze moet onderzoeken hoe zij de bescherming van persoonsgegevens in de praktijk uitvoert en of voldaan wordt aan de wettelijke eisen.[3]

**De Koninklijke Marechaussee betoogde dat "de uitkomst van een dergelijke audit op voorhand al vaststaat."**

Het is ontzettend belangrijk dat de politie de bescherming van gegevens goed inricht. Het gaat immers om persoonsgegevens in een zeer gevoelige context. Zorgvuldige omgang met die gegevens is ook in het belang van de politie zelf, omdat daarmee het vertrouwen van de Nederlandse burger in de politie en haar werk wordt vergroot. Het is bovendien ontzettend zonde als strafonderzoeken stranden door een onverantwoorde omgang met gegevens. Het werk van de politie is te belangrijk om teniet te worden gedaan door slordigheden in de toepassing van bevoegdheden.

De deadline voor de eerste audit was twee jaar na het in werking treden van de wet, 1 januari 2011. Uit besluiten van de College Bescherming Persoonsgegevens (CBP) bleek echter dat geen van de politiekorpsen de controle uitgevoerd had. De Koninklijke Marechaussee betoogde dat "[...] de uitkomst van een dergelijke audit op voorhand al vaststaat."[4] Het CBP zag dat door de vingers en verleende de korpsen uitstel. Maar een half jaar later bleken de diensten nog altijd de wet te overtreden; alleen de FIOD en het korps Zeeland hadden de controle uitgevoerd.[5] De korpsen kregen opnieuw zes maanden respijt. Half januari 2012 hebben de korpsen de controle wel uitgevoerd door middel van audits.

### Aanpak van de auditors

De audits zijn bijna allemaal uitgevoerd door de Departementale Auditdienst (DAD) van het ministerie van Veiligheid en Justitie. De auditors hebben de korpsen op basis van een normenkader onderzocht. Dit normenkader is gebaseerd op de eisen in de Wpg, het Besluit politiegegevens[6] (Bgt) en de Regeling periodieke audit politiegegevens.[7] De normen hebben betrekking op onder meer de bewaartermijnen en de beveiliging van gegevens, maar ook op de rechten van betrokkenen.[8] Voor elk van de normen is een van de volgende waarderingen mogelijk: "in hoofdlijnen voldaan aan de norm", "niet of niet geheel voldaan aan de norm of er is een acceptabel actieplan" en "niet voldaan aan de norm en er is geen acceptabel actieplan".[9]

### Analyse Bits of Freedom

Bits of Freedom heeft de resultaten van deze audits met tientallen verzoeken op grond van de Wet openbaarheid van bestuur (Wob) opgevraagd.[10] Zij heeft vervolgens de rapporten, die in totaal meer dan 1.100 pagina's beslaan, geanalyseerd.

De door Bits of Freedom geanalyseerde rapporten hebben betrekking op de Kmar, het Korps Landelijke Politiediensten (KLPD) en alle regionale politiekorpsen, met uitzondering van het korps Zeeland. Bij het korps Zeeland is een afwijkende systematiek voor

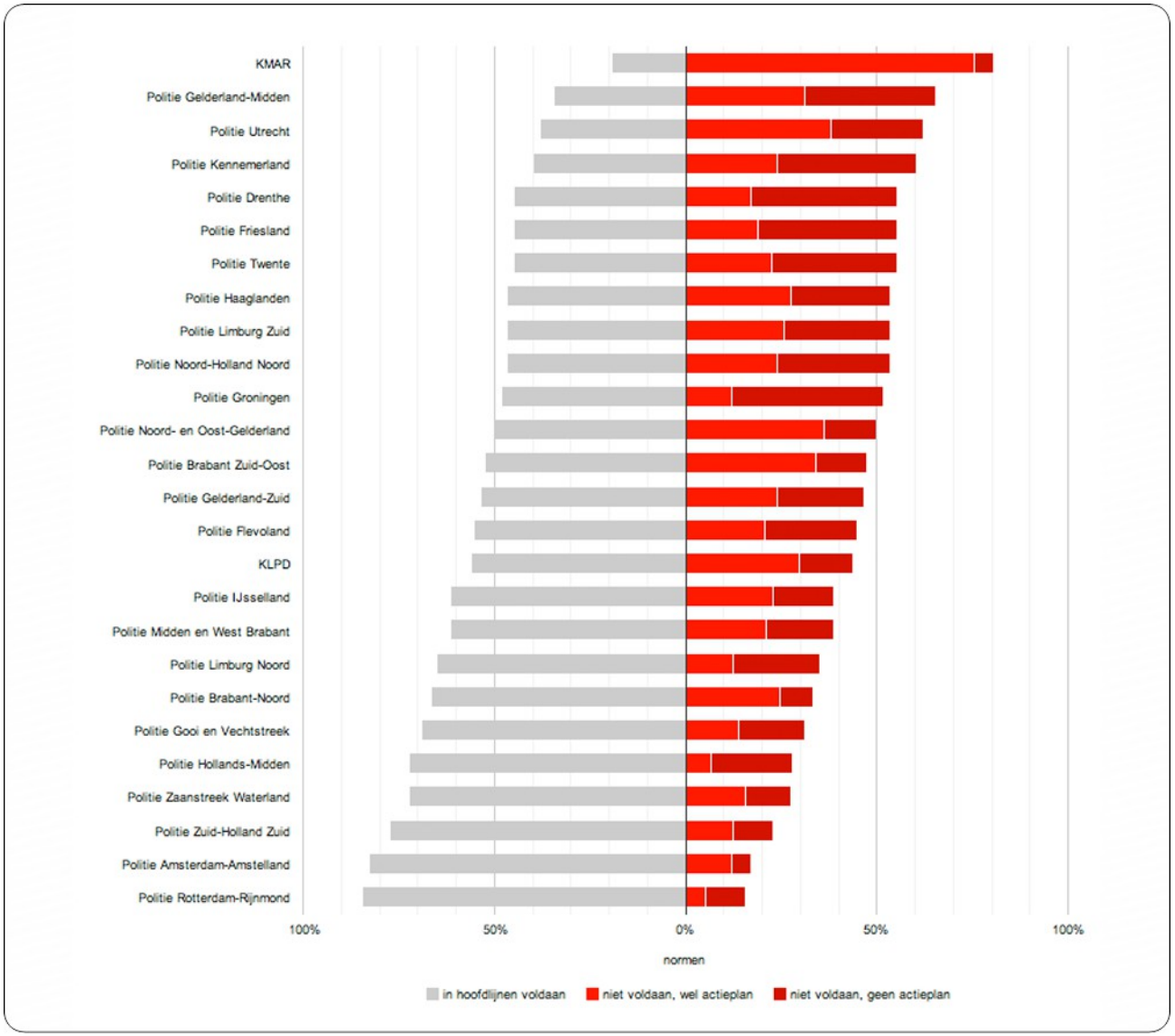
het beoordelen van de normen toegepast, waardoor die resultaten zich niet goed laten vergelijken met de overige resultaten.

