Agentschap Telecom
Ministerie van Economische Zaken, Landbouw en Innovatie

Toezicht Dataretentie en het verwerken van persoons-en locatiegegevens voor bedrijfsdoeleinden

De 1-meting

Colofon

Aan	Hoofd Toezicht Team Informatieveiligheid
Bewerkt door	[redacted]
Nummer	Versie 1.7
Datum	26 april 2012

Samenvatting

Sinds september 2009 is de Wet bewaarplicht telecommunicatiegegevens van kracht. Bij de behandeling van deze wet in de Eerste Kamer heeft de toenmalige Minister van Justitie de toezegging gedaan dat Agentschap Telecom een 0-meting zou houden. Van deze 0-meting is in mei 2010 een eindrapport openbaar gemaakt en aangeboden aan de Eerste Kamer.

In navolging van de 0-meting is eind 2010 de 1-meting gehouden op basis van het 'Toezichtarrangement Dataretentie'. Het doel is om te onderzoeken hoe de stand van zaken is met betrekking tot de naleving van de wetgeving op dat moment.

De opzet van beide metingen is niet identiek, maar kent wel een overlap. Bij de 0-meting is gekeken naar de Internet Service Providers die op dat moment in 2009 bij de Openbare Post en Telecommunicatie Autoriteit (hierna: OPTA) zijn geregistreerd. Bij de 1-meting zijn alle op dat moment bij de OPTA geregistreerde aanbieders van openbare elektronische communicatie netwerken en/of diensten als doelgroep meegenomen. Daarnaast zijn in de 1-meting de verplichte beveiligingswaarborgen uitgebreider onderzocht. Bovendien is ook de verwerking van verkeersgegevens en locatiegegevens voor bedrijfsdoeleinden onderzocht. Agentschap Telecom houdt hierop eveneens toezicht, met ingang van de invoering van dataretentie.

Het onderzoek is uitgevoerd op basis van een enquête met gesloten vragen. Aanbieders zijn volgens de Telecommunicatiewet verplicht de gevraagde informatie te verstrekken. Een klein aantal heeft niet gereageerd, waarna een bestuursrechtelijk sanctietraject is gestart. De antwoorden van 229 aanbieders zijn volledig in deze rapportage verwerkt.

De onderzoeksvragen, bevindingen en conclusies van de 1-meting zijn hieronder beknopt weergegeven.

1. Dataretentie

Wat is de situatie bij de aanbieders wat betreft de realisatie van de bewaarplicht?
Het onderzoek wijst uit dat de Wet bewaarplicht door een groot deel van de aanbieders geheel of gedeeltelijk is geïmplementeerd.
De naleving van de wet op het gebied van bewaren en beveiligen van gegevens is bij de grote aanbieders goed geregeld. Dit is belangrijk omdat de behoeftestellers, zoals de inlichtingen en veiligheidsdiensten, het merendeel van de inlichtingenverzoeken aan deze groep richten;

Wanneer denkt men te voldoen aan de verplichting van de Wet bewaarplicht?
De aanbieders die de verplichtingen op dit gebied nog niet naleven, geven aan uiterlijk in 2012 aan de wet te kunnen voldoen.
In 2010 moesten voor het eerst de opgeslagen gegevens worden vernietigd, omdat sinds inwerkingtreding van de wet de eerste bewaartermijn van een jaar verliep. Dit proces verloopt goed bij de grote aanbieders, minder goed bij de middelgrote en kleinere operators. Er is wel een duidelijk verband met het verwerken van verkeers- en locatiegegevens voor bedrijfsdoeleinden. De gegevens die op basis van de Wet bewaarplicht moeten worden bewaard zijn vaak identiek aan de gegevens die worden verwerkt voor bedrijfsdoeleinden. Dat maakt dat bepaalde gegevens niet worden vernietigd maar verder worden gebruikt voor bedrijfsdoeleinden, hetgeen wettelijk is toegestaan.
De verplichting tot het tijdig vernietigen van de bewaarde gegevens wordt nageleefd bij de grote aanbieders, die het overgrote deel van de particuliere markt verzorgen. Echter, in veel gevallen is sprake van het langer bewaren van de opgeslagen gegevens met het oog op gebruik van bewaarde gegevens voor bedrijfsdoeleinden.

De kleine en middelgrote aanbieders vernietigen nog niet altijd conform de gestelde termijn.

2. Beveiliging

Is de beveiliging van de informatie en gegevens conform de Telecommunicatiewet en het Besluit beveiliging gegevens telecommunicatie (hierna: Bbgt) gewaarborgd?

Bij de 1-meting is gekeken naar het gehele (informatie) beveiligingsproces rond dataretentie.

De beveiliging van de gegevens bij de grote aanbieders is goed. Bij de middelgrote aanbieders is het beeld divers. Naarmate men zich bewuster wordt van het feit dat men dient te voldoen, gaat men op zoek naar systemen of methodieken. Dit leidt bijvoorbeeld tot invoering van een kwaliteitssysteem (zoals van ISO, de International Organization for Standardization) waarbij men ook de specifieke beveiligingsverplichtingen voor aftappen en dataretentie uit het Bbgt meeneemt. De kleine en een deel van de middelgrote aanbieders voldoen over het algemeen nog niet of niet geheel aan de minimale beveiligingsvereisten van de wet. Beveiligingsplannen zijn niet volledig en er is te weinig aandacht voor incidentbeheer.

3. Gebruik van verkeers- en locatiegegevens voor bedrijfsdoeleinden

Wat is de stand van zaken op het gebied van wetgeving met betrekking tot het verwerken van verkeers- en locatiegegevens voor bedrijfsdoeleinden?

De wetgeving die geldt voor verkeers- en locatiegegevens, gebruikt voor bedrijfsdoeleinden, is onvoldoende bekend bij de aanbieders en wordt niet voldoende nageleefd.

Het betreft zowel het op de juiste wijze, expliciet, vragen van toestemming, het duidelijk maken hoe lang deze gegevens dan wel worden bewaard en het bieden van de mogelijkheid de toestemming weer in te trekken. Tot slot is het van belang dat na afloop van de noodzaak van gebruik van zulke gegevens deze worden verwijderd of geanonimiseerd.

Inhoudsopgave

Verklaring van afkortingen

Bbgt	Besluit beveiliging gegevens telecommunicatie
CBP	College Bescherming Persoonsgegevens
CIOT	Centraal Informatiepunt Onderzoek Telecommunicatie
ETSI	European Telecommunications Standards Institute
ISO	International Organization for Standardization
ISP	Internet Service Provider
ITIL	Information Technology Infrastructure Library
MVNO	Mobile Virtual Network Operator
OPTA	Onafhankelijke Post en Telecommunicatie Autoriteit
Tw	Telecommunicatiewet

Inleiding

Sinds september 2009 is de Wet bewaarplicht telecommunicatiegegevens (hierna: Wet bewaarplicht) van kracht. Deze wet is een onderdeel geworden van hoofdstuk 13 van de Telecommunicatiewet (hierna: Tw). Omwille van de duidelijkheid wordt in dit document de term 'Wet bewaarplicht' gehanteerd. Bij de behandeling van deze wet in de Eerste Kamer heeft de Minister van Justitie de toezegging gedaan dat Agentschap Telecom een 0-meting zou uitvoeren onder Internet Service Providers. Dit onderzoek is gecombineerd met de aanvankelijk te houden 0-meting zoals deze is vastgelegd in het "Toezichtarrangement Dataretentie[1]". De Eerste Kamer was met name geïnteresseerd in de beveiligingswaarborgen en implementatie van dataretentie bij Internet Service Providers. Deze punten zijn in de 0-meting uitgevraagd. Van deze 0-meting is in mei 2010 een eindrapport openbaar gemaakt en aangeboden aan de Eerste Kamer.

Door middel van de 1-meting moet duidelijk worden in hoeverre niet alleen de Internet Service Providers, maar alle aanbieders van openbare telecommunicatienetwerken en/of -diensten (hierna: aanbieders) die bij de OPTA[2] staan geregistreerd de verplichtingen op het gebied van dataretentie en het gebruik van verkeers- en locatiegegevens voor bedrijfsdoeleinden naleven, één jaar na inwerkingtreding van de wet.

Op basis van de bevoegdheid van onze Minister om inlichtingen te vorderen heeft een enquête onder de aanbieders plaatsgevonden waarbij 21 vragen zijn gesteld. De set vragen is ingedeeld in drie categorieën: dataretentie, beveiliging en gebruik van verkeers- en locatiegegevens voor bedrijfsdoeleinden.
Na ontvangst van de antwoorden op de enquête, zijn de antwoorden verwerkt en geanalyseerd. De resultaten zijn terug te lezen in dit rapport.

