

Regionaal politiekorps Flevoland

Onderzoek naar de naleving van bewaartermijnen door de CIE

z2011-00941

Rapportage van definitieve bevindingen

Datum: Mei 2012

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 Flevoland alsmede de privacyfunctionaris van het korps verzocht om inlichtingen. Deze informatie is op 12 december 2011 verstrekt.

Uit de ontvangen inlichtingen, zowel van de CIE Flevoland alsmede 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 van het regionaal politiekorps Flevoland, de korpsbeheerder, de Rapportage van voorlopige bevindingen naar aanleiding van het onderzoek toegezonden. Bij brief van 26 april 2012 heeft de verantwoordelijke op deze bevindingen gereageerd. Dit heeft geleid tot aanpassing van het juridisch kader voor zover het betreft de frequentie van de periodieke controle. Dit heeft echter geen gevolgen voor de bevindingen en/of conclusies. Het CBP heeft de beoordeling en conclusie met betrekking tot het uitblijven van een jaarverslag van de privacyfunctionaris zoals weergegeven in de Rapportage van voorlopige bevindingen aangevuld.

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 tegen de belangen van betrokkene bij verwijdering anderzijds. Alle omstandigheden van het geval

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.

kunnen daarbij een rol spelen. Deze beoordeling kan leiden tot verwijdering van de gegevens nog voordat de uiterste bewaartermijn is verlopen.

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

De CIE-officier van justitie en de leiding van de CIE controleren vooraf of de zwacri-gegevens noodzakelijk zijn voor het doel van de verwerking. De gegevens moeten voldoen aan de criteria van artikel 10 Wpg en het Besluit politiegegevens, aldus het hoofd CIE.

Incidenteel wordt gecontroleerd of de opgeslagen zwacri-gegevens nog noodzakelijk zijn voor het doel van de verwerking. Een overzicht van dergelijke controles in 2010 en 2011 kon ten tijde van het onderzoek niet overgelegd worden.

Bij de beoordeling of een zwacri-gegeven noodzakelijk is wordt getoetst of de informatie voldoet aan de gestelde opslagcriteria genoemd in de artikelen 3, 4 en 10 Wpg. Daarnaast wordt verwezen naar het Bpg en de Instructie CIE Officier van Justitie. Er wordt bezien welke gegevens noodzakelijk zijn om inzicht te krijgen in de betrokkenheid van het subject of een relatie hiervan bij bepaalde ernstige bedreigingen van de rechtsorde.

Aan een nieuw op te nemen subject wordt ingevolge het Proceshandboek CIE een kenmerk gekoppeld dat de datum van schoning inhoudt. Deze datum ligt vijf jaar verwijderd van het opnamemoment van het subject. Het verloop van de termijn wordt incidenteel getoetst.

In paragraaf 11 van het Proceshandboek CIE is ten aanzien van het verwijderen en bewaren van persoonsgegevens aangegeven dat gegevens moeten worden verwijderd

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

uiterlijk vijf jaar na de datum van de laatste verwerking van het gegeven. "De datum laatste verwerking wordt bepaald aan de hand van de laatste [zwacri-waardige] informatie die bij het subject is geregistreerd."⁸

Beoordeling

Uit de verstrekte inlichtingen volgt dat de CIE van het korps de periodieke toets op noodzakelijkheid van de opgenomen zwacri-gegevens in relatie tot het doel van de verwerking niet uitvoert; deze vindt slechts incidenteel plaats. Bovendien is de enkele verwijzing naar wetsartikelen waarin de noodzaak als voorwaarde is opgenomen niet voldoende om te beoordelen dat in dit kader een belangenafweging plaatsvindt. Het niet uitvoeren van de periodieke toets op de noodzaak van de verwerkte gegevens voor het doel van de verwerking is in strijd met artikel 10, zesde lid Wpg en artikel 4, tweede lid Wpg.