Bits of Freedom heeft vervolgens voor elk van de korpsen in kaart gebracht in welke mate elk van de korpsen voldeed aan de gestelde normen.[11]

Op basis van deze gegevens heeft Bits of Freedom kunnen vaststellen in welke mate de korpsen de bescherming van persoonsgegevens op orde hebben. De conclusies uit deze analyse zijn in dit rapport beschreven.[12]

## Diep triest resultaat

Het is diep triest gesteld met de bescherming van persoonsgegevens van de Nederlandse burger bij de politie. Er is werkelijk geen enkel korps dat aan alle wettelijke regels voldoet. Bij de Koninklijke Marechaussee lijkt nog nooit iemand zich te hebben bekommerd  om de gevoeligheid van persoons-gegevens: zij leeft minder dan twintig procent van de normen na, en dan nog slechts "op hoofdlijnen". De twee grootste korpsen van het land hebben het beleid nog het beste op orde en laten op "slechts" één vijfde van de normen steken vallen.



Slechts drie korpsen scoren op meer dan driekwart van de normen een voldoende.[13] Twaalf korpsen halen voor de helft van de criteria het niveau "voldoet op hoofdlijnen" niet.[14]

De tabel op de vorige pagina spreekt boekdelen.

Met zulke schokkend slechte prestaties verbaast het ook niet dat de problemen zich over de hele breedte van de wet voordoen. De problemen zijn het grootst bij de beveiliging van de persoonsgegevens, het bijhouden van mutaties op autorisaties, het op tijd verwijderen van gegevens die niet langer bewaard mogen worden en de interne controle door het opstellen van een goed jaarverslag.

**Het is schokkend dat geen enkel korps voldoet aan alle wettelijke regels op dit gebied. De korpsen moeten de komende maanden keihard aan de slag om het beleid op orde te brengen en zich aan de wet gaan houden.**

Daarbij moet worden vastgesteld dat de beoordelingen vermoedelijk een positiever beeld dan de werkelijkheid schetsen. Zo is de hoogst haalbare waardering de bescheiden norm "voldoet op hoofdlijnen". Ook verdient een korps al een "voldoet gedeeltelijk" in het kader van de registratie van gegevensverstrekkingen, wanneer "een enkele leidinggevende stuurt op het vastleggen van verstrekkingen".[15]

## Conclusie en eisen

Eén van de pijlers van de vrije rechtsstaat is het respecteren van grondrechten, waaronder de eerbiediging van de persoonlijke levenssfeer. Om die vrijheid te beschermen heeft de politie speciale en soms vergaande bevoegdheden gekregen. Aan de toekenning van die bevoegdheden zijn voorwaarden verbonden. Eén van die voorwaarden is een verantwoordelijke omgang met de persoonsgegevens die haar worden toevertrouwd.

- Het is schokkend dat geen enkel korps voldoet aan alle wettelijke regels op dit gebied. Dat moet heel snel anders. De korpsen moeten de komende maanden keihard aan de slag om het beleid op orde te brengen en zich aan de wet gaan houden.
- De korpsen moeten gedwongen worden om élk jaar een volledige controle op het naleven van de regels voor de bescherming van persoonsgegevens uit te voeren. De verslagen van deze controles moeten bovendien altijd openbaar zijn. Nu zijn de normale controles beperkt tot ééns in de vier jaar en is de hercontrole beperkt tot die punten waarop gebreken zijn geconstateerd.
- De conclusies uit deze onderzoeken zijn ook van belang in de discussie over de introductie van nieuwe bevoegdheden. Voor Bits of Freedom is de conclusie duidelijk: zolang de korpsen de regels rondom de gegevensbescherming met de voeten treden, kan er van nieuwe bevoegdheden geen sprake zijn.

Afbeelding gebaseerd op Untitled van Bas Bogers, uitgebracht onder een Creative Commons BY-NC 2.0 licentie

## 02. TOEGANG TOT GEGEVENS NIET GEWAARBORGD

De Wpg bevat ten eerste bepalingen over de beveiliging van gegevens en over het verstrekken van machtigingen om gegevens te gebruiken.[16] Kort gezegd: de gegevens moeten afdoende beveiligd worden om er voor te zorgen dat onbevoegden geen toegang hebben. In de door Bits of Freedom opgevraagde onderzoeken wordt beoordeeld in welke mate de politiekorpsen zich aan deze artikelen houden.

### Slecht of volledig ontbrekend autorisatiebeheer

Uit de onderzoeken blijkt dat de beveiliging van de gegevens bij de politie ondermaats is. Door gebrek aan werkbare systemen slaan veel politieambtenaren gevoelige gegevens op in eigen of gedeelde directories waar controle op toegankelijkheid ontbreekt. Bij die directories kan doorgaans geen technische beperking aan de toegang worden aangebracht. Bij veel korpsen is er geen goed overzicht van welke informatie voor welke medewerkers toegankelijk moet zijn en welke niet. Dat overzicht is belangrijk, omdat binnen de politie bepaalde persoonsgegevens voor slechts een beperkte kring personen toegankelijk horen te zijn.