Leeswijzer

In dit rapport worden de resultaten weergegeven die de 1-meting heeft opgeleverd. In hoofdstuk 1 worden de onderzoeksvragen en de methodiek van onderzoek toegelicht. Vervolgens beschrijft hoofdstuk 2 het verloop van het onderzoek. Het doel van het rapport wordt in hoofdstuk 3 toegelicht. De bevindingen over dataretentie worden in hoofdstuk 4 besproken. Hoofdstuk 5 bevat de bevindingen over de beveiliging bij de aanbieders. In hoofdstuk 6 worden de bevindingen op gebied van het gebruik van verkeers- en locatiegegevens voor bedrijfsdoeleinden toegelicht. De overige reacties op de enquête worden in hoofdstuk 7 weergegeven. De conclusies staan in hoofdstuk 8 en het rapport wordt afgesloten met aandachtspunten in hoofdstuk 9.

[1] http://www.agentschaptelecom.nl/binaries/content/assets/agentschaptelecom/Veiligheid/Toezichtsarrangement-Dataretentie.pdf
[2] Onafhankelijke Post en Telecommunicatie Autoriteit

1 Onderzoeksvragen en methodiek

In navolging van de 0-meting is eind 2010 de 1-meting gehouden op basis van het 'Toezichtarrangement Dataretentie'. De doelstelling van de 1-meting is om inzicht te krijgen in hoeverre aanbieders voldoen aan de wetgeving één jaar na inwerkingtreding. Tevens wordt het verkregen inzicht gebruikt als input voor het actualiseren van de risicoanalyse van de doelgroep, om het toezicht te optimaliseren. Het uitvoeren van de 1-meting is ook een middel om inzicht te krijgen wat het effect is geweest van de inspanningen van Agentschap Telecom op dit gebied. Door de resultaten van de 0-meting te vergelijken met de bijbehorende resultaten van de 1-meting kan het verschil in de mate van naleving worden bepaald. Dit zal overigens in een separaat onderzoek worden uitgevoerd. Daarmee ontstaat input voor de evaluatie van de gehanteerde interventiemix. Heeft elk soort interventie de effectiviteit gebracht die vooraf was aangenomen.
Zo niet, dan kan een andere interventie wellicht efficiënter of effectiever zijn. Uiteindelijk gaat het om het creëren van beweging richting meer (spontane) naleving

1.1 Onderzoeksvragen

Vanwege het feit dat de 1-meting een vervolg is op de 0-meting zijn de onderzoeksvragen vergelijkbaar met de vragen uit de 0-meting. Wel zijn extra vragen toegevoegd over het onderwerp 'gebruik van verkeersgegevens en locatiegegevens in verband met bedrijfsdoeleinden'. Het toezicht op deze al sinds 2004 bestaande wetgeving is georganiseerd naast het toezicht op dataretentie, in verband met de overeenkomsten van de data die wordt verwerkt en het vernietigen van zulke gegevens.
De onderzoeksvragen zijn:

1. Wat is de stand van zaken ten aanzien van de bewaarplicht; voldoen de aanbieders aan de verplichtingen? Wordt de verplichting eventueel uitbesteed aan derden? Indien nog niet wordt voldaan aan de Wet bewaarplicht, wanneer denkt men te voldoen aan deze verplichtingen op het gebied van bewaren en vernietigen?
2. Is de beveiliging van de informatie en gegevens conform de Telecommunicatiewet en het Besluit beveiliging gegevens telecommunicatie gewaarborgd?
3. Wat is de stand van zaken op gebied van de wetgeving over het verwerken van verkeers- en locatiegegevens?

Op basis van de bovenstaande vragen zijn 21 enquêtevragen opgesteld.

1.2 Methodiek van onderzoek

Om de benodigde informatie te verkrijgen is gekozen voor het verzenden van een enquête naar de netwerk- en dienstenaanbieders.
Om de betrouwbaarheid te verhogen bij de verwerking van de antwoorden is gewerkt met gesloten vragen. De aanbieders zijn wettelijk verplicht mee te werken aan de enquête.

Bepalen van de doelgroep
Er is voor gekozen om de gehele populatie, de bij OPTA ingeschreven aanbieders van openbare elektronische communicatienetwerken en/of diensten[3] (hierna: OPTA geregistreerde aanbieders), aan te schrijven. Dit is een grotere populatie dan de doelgroep van de 0-meting. Dit heeft twee redenen:
Ten eerste: vanwege het verzoek van de Eerste Kamer tot 0-meting onder Internet Service Providers (hierna: ISP's) is de doelgroep toen beperkt gebleven tot enkel ISP's. Voor het vervolg is het zaak nalevingsmetingen te doen over alle doelgroepen. Op de tweede plaats is de doelgroep sterk groeiend. Inmiddels is de omvang twee maal zo groot geworden.
Vooraf was reeds bekend dat niet alle OPTA geregistreerde aanbieders op basis van de door hun aangeboden diensten relevant zijn voor de eisen van de hoofdstukken 11 en 13 van de Tw. Bijvoorbeeld aanbieders van "dark fiber", IVR diensten (toets 1, toets 2 enz), call centre. Bij het begin van de enquête konden bedrijven dit aangeven door "anders" aan te vinken. Dit konden zij motiveren op basis van de door hen geleverde diensten.

Om te bepalen welke omvang een aanbieder heeft is ervoor gekozen de indeling aan te houden die de OPTA hanteert.

De OPTA hanteert een klasse in grootte naar aanleiding van de omzet van de aanbieders. Deze zijn:
- Klein: 0 - 2 miljoen euro
- Middel: 2 – 20 miljoen euro en
- Groot: 20 miljoen euro of meer

Mailing
Op 29 oktober 2010 is een brief verstuurd naar de aanbieders met als bijlage de enquête, (zie bijlage 1) bestaande uit 21 vragen en twee aanvullende verzoeken. In het schrijven is de aanbieders verzocht de vragen te beantwoorden en te retourneren binnen de gestelde termijn van drie weken. De aanvullende vragen betreffen het verkrijgen van een actuele versie van het beveiligingsplan en een lijst met de ketenpartners.

De hoofdonderwerpen zijn als volgt toegelicht in de brief:

Dataretentie
De Wet bewaarplicht, ook wel dataretentie genoemd, regelt onder meer een bewaartermijn voor internet- en telefoniegegevens.
Daarmee worden de zogenaamde verkeers- en locatiegegevens bedoeld en enkele identificerende gegevens die nodig zijn voor facturering. Bijvoorbeeld: wie belt met wie, op welk moment en vanaf welke locaties.
Het gaat overigens niet om de inhoud van de communicatie, dus wat er gezegd of geschreven wordt. Naast de bewaartermijn is ook bepaald dat de bewaarde gegevens en informatie beveiligd en uiteindelijk binnen een vastgestelde termijn moeten worden vernietigd.

Verwijderen / anonimiseren

[3] Zie voor registratieplicht: http://www.opta.nl/nl/registraties/geregistreerde-partijen/

Hoofdstuk 11 van de Tw[4] bevat onder meer regels over het verwerken van verkeers- en locatiegegevens die nodig zijn voor -kort gezegd- de zakelijke doeleinden van telecomaanbieders. Bijvoorbeeld voor de bedrijfsvoering van bij de OPTA geregistreerde aanbieders. Dit betreft bijvoorbeeld het overbrengen van communicatie, facturering, verkoopactiviteiten, enzovoort. Voor deze verkeersgegevens geldt geen verplichting tot bewaring, maar wel tot verwijderen of anonimiseren. De verkeersgegevens mogen niet langer worden verwerkt en opgeslagen dan noodzakelijk is voor de bedrijfsvoering van de aanbieder.
Met de komst van de Wet bewaarplicht heeft Agentschap Telecom eveneens de wettelijke taak gekregen toezicht te houden op (onder meer) de naleving van het verwijderen danwel anonimiseren van deze verkeers- en locatiegegevens, op basis van de artikelen 11.5, 11.5a en 11.13 van de Tw.

De vragen in de enquête hebben als onderwerp dataretentie, beveiliging en gebruik van verkeers- en locatiegegevens voor bedrijfsdoeleinden.
Bij de brief met enquête is de brochure "Regels voor openbare aanbieders"[5] toegevoegd voor extra informatie over de onderwerpen.

Verwerking antwoorden enquête
De antwoorden op de enquête zijn verwerkt.
281 OPTA geregistreerde aanbieders geven aan een relevante aanbieder te zijn. Alleen de aanbieders die de enquête volledig hebben beantwoord zijn meegenomen in de resultaten. Dit betreft 229 aanbieders ofwel 82 procent.

