

Vergaderjaar 2017–2018

34 775 VI

Vaststelling van de begrotingsstaten van het Ministerie van Justitie en Veiligheid (VI) voor het jaar 2018

Nr. 116

BRIEF VAN DE MINISTER VAN JUSTITIE EN VEILIGHEID

Aan de Voorzitter van de Tweede Kamer der Staten-Generaal

Den Haag, 13 juli 2018

Met deze brief bied ik u conform artikel 8.2 van het besluit verstrekking gegevens telecommunicatie het verslag aan van de audits over 2016 naar de goede uitvoering van dit besluit door de aanbieders van openbare telecommunicatiediensten of van openbare telecommunicatienetwerken, het informatiepunt, de arrondissementsparketten en de politie, of andere opsporingsdiensten.

Aanleiding

Het Centraal Informatiepunt Onderzoek Telecommunicatie (CIOT) is, op grond van hoofdstuk 13 van de Wet op telecommunicatiegegevens aangewezen om de informatieverzoeken van de behoeftestellers, zijnde de (bijzondere) opsporingsdiensten en inlichtingendiensten door te geleiden naar de aanbieders van telecommunicatiediensten. Conform artikel 8.2 van het Besluit verstrekkingen telecommunicatiegegevens informeer ik uw Kamer over de audit naar de goede uitvoering van dit besluit door de betrokken partijen.

De Auditdienst Rijk (ADR) heeft een audit naar het beheer van het CIOT-informatiesysteem (CIS) en een naar de rechtmatigheid van de bevragingen door de Koninklijke Marechaussee (KMar), Inspectie Sociale Zaken en Werkgelegenheid (ISWZ) en de Fiscale Inlichtingen- en Opsporingsdienst (FIOD) uitgevoerd. Conform de afspraken in de ministerraad, zijn beide rapporten en managementreactie openbaar gemaakt op de website van de rijksoverheid.nl.¹ Tevens vindt u deze rapporten bijgevoegd².

¹ <https://www.rijksoverheid.nl/documenten/rapporten/2016/07/01/adr-rapporten-justitie-en-veiligheid>

² Raadpleegbaar via www.tweedekamer.nl

Daarnaast heeft Concernaudit Politie, de interne auditdienst van de politie, over 2015 en 2016 audits uitgevoerd naar de juiste uitvoering van het Besluit verstrekking gegevens telecommunicatie.

In samenspraak tussen de ADR en Concernaudit Politie is een vergelijking gemaakt tussen de aanpak van de audits CIOT 2016, die door Concernaudit Politie en de ADR afzonderlijk zijn uitgevoerd. Uit deze vergelijking is gebleken dat het type onderzoek, evenals de diepgang, uitgangspunten en gehanteerde normen overeenkomen. Over de uitkomsten van de audits wordt u geïnformeerd in dit verslag.

Toelichting

Het CIOT is een onderdeel van het Ministerie van Justitie en Veiligheid en is aangewezen om de informatieverzoeken van de behoeftestellers, zijnde de (bijzondere) opsporingsdiensten en inlichtingendiensten door te geleiden naar de aanbieders van telecommunicatiediensten. Het CIOT kan worden beschouwd als een «berichtenmakelaar». Daartoe beheert het CIOT het geautomatiseerd CIOT informatiesysteem (CIS), waarin het vraag- en antwoordverkeer van de door de behoeftestellers expliciet gevraagde gegevens wordt doorgeleid.

Het CIOT schept randvoorwaarden zodat de gegevens van gebruikers van telecommunicatie met de juiste zorgvuldigheid worden behandeld. Conform het Besluit Verstrekking Gegevens Telecommunicatie moeten alle aanbieders van telecommunicatiediensten ten minste iedere 24 uur hun gegevens in het CIS bij het CIOT actualiseren. De door de aanbieders geleverde gegevens moeten overeenstemmen met de gegevens die de aanbieder bij zijn bedrijfsvoering gebruikt. De gegevenslevering door de aanbieder dient elke keer de volledige set van alle gebruikers van telecommunicatiediensten te bevatten.