In de praktijk blijkt dat die regel niet wordt nageleefd. Bij minstens 11 korpsen levert het beheer over bestaande autorisaties problemen op.[17] Controles worden niet vaak genoeg of zelfs niet uitgevoerd, de beschrijving van het controleproces is niet vastgelegd en een actueel overzicht van autorisaties ontbreekt. Neem bijvoorbeeld het korps Drenthe, waar "samenvattende overzichten van toegekende autorisaties niet gemakkelijk te verkrijgen zijn", ook al zijn "volgens een intern onderzoek naar de [Wpg] in 2009 / 2010 alle autorisaties in beeld gebracht". Ook vindt er geen controle op de toegekende autorisaties plaats.[18] Bij het korps Gelderland-Midden ontvangen leidinggevenden "geen periodieke overzichten om te controleren of autorisaties juist gemuteerd en up to date zijn" en ook de privacyfunctionaris voert geen controles op de autorisaties uit.[19] Bij korps Twente stamt het overzicht van autorisaties uit 2007 en is deze met een "aan zekerheid grenzende waarschijnlijkheid" sindsdien niet gewijzigd, waarbij wordt opgemerkt dat het "niet realistisch" is om "te verwachten dat deze matrix niet behoorde te wijzigen in de tussentijd".[20] Daarnaast ontbreken in Twente beheer en controles van autorisaties, evenals een procesbeschrijving voor het beheer.[21] "Controle door leidinggevenden op uitgegeven autorisaties" vindt bij het korps Utrecht

slechts “voor een beperkt aantal systemen” plaats.[22]

## Wie vertrekt behoudt toegang

Veel problemen zijn er ook met de autorisaties van medewerkers die vertrekken of van functie veranderen. Autorisaties worden soms niet ingetrokken, waardoor voormalige medewerkers bij gevoelige gegevens kunnen waartoe ze geen toegang meer mogen hebben. Ook de controles op het intrekken van autorisaties vinden niet plaats of de procedures voor zulke controles zijn onvoldoende ontwikkeld. Bij minstens 16 korpsen komen deze problemen voor.[23] Bij drie van deze korpsen wordt in de audits “vervuiling” van de autorisaties vastgesteld.[24] Bij twee korpsen worden de autorisaties jaarlijks door de privacyfunctionaris opgeschoond, waarbij de auditoren opmerken dat dit eigenlijk helemaal geen taak is van de privacyfunctionaris is en dat het schonen van de autorisaties “een gedocumenteerd en controleerbaar proces via de lijn” hoort te zijn.[25]

Voorbeelden zijn makkelijk te vinden. Bij het korps Kennemerland is “niet overal duidelijk op welke wijze bestaande autorisaties worden aangepast indien een medewerker van functie verandert”.[26] Bij het korps Flevoland wordt opgemerkt: “Wanneer een medewerker van functie of afdeling wisselt, dan wordt deze mutatie niet automatisch doorgevoerd in de autorisatiematrix. Als een medewerker uit dienst gaat worden niet automatische alle autorisaties ingetrokken.”[27] Bij het korps Haaglanden worden autorisaties “alleen verwijderd bij het wisselen van functie”, is er “onvoldoende controle op het intrekken van autorisaties bij ontslag, mutaties en beëindiging van tijdelijke inzet” en is “de werking van het proces wijziging en verwijdering” niet gewaarborgd.[28]

## Gegevens verdachten in persoonlijke en gedeelde mappen

Een ander probleem dat veel voorkomt is het opslaan van gevoelige gegevens in persoonlijke mappen en afdelingsmappen buiten de systemen die voor politie-gegevens bestemd zijn. Medewerkers die niet geautoriseerd zijn kunnen in deze mappen gegevens inzien die niet voor hen bestemd zijn. Gegevens die voor verschillende doeleinden zijn verzameld, en waarvoor verschillende personen zijn geautoriseerd, zijn in zulke mappen niet altijd gescheiden. Het blijkt soms nauwelijks mogelijk om te controleren of er in zulke mappen politiegegevens worden bewaard en of die gegevens niet langer worden bewaard dan volgens de wet is toegestaan. Het gebruik van eigen mappen


Afbeelding gebaseerd op Politie toezicht van Max Bisschop, uitgebracht onder een Creative Commons BY-NC-SA 2.0 licentie

heeft dus niet alleen gevolgen voor de toegankelijkheid van gegevens, maar ook voor de omgang met de wettelijke bewaartermijnen.

Zo staan er bij het korps Noord-Holland Noord "op de gezamenlijke schijfruimte directory's uit het jaar 1997" en wordt geconcludeerd "dat de informatie in deze mappen niet Wpg-proof is".[29] In de audit van het korps Utrecht wordt gemeld dat politiegegevens "ook op persoonlijke en afdelingsmappen opgeslagen" worden én dat het "niet mogelijk" is "om na te gaan of er politiegegevens op persoonlijke mappen staan".[30] Dergelijke problemen komen voor bij minstens 14 korpsen.[31] In de audit van het korps Utrecht wordt als oorzaak aangegeven dat "de systemen die de primaire processen ondersteunen" door agenten niet als gebruiksvriendelijk worden ervaren en dat het daarnaast voorkomt dat "medewerkers het nut niet erkennen van het gebruik van de formele systemen".[32]

Over het korps Zaanstreek-Waterland wordt gemeld dat daar de publieke map veel politiegegevens bevatte als gevolg van de beperkte mogelijkheden om documenten te bewerken in de speciaal voor politiegegevens bedoelde applicatie BVH.[33] Processenverbaal werden dan eerst in Microsoft Word opgeslagen in de publieke map en pas daarna naar BVH gekopieerd. Vervolgens was het aan de verbalisant zelf om het Word-document uit de publieke map te verwijderen.[34]

**In de meeste rapportages wordt verder benadrukt dat ook de technische systemen die wél bedoeld zijn voor het verwerken van deze persoonsgegevens, zoals de landelijke systemen BVH en BVO, nog niet aan de vereisten van de Wpg voldoen.**

In de meeste rapportages wordt verder benadrukt dat ook de technische systemen die wél bedoeld zijn voor het verwerken van deze persoonsgegevens, zoals de landelijke systemen BVH en BVO[35], nog niet aan de vereisten van de Wpg voldoen. De auditors wijzen op de gebrekkige scheiding van gegevens die voor verschillende doeleinden zijn verzameld en op gebrekkige voorzieningen voor het tijdig verwijderen en vernietigen van gegevens. Dit geldt voor een meerderheid van de korpsen.[36]