[4] In het bijzonder in de artikelen 11.5, 11.5a en 11.13 van de Telecommunicatiewet.
[5] http://www.agentschaptelecom.nl/binaries/content/assets/agentschaptelecom/Folders-en-brochures/Brochure-regels-voor-openbare-aanbieders.pdf

2 Doel van dit rapport

Met de uitvoering van dit onderzoek brengt Agentschap Telecom in beeld wat het niveau van naleving is van de wet- en regelgeving voor dataretentie en het gebruik van verkeers- en locatiegegevens door de markt.

Ten eerste dient de 1-meting om het huidig niveau van naleving zichtbaar te maken. Door de 0- en 1-meting te vergelijken kunnen de verbeteringen in de naleving zichtbaar worden gemaakt. Dit zal in een separaat traject gebeuren. Daarnaast dient de uitkomst van dit onderzoek als input voor de risicoanalyse (op doelgroep niveau, niet op individueel niveau) die de basis vormt voor de verder te houden inspecties en audits. Er wordt voor de uitvoering van het toezicht door het agentschap bepaald welke verbeterpunten er opgepakt moeten worden om de markt in beweging te krijgen en te houden richting betere naleving.

Voor het Directoraat-Generaal Energie, Telecom en Markten geeft deze rapportage inzicht in het halen van de beleidsdoelen van de Wet bewaarplicht een jaar na inwerkingtreding van de wet. De Wet bewaarplicht is een relatief nieuwe wet, waardoor het van belang is dat aan de beleidsmakers wordt teruggekoppeld wat het nalevingsniveau is. Met dit rapport worden mogelijke aandachtspunten in de uitvoering van de wet- en regelgeving inzichtelijk gemaakt.

Tot slot, maar niet minder belangrijk is dat Agentschap Telecom het resultaat van de 1-meting terugkoppelt aan de markt. De aanbieders hebben meegewerkt aan de enquête. Dus is het zorgvuldig hen ook te laten delen in het resultaat. Aanbieders kunnen aan de hand van dit rapport zien in welke mate de markt voldoet aan de huidige wet- en regelgeving, en waar zij zelf mogelijk verbeterpunten hebben. Ook wordt hiermee duidelijk voor de markt waar accenten komen te liggen in het toezicht.

3 Verloop van het onderzoek

In totaal zijn 551 OPTA geregistreerde aanbieders aangeschreven op 29 oktober 2010. De eerste reactie hierop was matig, waardoor het noodzakelijk was om na drie weken aan 461 aanbieders een eerste rappel te verzenden. De aanbieders die hier nog niet op reageerden (176) zijn na twee weken aangeschreven met een laatste, aangetekend, rappel.
De aanbieders die vervolgens nog geen reactie hebben gegeven zijn, voor zover mogelijk, gebeld om duidelijkheid te krijgen.
Van de 551 aangeschreven OPTA geregistreerde aanbieders zijn er 62 afgevallen in verband met faillissement, overname, het staken van de activiteiten, verkeerde adressering, enz.

Uiteindelijk is in 20 gevallen een rapport van bevindingen opgemaakt wegens het niet reageren op de vordering tot het leveren van informatie. Hiervoor is een sanctietraject opgestart.

Van de 551 OPTA geregistreerde aanbieders hebben 281, ofwel 60 procent van de respondenten (469) aangegeven een relevante aanbieder te zijn. 188, 40 procent, van de 469 respondenten hebben aangegeven "anders" te zijn. Deze laatste groep OPTA geregistreerde aanbieders is nader onderzocht om een beeld te krijgen in hoeverre haar stelling terecht is dat de verplichtingen uit Hoofdstuk 13 en in mindere mate Hoofdstuk 11 van de Tw op deze organisaties niet van toepassing zijn. Zoals al aangegeven hebben uiteindelijk 229 aanbieders een valide set antwoorden aangeleverd die zijn meegenomen in dit onderzoek.

4 Bevindingen dataretentie

De Wet bewaarplicht bestaat uit verschillende elementen.
- Het opslaan en bewaren van NAW, verkeers- en locatiegegevens van eindgebruikers voor één jaar[6];
- Het beveiligen van de bewaarde gegevens;
- De levering van opgevraagde gegevens aan behoeftestellers moet worden beveiligd op een wijze die voldoet aan de verplichtingen uit Bbgt.
- Het onverwijld vernietigen van de bewaarde gegevens.

In de volgende paragrafen komen deze onderdelen aan de orde.

4.1 Wet bewaarplicht

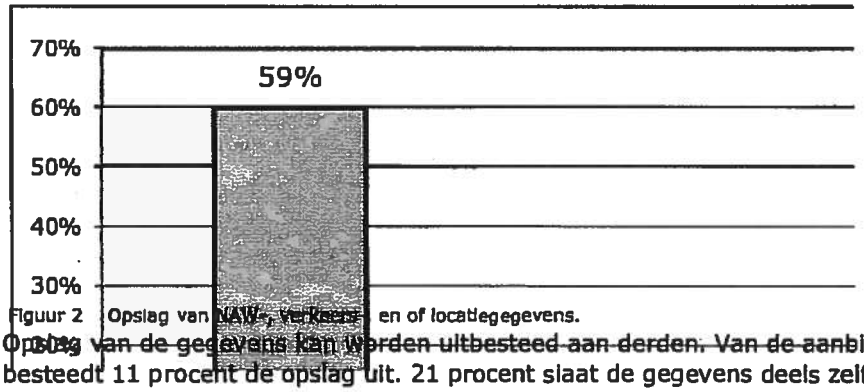
Van de aanbieders geeft 53 procent aan dat zij voldoen aan de Wet bewaarplicht. De overige geven aan nog niet (7 procent) of bijna (40 procent) te kunnen voldoen aan de verplichtingen uit deze wet.

Van de aanbieders die aangeven nog niet aan de Wet bewaarplicht te voldoen, kan het merendeel gekenmerkt worden als "klein", zoals bedoeld in de OPTA gradatie. Ook geven zij aan dat zij pas zullen voldoen aan de verplichtingen in het jaar 2012.

Van de aanbieders die nog niet of bijna voldoen aan de Wet bewaarplicht (in onderstaande grafiek staat deze groep voor 100 procent) geeft ongeveer de helft aan in Q3 2011 klaar te zijn. Eind 2012 zullen, op basis van de eigen antwoorden, alle aanbieders die aan de 1-meting hebben deelgenomen, volledig voldoen aan de Wet bewaarplicht.

4.2 Opslag van gegevens

Wanneer specifiek wordt gekeken naar het opslaan van gegevens uit de Wet bewaarplicht, komt het volgende beeld naar voren. Ten tijde van deze nalevingsmeting is het wetsvoorstel om de bewaartermijn voor internetgegevens te verkorten tot zes maanden nog niet in behandeling.
59 procent van de aanbieders geeft aan gegevens op te slaan en 34 procent slaat een gedeelte van de gegevens op. 7 procent van de aanbieders slaat niets op.



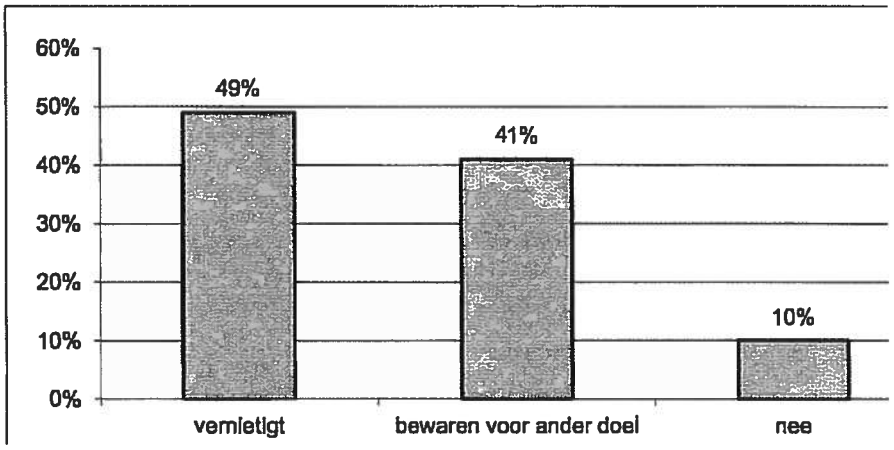
Figuur 2 Opslag van NAW-, verkeers- en of locatiegegevens.

Opslag van de gegevens kan worden uitbesteed aan derden. Van de aanbieders besteedt 11 procent de opslag uit. 21 procent slaat de gegevens deels zelf op en deels bij een derde. De overige 68 procent van de aanbieders slaan alle gegevens onder eigen beheer op.

