Auditdienst Rijk
Ministerie van Financiën

Onderzoeksrapport CIOT Aanbieders 2018

Definitief v1.0

Colofon

Titel	CIOT Aanbieders 2018
Uitgebracht aan	Directeur-Generaal Rechtspleging en Rechtshandhaving
Datum	20 januari 2020
Kenmerk	2020-0000012204

Inlichtingen
Auditdienst Rijk
070-342 7700

Inhoud

Managementsamenvatting

De minister van Justitie Veiligheid is conform artikel 8 tweede lid van het Besluit Verstrekking Gegevens Telecommunicatie (hierna Besluit) gehouden jaarlijks een verslag op te stellen van een audit naar de goede uitvoering van het Besluit door aanbieders van openbare telecommunicatiediensten of van openbare telecommunicatienetwerken, het Informatiepunt, de arrondissementsparketten en de politiekorpsen of andere opsporingsdiensten.

De directeur-generaal Rechtspleging en Rechtshandhaving (dgRR) heeft de Auditdienst Rijk (ADR) gevraagd onderzoek te doen naar de maatregelen van de verstrekking van deze gegevens bij twee aanbieders (telecomproviders).

De ADR constateert dat bij beide aanbieders de geheimhouding voor medewerkers betrokken bij het aanleverproces aan het Centraal Informatiepunt Onderzoek Telecommunicatie (CIOT) is geregeld in een arbeidsovereenkomst of gedragscode maar dat de naleving hiervan bij één aanbieder niet aantoonbaar is ingeregeld. Bij beide aanbieders ontbreekt een procedurebeschrijving voor:

- het schriftelijk informeren van het CIOT ingeval van een calamiteit;
- de registratie van het aantal NAW verzoeken en de registratie van voorkomende redenen;
- de beoordeling van de aanlevering van het klantenbestand, de analyse en te rapporteren over waarborgen.

We hebben vastgesteld dat beide aanbieders in de praktijk wel een registratie bijhouden van het aantal N.A.W. verzoeken naar aanleiding van een no-hit. Bij één aanbieder hebben we ten aanzien van de aanlevering een afwijking op de SLA geconstateerd.

Bij één aanbieder zijn de toegangsrechten in de directory van het klantenbestand te ruim ingeregeld. Bij de andere aanbieder konden we dat niet vaststellen in verband met het ontbreken van een autorisatiematrix.

Incidenten en wijzigingen worden bij beide aanbieders niet op basis van een beschreven incidenten- en wijzigingenproces gemeld en verwerkt.

1 Aanleiding opdracht

Aanbieders van een openbaar telecommunicatienetwerk of een openbare telecommunicatiedienst zijn wettelijk verplicht om de gegevens als bedoeld in artikel 13.4, eerste lid van de Telecommunicatiewet juncto artikel 4 van het Besluit – zoals bijvoorbeeld naam, adres, postcode, woonplaats, nummer en soort dienst van gebruikers – beschikbaar te stellen behoeve van opsporingsactiviteiten.

Aanbieders van openbare telecommunicatienetwerken (zoals providers van internet en telefonie) zijn wettelijk verplicht om elke 24 uur een actueel databestand met klantgegevens aan te leveren aan het CIOT.

De dgRR heeft de Auditdienst Rijk (ADR) gevraagd onderzoek te doen naar de maatregelen van de verstrekking van deze gegevens door de aanbieders (telecomproviders). De ADR heeft hiertoe in de maanden maart t/m juni 2019 onderzoek uitgevoerd bij een tweetal door de opdrachtgever bepaalde aanbieders. Op basis van de afspraken met opdrachtgever worden de aanbieders geanonimiseerd opgenomen in deze rapportage.

Over de afwijkingen op de onderzochte normen wordt in deze rapportage feitelijk en op hoofdlijnen gerapporteerd. Het rapport verschaft geen zekerheid, omdat er geen assurance-opdracht is uitgevoerd.

De feitelijke bevindingen van dit onderzoek met betrekking tot de aanbieders worden per onderwerp gegroepeerd weergegeven in hoofdstuk 2. De verantwoording van het onderzoek is in hoofdstuk 3 beschreven. Hoofdstuk 4 betreft de ondertekening. Bijlage 1 bevat de managementreactie van de DGRR op dit onderzoek.

2 Feitelijke bevindingen

Dit hoofdstuk bevat de feitelijke bevindingen en geconstateerde afwijkingen van alle normen en geeft antwoord op de volgende onderzoeksvraag:

> *Welke maatregelen zijn door de aanbieder getroffen om te waarborgen dat voldaan wordt aan het Besluit en overeengekomen afspraken?*

De afwijkingen worden in deze rapportage op hoofdlijnen beschreven en voor een volledig en gedetailleerd overzicht verwijzen wij u naar de bevindingenmatrix die separaat voor beide aanbieders zijn opgesteld.