## Verbeteringsplannen onvoldoende

Bij een aantal korpsen werden er op het moment van de audits al maatregelen genomen of gepland om de problemen aan te pakken. Het KLPD is van plan om dit jaar een proces te ontwikkelen voor het aanpassen van autorisaties naar aanleiding van interne personeelsmutaties.[37] Het korps Rotterdam-Rijnmond heeft een "acceptabel" plan voor een centralisering van het proces voor het wijzigen en opschonen van autorisaties.[38] Het korps Zaanstreek-Waterland heeft in oktober 2011 de gehele publieke map verwijderd en een project opgezet om de kantoorautomatisering in te richten volgens de Wpg.[39] Het korps Amsterdam-Amstelland tot slot, mist een autorisatiematrix maar is deze wel aan het ontwikkelen.[40]

Dat is de auditors niet genoeg en zij doen dan ook tal van aanbevelingen. Het korps Flevoland wordt aanbevolen om het vastleggen van politiegegevens in de kantoorautomatisering te beperken, om voor

Afbeelding gebaseerd op 2010_09_21_0686 van nico1959, uitgebracht onder een Creative Commons BY-NC-SA 2.0 licentie

actuele autorisaties te zorgen door de autorisatiematrix te koppelen aan het personeelssysteem en om het overzicht over autorisaties binnen de kantoorautomatisering te verbeteren.[41] Het advies aan korps Gelderland-Midden is om een proces in te richten waarmee leidinggevenden de autorisaties van hun medewerkers kunnen beoordelen en om systemen waar nog verouderde autorisaties in staan op te schonen.[42] Het korps Twente wordt onder andere geadviseerd om een tool in gebruik te nemen om autorisaties geautomatiseerd vast te leggen en te beheren, om een schriftelijke procedure vast te stellen voor het toekennen, wijzigen en verwijderen van autorisaties en voor de controle daarop, om autorisatieoverzichten samen te stellen waarmee leidinggevenden de autorisaties van hun medewerkers kunnen beoordelen en om voor een structurele controle van de toegekende autorisaties te zorgen.[43] Het korps Utrecht krijgt onder meer het advies om de controle te verbeteren op het aanhouden van de wettelijke bewaartermijnen van gegevens in de mappen binnen de kantoorautomatisering, om een inrichting van die mappen vast te leggen die voldoet aan de Wpg, om een tool of proces in gebruik te nemen om autorisaties geautomatiseerd vast te leggen en te beheren en om een eenduidige procesbeschrijving op te stellen voor het intrekken van autorisaties.[44]

## 03. RECHTEN VAN BETROKKENEN NIET BESCHERMD

De Wpg bevat bepalingen over de rechten van degenen van wie de politie persoonsgegevens verwerkt. Iedereen kan zijn of haar gegevens die door de politie worden verwerkt inzien.[45] Als er iets aan de gegevens mankeert, heeft de betrokkene het recht de gegevens te laten verbeteren, aanvullen, verwijderen of afschermen.[46] Als de gegevens naar aanleiding van zo'n verzoek zijn aangepast moet de politie dat laten weten aan derden aan wie de gegevens eerder zijn verstrekt zodat ook zij de gegevens kunnen corrigeren. Degene van wie persoonsgegevens zijn verstrekt moet hiervan op de hoogte worden gebracht.[47]

Naast de bovengenoemde artikelen, waarin de rechten van de betrokkene zijn vastgelegd, bevat de Wpg nog bepalingen over uitzonderingen op die rechten en over formaliteiten en andere zaken, zoals de (administratie)kosten. In de audits is gekeken in hoeverre de korpsen zich aan dit alles houden.

Iets minder dan de helft van de korpsen voldoet niet de relevante normen.[48]

### Goede afhandeling inzageverzoeken niet gegarandeerd

Volgens de audits hebben 13 korpsen procedures ontwikkeld voor het afhandelen van dit soort verzoeken.[49] Van de overige korpsen zijn er tenminste 9 bij wie procedures voor de afhandeling van verzoeken om inzage in gegevens en/of procedures voor de afhandeling van verzoeken om verbetering van gegevens incompleet zijn, of zelfs helemaal niet zijn vastgelegd.[50]

**Bij politie Kennemerland is zelfs "niet bekend wie daarvoor verantwoordelijk is en door wie dit wordt uitgevoerd."**

Twee voorbeelden: het korps Amsterdam-Amstelland heeft "geen richtlijnen beschreven voor verbetering, aanvulling, verwijdering of afscherming van politiegegevens ingeval van feitelijk onjuiste gegevens", maar deze taak "wordt wel uitgevoerd".[51] Bij het korps Gelderland-Zuid is de afhandeling van inzage- en verbeteringsverzoeken "vastgelegd in een stroomschema", maar is het "proces niet beschreven".[52]

Het ontbreken van schriftelijke procedures betekent echter wél dat een juiste afhandeling minder goed gewaarborgd en niet te controleren is.

Het korps Kennemerland kent nog meer problemen. Bij dat korps is niet alleen geen procedure of werkinstructie voor de correctie van onjuiste gegevens bekend , maar is zelfs "niet bekend wie in Kennemerland daarvoor verantwoordelijk is en/of door wie dit wordt uitgevoerd".[53] Wat dit in de praktijk betekent voor de afhandeling van verzoeken om correctie blijkt niet uit de audit. Onduidelijkheid over de interne verantwoordelijkheid ten aanzien van het inzage- en correctierecht speelt ook elders. Bij het korps Noord- en Oost-Gelderland "kan het voorkomen" dat verzoeken tot verbetering "niet juist of niet volledig worden afgehandeld" als gevolg van onvoldoende afstemming tussen medewerkers.[54] In de procesbeschrijvingen voor de verschillende diensten binnen het KLPD is niet omschreven wie voor de afhandeling van verzoeken om inzage en verbetering verantwoordelijk is.[55]