[6] Bij wet van 6 juli 2011 is de bewaartermijn voor bepaalde gegevens ingekort tot 6 maanden Stb 2011, 350

4.3 Vernietigen van gegevens

Het vernietigen van de gegevens is een onderdeel van de Wet bewaarplicht. In onderstaand figuur is te zien dat bijna de helft van de aanbieders de gegevens vernietigt met de kanttekening dat 11 procent dit nog doet buiten de gestelde termijn en twee procent niet onomkeerbaar vernietigt. Slechts 10 procent geeft aan de gegevens niet te vernietigen. De overige gebruiken de gegevens voor een ander wettelijk toegestaan doel, noodzakelijk voor bedrijfsdoeleinden.



Figuur 3 Vernietigen na de bewaartermijn van één jaar.

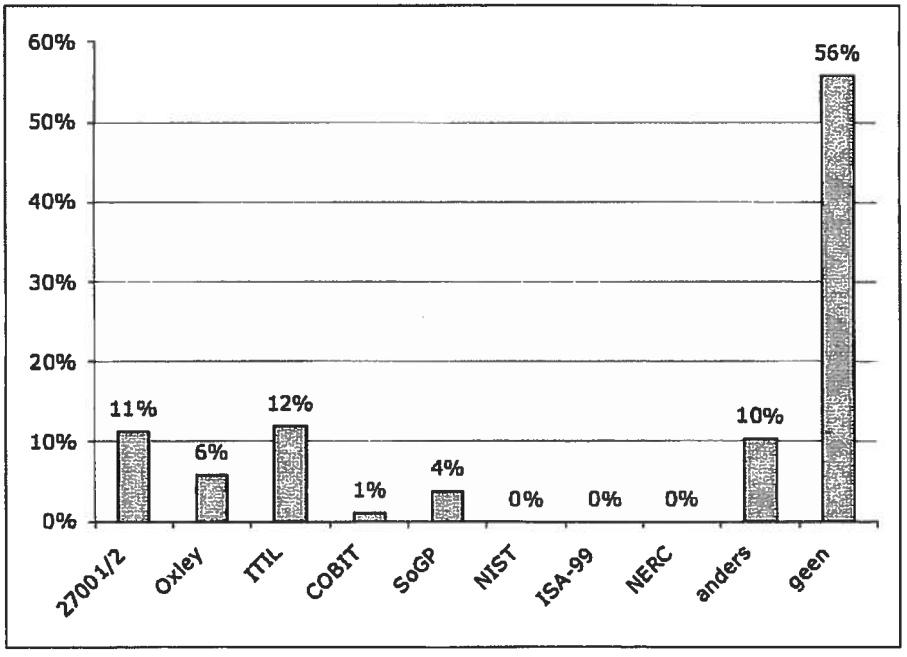
5 Bevindingen beveiliging

Beveiliging is een onderwerp waaraan extra aandacht wordt besteed bij het huidige toezicht. Beveiliging gaat verder dan enkel het opstellen van een beveiligingsplan. Verhoging van bewustwording van risico's, en een goed beveiligingsbeleid bij aanbieders is belangrijk voor het niveau en de continuïteit van de beveiliging.
Bij de 0-meting is ingezoomd op de beveiliging rondom opslag van verkeers- en locatiegegevens bij ISP's. De 1-meting gaat een niveau dieper door naar het gehele (informatie)beveiligingsproces te kijken en breder door alle doelgroepen te onderzoeken.
Om duidelijk inzicht te krijgen in de beveiligingsmaatregelen en de wijze waarop aanbieders om gaan met beveiliging zijn er verschillende vragen gesteld. Die moeten duidelijkheid verschaffen over de mate van beveiligingsbewustzijn bij de aanbieders.

5.1 Systematiek en standaarden

Een goed middel om afdoende beveiligingsmaatregelen te treffen en procesmatig te werken is het gebruik maken van een systematiek, methodiek of standaard. Er zijn verschillende vormen van methodieken die hiervoor gebruikt kunnen worden zoals ITIL, COBIT of de NEN 27001/27002 normen (zie bijlage 2).
Om een indruk te krijgen of men bekend is met informatiebeveiliging (-cyclus) is de vraag gesteld of men een methodiek hanteert waarbij mogelijke beveiligingsrisico's worden vastgesteld, beoordeeld en behandeld. Hierop antwoordde 37 procent dat zij dit gedeeltelijk gebruiken, 31 procent gaf aan dat zij dit volledig hanteren en 32 procent erkende dat zij geen methodiek gebruiken.

Op de vraag of, en zo ja, welke standaard wordt gebruikt ten behoeve van informatiebeveiliging geeft meer dan de helft aan hiervoor geen standaard te hanteren.



Figuur 4 Gebruik van standaarden.

Hieruit is op te maken dat er weinig gewerkt wordt met standaarden die niet alleen de beveiliging, maar ook de procesmatige bedrijfsvoering kunnen verbeteren.

Het zijn veelal de kleine en middelgrote aanbieders die aangeven geen standaard te volgen ten behoeve van informatiebeveiliging. Zij houden grotendeels het Bbgt aan als leidraad.
Voor de grotere aanbieders geldt dat een standaard vaak wordt vereist, door de klanten, de verzekeringsmaatschappij of om commerciële redenen. De standaard die hierin het meest gevolgd wordt is ITIL. Daarnaast schept het voor de klant vertrouwen dat met hun gegevens vertrouwelijk wordt omgegaan aan de hand van de toepassing van zo'n standaard.
De standaard die het beste aansluit bij het Bbgt is de ISO 27002. 11 procent van de aanbieders, veelal de groteren, gebruikt deze standaard.

5.2 Beveiligingsplan

Een vereiste in de wet- en regelgeving is het hebben van een beveiligingsplan. In dit beveiligingsplan beschrijft de aanbieder de maatregelen die zijn genomen met het oog op het beveiligen van informatie en gegevens.
Door de komst van dataretentie heeft de beveiliging aan belang gewonnen. Er worden gegevens van klanten opgeslagen. Deze gegevens moeten in het kader van privacy worden beveiligd. Maar ook in het kader van opsporing en terrorismebestrijding moeten de gegevens uitgebreid worden beschermd. Beide motieven zijn zaken die hoog op de politieke agenda staan. Het beveiligingsplan is dan ook een essentieel onderdeel voor het toezicht door Agentschap Telecom.

De uitkomst van de beantwoording of men een beveiligingsplan heeft is opvallend. Van de aanbieders geeft iets meer dan de helft aan (124 ofwel 54 procent) een beveiligingsplan te hebben. 39 aanbieders ofwel 17 procent geeft aan geen beveiligingsplan te hebben. De rest, 66 aanbieders ofwel 29 procent, is nog niet in het bezit van een volledig beveiligingsplan.
In de vragenlijst is aan de aanbieders het verzoek gedaan om een actualisatie van het beveiligingsplan aan het agentschap te zenden. Hieraan is minimaal gehoor gegeven.
In de praktijk komt het voor dat een aanbieder wel degelijk maatregelen heeft getroffen maar dit administratief (nog) niet in een beveiligingsplan heeft vastgelegd. Een andere reden voor het ontbreken van een beveiligingsplan kan zijn dat de kleine aanbieders binnen bepaalde ketenconstructies geen enkele bemoeienis hebben met het verstrekken van gegevens aan behoeftestellers. Alle gegevens zijn bekend bij hun *wholesale* leverancier. De leverancier heeft alle contacten met de behoeftestellers en verstrekt alle gegevens aan de behoeftestellers namens de aanbieder. Echter, de betreffende aanbieders moeten deze constructie wel vast leggen in een overeenkomst aangezien de aanbieder de eindverantwoordelijke blijft.

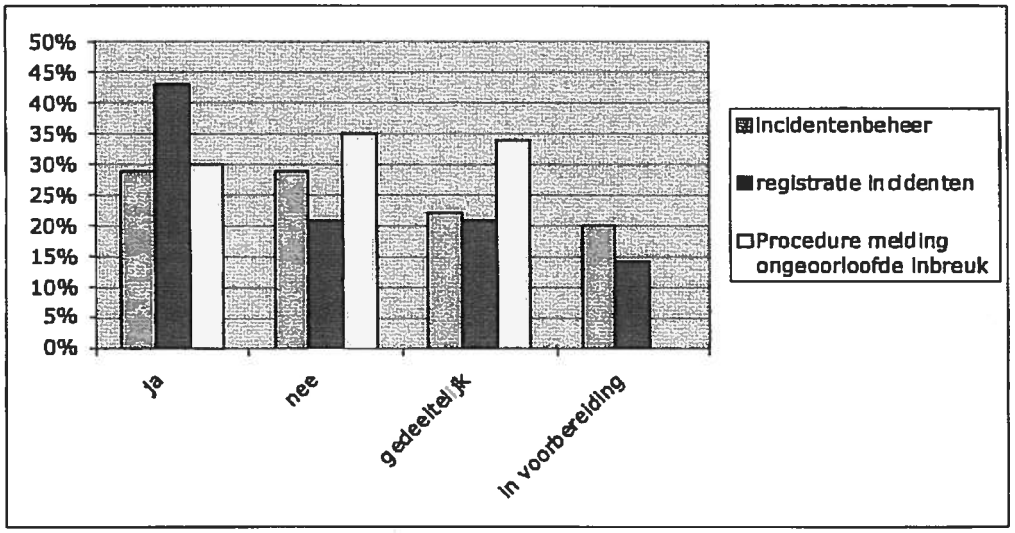
5.3 Classificatie van informatie

Om de vertrouwelijkheid van een document te kenmerken moeten de documenten worden gerubriceerd als vertrouwelijk indien dat nodig is. Zowel het verzoek tot het leveren van bewaarde gegevens door een behoeftesteller als de te verstrekken verzameling van gegevens zijn (of horen te zijn) gerubriceerd.
Een groot deel (40 procent) geeft aan niets aan classificatie te doen binnen de organisatie.

