

POSTADRES Postbus 93374, 2509 AJ Den Haag BEZOEKADRES Juliana van Stolberglaan 4-10

TEL 070 - 88 88 500 FAX 070 - 88 88 501 E-MAIL info@cbpweb.nl INTERNET www.cbpweb.nl

Koninklijke Marechaussee

Onderzoek naar de naleving van bewaartermijnen door de CIE

z2011-00943

Rapportage van definitieve bevindingen

Inhoud

Inleiding.....	3
Achtergrond	3
Aanleiding voor het onderzoek.....	3
Doel en reikwijdte van het onderzoek.....	4
Werkwijze	4
Bevindingen	5
Bewaartermijnen.....	5
Automatische schoningsmodule	7
Controle door de privacyfunctionaris	8
Conclusies.....	10

INLEIDING

Achtergrond

De Criminele Inlichtingeneenheden (CIE's) bij de politie, Koninklijke Marechaussee, Rijksrecherche en Bijzondere opsporingsdiensten (BOD's) verwerken politiegegevens om inzicht te verkrijgen in de betrokkenheid van personen bij het beramen en plegen van ernstige en georganiseerde misdrijven; dit zijn gegevens omtrent zware criminaliteit (verder: zwacri). Hiertoe wordt informatie verzameld en verwerkt over verdachten, over betrokkenen maar ook over niet-verdachten.

De CIE verkrijgt informatie onder meer door informanten te raadplegen. Deze informatie is niet altijd even betrouwbaar. Daarom kan gezegd worden dat de CIE werkt met zachte gegevens: gegevens waarvan de juistheid en volledigheid onvoldoende vaststaan. Verwerking van dergelijke zeer gevoelige gegevens vormt een risico voor degenen over wie informatie wordt verwerkt; het enkele gegeven dat een persoon is opgenomen in een zwacri-bestand wijst immers op mogelijke of veronderstelde betrokkenheid bij zware criminele activiteiten en kan gevolgen hebben voor diens bejegening. Ook voor de informanten waarvan de CIE afhankelijk is voor het verkrijgen van informatie en voor de CIE zelf in verband met het afbreukrisico van onderzoeken vormt deze verwerking een risico.

Aanleiding voor het onderzoek

CIE-verwerkingen bestaan uit gevoelige informatie die voor een deel relatief onbetrouwbaar is. Deze verwerkingen zijn doorgaans langdurig van aard. Dit terwijl effectieve opsporing gediend is met actuele gegevens die niet vervuild zijn met niet (meer) ter zake dienende informatie. De wetgever heeft dan ook -kort gezegd- voor de verwerking van zwacri-gegevens een uiterste bewaartermijn bepaald van vijf jaar, zolang de gegevens noodzakelijk zijn: wanneer zwacri-gegevens niet langer noodzakelijk zijn voor het doel van de verwerking, dienen zij verwijderd te worden. De onbepaaldheid van de noodzakelijkheid levert hierbij problemen op: de wetgever heeft voor de invulling daarvan geen gedetailleerde voorschriften gesteld. Bovendien zouden de CIE's de capaciteit niet in huis hebben om deze arbeidsintensieve toets uit te voeren.¹

Het niet-naleven van bewaartermijnen waardoor gegevens langer bewaard worden dan noodzakelijk is voor het doel van de verwerking vormt zodoende een reëel risico voor de rechtmatige verwerking van zwacri-gegevens. Dat de betrokkene over het algemeen niet op de hoogte zal zijn van de verwerking van diens gegevens en zodoende zijn rechten niet kan uitoefenen draagt hieraan bij. Controle op de naleving van de bewaartermijnbepalingen is daarom van groot belang. Het CBP is als toezichthouder hiermee belast. Daarnaast dient de verantwoordelijke uitvoering te geven aan zijn eigen verantwoordelijkheid ten aanzien van de rechtmatige verwerking van gegevens. Dit doet hij onder meer door zorg te dragen voor interne controle door de privacyfunctionaris.