Vier korpsen hebben geen procedure voor het informeren van derden over de verbetering van eerder verstrekte gegevens.[56] In het korps Gelderland-Zuid wordt er in zulke situaties "ad hoc" "maatwerk geleverd".[57] Bij het korps Zuid-Holland Zuid, daarentegen, "vindt geen mededeling van verbetering, aanvulling, verwijdering of afscherming plaats" aan derden. Hiervoor worden technische oorzaken aangevoerd.[58]

## Procedures moeten nog ontwikkeld worden

De auditors ook aanbevelingen voor het aanpakken van de genoemde problemen. Het korps Amsterdam-Amstelland krijgt het advies om "richtlijnen" op te stellen "voor verbetering, aanvulling, verwijdering of afscherming van politiegegevens ingeval van feitelijk onjuiste gegevens".[59] Kennemerland wordt aangeraden "duidelijk" te maken wie "verantwoordelijk is voor correctie of verwijdering van gegevens naar aanleiding van een verzoek tot kennisneming".[60] Het KLPD krijgt onder meer het advies om "op basis van de in de praktijk reeds gehanteerde informele procedure een korpsbrede procedure te ontwikkelen en vast te stellen teneinde een uniforme beantwoording van vragen die betrokkenen hebben naar aanleiding van de registratie in systemen te kunnen waarborgen" en het advies om "deze procedure te implementeren en te borgen binnen de organisatie".[61] Het korps Limburg-Zuid wordt geadviseerd de procesbeschrijving voor de afhandeling van correctieverzoeken zo aan te passen dat daaruit "blijkt hoe partners worden geïnformeerd over wijzigingen in verstrekte politiegegevens".[62]

Bij drie korpsen die voor de afhandeling van verzoeken om inzage in persoonsgegevens of voor de afhandeling van verzoeken om verbetering geen complete procedures hebben was ten tijde van de audits wel een begin gemaakt met het opstellen van zulke procedures.[63]

Afbeelding gebaseerd op Politie charges in Amsterdam van Jos Zetten, uitgebracht onder een Creative Commons BY-NC-SA 2.0 licentie

## 04. INTERN TOEZICHT ONVOLDOENDE

De Wpg bevat bepalingen over het interne toezicht binnen de politie op de behoorlijke en zorgvuldige omgang met de persoonsgegevens van burgers. Een belangrijke basis voor die controles vormen verplichte registraties van verschillende soorten verwerkingen die door de wetgever als extra risicovol zijn beoordeeld.[64] Daarnaast moeten belangrijke procedures vooraf op papier zijn vastgelegd, waaronder de doelstellingen van onderzoeken naar specifieke strafbare feiten, de toekenning van autorisaties, het gebruik van gegevens van burgers voor ondersteunende taken, het delen van gegevens met derden, het geautomatiseerd vergelijken van gegevens en alle aanwijzingen van mogelijk onrechtmatige verwerkingen.

**"Het is achteraf niet te achterhalen op welke wijze politiegegevens aan externen zijn verstrekt."**

Ook moet de korpsen zichzelf regelmatig controleren. Voldoet een korps niet aan alle normen, dan moet het de fouten herstellen en binnen een jaar een nieuwe controle uitvoeren. Het CBP moet een afschrift ontvangen van de resultaten van de controles.[65] Tenslotte zijn de korpsen verplicht om een privacy-functionaris aan te stellen.[66] De functionaris heeft zowel een toezichthoudende als een adviserende taak en moet ieder jaar een jaarverslag opstellen.[67]

Niet één korps voldoet op alle punten aan de regels. De twee grootste korpsen doet het nog het best, maar korpsen als Groningen en Kennemerland voldoen aan het merendeel van de normen in het geheel niet. De korpsen Drenthe, Friesland, Haaglanden en de Koninklijke Marechaussee voldoen aan slechts één derde van de normen volledig.

### Administratie verstrekking aan derden onwerkbaar

Uit de overzichten van de mate waarin de normen worden nageleefd, maar vooral uit het begeleidende commentaar van de auditors, is duidelijk dat veel korpsen flinke steken laten vallen. Eén van de grootste pijnpunten is de registratie van verstrekkingen van gegevens aan partijen buiten de politie. Om dat te vereenvoudigen is daar een landelijk standaard formulier voor ontwikkeld, het zogenoemde I90-formulier.

Politieagenten hebben daar weinig mee op. Bij driekwart van de korpsen wordt het formulier niet of nauwelijks ingevuld.[68] Zo is bij de Koninklijke Marechaussee een onvolledige administratie te wijten aan onwetendheid: "In de praktijk worden niet alle verstrekkingen op juiste wijze geprotocolleerd, omdat criteria niet bekend zijn de medewerkers."[69] Bij de het korps Noord-Oost Gelderland worden verstrekkingen "ten dele geprotocolleerd" en wordt dat "als lasten-verzwarend beschouwd." Daar zijn ook "aantallen verstrekkingen I90 uit BHV [...] niet in evenwicht met aantal feitelijke verstrekkingen."[70] Er zijn meer korpsen waar men het werkelijke aantal verstrekkingen niet kan vaststellen. Over het korps IJsselland constateren de auditors: "[Politieagenten] zijn niet op de hoogte van de Wpg. Zij verstrekken informatie maar protocolleren dit niet. Het is achteraf niet te achterhalen op welke wijze politiegegevens aan externen zijn verstrekt."[71]

Het zal dan niet verbazen dat ook het toezicht hierop faalt, zoals blijkt uit de onderzoeken. De auditors vellen veelal een negatief oordeel, en dan te bedenken

Afbeelding gebaseerd op Untitled van bogers, uitgebracht onder een Creative Commons BY-NC 2.0 licentie

dat een korps al een "voldoet gedeeltelijk" scoort als "een enkele leidinggevende stuurt op het vastleggen van verstrekkingen".[72]

## Zelfs definities ontbreken

Gebrekkige vastlegging komt voortdurende terug in de verslagen. Ook al heeft bijna de helft van de korpsen de registratie van het hergebruik van gearchiveerde gegevens op orde, de andere helft voldoet in het geheel niet aan de normen. "Er zijn geen richtlijnen voor hernieuwde verwerkingen aanwezig," wordt bij het korps Flevoland geconstateerd.[73] In het korps Rotterdam-Rijnmond: "[Bepaalde] gegevens worden nog niet verwijderd. [...] Hierdoor kan nog worden gezocht in [...] gegevens die niet meer toegankelijk hadden mogen zijn, zonder dat het bevoegd gezag daartoe toestemming heeft gegeven."[74]

Korpsen zijn ook verplicht om het te registreren als gevoelige gegevens mogelijk onrechtmatig zijn gebruikt. Ruim een derde van de korpsen doet dat echter niet. Dat is naar de mening van Bits of Freedom extra schokkend, nu juist de politie het goede voorbeeld moet geven.