Iedere 24 uur wordt het bestand in het CIS bij het CIOT overschreven, het CIOT beheert dus zelf geen historische gegevens. Het opvragen van gegevens bij de aanbieders van telecommunicatiediensten door middel van het CIS is gebonden aan wettelijke voorschriften. Het Wetboek van Strafrecht en het Wetboek van Strafvordering geven aan onder welke voorwaarden de informatie door de behoeftestellers kan worden opgevraagd. De behoeftestellers moeten het bevragsingsproces zodanig inrichten dat gewaarborgd is dat de bevragingen voldoen aan het wettelijk kader en tevens moet dat achteraf vastgesteld kunnen worden.

Belangrijkste bevindingen

Beheer bij CIOT

De ADR heeft aan de hand van een normenkader onderzoek gedaan naar de beheersmaatregelen die het CIOT heeft getroffen. Het doel van het onderzoek was hierbij inzicht te verschaffen in mogelijke risico's op het gebied van de gegevensaanlevering en -verstrekking. Op basis van dit onderzoek ben ik van mening dat de beheersmaatregelen bij het CIOT toereikend zijn om de risico's op inbreuken op beveiliging of integriteit van de informatie-uitwisseling te beperken.

Een aantal bevindingen die met name betrekking hebben op de interne beheerprocessen van het CIOT, vragen nadere aandacht. Justitiële Informatiedienst/Informatiepunt Bijzondere Opsporingsonderzoeken (Justid/IBO), die het CIS als opdrachtnemer onder beheer heeft, heeft deze bevindingen overgenomen en waar nodig reeds verbeteracties ingezet. In

de managementreactie, bijgevoegd bij het auditrapport gaat Justid/IBO hier nader op in³. Twee bevindingen wil ik nader toelichten:

De ADR stelt vast dat Justid/IBO maatregelen heeft getroffen conform de normen voor vastlegging validatieproces, importproces en van de beheerdershandelingen. De ADR stelt vast dat er een overzicht met daarin bewaartermijnen, toelichting op de gegevens, de opslaglocatie, verantwoordelijken en de onderliggende wettelijke bepaling aanwezig is, doch geactualiseerd moet worden. Justid/IBO heeft deze tekortkoming onderkend en ter hand genomen.

De ADR stelt vast dat IBO maatregelen heeft getroffen conform de normen voor het proces certificatenbeheer, de bevestigingen en de rapportagefunctie «aantal bevestigingen». Ten aanzien van back-up en recovery stelt de ADR vast dat voor de continuïteit en integriteit van het dienstverleningsproces het van belang is dat kopieën van programmatuur en gegevens aanwezig zijn in geval van een grote verstoring. Het back-up beleid is aanwezig, echter gefragmenteerd. Het regulier testen van een back-up en een restore wordt niet periodiek uitgevoerd en de rapportage hierover vindt beperkt plaats. Justid/IBO heeft aangegeven dat in 2018 deze omissie wordt opgepakt en dat het back-up beleid wordt aangepast.

Bevestigingsproces KMar, ISZW, FIOD

Aan de hand van een normenkader heeft de ADR getoetst of de bevestigingen van het CIOT uitgevoerd door de (bijzondere) opsporingsdiensten FIOD, KMar en de ISZW rechtmatig, conform wet- en regelgeving, zijn uitgevoerd. De centrale vraag bij de uitvoering van de audit is in welke mate door de (bijzondere) opsporingsinstanties maatregelen zijn getroffen zodat de bevestigingen in het systeem rechtmatig plaatsvinden en in welke mate deze maatregelen worden nageleefd.

Uit de audit is gebleken dat de (bijzondere) opsporingsdiensten FIOD, KMar en de ISZW in opzet, bestaan en werking aan het overgrote deel van de normen voldoen.⁴ De ADR heeft vastgesteld dat de maatregelen om de bevestigingen in het proces rechtmatig te laten plaatsvinden zijn getroffen, en dat deze worden nageleefd. Een beperkt aantal bevindingen van de ADR hebben betrekking op het formaliseren van de procedure of werkinstructie, dan wel het expliciet opnemen van werkzaamheden. Hierop zijn de betrokken diensten reeds verbeteracties ingezet.