Bij het weergeven van de feitelijke bevindingen in onderstaande paragrafen volgen wij de volgorde van behandelde onderwerpen uit het referentiekader zoals beschreven in paragraaf 3.2.

2.1 Geheimhouding is geregeld in de arbeidsovereenkomst of gedragscode; de naleving hiervan is bij één aanbieder niet aantoonbaar

Norm: Er is een proces ingericht waarin waarborgen zijn getroffen om te voldoen aan de geheimhoudingsplicht van de aanbieder. Het verloop van dit proces en de waarborgen hierin worden regelmatig beoordeeld. De geheimhoudingsplicht wordt aantoonbaar nageleefd.

Beide aanbieders hebben de geheimhouding voor medewerkers die betrokken zijn bij het aanleverproces aan het Centraal Informatiepunt Onderzoek Telecommunicatie (CIOT) geregeld in het generieke HR-proces middels de arbeidsovereenkomst of gedragscode. We hebben vastgesteld dat één aanbieder een periodieke training met aandacht voor het naleven van de gedragscode verplicht stelt waarin medewerkers worden getoetst. De naleving van de geheimhoudingsplicht is bij de andere aanbieder niet aantoonbaar. Het generieke HR-proces en de beoordeling van de waarborgen omtrent geheimhouding zijn niet onderzocht omdat het buiten de scope van het onderzoek valt.

Risico: inbreuk op de geheimhoudingsplicht met als gevolg het bewust lekken of de manipulatie van gegevens. Vanwege de verplichting tot het aanleveren van een verklaring omtrent het gedrag (VOG) voor nieuwe medewerkers en het verkrijgen van een verklaring van geen bezwaar (VGB) voor medewerkers die werken met hoog vertrouwelijke informatie wordt dit als een beperkt risico ingeschat.

2.2 Het direct na constatering schriftelijk informeren van het CIOT en het in onderling overleg nemen van maatregelen is niet opgenomen in een procedure

Norm: In geval van overmacht (bijv. na een calamiteit) is er een procedure die waarborgt dat de aanbieder het CIOT direct na constatering schriftelijk informeert en in onderling overleg maatregelen neemt om de gevolgen hiervan te beperken.

In geval van overmacht (wanneer bijvoorbeeld door een storing geen gebruik mogelijk is van de CIOT-omgeving) hebben beide providers een procedure die voorziet in de handmatige verwerking van bevragingen en verstrekking aan de aanvragende partij om zo toch aan het verzoek om informatie te kunnen voldoen. In de procedure is niet opgenomen dat IBO wordt geïnformeerd over de calamiteit en ook niet dat in overleg tussen aanbieder en IBO maatregelen worden getroffen om de gevolgen te beperken.

Een situatie van overmacht heeft zich in 2018 voor beide aanbieders niet voorgedaan. Hierdoor is het bestaan van deze norm niet onderzocht.

Risico: ingeval van een calamiteit wordt IBO niet tijdig geïnformeerd waardoor IBO te laat in staat wordt gesteld om maatregelen te treffen om de gevolgen te beperken.

2.3 De registratie van het aantal NAW verzoeken en de registratie van voorkomende redenen is niet opgenomen in een procedure

Norm: Er is een procedure ingericht waarin waarborgen zijn opgenomen zodat no-hit bevragingen kunnen worden afgehandeld en deze bevat tenminste hoe de no-hit procedure m.b.t. het CIOT Informatie Systeem (CIS) is ingericht; een registratie van het aantal N.A.W. verzoeken naar aanleiding van een no-hit in CIS; indien alsnog informatie kan worden verstrekt, een registratie van voorkomende redenen dat de vraag in eerste instantie geen informatie heeft opgeleverd; inzicht in welke activiteiten naar aanleiding van een NAW vraag worden ondernomen.

Wanneer een aanvraag in het CIS geen resultaten oplevert, bijvoorbeeld doordat het bevraagde nummer geen klant is of omdat het telefoonnummer is gedeactiveerd (een zogenoemde no-hit bevraging) is er bij beide aanbieders een procedure om deze no-hit bevraging te kunnen afhandelen. Deze procedure geeft inzicht in welke activiteiten naar aanleiding van een bevraging (N.A.W. verzoeken) worden ondernomen.
We hebben vastgesteld dat de afhandeling van een no-hit bevraging navolgbaar is en in lijn is met de in de procedures beschreven stappen.