Zoals hierboven is beschreven moeten ook procedures worden vastgelegd over het "geautomatiseerd

vergelijken en in combinatie zoeken" van persoonsgegevens. Uit de onderzoeken blijkt dat de korpsen geen heldere definities van deze termen hanteren.[75] Dat heeft zijn weerslag in de onderzoeken. "Binnen het KLPD wordt geen eenduidige definitie van de begrippen 'geautomatiseerd vergelijken' en 'in combinatie verwerken', gehanteerd."[76] Het gevolg is dat rond de helft van de korpsen op dit punt niet aan de regels voldoet.

## Geen investering in bescherming privacy

Om te kunnen controleren of de korpsen wel op een verantwoorde wijze met hun bevoegdheden om gaan is het uitvoeren van periodieke audits essentieel. Zoals in de introductie al werd beschreven, bleek het uitvoeren van een eerste audit voor veel korpsen al te veel gevraagd.

Slechts de helft van de korpsen heeft een behoorlijke interne auditfunctie. Bij één derde van de korpsen leidt dat echter niet tot rapportages die de toets der kritiek kunnen doorstaan. Minder dan een kwart van de korpsen beschikt over een goed plan voor het structureel borgen van die auditfunctie.

Op één na hebben alle korpsen de verplichte privacyfunctionaris aangesteld.[77] In de praktijk blijkt de rol van deze functionaris echter te beperkt. Een belangrijke taak van de privacyfunctionarissen is het toezicht houden op de hierboven genoemde registraties. Slechts zes korpsen voldoen aan deze norm.[78] Negen van de resterende korpsen voldoen in het geheel niet.[79] Functionarissen moeten jaarlijks een verslag van hun bevindingen opstellen[80], maar slechts acht korpsen halen daarvoor een voldoende.[81]

Uit de onderzoeken blijkt duidelijk dat stelselmatig te weinig capaciteit wordt ingeruimd de functionaris zijn werk te laten doen. "Door een veranderende prioriteitsstelling in het korps is [het jaarverslag] echter niet opgesteld," zo stellen de auditors vast over het korps Drenthe.[82] Bij het korps Utrecht wordt vastgesteld dat "de functionaris [...] nog hoofdzakelijk een adviserende functie" vervult.[83] Tenslotte constateert men: "In het algemeen is er veel werk en daardoor wordt er niet geïnvesteerd op de toezichthoudende taak."[84] Dit onderstreept opnieuw de ondergeschikte rol die de bescherming van privacy bij de Nederlandse politie heeft.


Afbeelding gebaseerd op Paardenstaarten van Roel Wijnants, uitgebracht onder een Creative Commons BY-NC 2.0 licentie

## 05. CONCLUSIES EN EISEN

### Bij verregaande bevoegdheden hoort een grote verantwoordelijkheid

Eén van de pijlers van de vrije rechtsstaat is het respecteren van grondrechten, waaronder de eerbiediging van de persoonlijke levenssfeer. Om die vrijheid te beschermen heeft de politie speciale en soms vergaande bevoegdheden gekregen. De politie en opsporingsdiensten vervullen op die manier een belangrijke taak in onze samenleving.

Aan de toekenning van die bevoegdheden zijn belangrijke voorwaarden verbonden. Die voorwaarden waarborgen een transparante inzet van die bevoegdheden en voorkomen misbruik. Eén van die voorwaarden is een verantwoordelijke omgang met de persoonsgegevens die aan de politie worden toevertrouwd. Ook moet de politie op dit punt worden gecontroleerd.

De resultaten van de controles – nu ze eindelijk zijn uitgevoerd – zijn schokkend. Geen enkel korps voldoet aan alle wettelijke regels. Voor sommige korpsen lijkt privacy  een volstrekt onbekend begrip. Met als gevolg dat persoonsgegevens van Nederlandse burger bij de politie lang niet altijd in veilige handen zijn.

### Voor het eind van het jaar op orde

Dat moet heel snel anders. De korpsen moeten de komende maanden keihard aan de slag om het beleid op orde te brengen en zich aan de wet gaan houden. Het mag niet gebeuren dat jarenlang problemen en aanbevelingen structureel genegeerd worden, zoals eerder is gebeurd bij de misstanden rondom het vorderen van gegevens over klanten van telefonie- en internetaanbieders.[85]

De wet verplicht de korpsen net na de jaarwisseling een nieuwe rapportage op te leveren over de punten waarop nu misstanden zijn geconstateerd.[86] Alle korpsen moeten dan in ieder geval voldoen aan de huidige hoogste norm, “voldoet op hoofdlijnen”.

### Eéns per vier jaar controleren is onverantwoord

De gebrekkige bescherming van persoonsgegevens bij de politie tonen echter haarfijn aan dat de toepassing van de bevoegdheden zeer regelmatig tegen het licht gehouden moet worden. De politie heeft het vertrouwen van de burger, en dat van de wetgever, ernstig geschaad. De wet geeft de handhavers van de wet op dit moment veel ruimte. De wet verplicht tot een hercontrole bij die korpsen waar fouten zijn geconstateerd, maar die hercontrole is beperkt tot die punten waarop eerder gebreken zijn geconstateerd. De normale, periodieke controles vinden slechts ééns in de vier jaar plaats.