¹ Mr. dr. H.H. Kielman, *Politiële gegevensverwerking en privacy: naar een effectieve waarborging*, Zutphen: WPS 2010. Daarnaast zijn gesprekken gevoerd met X, Y en Z.

Doel en reikwijdte van het onderzoek

Het onderzoek beoogt vast te stellen in hoeverre de verantwoordelijke de nodige maatregelen heeft getroffen opdat de CIE zich houdt aan de geldende bewaartermijnen ten aanzien van politiegegevens zoals bedoeld in artikel 10, eerste lid onder a Wet politiegegevens (Wpg). Het onderzoek is daarmee uiteindelijk gericht op de naleving door de CIE van de Wpg voor zover het gaat om het rechtmatig bewaren van deze gegevens. In de eerste plaats is nagegaan of de verantwoordelijke maatregelen heeft getroffen opdat de gegevens worden verwijderd of vernietigd zodra zij niet langer noodzakelijk zijn voor het doel waarvoor ze zijn verwerkt of dit door een wettelijke bepaling wordt vereist. In de tweede plaats is onderzocht, gelet op het belang dat de verantwoordelijke zijn eigen verantwoordelijkheid erkent en overeenkomstig handelt, of deze maatregelen zich ook uitstrekken tot de interne controle op de verwerking van zwacri-gegevens door de privacyfunctionaris.

Werkwijze

Bij brief van 15 november 2011 heeft het CBP het hoofd van de CIE van de Koninklijke Marechaussee alsmede diens privacyfunctionaris verzocht om inlichtingen. Deze informatie is op 6 december 2011 verstrekt.

Uit de ontvangen inlichtingen van andere onderzochte CIE's blijkt dat een automatische schoningsmodule voor de verwerking van zwacri-gegevens is ontwikkeld met als doel deze landelijk beschikbaar te maken. Om een volledig beeld te verkrijgen van de schoning van zwacri-gegevens door middel van deze module was een nadere toelichting en demonstratie hiervan geïndiceerd. Dit is aldus bij brief van 27 februari 2012 meegedeeld.

Nadat het tweemaal is uitgesteld, heeft het CBP uiteindelijk op 14 maart 2012 een bezoek gebracht aan de CIE Brabant Zuid-Oost teneinde nadere inlichtingen van algemene strekking te verkrijgen met betrekking tot de automatische schoningsmodule. Tijdens dit bezoek heeft tevens een demonstratie van deze schoningsmodule plaatsgevonden.

Op 3 april 2012 heeft het CBP aan de verantwoordelijke, de minister van Defensie, de Rapportage van voorlopige bevindingen naar aanleiding van het onderzoek toegezonden. Bij brief van 23 april 2012 is namens de verantwoordelijke op deze bevindingen gereageerd. Deze reactie heeft geleid tot aanpassing van het juridisch kader, de bevindingen en de conclusies zoals weergegeven in de Rapportage van voorlopige bevindingen.

Gelet op het voorgaande worden de bevindingen van het CBP hiermee definitief vastgesteld.

BEVINDINGEN

Bewaartermijnen

Juridisch kader

Uitgangspunt is dat politiegegevens worden verwerkt zolang dit noodzakelijk is voor het betreffende doel (artikel 3, eerste lid Wpg). Zodra de gegevens niet langer noodzakelijk zijn voor het doel waarvoor ze worden verwerkt, dienen zij ingevolge artikel 4, tweede lid Wpg te worden verwijderd/vernietigd. De verantwoordelijke dient hiertoe de nodige maatregelen te treffen om hieraan gevolg te kunnen geven, net als wanneer enige wettelijke bepaling die verwijdering of vernietiging vereist. Dit laatste betreft de uiterste bewaartermijnen die meer specifiek per doel voor het verwerken van gegevens zijn aangegeven.²