Dit betekent onder andere dat het voor (on)bevoegde lezers niet zichtbaar is of er sprake is van een document met een vertrouwelijk, confidentieel, geheim of zeer geheim karakter. De grote aanbieders, die het merendeel van de verzoeken voor hun rekening nemen, voldoen wel aan hun verplichtingen op dit gebied.

5.4 Incidentbeheer

Incidentbeheer binnen een bedrijf is een belangrijk proces om beveiligingslekken te detecteren en te repareren. Een aantal van 66 ofwel 29 procent van de aanbieders geeft aan geen proces te hebben ten behoeve van incidentenbeheer. Wel is te zien dat een deel van de aanbieders een registratie van incidenten bijhoudt (43 procent). Een *follow-up* van de incidenten wordt dus bij een groot deel van deze aanbieders niet bijgehouden.



Figuur 5 Aanwezigheid proces op gebied van incidentenbeheer.

Uit de grafiek blijkt dat niet alle aanbieders bekend zijn met de verplichting om aan de behoeftesteller te melden dat er inbreuk is geweest op de vertrouwelijkheid van bepaalde gegevens of informatie bij de levering van de gevraagde informatie.

5.5 Beveiliging in overeenkomsten met derden

Het aantal van 163 aanbieders, ofwel 59 procent, geeft aan dat men gedeeltelijk of volledig uitbesteedt.
Van de groep aanbieders die uitbesteedt, geeft 34 procent aan een volledig dekkende overeenkomst te hebben, inclusief beveiligingsafspraken. 52 procent geeft aan een overeenkomst te hebben die de lading niet volledig dekt. 14 procent van de aanbieders geeft aan dat zij uitbesteden, maar hebben dit, althans het aspect beveiliging, niet in een overeenkomst vastgelegd.
Deze cijfers geven aan dat er aandacht moet worden besteed aan het genereren van een goede overeenkomst die de lading volledig dekt en weergeeft welke partijen voor welke diensten aansprakelijk zijn.

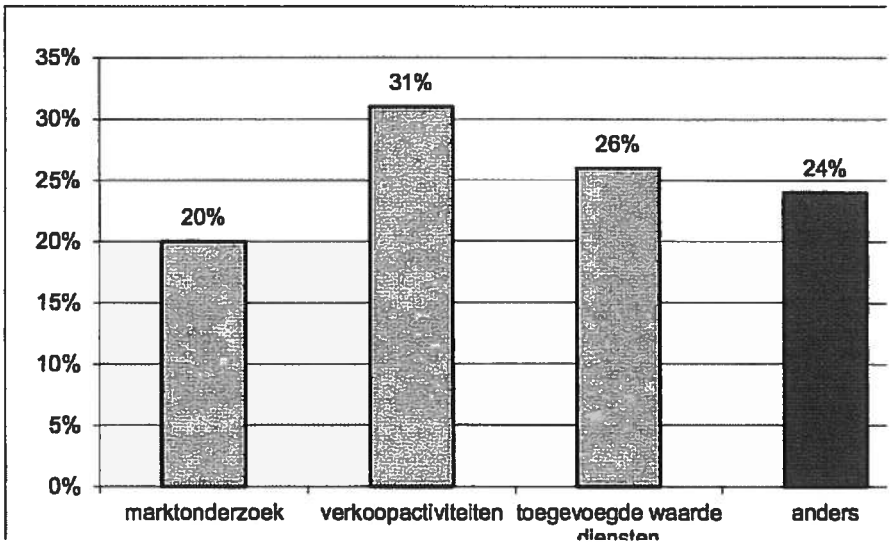
6 Bevindingen gebruik van verkeers- en locatiegegevens voor bedrijfsdoeleinden.

Agentschap Telecom houdt sinds 1 september 2009 toezicht op de artikelen 11.5, 11.5a en 11.13 van de Tw. Deze wetgeving is over het algemeen niet goed bekend bij de aanbieders. Toch zijn deze artikelen al sinds 2004 van kracht.
Aanbieders mogen voor een limitatief aantal doelen onder voorwaarden verkeers- en locatiegegevens verwerken die noodzakelijk zijn voor de normale bedrijfsvoering, bijvoorbeeld voor facturering. Om een overzicht te krijgen van gegevens die door aanbieders worden verwerkt ten behoeve van hun bedrijfsvoering is de vraag gesteld voor welk van de toegestane doelen aanbieders verkeers- en locatiegegevens verwerken. Bij deze vraag zijn meerdere antwoorden mogelijk.
De toegestane doelen zijn:

- Facturering
- Marktonderzoek
- Verkoopactiviteiten
- Toegevoegde waarde diensten

200 aanbieders, ofwel 87%, geven aan de gegevens te verwerken voor de facturering.

In totaal vermelden 168 (73%) aanbieders ook gegevens te verwerken voor een ander doel dan de facturering. Van deze 168 aanbieders antwoorden 128 (76%) aanbieders dat men gegevens verwerkt voor een of meerdere toegestane doelen en in voorkomende gevallen andere dan wettelijk toegestane doelen. 40 (24%) aanbieders erkennen de gegevens louter voor andere dan de wettelijk toegestane doelen te verwerken.



Figuur 6 Doeleinden, anders dan facturering, voor het verwerken van gegevens.

Voor de doelen, anders dan de facturering, moet de aanbieder aan de klant expliciet toestemming vragen voor de verwerking van de verkeers- en locatiegegevens. Tevens moet deze toestemming te allen tijde kunnen worden ingetrokken. 147 (64 procent) aanbieders geven aan toestemming te vragen, vermoedelijk grotendeels via de algemene voorwaarden. 82 aanbieders ofwel 36 procent erkent nog niet om toestemming te verzoeken.

Naast het vragen om toestemming moet de aanbieder de klant informeren over de duur van de verwerking van de verkeers- en locatiegegevens voor het toegestane doel. 144 aanbieders (63 procent) geeft aan niet te informeren over de duur van de verwerking.

7 Overige bevindingen

De overige bevindingen betreffen de aansluiting bij het CIOT, de relatie die aanbieders mogelijk hebben met ketenpartners en de registratie bij OPTA.

7.1 Centraal Informatiepunt Opsporing Telecommunicatie (CIOT)

Van de 229 aanbieders geven 115 aanbieders (50 procent) aan aangesloten te zijn op het CIOT-informatiesysteem. 36 procent (82 aanbieders) geeft aan niet aangesloten te zijn bij het CIOT. De overige 32 aanbieders (14 procent) hebben zich gemeld bij het CIOT.
Ook de aansluiting op het CIOT- systeem is niet bij alle aanbieders bekend. Het gaat hier vooral om de kleine, startende aanbieder. Deze aanbieders kopen in de regel op wholesale basis in. Hierbij worden vergaande faciliteiten aangeboden. In veel gevallen zijn de NAW gegevens al bekend bij de wholesale partij die de gegevens aanlevert aan het CIOT. Dit kan mogelijk het beeld verklaren dat een groot aantal aanbieders aangeeft zelf niet aangesloten te zijn bij het CIOT.

7.2 Ketenpartners

In de enquête is ook de vraag gesteld om een lijst van ketenpartners mee te sturen met de ingevulde formulieren. Doel hiervan is om actueel inzicht te krijgen in de omvang en dynamiek van de markt.
Opvallend genoeg is dit door de meerderheid niet gedaan. Veel aanbieders beroepen zich op de geheimhoudingsplicht die zij hebben tegenover hun derde partij.