In haar deelwaarneming heeft de ADR vast kunnen stellen dat in tweeënzeventig van de vijfenzeventig bevestigingen de rechtmatigheid aantoonbaar is. Alle bevestigingen zijn door geautoriseerde medewerkers uitgevoerd. Bij twee bevestigingen kon de vordering niet worden getoond. Bij één bevestiging ontbrak een handtekening van bevoegde autoriteit op de vordering. Dit betekent overigens niet dat deze bevestigingen per definitie onrechtmatig zijn, alleen dat de rechtmatigheid niet kon worden aangetoond.

Door de ADR is vastgesteld dat het mogelijk is voor geautoriseerde medewerkers om het CIS buiten de kritisch ingerichte locatie te benaderen, bijvoorbeeld middels thuiswerken. Er zal in overleg met de (bijzondere) opsporingsdiensten nader uitvoering gegeven aan de aanbeveling van de ADR om overeenstemmende afspraken te maken over

³ <https://www.rijksoverheid.nl/documenten/rapporten/2017/12/20/rapport-van-bevindingen-ibo-beheer-processen-2016> en raadpleegbaar via www.tweedekamer.nl

⁴ <https://www.rijksoverheid.nl/documenten/rapporten/2017/06/19/onderzoeksrapport-cis-2016-iszw-fioid-kmar>

het gebruik van het CIS buiten de specifiek ingerichte locatie door geautoriseerde medewerkers.

Bevragingsproces politie

Aan de hand van een normenkader heeft Concernaudit Politie over 2015 en 2016 getoetst in welke mate de politie voldoet aan de regels en afspraken gesteld aan de uitvoering van de bevraging van klantgegevens van telecom- en internetbedrijven via het CIOT.

De resultaten van de uitgevoerde audits over 2015 en 2016 laten zien dat de eerder geconstateerde verbeterlijn⁵ zich verder heeft doorgezet. Ik ga hieronder met name in op de specifieke bevindingen uit de audit over 2016.

De bevindingen in de audit over 2016 laten zien dat mede op basis van voorgaande audits verbeteringen in de procedure rond CIS-bevragingen zijn aangebracht en dat de landelijke uniformiteit beter is geborgd. De kwaliteit van de aanvragen en van de bevragingen is verbeterd. De nieuwe landelijke procedure, het gebruik van formats en het ondersteunende systeem hebben hieraan bijgedragen. Ook de systematische wijze waarop aanvragen met fouten zijn teruggelegd door de CIS-bevragers bij de aanvragers heeft een bijdrage geleverd aan de verbetering van de kwaliteit van de aanvragen door de opsporingsbevoegden.

Tevens bevestigen de bevindingen dat de landelijke procedure bijdraagt aan de uniformiteit en continuïteit in de kwaliteit van de bevragingen. Concernaudit Politie heeft vastgesteld dat de procedure op een beperkt aantal punten nog aanscherping behoeft. Er is nog onduidelijkheid over de wijze waarop bevragingen van niet-actuele informatie, internationale rechtshulpverzoeken en embargo-onderzoeken dient plaats te vinden. Niet-actuele informatie kan niet uit het CIS worden gehaald en dient dus rechtstreeks bij de provider te worden opgehaald. Daarnaast is het niet duidelijk welke archiveringstermijnen gehanteerd dienen te worden, mede gezien de eisen die ook de WPG hieraan stelt. Deze punten worden meegenomen in de lopende actualisatie van de landelijke procedure.

Concernaudit Politie heeft ter validatie een steekproef uitgevoerd op de CIS-bevragingen in 2016. Deze CIS-bevragingen zijn de basis geweest voor het bepalen van een (representatieve) steekproef van ruim 800 bevragingen. De uitkomst van deze steekproef bevestigt de genoemde opgaande lijn. Er zijn geen bijzondere afwijkingen geconstateerd. In enkele gevallen zijn er nog administratieve onjuistheden en onvolledigheden geconstateerd.