In artikel 10, zesde lid Wpg wordt de verwerkingstermijn van zwacri-gegevens nader uitgewerkt. Daarin wordt in de eerste plaats bepaald dat zwacri-gegevens dienen te worden verwijderd zodra zij niet langer noodzakelijk zijn voor het doel van de verwerking. Hiertoe heeft de wetgever voorzien in een periodieke controle. In de Memorie van Toelichting bij de Wet van 26 november 2009³ is de invulling van de periodieke controle vervolgens afgestemd op de regeling van de audit.⁴ In artikel 3, eerste lid, Regeling periodieke audit politiegegevens is bepaald dat de verantwoordelijke ervoor zorg dient te dragen dat tenminste jaarlijks een interne audit plaatsvindt.⁵ Hieruit volgt dat zwacri-gegevens jaarlijks dienen te worden geschoond, waarbij de gegevens die niet langer noodzakelijk zijn voor het doel dienen te worden verwijderd.

Invulling van het noodzakelijkheids criterium maakt onderdeel uit van de maatregel betreffende de periodieke controle; dit bewerkstelligt immers een eenduidige toetsing en controle. Standpunt van het CBP⁶ ten aanzien van de beoordeling of een geregistreerd gegeven in het algemeen nog noodzakelijk is voor het doel van de verwerking luidt dat, naast het belang van de geregistreerde allereerst –meer in het algemeen – in ogenschouw zal moeten worden genomen of het voor de politie, op basis van ervaringsregels uit de politiepraktijk, noodzakelijk is om dergelijke gegevens voor een bepaalde termijn te registreren. De uiterste bewaartermijnen per doel waarin de Wpg voorziet gelden hierbij als buitengrens. Daarnaast vergt de beoordeling van de rechtmatigheid van het handhaven van de betreffende gegevens een beoordeling in concreto. Deze beoordeling van de binnengrens ziet op een afweging van het belang van de registratie voor de uitvoering van de politietoek taak enerzijds tegen de belangen van betrokkene bij verwijdering anderzijds. Alle omstandigheden van het geval kunnen daarbij een rol spelen. Deze beoordeling kan leiden tot verwijdering van de gegevens nog voordat de uiterste bewaartermijn is verlopen.

² Tweede Kamer, 2005-2006, 30 327, nr. 3, p. 32.

³ Wet van 26 november 2009, houdende partiële wijziging van het Wetboek van Strafrecht, Wetboek van Strafvordering en enkele aanverwante wetten in verband met rechtsontwikkelingen, internationale verplichtingen en geconstateerde wetstechnische gebreken en leemten.

⁴ Tweede Kamer, vergaderjaar 2007-2008, 31 391, nr. 3, p. 13.

⁵ Op grond van artikel 33, lid 5, Wpg j° artikel 6:5, lid 5, Bpg j° artikel 3, lid 1, Regeling periodieke audits politiegegevens.

⁶ Advies aan de rechtbank Utrecht, 6 december 2004, z2004-01392.

In de tweede plaats is voor de verwerking van gegevens op grond van artikel 10, eerste lid, onder a Wpg de uiterste bewaartermijn gesteld op vijf jaar na de laatste opname van gegevens die blijken geven van de noodzaak tot de gegevensverwerking.⁷ Hieruit volgt dat de toegevoegde gegevens bepalend zijn voor de uiterste verwerkingstermijn van politiegegevens van de betrokkene: het laatste gegeven waaruit de noodzaak tot verwerking blijkt is het beginpunt van de maximale bewaartermijn. Het kunnen vaststellen van dit beginpunt en de daarop volgende termijn is een nodige maatregel in de zin van artikel 4, tweede lid Wpg.

Omdat de vijfjaartermijn gekoppeld is aan de laatste opname van gegevens die de noodzaak van de verwerking van betrokkene betreffende gegevens ondersteunt, is uitvoering van de periodieke noodzakelijkheidstoets op de gegevens uiterst relevant voor het instellen, wijzigen en daarmee kunnen naleven van de vijfjaartermijn. Zonder deze toets, waarin zowel het verloop van de vijfjaartermijn als de omstandigheden van het geval ten behoeve van de toetsing in concreto moeten worden meegenomen, kan naleving van de wettelijke bepaling omtrent de uiterste bewaartermijn niet worden gegarandeerd.