De registratie van het aantal NAW verzoeken naar aanleiding van een no-hit in het CIS en van voorkomende redenen dat de vraag in eerste instantie geen informatie heeft opgeleverd bij te houden, is in beide no-hit procedures niet opgenomen.

We hebben vastgesteld dat beide aanbieders in de praktijk alleen een registratie bijhouden van het aantal N.A.W. verzoeken naar aanleiding van een no-hit in het CIS. Een registratie van voorkomende redenen dat de vraag in eerste instantie geen informatie heeft opgeleverd, wordt in de praktijk niet bijgehouden.

Risico: het niet bijhouden van een registratie van redenen betekent dat er niet gestuurd kan worden op verbeteringen om dit op te lossen.

2.4 De beoordeling, analyse en rapportage van waarborgen van aanlevering van het klantenbestand zijn niet beschreven. Eén aanbieder heeft een afwijking op de SLA.

Norm: Er is een procedure ingericht om te kunnen voldoen aan de vereisten van de levering van gegevens zoals in het Besluit is opgenomen. In de procedure zijn waarborgen getroffen voor het juist, volledig en tijdig aanleveren van alle gegevens zoals telefoonnummers, IP-adressen en NAW-klantgegevens.

Beide aanbieders hebben de dagelijks verplichte gegevensaanlevering opgenomen in een procedurebeschrijving als een geautomatiseerd proces dat dagelijks wordt uitgevoerd. Deze procedure gaat in op de getroffen waarborgen voor het juist, volledig en tijdig aanleveren van alle klantgegevens.

Juistheid, volledigheid en tijdigheid
Beide aanbieders hebben in een handleiding opgenomen dat de brondata van het klantenbestand een exacte weergave is van de data zoals verstrekt aan het CIOT. Om een correct bestand op te leveren dient het samen te stellen klantenbestand aan een aantal voorwaarden te voldoen. Wanneer niet is voldaan aan de voorwaarden, is verwerking van de gegevens niet mogelijk (zie ook paragraaf 2.5

en 2.6). Daarnaast is opgenomen dat elke dienstaanbieder per nummersoort elke 24 uur een compleet en actueel klantenbestand dient aan te leveren.
Bij één aanbieder is de aanleverfrequentie van 98% in de Service Level Agreement beschreven. Bij de andere aanbieder is de in de norm vereiste jaarlijkse aanleverfrequentie van 98% beschreven in de Diensten Niveau Overeenkomst (DNO).

We hebben vastgesteld dat beide klantenbestanden de in de norm genoemde velden naam, adres, woonplaats, postcode, aansluitnummer, soort telecommunicatiedienst en de identiteit van de telecommunicatieaanbieder bevatten en dat de door het CIOT voorgeschreven validatie van opmaak en velden (op basis van XSD) is uitgevoerd.

Bij één aanbieder hebben wij vastgesteld dat in 2018 in de praktijk niet wordt voldaan aan de minimale aanleverfrequentie van 98%.

Risico: onjuiste, onvolledige of niet tijdige aanlevering van het klantenbestand.

2.5 Verstrekking klantenbestand geschiedt overeenkomstig standaarden

Norm: De verstrekking geschiedt zo veel mogelijk overeenkomstig de standaarden NEN 1888 (persoonsgegevens) en NEN 5825 (adressen). Indien deze standaarden niet worden gehanteerd, worden door de aanbieder niet gebruikte velden in het bestand <<leeg>> genomen. Het verloop van de waarborgen wordt regelmatig beoordeeld.

Bij beide aanbieders is er een handleiding voor het samenstellen van het klantenbestand gebaseerd op de standaarden NEN 1888 (persoonsgegevens) en NEN 5825 (adressen). Hierin opgenomen is de waarborg om aan de hand van z.g. XSD-schema's de opmaak van gegevens automatisch te controleren voordat het klantenbestand wordt aangeleverd. In de handleiding staat onder meer wat de elementen zijn van het klantenbestand, waar zij voorkomen en wat de kenmerken zijn waaraan ze moeten voldoen.

We hebben vastgesteld dat de velden naam, adres, woonplaats, postcode, aansluitnummer, soort telecommunicatiedienst en de identiteit van de telecommunicatieaanbieder conform de NEN 1888 en NEN 5825 zijn opgebouwd in beide klantenbestanden. Daarnaast hebben we vastgesteld dat beide klantenbestanden worden gespecificeerd en gevalideerd op basis van XSD-schema's. Vanwege de geautomatiseerde validatiehandeling vindt geen regelmatige beoordeling van het verloop van waarborgen plaats.