Gegeven de schokkende resultaten van deze audits eist Bits of Freedom daarom dat artikel 33 Wpg wordt aangescherpt. De politiekorpsen moeten gedwongen worden om elk jaar een volledige controle op het naleven van de regels voor de bescherming van persoonsgegevens uit te voeren. De verslagen van deze controles moeten bovendien altijd openbaar zijn. Pas als blijkt dat de politiekorpsen slechts bij hoge uitzondering de Wpg niet naleven kan worden overwogen om de controlefrequentie terug te brengen.

**De korpsen moeten de komende maanden keihard aan de slag om het beleid op orde te brengen en zich aan de wet gaan houden.**

## Geen nieuwe bevoegdheden als verantwoordelijkheid bestaande niet gedragen kan worden

De conclusies uit deze audits zijn ook van belang in de discussie over de introductie van nieuwe bevoegdheden. Bevoegdheden mogen alleen worden geïntroduceerd als daarvan vooraf de noodzaak, effectiviteit, proportionaliteit en subsidiariteit zijn aangetoond. Hierbij speelt ook een rol in hoeverre de politie verantwoordelijk omgaat met de gegevens die in het kader hiervan worden verzameld. De conclusies uit de onderzoeken zaaien twijfel over óf de politie wel op verantwoorde wijze met zulke nieuwe bevoegdheden kan omgaan en welke waarborgen ingebouwd moeten worden om misbruik tegen te gaan. Voor Bits of Freedom is de conclusie duidelijk: zolang de korpsen de regels rondom de gegevensbescherming met de voeten treden, kan er van nieuwe bevoegdheden geen sprake zijn.


Afbeelding gebaseerd op 2010_09_21_0697-a van nico1959, uitgebracht onder een Creative Commons BY-NC-SA 2.0 licentie

# EINDNOTEN

1. Zie: http://wetten.overheid.nl/BWBR0022463/
2. Artikel 33 Wpg en artikel 6:5 Besluit politiegegevens
3. Artikel 6:5 lid 2 Besluit politiegegevens luidt "De controle heeft betrekking op de wijze waarop het verwerken van politiegegevens is georganiseerd, de maatregelen en procedures die daarop van toepassing zijn en de werking van deze maatregelen en procedures."
4. Zie: http://www.cbpweb.nl/downloads_rapporten/rapporten_wpg/DB_Kmar.pdf
5. Zie: http://www.cbpweb.nl/Pages/rap_2011_privacyaudit_politie_bod.aspx
6. Zie: http://wetten.overheid.nl/BWBR0023086/
7. Zie: http://wetten.overheid.nl/BWBR0025038
8. De onderzochte thema's zijn beschreven in paragraaf 3.3 van elk van de onderzoeken.
9. De waarderingen voor elk van de normen zijn beschreven in het begin van hoofdstuk 2 van elke van de onderzoeken.
10. De rapporten zijn gepubliceerd op: https://www.bof.nl/politie-privacy-audits-2012
11. De verzamelde gegevens zijn gepubliceerd op: https://www.bof.nl/politie-privacy-audits-2012
12. Dit rapport is geschreven door Bits of Freedom met medewerking van onder meer Koen Versmissen en Clasijn Witvliet.
13. Amsterdam-Amstelland, Rotterdam-Rijnmond en Zuid-Holland Zuid
14. Koninklijke Marechaussee, Drenthe, Friesland, Gelderland-Midden, Groningen, Haaglanden, Kennemerland, Limburg-Zuid, Noord-Oost Gelderland, Noord-Holland Noord, Twente, Utrecht
15. Audit Wpg Midden en West Brabant, 16 december 2011, p. 13
16. Artikel 4 lid 3 en artikel 6 Wpg
17. Amsterdam-Amstelland, Drenthe, Friesland, Gelderland-Midden, Koninklijke Marechaussee, Limburg Noord, Limburg-Zuid, Twente, Utrecht, IJsselland en Zeeland
18. Audit Wpg politie Drenthe. 6 januari 2012, p. 24
19. Audit Wpg politie Gelderland-Midden. 10 januari 2012, p. 25
20. Audit Wpg politie Twente. 6 januari 2012, p. 30
21. Audit Wpg politie Twente. 6 januari 2012, p. 11
22. Audit Wpg politie Utrecht. 10 januari 2012, p. 31
23. Drenthe, Flevoland, Friesland, Gelderland-Midden, Groningen, Haaglanden, Hollands-Midden, Kennemerland, Zuid-Holland Zuid, KLPD, Koninklijke Marechaussee, Midden en West Brabant, Noord-Holland Noord, Rotterdam-Rijnmond, Utrecht, Zeeland
24. Audit Wpg politie Drenthe, 6 januari 2012, p. 24; Audit Wpg politie Gelderland-Midden, 10 januari 2012, p. 25; Audit Wpg politie Rotterdam-Rijnmond, 16 december 2011, p. 11
25. Audit Wpg politie Friesland, 6 januari 2012, p. 10; Audit Wpg politie Groningen, 6 januari 2012, p. 10
26. Audit Wpg politie Kennemerland, 10 januari 2012, p. 28
27. Audit Wpg politie Flevoland, 20 december 2011, p. 23
28. Audit Wpg politie Haaglanden, 16 december 2011, p. 11
29. Audit Wpg politie Noord-Holland Noord, 10 januari 2012, p. 28
30. Audit Wpg politie Utrecht, 10 januari 2012, p. 10
31. Drenthe, Flevoland, Friesland, Gelderland-Midden, Gooi en Vechtstreek, Groningen, Haaglanden, Kennemerland, Limburg Noord, Midden en West Brabant, Noord-Holland Noord, Twente, Utrecht en Zaanstreek-Waterland