Bevindingen

Een jaar na invoer van CIE-informatie worden de gegevens bekeken of het nog noodzakelijk is dat deze gegevens in het systeem opgenomen blijven. Hiertoe worden de gegevens 'gevlagd'. Deze toets vindt jaarlijks opnieuw plaats: na de controle worden de gegevens opnieuw 'gevlagd' voor controle het jaar daarop. Het hoofd CIE controleert maandelijks de gevlagde gegevens. Bij noodzaak wordt aangegeven waarom het nog noodzakelijk is. Indien het niet meer noodzakelijk is, worden de gegevens verwijderd, aldus het hoofd CIE.

Ten aanzien van de wijze waarop een zwacri-gegeven als noodzakelijk wordt beoordeeld is aangegeven dat "bij de periodieke beoordeling of een gegeven nog valide is, wordt gekeken naar de 'plus' om een gegeven nog als noodzakelijk aan te merken. Dit houdt in dat er 'rondom' het subject omstandigheden zijn die langere opname rechtvaardigen."⁸

Gevraagd naar de manier waarop het beginpunt van de maximale bewaartermijn inzichtelijk wordt gemaakt, is aangegeven dat in het systeem de termijn van de invoer of de datum van invoer van nieuwe gegevens 'gevlagd' wordt. Na ommekomst van de termijn wordt het gevlagde gegeven zichtbaar.

Beoordeling

Uit het voorgaande blijkt dat jaarlijks de verplichte periodieke toets op de noodzakelijkheid van de gegevens in relatie tot het doel van de verwerking wordt uitgevoerd. Hierbij blijft echter de inhoud van deze toets, namelijk op welke wijze het noodzakelijkheids criterium wordt ingevuld, onduidelijk: niet nader gespecificeerd is wat verstaan dient te worden onder de 'plus' van een gegeven, anders dat dit betrekking heeft op de omstandigheden 'rondom' het subject. Nu de invulling van het

⁷ Artikel 10, zesde lid Wpg; zie ook: Tweede Kamer, 2005-2006, 30 327, nr. 3, p. 51.

⁸ Brief van 6 december 2011 van het Hoofd Criminele Inlichtingen Eenheid Koninklijke Marechaussee.

noodzakelijkheids criterium onderdeel uitmaakt van de maatregel betreffende de periodieke controle en hiervan onvoldoende blijk wordt gegeven, wordt in strijd gehandeld met artikel 4, tweede lid Wpg.

Ten aanzien van de maximale bewaartermijn merkt het CBP het volgende op. Nu onvoldoende gevolg wordt gegeven aan de invulling van de noodzakelijkheidstoets, is niet aannemelijk geworden dat voldoende maatregelen zijn getroffen om de gegevens te verwijderen uiterlijk na vijf jaar na de datum van de laatste verwerking van de gegevens die blijk geven van de noodzaak tot het verwerken van de politiegegevens van betrokkene. Wanneer immers opgenomen gegevens op enig moment niet langer noodzakelijk blijken te zijn, valt de uiterste bewaartermijn eerder dan voorzien. De verantwoordelijke schiet daarmee ten aanzien van de benodigde maatregelen te kort. Dit is in strijd met artikel 4, tweede lid Wpg.

Conclusie: de verantwoordelijke handelt in strijd met artikel 4, tweede lid Wpg nu hij onvoldoende maatregelen heeft getroffen opdat politiegegevens worden verwijderd zodra zij niet langer noodzakelijk zijn voor het doel waarvoor ze zijn verwerkt of dit door enige wettelijke bepaling wordt vereist.