2.6 Klantenbestanden worden aangeleverd conform de voorgeschreven tekenset

Norm: De aanbieder maakt gebruik van de tekenset <<Extended ASCII>> die is voorzien van veld -en recordscheiding. De aanbieder draagt zorg voor goed leesbare gegevens.

Bij beide aanbieders is er een handleiding voor het samenstellen van het klantenbestand. Hierin is beschreven dat er wordt uitgegaan van de ISO 10646 UTF-8 (NEN-ISO/IEC 10646)[1] als de te gebruiken tekenset.

We hebben vastgesteld dat beide aanbieders gebruik maken van de UTF-8 tekenset voor het klantenbestand.

[1] Voor dit onderzoek gaan we ervan uit dat in (extended) ASCII gecodeerde tekst ongewijzigd geldig is als UTF-8-tekst

2.7 Verstrekking klantenbestand via informatiedrager op basis van een beveiligde netwerkverbinding

Norm: De aanbieder maakt gebruik van een informatiedrager die functioneel is voor de interface. Bij voorkeur wordt gebruik gemaakt van een beveiligde netwerkverbinding (zoals de koppelvlakstandaard ebMS voor berichtenuitwisseling over de Digikoppeling).

Beide aanbieders hebben in ontwerpdocumentatie opgenomen dat aanlevering van het klantenbestand aan het CIOT via het EbXML-protocol dient te gebeuren op basis van een beveiligde verbinding.

We hebben vastgesteld dat beide aanbieders de klantgegevens aanleveren via de Digikoppeling aan de JUstitie BErichten Service (JUBES), conform het open standaard ebusiness XML-messaging standaard (ebMS) protocol. In beide gevallen wordt gebruik gemaakt van een interface die de beveiligde verzending van het klantenbestand met behulp van het versleutelingsprotocol (HTTPS) borgt.

HTTPS maakt voor de versleuteling gebruik van SSL of TLS. Het NCSC geeft in de 'ICT-beveiligingsrichtlijn voor TLS' aan dat TLS de communicatie tussen een cliënt en een server beschermt maar dat de oudste versies van TLS (SSL 2.0 en SSL 3.0) niet veilig zijn in het gebruik[2].
We hebben vastgesteld bij één aanbieder dat de SSL-parameters dusdanig zijn geconfigureerd dat ondersteuning voor SSL 2.0 en 3.0 is uitgeschakeld en dat de ondersteuning voor TLS 1.0, TLS 1.1 en TLS 1.2 is ingeschakeld. Bij de andere aanbieder hebben we niet kunnen vaststellen welke SSL-parameters in gebruik zijn.

Risico: mogelijk wordt er bij één aanbieder met verouderde algoritmes gewerkt (SSL 2.0 en SSL 3.0) waarvan bekend is dat deze kwetsbaarheden bevatten.

2.8 Ongeautoriseerde toegang tot de verbinding middels versleuteling afgedwongen. Toegangsrechten in de directory van het klantenbestand te ruim ingeregeld. Eén aanbieder mist een autorisatiematrix.

Norm: De gegevens worden zodanig verstrekt dat ongeautoriseerde toegang tot zowel het bestand als de verbinding niet mogelijk is en dat de integriteit en de onaantastbaarheid van het bestand verzekerd is.

Bij één aanbieder is in het beveiligingsbeleid opgenomen dat de toewijzing van toegangsrechten gebaseerd is op de individuele taken en de noodzaak om toegang te krijgen tot een specifiek gegeven op basis van de 'need-to-know' en 'least privileged' principes. De andere aanbieder heeft in het toegangsbeleid opgenomen dat de toegang beperkt wordt tot geautoriseerde en geregistreerde gebruikers en dat toegang alleen wordt toegekend op het minimumniveau dat vereist is voor de noodzakelijke uitvoering van taken, op basis van het 'least privileged' principe.

Om inzicht te krijgen in de benodigde toegangsrechten (inzien en bewerken) heeft één aanbieder voor het aanleveringsproces aan het CIOT een autorisatiematrix opgesteld. We hebben vastgesteld dat de toegangsrechten in de directory van het klantenbestand bij deze aanbieder te ruim zijn ingeregeld en niet in lijn zijn met de autorisatiematrix.
We hebben vastgesteld dat de toegangsrechten op het klantenbestand bij de tweede aanbieder beperkt is tot een aantal medewerkers. Wegens het ontbreken van een autorisatiematrix bij deze aanbieder hebben we niet kunnen vaststellen of de rechten op het klantenbestand conform het toegangsbeleid zijn ingeregeld.