7.3 Overige bevindingen

Op basis van de antwoorden is een aantal respondenten nader onderzocht:

- 188 aanbieders hebben aangegeven "anders" te zijn. Naar deze groep aanbieders heeft een *desktop research* plaatsgevonden. Vervolgens is gebleken dat 44 bedrijven vermoedelijk wel een relevante aanbieder zijn. Deze bedrijven zijn of worden bezocht. De overige 144 aanbieders staan wel geregistreerd bij de OPTA als aanbieder van een openbaar elektronisch communicatienetwerk/dienst, maar bieden geen relevante diensten aan.
- Van 281 respondenten die aangaven aanbieder te zijn bleken na *desktop research* 29 geen relevante aanbieder te zijn. Ook deze bedrijven staan dus wel bij de DPTA geregistreerd als aanbieder, maar bieden de bedoelde netwerken of diensten niet of niet meer aan. Deze bedrijven zijn niet meegenomen in de resultaten van dit onderzoek.

8 Conclusie

De bevindingen uit de voorgaande hoofdstukken ielden tot het trekken van een aantal conclusies. Deze zijn hieronder weergegeven.

8.1 Dataretentie

De grote aanbieders voldoen op dit moment aan de bewaarplicht.
Voor de overige, middelgrote en kleinere aanbieders geldt dat deze voldoen of zelf verwachten in de loop van 2012 te gaan voldoen aan hun verplichtingen op het gebied van dataretentie.
Een klein deel, 7%, slaat nog niets op.
Een derde deel van de aanbieders heeft de opslag van gegevens geheel of gedeeltelijk uitbesteed. Twee derde deel slaat alle gegevens in eigen beheer op.

De aanbieders die zich richten op de zakelijke markt slaan nog niet alle gegevens op. Dit betreft voornamelijk kleine en middelgrote aanbieders.

Voor wat betreft het bewaren van de gegevens voor andere wettelijk toegestane doelen zijn er nog omissies. Vooral het samenspel tussen dataretentie en het gebruik van verkeers- en locatiegegevens voor bedrijfsdoeleinden is complex.
Wat betreft het vernietigen van gegevens is het beeld dat de helft van de aanbieders de bewaarde gegevens vernietigt. Veertig procent van de aanbieders wacht met vernietigen omdat zij de bewaarde (verkeers- en locatie)gegevens nodig heeft voor bedrijfsdoeleinden. Tien procent van de aanbieders geeft aan nog geen gegevens te vernietigen. Hierbij is de conclusie te trekken dat de mogelijkheid om de gegevens nog langer te bewaren in verband met gebruik voor bedrijfsdoeleinden veelvuldig wordt benut. Dit leidt uiteindelijk wel tot de problematiek die aan de orde komt in paragraaf 8.3.

8.2 Beveiliging

Bij 68% van de aanbieders wordt volledig of op onderdelen gebruik gemaakt van een systematische methode om beveiligingsrisico's te beheersen. Het overige gedeelte van de aanbieders hanteert nog niet zo'n methodiek. Overigens is het ook mogelijk om zonder het gebruik van een standaard beveiligingsmethodiek te voldoen aan de veiligheidsvereisten.
Van de aanbieders gebruikt 56% daadwerkelijk een beveiligingsstandaard. Het referentiekader voor het inrichten van bedrijfsprocessen ITIL, de Information Technology Infrastructure Library, en ISO 27002 zijn de meest gebruikte standaards hiervoor, waarvan de laatste weer het best aansluit op het Bbgt.

Met name de kleine aanbieders zijn nog onbekend met een beveiligingsplan of standaarden. In zulke gevallen is er eveneens onbekendheid met rubricering van vertrouwelijke documenten en onbewustheid van het belang van incidentenbeheer. Toch is het van belang om de levering van gevraagde gegevens goed te beveiligen. Incidenten bij de levering van opgevraagde gegevens moeten ook aan de behoeftesteller worden gemeld. Relativerend; de kans dat zo'n kleine aanbieder wordt bevraagd is zeer gering.

Incidentenbeheer is een belangrijk proces om beveiligingslekken te detecteren en te repareren. Bij een derde van de aanbieders is dit nog onvoldoende geïmplementeerd.

Door de komst van dataretentie heeft beveiliging van gegevens bij aanbieders aan belang gewonnen. Het bedrijfsbelang en de verplichting uit de wet bewaarplicht liggen hier in één lijn. Het hebben van een beveiligingsplan is hierbij relevant.
190 aanbieders, ofwel 83 procent, heeft een beveiligingsplan, waarvan twee derde over een volledig ingevuld exemplaar beschikt.
Een klein deel, 17% heeft nog geen beveiligingsplan. Dit hoeft niet te betekenen dat er niets is beveiligd. Alleen zijn de beveiligingsmaatregelen nog niet administratief vastgelegd.

Duidelijk blijkt dat op het gebied van beveiliging de overeenkomst met een derde, waarin wordt vastgelegd wat de verantwoordelijkheden zijn van beide partners, nog niet voldoende op orde is. Hierover heerst veel onduidelijkheid omdat men zich niet altijd realiseert dat de aanbieder eindverantwoordelijk blijft, ondanks de uitbesteding.
Het contractmanagement in de keten behoeft aandacht om verplichtingen op het gebied van beveiliging niet tussen wal en schip te laten vallen.

8.3 Gebruik van verkeers- en locatiegegevens voor bedrijfsdoeleinden

De aanbieders zijn over het algemeen onvoldoende op de hoogte van de verplichtingen in het kader van het verwerken van verkeers- en locatiegegevens voor bedrijfsdoeleinden. Het is van belang de verplichtingen op dit gebied nog eens goed onder de aandacht te brengen van de doelgroep.
40 aanbieders geven aan gegevens te verwerken voor andere doeleinden dan wettelijk toegestaan. Hiernaar wordt nader onderzoek gedaan.
Een deel van de aanbieders vraagt geen toestemming om dergelijke gegevens te gebruiken.
Een groot aantal aanbieders (64%) geeft aan toestemming te vragen. De ervaring leert dat toestemming vaak is gebaseerd op summiere informatie die is beschreven in de algemene voorwaarden en/of het privacy statement. Het niet voldoen aan deze vereisten raakt de kern van de wetsbepaling. De privacy van de klant wordt hierdoor onvoldoende gewaarborgd.
Ook op dit punt is voorlichting, gevolgd door nader toezicht van belang om beweging richting betere naleving te bewerkstelligen.

Informatie over de duur van de verwerking van de verkeers- en locatiegegevens wordt door een groot aantal aanbieders (144, of wel 63%) niet kenbaar gemaakt. Hierdoor is het tijdstip van verwijderen of anonimiseren ook niet helder. Dat maakt het controleren op tijdig verwijderen of anonimiseren ook moeilijker.
Concluderend: het vragen van toestemming, het aangeven van de duur van de verwerking en ook het na afloop verwijderen van gegevens die zijn gebruikt voor bedrijfsdoeleinden zijn aspecten die goed onder de aandacht van de doelgroep moeten worden gebracht. Vervolgens moet er toezicht zijn op naleving om de gedragsverandering te weeg te brengen.

8.4 Overige bevindingen

Een aantal andere bevindingen is van belang voor het toezicht op deze doelgroep.

CIOT

Uit de resultaten is op te maken dat een groot aantal aanbieders niet is aangesloten bij het CIOT. De oorzaak hiervan kan zijn dat deze activiteit is uitbesteed aan een derde. In veel gevallen is dit een *wholesale* partij. Zo worden binnen de keten gegevens van uitbestedende aanbieders door een derde, wel bij het CIOT aangesloten partij aangeleverd. Door de keten na te lopen kan worden gecontroleerd of de gegevens in het CIOT-informatiesysteem juist en compleet zijn.

Ketenpartners

Veel zaken met betrekking tot aftappen, dataretentie en beveiliging worden georganiseerd in de keten. Hierover sluiten aanbieders overeenkomsten af met de desbetreffende partij. Zoals de resultaten laten zien in verband met het zicht op de keten en de overeenkomsten met betrekking tot beveiliging is hiervoor extra aandacht noodzakelijk.
Door een duidelijk inzicht te hebben in de keten, en daarmee in de dynamiek in de markt, wordt efficiënt en effectief toezicht bevorderd en kan de toezichtlast worden verminderd.

Registratie bij de OPTA

Opmerkelijk is dat 188 (40%) van de 551 aanbieders die geregistreerd staan bij OPTA aangeven geen relevante aanbieder in de zin van hoofdstuk 11 en 13 van de Tw te zijn. Uit nader onderzoek blijkt dat 44 aanbieders wel degelijk als relevante aanbieder moeten worden gekenmerkt.

In het volgende hoofdstuk worden aanbevelingen gedaan om de aanbieders meer te ondersteunen bij het naleven van de wet. Deze aanbevelingen worden in acht genomen bij het uit te voeren toezicht op naleving.