Automatische schoningsmodule

Hoewel de CIE Kmar niet heeft aangegeven gebruik te gaan maken van de automatische schoningsmodule, zoals dat wel door de andere onderzochte CIE's is gedaan, hecht het CBP er aan het volgende op te merken nu deze landelijke toepassing zal gaan krijgen.

Naar aanleiding van de demonstratie en toelichting van de automatische schoningsmodule bij de CIE Brabant Zuid-Oost is gebleken dat deze module beperkt is tot het automatisch bepalen van de uiterste bewaartermijn. Hiertoe wordt vijf jaar bij de datum van het laatst opgenomen zwacri-waardige gegeven automatisch opgeteld. Een actieve instelling van de CIE is vervolgens nodig om, door middel van een door de CIE zelf ingestelde peildatum, de te schonen subjecten desgevraagd te laten verschijnen. Deze peildatuminstelling kan per CIE verschillen.

Wanneer de module niet actief wordt bevraagd, loopt deze door zonder een signaal af te geven. De module biedt daarmee geen garantie voor het tijdig schonen van de artikel 10, eerste lid sub a Wpg-gegevens. Daarbij is eveneens opgevallen dat de module enkel bijdraagt aan het houden van zicht op de maximale bewaartermijn; een handvat voor de verplichte periodieke toets op de noodzakelijkheid van de verwerking van de gegevens in relatie tot het doel van de verwerking biedt de instelling van de schoningsmodule niet.

Het CBP concludeert dan ook dat de module de CIE kan ondersteunen in het handhaven van de uiterste bewaartermijn, maar dat deze niet geschikt is als nodige maatregel in de zin van artikel 4, tweede lid Wpg, zeker niet waar het de noodzakelijkheidstoets betreft.

Controle door de privacyfunctionaris

Juridisch kader

De verantwoordelijke treft de nodige maatregelen teneinde zorg te dragen dat de voorgeschreven bewaartermijnen worden nageleefd.⁹ Om de grenzen te bewaken die in de wet zijn gesteld, waaronder de bewaartermijnen en gronden daarvoor, voorziet de Wpg in intern toezicht: de verantwoordelijke is verplicht een privacyfunctionaris te benoemen die onder meer als taak heeft gegevensverwerkingen te controleren.¹⁰ Hiermee ondersteunt hij de verantwoordelijke in zijn verantwoordelijkheid de wettelijke verplichtingen na te leven.¹¹

Om uitvoering te kunnen geven aan zijn controlerende taak zal de privacyfunctionaris toegang dienen te krijgen tot de betreffende gegevens, voor zover hij deze behoeft voor de uitvoering van zijn taak; de verantwoordelijke verleent deze op grond van artikel 4, vijfde lid Wpg. Vervolgens zal de invulling van voornoemde taak blijken uit een vorm van concreet onderzoek dat de privacyfunctionaris heeft uitgevoerd waarvan de bevindingen zijn opgenomen in zijn jaarverslag ingevolge artikel 34, derde lid Wpg. Hieruit kan worden afgeleid of de verantwoordelijke de benodigde maatregelen heeft getroffen om naleving van de bewaartermijnen te bevorderen.

Bevindingen

Uit de beantwoording van de schriftelijke vragen blijkt dat een nadere invulling is gegeven aan de toegang tot politiegegevens als bedoeld in artikel 4, vijfde lid Wpg. De privacyfunctionaris heeft geen autorisatie tot de CIE-gegevens toegekend gekregen. Indien de privacyfunctionaris evenwel toegang nodig heeft tot de bestanden met CIE-gegevens, verleent het hoofd CIE hem op verzoek de feitelijke toegang daartoe. Verder stelt het CBP vast dat de privacyfunctionaris noch in 2010 noch in 2011 onderzoek heeft uitgevoerd naar (de naleving van de bewaartermijnen van) gegevensverwerkingen door de CIE.