[2] https://www.ncsc.nl/documenten/publicaties/2019/mei/01/ict-beveiligingsrichtlijnen-voor-transport-layer-security-tls

Het NCSC geeft in de 'ICT-beveiligingsrichtlijn voor TLS' aan dat het gebruik van TLS bij een versleutelde verbinding waarborgt dat de verstuurde gegevens tijdens het transport niet door derden bekeken (vertrouwelijkheid) of gewijzigd (integriteit) kunnen worden[3]. We hebben vastgesteld dat beide aanbieders het klantenbestand versleuteld opslaan voordat verzending plaatsvindt en dat verzending op basis van het TLS-protocol geschiedt (zie ook paragraaf 2.7).

Risico: door het ontbreken van een autorisatiematrix bij één aanbieder is er geen inzicht in de benodigde toegangsrechten (inzien en bewerken) waardoor de toegangsrechten niet gevalideerd konden worden. Bij de andere aanbieder hebben onbevoegden door de ruimere inrichting van de toegangsrechten mogelijk inzage in gegevens ingezien of kunnen deze manipuleren.

2.9 Geen specifiek incident- en wijzigingsproces voor het aanleverproces; in de onderzoeksperiode waren er geen incidenten en wijzigingen op het aanleverproces

Norm: Er is een incidentenproces ingericht om incidenten van de aanbieder aan het CIOT te melden en te verwerken. Het proces is ook ingericht om incidenten te verwerken die door het CIOT zijn gemeld aan de aanbieder.
Norm: Alle beveiligingsincidenten met betrekking tot het CIOT Informatiesysteem, de toegang daartoe of het genereren van de klantenbestanden moeten onverwijld gemeld worden bij het CIOT. Het verloop wordt regelmatig beoordeeld.

Norm: Er is een wijzigingenproces ingericht om geplande wijzigingen die van invloed kunnen zijn op het aanleveren van het klantenbestand door de aanbieder en/of de beschikbaarheid van het CIS te beheersen. Deze worden aangekondigd bij de CIOT Servicedesk. Dit proces is ingericht, navolgbaar en over het verloop hiervan wordt gerapporteerd. Het verloop van dit proces en de waarborgen hierin worden regelmatig beoordeeld.

Beide aanbieders hanteren voor de afhandeling van incidenten of de uitvoering van wijzigingen geen specifiek incident- en wijzigingsproces voor het aanleveringsproces aan het CIOT. Als reden geven de aanbieders aan de lage frequentie van optreden (1x per jaar). Bij beide aanbieders is er wel een generiek incident- en wijzigingsproces voor de afhandeling van andere soorten incidenten en andere geplande wijzigingen maar deze worden niet gehanteerd om incidenten en wijzigingen aan IBO te melden en te verwerken.
Eén van de aanbieders heeft een instructie opgesteld die ingaat op de operationele verstoringen binnen de CIOT-omgeving en bevat operationele instructies ingeval van een incident.

Gedurende de onderzoeksperiode hebben zich geen incidenten en wijzigingen met betrekking tot het aanleverproces van het klantenbestand voorgedaan. De aanbieders hebben aangegeven dat eventuele incidenten en wijzigingen met betrekking tot het aanleverproces die worden gemeld worden opgepakt en worden afgehandeld. Dit hebben we wegens het ontbreken van een incident of wijziging tijdens de onderzoeksperiode niet vast kunnen stellen.

Bij beide leveranciers hebben we vastgesteld dat naar aanleiding van een fout in de aanlevering van het klantenbestand er communicatie is geweest met het CIOT en de leverancier voor een analyse van het probleem en het verhelpen van de storing.

Risico: door het niet werken volgens een procedure kunnen incidenten of wijzigingen blijven liggen, ontbreekt registratie of mist bevoegdheid. In geval van

[3] https://www.ncsc.nl/documenten/publicaties/2019/mei/01/ict-beveiligingsrichtlijnen-voor-transport-layer-security-tls

de aanbieders is de frequentie van optreden dermate laag dat het niet rendabel is om een specifiek proces hiervoor in te richten. We achten het risico dan ook klein.

3 Verantwoording onderzoek

3.1 Doelstelling

Het doel van het onderzoek is om inzicht te geven in de kwaliteit van de maatregelen die de aanbieder heeft getroffen, zodat deze kan voldoen aan de wetgeving en de met Justid overeengekomen afspraken, zoals deze zijn opgenomen in de Dienstniveau-, de audit- en de verwerkersovereenkomsten.

De DGRR kan op basis van dit onderzoek de minister van Justitie en Veiligheid informeren om deze in staat te stellen verslag te doen aan de Tweede Kamer conform de wettelijke bepaling in artikel 8 van het Besluit verstrekking gegevens telecommunicatie.