9 Aandachtspunten

Uit de conclusies kunnen de volgende aandachtspunten voor het toezicht worden gedestilleerd om de aanbieders verder te bewegen de betreffende wet- en regelgeving na te leven.

- Extra controle op de overeenkomsten met ketenpartners, zodat een duidelijk beeld wordt verkregen waar de verantwoordelijkheden zijn belegd voor het bewaren, vernietigen, beveiligen en aansluiten op het CIOT-informatiesysteem.
- Inzicht in de keten is van groot belang. Door het hebben van een volledig en actueel beeld van de markt is het mogelijk om toezicht efficiënt en effectief in te zetten. Er is een tool beschikbaar om hierin inzicht te krijgen. Hiervoor moet regelmatig tijd worden gereserveerd.
- Er zal meer aandacht worden besteed aan het gehele (informatie)-beveiligingsproces. De aanbieders moeten zich meer bewust worden van nut en noodzaak op gebied van (informatie)beveiliging en het waarborgen van continuïteit in het (informatie)beveiligingsproces.
- Het toezicht op de verplichtingen bij het gebruik van verkeers- en locatiegegevens moet worden geïntensiveerd. Met name de verplichting omtrent de expliciete toestemming voor het verwerken van verkeers- en locatiegegevens verdient extra aandacht. Het is aan te bevelen om dit traject in nauwe samenwerking met het College Bescherming Persoonsgegevens uit te voeren.
- Extra aandacht is noodzakelijk voor de voorlichting over het vernietigen van de op basis van de Wet bewaarplicht opgeslagen gegevens in combinatie met de toegestane verwerking voor andere doeleinden van dezelfde gegevens.

Vervolg op de 1-meting

Het vervolg op de 1-meting bestaat uit twee onderdelen:

1. De effectmeting.
   Het verschil tussen de resultaten van de uitgevoerde nalevingsmetingen, de 0-meting en de 1-meting, geeft een indicatie voor het effect van het toezicht in de tussenliggende periode. Deze effectmeting is in opzet afhankelijk van de scope van de 0-meting. De doelgroep bestond toen enkel uit ISP's, vanwege het verzoek van de Eerste Kamer om informatie over die specifieke doelgroep. Zodra vervolgmetingen worden verricht kan een volgende effectmeting over de gehele doelgroep worden gemaakt. Wel worden bij de effectmetingen ook de ervaringen van het toezicht in de praktijk meegenomen.

2. De resultaten geven input voor herijking van de risicoprofielen. De herijkte risicoprofielen kunnen uiteindelijk aanleiding zijn voor het plannen van inspecties of audits bij bepaalde groepen aanbieders.

Naast de input van de bevindingen uit de enquêtes zal er voor de indeling van inspecties of audits ook gekeken worden naar overige selectiecriteria:

- De mate van kwaliteit van de reactie op de verzoeken (0-meting en/of 1-meting) en voorgaande afspraken;
- Wanneer men zichzelf ten onrechte als "geen aanbieder" heeft gekenmerkt;
- Op basis van kennis en ervaringen met bepaalde aanbieders;
- Informatie uit open bronnen over aanbieders.

Tijdens de inspecties en audits zal onder meer gekeken worden naar de onduidelijkheden die blijken uit de enquête en zal dieper worden ingegaan op de gebieden waar de aanbieder moeite mee heeft.

Bijlage 1 Enquête

Verzoek om informatie

Verzoek om informatie in verband met de 1-meting inzake de mate van naleving van de Telecommunicatiewet, wat betreft de bewaarplicht van telecommunicatiegegevens.

De beantwoording van de vragen in deze enquête is niet vrijblijvend. De informatie wordt namens de Minister van Economische Zaken opgevraagd op basis van artikel 18.7 van de Telecommunicatiewet. De antwoorden kunnen door Agentschap Telecom op juistheid worden getoetst.

Vestiging - & contactgegevens :

Bedrijfsnaam:
Straat:
Postcode:
Plaats:

Postadres:
Postbus:
Postcode:
Plaats:

Algemeen telefoonnummer vestiging:

Security Officer:
Naam:
Telefoon:
E-mail:
Registratienummer Kamer van Koophandel:

Staat uw onderneming ingeschreven bij de OPTA?

- ☐ Ja
- ☐ Nee

N.B. Graag aankruisen wat van toepassing is.

OPTA registratie nummers:

1.
2.

Ketenpartners (vraag en aanbod)

Wij verzoeken u vriendelijk een actueel overzicht van uw huidige, directe en zakelijke, telecommunicatie (keten)partners toe te sturen aan Agentschap Telecom. Indien van toepassing vragen wij dus een overzicht van zowel uw "toeleveranciers" als uw "resellers".

Omvang van uw onderneming naar omzetgegevens :

1. In welke categorie valt uw onderneming wanneer u de totale omzet uit telecommunicatiediensten van uw onderneming beschouwt?

- ☐ 0 - 2 miljoen euro
- ☐ 2 – 20 miljoen euro
- ☐ 20 miljoen euro of meer

N.B. Graag aankruisen wat van toepassing is.

Dienstverlening :

2. Zijn de activiteiten van uw bedrijf te kenmerken als de activiteiten van een:

- ☐ Aanbieder van openbare telecommunicatienetwerken en/of openbare telecommunicatiediensten
- ☐ Anders (Wanneer u deze optie aankruist behoeft u de vragen 3 t/m 21 NIET te beantwoorden, tenzij u diensten verricht voor aanbieders van openbare telecommunicatienetwerken en/of openbare telecommunicatiediensten welke gerelateerd kunnen worden aan het tapproces en /of het dataretentie proces.)

N.B. Graag aankruisen wat van toepassing is.

Bewaarplicht

3. Worden de bij uw dienstverlening gegenereerde NAW-, verkeers- en locatiegegevens, zoals bedoeld in de Telecommunicatiewet, door uw organisatie opgeslagen?

- ☐ Ja
- ☐ Nee
- ☐ Gedeeltelijk

N.B. Graag aankruisen wat van toepassing is.

4. Worden alle binnen uw bedrijf gegenereerde NAW-, verkeers- en locatiegegevens onder eigen beheer bewaard ?

- ☐ Ja
- ☐ Nee
- ☐ Gedeeltelijk

N.B. Graag aankruisen wat van toepassing is

Vernietigen van gegevens

5. Worden bij uw dienstverlening gegenereerde NAW-, verkeers- en locatiegegevens, zoals bedoeld in de Telecommunicatiewet, door uw organisatie na de gestelde bewaartermijn van 12 maanden onomkeerbaar vernietigd?

- ☐ Ja
- ☐ Nee
- ☐ De gegevens worden onomkeerbaar vernietigd, echter nog niet na de gestelde bewaartermijn
- ☐ De gegevens worden wel na de gestelde bewaartermijn vernietigd, echter nog niet onomkeerbaar
- ☐ Gedeeltelijk
- ☐ De gegevens worden op basis van een ander wettelijk toegestaan doel bewaard

N.B. Graag aankruisen wat van toepassing is.

Naleving

6. Is uw onderneming op dit moment aangesloten op het CIOT informatiesysteem?

- ☐ Ja
- ☐ Nee
- ☐ U bent nog niet aangesloten op het CIOT, echter u heeft zich al wel aangemeld

N.B. Graag aankruisen wat van toepassing is.

7. Voldoet u aan de eisen van de Telecommunicatiewet, wat betreft de bewaarplicht voor telecommunicatiegegevens?

- ☐ Ja (ga naar vraag 9)
- ☐ Nee (ga naar vraag 8)
- ☐ Gedeeltelijk (ga naar vraag 8)

N.B. Graag aankruisen wat van toepassing is.

8. Wanneer denkt u volledig te voldoen aan de eisen van de Telecommunicatiewet, wat betreft de bewaarplicht van telecommunicatiegegevens?

- ☐ 4e kwartaal 2010
- ☐ 1e kwartaal 2011
- ☐ 2e kwartaal 2011
- ☐ 3e kwartaal 2011
- ☐ 4e kwartaal 2011
- ☐ In het jaar 2012

N.B. Graag aankruisen wat van toepassing is.

Beveiliging

9. Is er sprake van een systematiek waarbij mogelijke beveiligingsrisico's worden vastgesteld, beoordeeld en behandeld (risicobeheer), is dit proces beschreven en opgenomen in het beveiligingsplan?

- ☐ Ja
- ☐ Nee
- ☐ Gedeeltelijk

N.B. Graag aankruisen wat van toepassing is.

10. Werkt u volgens een standaard welke een relatie heeft met informatiebeveiliging?

- ☐ Ja, NEN-ISO IEC 27001 en 27002
- ☐ Ja, Sarbanes-Oxley
- ☐ Ja, ITIL
- ☐ Ja, COBIT
- ☐ Ja, SoGP, Standard of good practice
- ☐ Ja, NIST
- ☐ Ja, ISA-99
- ☐ Ja, NERC
- ☐ Ja, wij volgen echter de richtlijnen van een andere standaard
- ☐ Nee

N.B. Graag aankruisen wat van toepassing is.