# EINDNOTEN

32. Audit Wpg politie Utrecht, 10 januari 2012, p. 47
33. BVH is de afkorting voor "Basis Voorzienings- & handhavingssysteem" en is de applicatie die wordt gebruikt voor de administratieve afhandeling van melding.
34. Audit Wpg politie Zaanstreek-Waterland, 3 januari 2012, p. 29
35. BVO is de "Basisvoorziening Opsporing" waarin gegevens met betrekking tot opsporingsonderzoeken worden opgeslagen.
36. In het bijzonder: Gelderland-Midden, Gooi en Vechtstreek, Limburg Noord, Limburg-Zuid, Noord- en Oost-Gelderland, Rotterdam-Rijnmond en IJsselland
37. Audit Wpg politie KLPD, 6 januari 2012, p. 11
38. Audit Wpg politie KLPD, 6 januari 2012, p. 11
39. Audit Wpg politie Zaanstreek-Waterland, 3 januari 2012, p. 11
40. Audit Wpg politie Amsterdam-Amstelland, 13 januari 2012, p. 10
41. Audit Wpg politie Flevoland, 20 december 2011, p. 22 en 24
42. Audit Wpg politie Gelderland-Midden, 10 januari 2010, p. 26
43. Audit Wpg politie Twente, 6 januari 2012, p. 30
44. Audit Wpg politie Utrecht, 10 januari 2012
45. Artikel 25 lid 1 Wpg
46. Artikel 28 lid 1 Wpg
47. Artikel 30 lid 1 Wpg
48. Korps Landelijke Politiediensten, Amsterdam-Amstelland, Brabant Zuid-Oost, Gelderland-Midden, Gelderland-Zuid, Kennemerland, Limburg-Zuid, Midden en West Brabant, Noord- en Oost-Gelderland, Noord-Holland Noord, Utrecht en Zuid-Holland Zuid
49. Brabant-Noord, Drenthe, Flevoland, Friesland, Gooi en Vechtstreek, Groningen, Haaglanden, Hollands-Midden, IJsselland, Limburg Noord, Rotterdam-Rijnmond, Twente en Zaanstreek-Waterland.
50. Amsterdam-Amstelland, Brabant Zuid-Oost, Gelderland-Midden, Gelderland-Zuid, Kennemerland, KLPD, Noord-Holland Noord, Utrecht en Zeeland
51. Audit Wpg politie Amsterdam-Amstelland, 13 januari 2012, p. 15
52. Audit Wpg politie Gelderland-Zuid, 6 januari 2012, p. 15
53. Audit Wpg politie Kennemerland, 10 januari 2012, p. 18, 32
54. Audit Wpg politie Noord- en Oost-Gelderland, 7 december 2011, p. 16
55. Audit Wpg politie KLPD, 6 januari 2012, p. 48, 49
56. Gelderland-Zuid, Limburg-Zuid, KLPD en Zuid-Holland Zuid
57. Audit Wpg politie Gelderland-Zuid, 6 januari 2012, p. 32
58. Audit Wpg politie Zuid-Holland Zuid, 3 januari 2012, p. 60
59. Audit Wpg politie Amsterdam-Amstelland, 13 januari 2012, p. 30
60. Audit Wpg politie Kennemerland, 10 januari 2012, p. 32
61. Audit Wpg politie KLPD, 6 januari 2012, p. 30
62. Audit Wpg politie Limburg-Zuid, 6 januari 2012, p. 35
63. Brabant Zuid-Oost, Utrecht en Zeeland

# EINDNOTEN

64. Artikel 32 lid 1 Wpg
65. Artikel 33 Wpg
66. Artikel 34 lid 1 Wpg
67. Artikel 34 lid 2 en artikel 34 lid 3 Wpg
68. Koninklijke Marechaussee, Brabant-Noord, Brabant Zuid-Oost, Drenthe, Friesland, Gelderland-Midden, Groningen, Haaglanden, Hollands-Midden, IJsselland, Kennemerland, Limburg-Noord, Limburg-Zuid, Midden en West Brabant, Noord- en Oost-Gelderland, Twente, Utrecht, Zaanstreek-Waterland en Zuid-Holland Zuid
69. Audit Wpg Koninklijke Marechaussee, 12 januari 2012, p. 8
70. Audit Wpg Noord-Oost Gelderland, 7 december 2011, p. 15
71. Audit Wpg IJsselland, 22 december 2011, p. 16
72. Audit Wpg Midden en West Brabant, 16 december 2011, p. 13
73. Audit Wpg Flevoland, 20 december 2011, p. 11
74. Audit Wpg Rotterdam-Rijnmond, 16 december 2011, p. 13
75. Het korps Utrecht verstaat onder "geautomatiseerd vergelijken" het "vergelijken van een concreet zoekgegeven (bijvoorbeeld een volledig kenteken, volledige personalia, concreet adres) met geregistreerde politiegegevens waarbij het resultaat van de vergelijking relevante hits oplevert" Onder "in combinatie zoeken" verstaat zij "het vergelijken met meerdere, soms onvolledige, zoekgegevens (bijvoorbeeld een onvolledig kenteken, merk en kleur van een motorvoertuig) met geregistreerde politiegegevens, waarbij het resultaat ook niet-relevante hits bevat [...]. Deze manier van zoeken impliceert een grotere inbreuk op de persoonlijke levenssfeer van – soms grote aantallen – personen."
76. Audit Wpg KLPD, 6 januari 2012, p. 13
77. Audit Wpg Noord-Holland Noord, 10 januari 2012, p. 18
78. Flevoland, Gooi en Vechtstreek, Limburg-Noord, Limburg-Zuid, Rotterdam-Rijnmond en Zaanstreek-Waterland
79. Brabant-Noord, Drenthe, Friesland, Groningen, Hollands-Midden, IJsselland, Kennemerland, Noord-Holland Noord en Utrecht
80. Artikel 34 lid 3 Wpg
81. KLPD, Koninklijke Marechaussee, Brabant Zuid-Oost, Hollands-Midden, Limburg-Noord, Midden en West Brabant, Rotterdam-Rijnmond en Zaanstreek-Waterland
82. Audit Wpg Drenthe, 6 januari 2012, p. 16
83. Audit Wpg Utrecht, 10 januari 2012, p. 19
84. Audit Wpg Utrecht, 10 januari 2012, p. 47
85. Zie hierover: https://www.bof.nl/2011/11/03/de-stok-achter-opsteltens-deur/
86. Artikel 33 lid 3 Wpg: "Indien uit de controleresultaten blijkt dat niet wordt voldaan aan [deze wet], laat de verantwoordelijke binnen een jaar een hercontrole uitvoeren op die onderdelen die niet voldeden aan de gestelde voorwaarden. [...]"