In dit onderzoek wordt de volgende onderzoeksvraag beantwoord:

> *Welke maatregelen zijn door de aanbieder getroffen om te waarborgen dat voldaan wordt aan het Besluit en overeengekomen afspraken?*

3.2 Werkzaamheden en periode van uitvoering

Voor dit onderzoek zijn gedurende de periode maart 2019 t/m juni 2019 documenten geanalyseerd, interviews gehouden en zijn waarnemingen ter plaatse uitgevoerd.
De ADR heeft voor dit onderzoek in samenwerking met de opdrachtgever een referentiekader ontwikkeld gebaseerd op de overeengekomen afspraken vastgelegd in de DNO Aanbieder en Justitiële Informatiedienst en het Besluit verstrekking gegevens telecommunicatie. Het referentiekader is als bijlage 2 bijgevoegd. Dit referentiekader is voorafgaand aan het onderzoek met de opdrachtgever afgestemd en omvat de volgende onderwerpen:

- Geheimhouding (norm 1)
- Procedures met betrekking tot de aanlevering:
  - Overmacht procedure (norm 2);
  - No-hit procedure (norm 3).
- Verstrekking gegevens:
  - Verplichte gegevensaanlevering (norm 4);
  - Standaarden (norm 5 en 6);
  - Beveiligde netwerkverbinding (norm 7).
- Vertrouwelijkheid van gegevens (norm 8).
- Beheerprocessen:
  - Incidentmanagement (norm 9 en 10);
  - Wijzigingenbeheer (norm 11).

De conceptbevindingen uit ons onderzoek zijn in het kader van hoor wederhoor op 5 september 2019 en op 25 september 2019 respectievelijk met de aanbieders besproken. Voor zover de opmerkingen betrekking hadden op feitelijke onjuistheden zijn deze aangepast in de bevindingenmatrix. De definitieve bevindingenmatrixen zijn in oktober 2019 aan de aanbieders aangeboden.

3.3 Context

Elke aanbieder heeft met de Staat, namens deze de directeur Justitiële Informatiedienst (Justid) van het ministerie van Veiligheid en Justitie, een Dienstniveau Overeenkomst 'Aanbieder en Justitiële Informatiedienst' (hierna DNO) en een verwerkersovereenkomst gesloten. Met de Directeur-Generaal Rechtspleging en Rechtshandhaving (DGRR) is een auditovereenkomst overeengekomen. In deze overeenkomsten zijn de nadere afspraken en verantwoordelijkheden opgenomen.

De afspraken in de DNO tussen de aanbieder en Justid en het Besluit worden getoetst in dit onderzoek.

Als onderdeel van de Justitiële Informatiedienst (Justid) van het ministerie van Justitie en Veiligheid voert IBO voor de productlijn CIOT het technisch beheer, functioneel beheer en applicatiebeheer uit. IBO beheert het geautomatiseerde informatiesysteem CIOT-informatiesysteem (CIS) voor de persoonsgegevens die horen bij IP-adressen, telefoonnummers en e-mailadressen. Opsporingsdiensten, veiligheidsdiensten en inlichtingendiensten kunnen het CIS bevragen op nadere informatie ten behoeve van hun opsporingsactiviteiten

3.4 Object van onderzoek en afbakening

Het onderzoek wordt uitgevoerd bij een tweetal door de opdrachtgever bepaalde aanbieders en richt zich op processen en maatregelen die de aanbieder heeft ingericht om te kunnen voldoen aan de eisen en afspraken uit het Besluit inzake de aanlevering van telecomgegevens aan het CIOT.

De ADR heeft onderzoek gedaan naar opzet en bestaan van de getroffen maatregelen voor de in paragraaf 3.2 genoemde onderwerpen. De peildatum voor vaststelling van de opzet en het bestaan is december 2018.

Onder opzet verstaan we dat organisatorische processen en procedures zijn gedocumenteerd. Onder bestaan verstaan we dat de processen en procedures daadwerkelijk zijn ingericht conform de opzet.

3.5 Gehanteerde Standaard en Kwaliteitsborging

Deze opdracht is uitgevoerd in overeenstemming met de Internationale Standaarden voor de Beroepsuitoefening van Internal Auditing (Standaarden IIA 2200-2440 en 2600).

In dit rapport wordt geen zekerheid verschaft, omdat er geen assurance-opdracht is uitgevoerd. Het rapport bevat de feitelijke bevindingen van het uitgevoerde onderzoek.

De opdracht is uitgevoerd conform de bij de ADR geldende kwaliteitsrichtlijnen. Het voor dit onderzoek aangelegde dossier is conform deze richtlijnen ingericht en blijft eigendom van de ADR.