Ten aanzien van de maximale bewaartermijn merkt het CBP op dat het hoofd CIE aangeeft dat deze niet wordt gekoppeld aan het laatste gegeven dat blijkt geeft van de noodzaak van de verwerking zoals bedoeld in artikel 10, eerste lid onder a Wpg, maar aan het subject zelf. Dit stemt niet overeen met het Proceshandboek CIE, waar tegelijkertijd naar verwezen wordt, maar is tevens in strijd met artikel 10, zesde lid Wpg.

Conclusie: de verantwoordelijke handelt in strijd met artikel 10, zesde lid Wpg voor zover het betreft het niet uitvoeren van de periodieke toets op de noodzaak van de verwerkte gegevens voor het doel van de verwerking.

Conclusie: de verantwoordelijke handelt in strijd met artikel 10, zesde lid Wpg nu de datum van de laatste verwerking van gegevens die blijkt geeft van de noodzaak tot het verwerken van de politiegegevens van de betrokkene niet de verwijdering van die gegevens na uiterlijk vijf jaar bepaalt.

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

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

⁸ Proceshandboek CIE, Verwerven informatiepositie zware en georganiseerde criminaliteit (artikel 10 lid 1 sub a Wpg), d.d. 20-05-2011, versie 2.0.

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 wegens de gevoeligheid van die gegevens. Indien hij toegang nodig heeft tot de CIE-verwerkingen, heeft hij in de praktijk “te allen tijde toegang tot de door hem gevraagde verwerkingen van politiegegevens”, aldus de privacyfunctionaris. Volgens de privacyfunctionaris heeft hij hierover met het hoofd CIE afspraken gemaakt.

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.

Verder blijkt uit de bijgevoegde stukken dat in 2010 door de privacyfunctionaris van het korps Gooi&Vechtstreek en de projectleider Wpolg van de politie Flevoland een gesprek heeft plaatsgevonden met het toenmalige hoofd van de CIE betreffende de implementatie van de Wpg bij de CIE. Uit de bijlage blijkt niet dat voor dit onderzoek toegang is verkregen tot CIE-verwerkingen.

Tot slot stelt het CBP vast dat de privacyfunctionaris geen jaarverslag heeft opgesteld. De privacyfunctionaris geeft aan dat zijn rol en mogelijkheden tot het uitvoeren van toezicht of het geven van advies beperkt zijn, onder meer door de opgelegde prioriteit en dus zijn capaciteit. Namens de gemandateerd korpschef is aan de privacyfunctionaris de prioriteit gegeven aan het verstrekken van informatieverzoeken van derden, het uitvoeren van kennisnemingsverzoeken en het adviseren/begeleiden van het korps om dit op 1 januari 2010 zoveel mogelijk Wpg-proof te laten zijn.

Beoordeling

Een gesprek met het hoofd CIE is naar het oordeel van het CBP geen onderzoek in de zin van de door de wetgever bedoelde interne controle. 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 bevorderen. Dit klemmt 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 verantwoordelijk in strijd met artikel 4, tweede lid Wpg j° artikel 34, eerste lid Wpg. Het nalaten van het opstellen van een jaarverslag is bovendien in strijd met artikel 34, derde 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.

Conclusie: de verantwoordelijke handelt in strijd met artikel 34, derde lid Wpg nu de privacyfunctionaris geen jaarverslag heeft opgesteld.

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 10, zesde lid Wpg voor zover het betreft het niet uitvoeren van de periodieke toets op de noodzaak van de verwerkte gegevens voor het doel van de verwerking. Tevens handelt de verantwoordelijke in strijd met artikel 10, zesde lid Wpg nu de datum van de laatste verwerking van gegevens die blijkt geeft van de noodzaak tot het verwerken van de politiegegevens van de betrokkene niet de verwijdering van die gegevens na uiterlijk vijf jaar bepaalt. Daarmee handelt de verantwoordelijke 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 j° artikel 34, eerste lid Wpg. Daarnaast handelt de verantwoordelijke in strijd met artikel 34, derde lid Wpg nu de privacyfunctionaris geen jaarverslag heeft opgesteld.