De auditdienst van de politie concludeert dat ten aanzien van het proces van autoriseren op een aantal punten nog niet volledig wordt voldaan aan de regelgeving. De voorgeschreven aanwijzing door de korpschef gebeurt per half jaar achteraf in plaats van vooraf. Er ontbreekt (historisch) inzicht in de deelname aan de verplichte opleidingsdagen door CIS-bevragers en -beheerders. Sinds 2017 geeft CIOT (opleidings-)certificaten uit na deelname aan de opleidingsdag. De beheerder en de landelijk coördinator kunnen hiermee toetsen of voldaan wordt aan de opleidingseis voordat zij CIS-bevragers en beheerders aanmelden bij het CIOT. De politie gaat binnen de mogelijkheden die de regelgeving hiervoor biedt de autorisatieprocedure aanpassen, zodat de daarvoor bevoegde autoriteit de CIS-bevragers sneller en flexibeler kan aanwijzen dan nu het geval is. Deze herziene procedure moet daarbij ook de garantie bieden dat bevragers uitsluitend nog geautoriseerd kunnen worden voor het

⁵ Kamerstuk 34 000 VI, nr. 98

CIS-bevragingssysteem nadat zij voor de uitvoering van deze werkzaamheden zijn aangewezen.

Tot slot heeft de Concernaudit Politie een laatste punt geconstateerd ten aanzien van de bevragingen door de 112-centrale in het kader van noodhulp en dusdanig misbruik van de 112-centrale dat de bereikbaarheid van de 112-centrale in gevaar komt. Concernaudit constateert dat er voor het toestaan van het doen van CIS-bevragingen door de 112-centrale en de kaders waarbinnen dit zou mogen, het tijdens de audit niet is gelukt om een eenduidig inzicht te krijgen in het juridisch kader.

Ik erken deze bevinding en merk hier nog het volgende over op. Ik ben van mening dat noodhulp aan burgers op een zo doeltreffende en efficiënt mogelijke wijze dient plaats te vinden, binnen de hiervoor geldende wettelijke kaders. Bevragingen ten aanzien van noodhulp kennen een andere wettelijke basis in de telecomwet, te weten artikel 11. Er geldt op grond van artikel 11.10, eerste lid, onderdeel b van de Telecommunicatiewet een wettelijke verplichting om de NAWP-gegevens rechtstreeks mee te leveren aan de politie. De politie mag derhalve rechtmatig beschikken over deze gegevens voor het doel van noodhulpverlening en misbruikbestrijding. Deze rechtstreekste aanlevering is echter nog niet volledig geoperationaliseerd. Daarom wordt er voor noodhulpverlening of misbruikbestrijding een CIOT bevraging uitgevoerd, wanneer dit noodzakelijk is.

In de zomer van 2018 zal het nieuwe platform 1-1-2 operationeel gaan. In deze oplossing is voorzien dat de NAWP-gegevens zichtbaar zullen zijn voor de 1-1-2-centrale. Deze gegevens worden dan ook gelogd en blijven beschikbaar voor navraag, noodhulp of bestrijding misbruik. Met de invoering van het platform 1-1-2-centrale zal de noodzaak voor de CIOT-bevragingen niet langer aan de orde zijn.

Aanbieders

Het in de brief van 11 mei 2017⁶ aangekondigde onderzoek naar de aanbieders van telecommunicatiediensten zal in 2018 uitgevoerd worden door de Auditdienst Rijk.

Publicatie jaarcijfers

Het CIOT publiceert, conform de wettelijke verplichting, jaarlijks cijfers over het aantal afgehandelde informatieverzoeken. Dit gebeurt door publicatie van een rapport van de cijfers via de website www.rijksoverheid.nl. Sinds 2015 worden deze cijfers met het verschijnen van het jaarverslag van het Ministerie van Justitie en Veiligheid gepubliceerd.⁷

De Minister van Justitie en Veiligheid,
F.B.J. Grapperhaus

⁶ Kamerstuk 34 550 VI, nr. 109

⁷ <https://www.rijksoverheid.nl/documenten/publicaties/2018/05/22/jaarverslag-ciot-2017>