De interne Opdrachtgerichte Kwaliteitsbeoordeling (OKB) waarborgt de kwaliteit van de producten. Deze is uitgevoerd door een onafhankelijke kwaliteitsbeoordelaar van de ADR, welke niet betrokken is geweest bij de uitvoering van het onderzoek.

3.6 Verspreiding rapport

De opdrachtgever [redacted] Directeur-Generaal Rechtspleging en Rechtshandhaving, is eigenaar van dit rapport. De opdrachtgever is verantwoordelijk voor de verdere verspreiding van het rapport.

De ADR is de interne auditdienst van het Rijk. Dit rapport is primair bestemd voor de opdrachtgever met wie wij deze opdracht zijn overeengekomen. In de

ministerraad is besloten dat het opdrachtgevende ministerie waarvoor de ADR een rapport heeft geschreven, het rapport binnen zes weken op de website van de rijksoverheid plaatst, tenzij daarvoor een uitzondering geldt. De minister van Financiën stuurt elk halfjaar een overzicht naar de Tweede Kamer met de titels van door de ADR uitgebrachte rapporten en plaatst dit overzicht op de website.

4 Ondertekening

Den Haag, 20 januari 2020

IT-Auditor

Auditdienst Rijk

Bijlage 1 Managementreactie opdrachtgever

Ministerie van Justitie en Veiligheid

Retouradres Postbus 20301 2500 EH Den Haag

Directoraat-Generaal Rechtspleging en Rechtshandhaving
Directie Rechtshandhaving en Criminaliteitsbestrijding
Cluster Fraude en Ordening

Turfmarkt 147
2511 DP Den Haag
Postbus 20301
2500 EH Den Haag
www.rijksoverheid.nl/jenv

Contactpersoon
[redacted]

Ons kenmerk
2773192

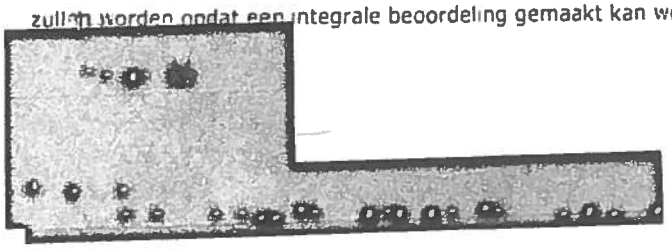
Bij beantwoording de datum en ons kenmerk vermelden. Wilt u slechts één zaak in uw brief behandelen

Datum 10 januari 2020
Onderwerp Managementreactie op audit CIOT aanbieders 2018

De minister van Justitie en Veiligheid is conform artikel 8 tweede lid van het Besluit Verstrekking Gegevens Telecommunicatie gehouden jaarlijks een verslag op te stellen van een audit naar de goede uitvoering van het besluit door aanbieders van openbare telecommunicatiediensten of -netwerken, het informatiepunt, de arrondissementsparketten en de politiekorpsen, of andere opsporingsdiensten. In opdracht van de directeur-generaal Rechtspleging en Rechtshandhaving is derhalve onderzoek gedaan naar de maatregelen die worden genomen bij de verstrekking van deze gegevens bij enkele aanbieders (telecomproviders).

Ik heb kennisgenomen van het concept "Onderzoeksrapport CIOT-aanbieders 2018". Ik stel vast dat u met succes inzicht heeft kunnen verschaffen in de vraag naar de maatregelen die zijn getroffen om te waarborgen dat wordt voldaan aan het Besluit Verstrekking gegevens Telecommunicatie en de overeengekomen afspraken. Met de aanbieders zal worden besproken hoe mogelijke verbeteringen ter hand zullen worden genomen.

Uw bevindingen uit dit onderzoek zullen betrokken worden bij het brede verslag dat opgesteld zal worden naar aanleiding van dit onderzoeksrapport, waarin tevens de bevindingen uit de door u opgeleverde onderzoeken en het nog af te ronden onderzoek van de politie ten aanzien van de CIOT bevragingen betrokken zullen worden opdat een integrale beoordeling gemaakt kan worden.