Tot slot stelt het CBP vast dat de privacyfunctionaris een jaarverslag met bevindingen heeft opgesteld. Uit de bevindingen blijkt niet dat de privacyfunctionaris toegang heeft gekregen tot de CIE-verwerkingen. De privacyfunctionaris constateert in zijn jaarverslag onder het kopje 'Conclusies' dat aan zijn controlerende taak in de periode 2008-2010 'minder dan gewenst invulling is gegeven als gevolg van capaciteitsgebrek.

Beoordeling

Nu uit de bevindingen niet is gebleken dat de privacyfunctionaris controle heeft uitgevoerd op de naleving van de bewaartermijnen van CIE-gegevens, schiet de invulling van de maatregel inhoudende interne controle tekort. Dit is verplicht gesteld om de grenzen van de Wpg te bewaken. Daarmee heeft de verantwoordelijke onvoldoende maatregelen getroffen om naleving van de bewaartermijnen te

⁹ Artikel 4, tweede lid Wpg.

¹⁰ Artikel 34, eerste lid Wpg. En: MvT p. 89 "Teneinde zorg te dragen dat de door het wetsvoorstel voorgestelde grenzen in de praktijk niet worden overschreden, is het van belang passende waarborgen te creëren. Het wetsvoorstel voorziet hiertoe in twee vormen van intern toezicht. Ten eerste verplicht het wetsvoorstel de verantwoordelijke tot het periodiek laten uitvoeren van evaluaties en privacy audits ter controle op de naleving van de wet. [...] Ten tweede verplicht de wet de verantwoordelijke tot het aanwijzen van een privacyfunctionaris. Deze functionaris heeft mede tot taak de verwerking van de gegevens te controleren en de verantwoordelijke te adviseren ten aanzien van de naleving van deze wet."

¹¹ MvT p. 91.

bevorderen. Dit klemt te meer nu de privacyfunctionaris in dit kader onvoldoende in de gelegenheid wordt gesteld zijn controlerende taak volledig uit te voeren; dat de privacyfunctionaris aangeeft desgevraagd toegang te kunnen krijgen maakt dit niet anders. Hiermee handelt de verantwoordelijke in strijd met artikel 4, tweede lid Wpg j° artikel 34, eerste lid Wpg.

Conclusie: de verantwoordelijke heeft onvoldoende maatregelen getroffen om de interne controle te bevorderen en handelt daarmee in strijd met artikel 4, tweede lid Wpg j° artikel 34, eerste lid Wpg.

CONCLUSIES

Het doel van het onderzoek was vast te stellen in hoeverre de verantwoordelijke de nodige maatregelen heeft getroffen opdat de CIE zich houdt aan de geldende bewaartermijnen ten aanzien van politiegegevens zoals bedoeld in artikel 10, eerste lid onder a Wpg. In de eerste plaats is nagegaan of de verantwoordelijke maatregelen heeft getroffen opdat de gegevens worden verwijderd of vernietigd zodra zij niet langer noodzakelijk zijn voor het doel waarvoor ze zijn verwerkt of dit door een wettelijke bepaling wordt vereist. In de tweede plaats is onderzocht, gelet op het belang dat de verantwoordelijke zijn eigen verantwoordelijkheid erkent en overeenkomstig handelt, of deze maatregelen zich ook uitstrekken tot de interne controle op de verwerking van zwacri-gegevens door de privacyfunctionaris.

De conclusies ten aanzien van de twee te onderzoeken onderdelen zijn de volgende:

Ten aanzien van de bewaartermijnen

De verantwoordelijke handelt in strijd met artikel 4, tweede lid Wpg nu hij onvoldoende maatregelen heeft getroffen opdat politiegegevens worden verwijderd zodra zij niet langer noodzakelijk zijn voor het doel waarvoor ze zijn verwerkt of dit door enige wettelijke bepaling wordt vereist.

Ten aanzien van de controle door de privacyfunctionaris

De verantwoordelijke heeft onvoldoende maatregelen getroffen om de interne controle te bevorderen en handelt daarmee in strijd met artikel 4, tweede lid Wpg^o artikel 34, eerste lid Wpg.