Bijlage 2 Referentiekader CIOT Aanbieders

Nr.	Norm
1	**Geheimhoudingsplicht aanbieder** Er is een proces ingericht waarin waarborgen zijn getroffen om te voldoen aan de geheimhoudingsplicht van de aanbieder. Het verloop van dit proces en de waarborgen hierin worden regelmatig beoordeeld. De geheimhoudingsplicht wordt aantoonbaar nageleefd.
2	**Overmacht procedure** In geval van overmacht (bijv. na een calamiteit) is er een procedure die waarborgt dat de aanbieder het CIOT direct na constatering schriftelijk informeert en in onderling overleg maatregelen neemt om de gevolgen hiervan te beperken.
3	**No-hit procedure** Er is een procedure ingericht waarin waarborgen zijn opgenomen zodat no-hit bevragingen kunnen worden afgehandeld. Met daarin tenminste: • Hoe de no-hit procedure m.b.t. het CIS is ingericht; • Registratie van het aantal NAW verzoeken naar aanleiding van een no-hit in CIS; • Indien alsnog informatie kan worden verstrekt, een registratie van voorkomende redenen dat de vraag in eerste instantie geen informatie heeft opgeleverd; • Inzicht in welke activiteiten naar aanleiding van een NAW vraag worden ondernomen.
4.	**Verplichte gegevensaanlevering** Er is een procedure ingericht om te kunnen voldoen aan de vereisten van de levering van gegevens zoals in het Besluit is opgenomen. In de procedure zijn waarborgen getroffen voor het juist, volledig en tijdig aanleveren van alle gegevens zoals telefoonnummers, IP-adressen en NAW-klantgegevens. <u>Juistheid</u> Het aangeleverde klantenbestand is een 100% getrouwe afspiegeling van het bronbestand. De aanbieder verstrekt de gegevens die in de bedrijfsvoering zijn opgenomen. <u>Volledigheid</u> Het bestand voldoet aan de in het Besluit gestelde eisen en bevat tenminste: • naam; • adres; • woonplaats; • postcode; • aansluitnummer; • soort telecommunicatiedienst; • de identiteit van de telecommunicatieaanbieder. <u>Tijdigheid</u> Er is een vaste periodiciteit voor aanlevering van klantgegevens aan het CIS.

	Aanlevering vindt 1x per 24 uur plaats. Op jaarbasis moet minimaal een aanleverfrequentie van 98% worden behaald. Het verloop van dit proces en de waarborgen hierin worden regelmatig beoordeeld, geanalyseerd en er wordt over gerapporteerd.
5	**Standaarden voor verstrekking van de gegevens** De verstrekking geschiedt zo veel mogelijk overeenkomstig de standaarden NEN 1888 (persoonsgegevens) en NEN 5825 (adressen). Indien deze standaarden niet worden gehanteerd, worden door de aanbieder niet gebruikte velden in het bestand <<leeg>> genomen. Het verloop van de waarborgen worden regelmatig beoordeeld.
6	**Standaard voor de tekenset** De aanbieder maakt gebruik van de tekenset <<Extended ASCII>> die is voorzien van veld -en recordscheiding. De aanbieder draagt zorg voor goed leesbare gegevens.
7	**Informatiedrager** De aanbieder maakt gebruik van een informatiedrager die functioneel is voor de interface. Bij voorkeur wordt gebruik gemaakt van een beveiligde netwerkverbinding (zoals de koppelvlakstandaard ebMS voor berichtenuitwisseling over de Digikoppeling).
8	**Betrouwbaarheid bestand** De gegevens worden zodanig verstrekt dat: • ongeautoriseerde toegang tot zowel het bestand als de verbinding niet mogelijk is; • de integriteit en de onaantastbaarheid van het bestand verzekerd is (zoals de controle op malware).
9	**Incidentenproces** Er is een incidentenproces ingericht om incidenten van de aanbieder aan IBO te melden en te verwerken. Het proces is ook ingericht om incidenten te verwerken die door IBO zijn gemeld aan de aanbieder. Dit proces is ingericht, navolgbaar en over het verloop hiervan wordt gerapporteerd. Het verloop van dit proces en de waarborgen hierin worden regelmatig beoordeeld.
10	**Incidenten Aanbieder** <u>(Beveiligings) Incidenten Aanbieder</u> Alle beveiligingsincidenten met betrekking tot het CIOT Informatiesysteem, de toegang daartoe of het genereren van de klantenbestanden moeten onverwijld gemeld worden bij het CIOT. Het verloop wordt regelmatig beoordeeld.
11	**Wijzigingsproces** Er is een wijzigingenproces ingericht om geplande wijzigingen die van invloed kunnen zijn op het aanleveren van het klantenbestand door de aanbieder en/of de beschikbaarheid van het CIS te beheersen. Deze worden aangekondigd bij de CIOT Servicedesk. Dit proces is ingericht, navolgbaar en over het verloop hiervan wordt gerapporteerd. Het verloop van dit proces en de waarborgen hierin worden regelmatig beoordeeld.

Auditdienst Rijk
Postbus 20201
2500 EE Den Haag
(070) 342 77 00