Beveiligingsplan

Wij verzoeken u vriendelijk een actualisatie van uw huidige beveiligingsplan aan Agentschap Telecom toe te zenden.

11. Is er een beveiligingsplan, zoals bedoeld in het Besluit beveiliging gegevens telecommunicatie?

- ☐ Ja
- ☐ Nee
- ☐ Gedeeltelijk

N.B. Graag aankruisen wat van toepassing is.

12. Heeft u in het beveiligingsplan beschreven op welke wijze u uitvoering geeft aan uw beveiligingsplicht, bijvoorbeeld door de in de bijlage bij het Besluit beveiliging gegevens telecommunicatie genoemde processen te beschrijven?

- ☐ Ja
- ☐ Nee

N.B. Graag aankruisen wat van toepassing is.

Classificatie van informatie

13. Is er binnen uw organisatie sprake van classificatie van informatie, is dit proces beschreven en opgenomen in het beveiligingsplan?

- ☐ Ja
- ☐ Nee
- ☐ Gedeeltelijk
- ☐ Er wordt momenteel gewerkt aan de voorbereiding hiervan

N.B. Graag aankruisen wat van toepassing is.

Incidentbeheer

14. Is er in uw bedrijf sprake van een systematiek waar personeelsleden beveiligingsincidenten en mogelijk zwakke plekken in de beveiliging kenbaar kunnen maken, is dit proces beschreven en opgenomen in het beveiligingsplan?

- ☐ Ja
- ☐ Nee
- ☐ Gedeeltelijk
- ☐ Er wordt momenteel gewerkt aan de voorbereiding hiervan

N.B. Graag aankruisen wat van toepassing is.

15. Worden binnen uw onderneming incidenten geregistreerd en wordt hierbij de mogelijke impact, urgentie en de verwachte inspanning aangegeven?

- ☐ Ja
- ☐ Nee
- ☐ Gedeeltelijk
- ☐ Er wordt momenteel gewerkt aan de voorbereiding hiervan

N.B. Graag aankruisen wat van toepassing is.

16. Wordt in het beveiligingsplan van uw bedrijf beschreven hoe wordt gehandeld indien op de vertrouwelijkheid van enigerlei gegevens of informatie als bedoeld in het "Besluit beveiliging gegevens telecommunicatie"; artikel 2, eerste lid, een ongeoorloofde inbreuk is gemaakt.

- ☐ Ja
- ☐ Nee
- ☐ Er wordt momenteel gewerkt aan de voorbereiding hiervan

N.B. Graag aankruisen wat van toepassing is.

Beveiliging behandelen in overeenkomsten met derden

17. Besteedt uw organisatie werkzaamheden uit aan een derde waarbij in dat kader de derde kennis neemt of kan nemen van gegevens en informatie als bedoeld in Besluit beveiliging gegevens telecommunicatie, artikel 2, eerste lid ?

- ☐ Ja (ga naar vraag 18)
- ☐ Nee (ga naar vraag 19)
- ☐ Gedeeltelijk (ga naar vraag 18)

N.B. Graag aankruisen wat van toepassing is.

18. Bij uitbesteding bent u verantwoordelijk voor de naleving door de derde van de verplichtingen als bedoeld in het Besluit beveiliging gegevens telecommunicatie, artikel 8, eerste lid.

Dat wil zeggen dat u er zorg voor moet dragen dat de derde zich verplicht tot :

a. het beveiligen tegen kennisneming door onbevoegden m.b.t. de desbetreffende gegevens en informatie;

b. het betrachten van geheimhouding met betrekking tot de desbetreffende gegevens en informatie;

c. het naleven van de ingevolge het Besluit beveiliging gegevens telecommunicatie gestelde maatregelen;

d. het verstrekken van alle informatie die voor het toezicht op de naleving van de beveiligings- en geheimhoudingsverplichting noodzakelijk is.

Heeft u deze verplichtingen van de derde vastgelegd in een schriftelijke overeenkomst tussen uw organisatie en de derde en heeft u een kopie van deze overeenkomst opgenomen in het beveiligingsplan?

- ☐ Ja
- ☐ Nee
- ☐ Gedeeltelijk

N.B. Graag aankruisen wat van toepassing is.

Privacy

19. Het is mogelijk dat de bij uw dienstverlening gegenereerde NAW-, verkeers- en locatiegegevens, zoals bedoeld in de Telecommunicatiewet, door uw organisatie voor een mogelijk ander doel dan dataretentie worden bewaard. Welke doelen betreft dit ? U kunt bij beantwoording meerdere doelen aankruisen.

- ☐ Facturering
- ☐ Marktonderzoek
- ☐ Verkoopactiviteiten
- ☐ Toegevoegde waarde diensten
- ☐ Anders

N.B. Graag aankruisen wat van toepassing is.

20. Vraagt u alvorens u de NAW-, verkeers- en locatiegegevens van uw klanten wil gebruiken voor marktonderzoek, verkoopactiviteiten en toegevoegde waarde diensten, hiervoor bij uw klanten toestemming en kan deze toestemming ook zonder meer te allen tijde worden ingetrokken ?

- ☐ Ja
- ☐ Nee

N.B. Graag aankruisen wat van toepassing is.

21. Stelt u uw klanten op de hoogte van de periode waarin NAW-, verkeers- en locatiegegevens t.b.v. facturatie worden verwerkt en worden uw klanten geïnformeerd welke gegevens u daartoe bewaart?

- ☐ Ja
- ☐ Nee

N.B. Graag aankruisen wat van toepassing is.

Bijlage 2 Betekenissen systematieken/standaarden

- **NEN27001 / 27002**
  ISO 27001 is een ISO standaard voor informatiebeveiliging waarin wordt beschreven hoe Informatiebeveiliging procesmatig ingericht zou kunnen worden, om de beveiligingsmaatregelen uit ISO/IEC 17799 (NEN 27002) te effectueren. In Nederland is het vastgesteld als NEN norm NEN-ISO/IEC 27001:2005 en vertaald naar het Nederlands en verplicht gesteld voor Nederlandse overheden door het College standaardisatie.
  Deze internationale norm is van toepassing op alle typen organisaties (bijv. commerciële ondernemingen, overheidsinstanties, non-profitorganisaties). De norm specificeert eisen voor het vaststellen, implementeren, uitvoeren, controleren, beoordelen, bijhouden en verbeteren van een gedocumenteerd Information Security Management System (ISMS) in het kader van de algemene bedrijfsrisico's voor de organisatie.
  De norm specificeert eisen voor de implementatie van beveiligingsmaatregelen die zijn aangepast aan de behoeften van afzonderlijke organisaties of delen daarvan. Het ISMS is ontworpen om de keuze van adequate en proportionele beveiligingsmaatregelen die de informatie beschermen en vertrouwen bieden aan belanghebbenden te waarborgen.

- **Oxley**
  Deze wet legt tal van regels op aan bedrijven die aan een Amerikaanse beurs genoteerd zijn (en haar buitenlandse filialen), of een buitenlands bedrijf met een genoteerde vestiging. In 69 artikelen tracht de wet deugdelijk ondernemingsbestuur af te dwingen en schandalen te voorkomen.

- **ITIL**
  Information Technology Infrastructure Library, meestal afgekort tot ITIL, is ontwikkeld als een referentiekader voor het inrichten van de beheerprocessen binnen een ICT-organisatie. ITIL is geen methode of model, maar eerder een reeks van best practices (de beste praktijkoplossingen) en concepten. Het resultaat van procesimplementatie met behulp van ITIL is vergelijkbaar met de ISO 9000-reguliering in de niet-ICT-branche, waarbij alle onderdelen van de organisatie zijn beschreven en in een bepaalde hiërarchie qua bevoegdheid/verantwoordelijkheid zijn gerangschikt.

- **COBIT**
  Control Objectives for Information and related Technology (COBIT) is een framework voor het gestructureerd inrichten en beoordelen van een IT-beheeromgeving. COBIT is vanaf 1992 ontwikkeld door het Information Systems Audit and Control Association (ISACA) en het IT Governance Institute (ITGI). COBIT stelt IT managers in staat om op basis van algemeen geaccepteerde Best Practices de ICT beheersmaatregelen in te richten. Daarnaast kunnen auditors op basis van het framework hun controleprogramma beschrijven en uitvoeren.
  In december 2005 werd een nieuwe versie (4.0) uitgebracht, waarin de overlap met ITIL werd weggenomen door aan te sluiten bij de ITIL uitgangspunten. Ook werd voor de aspecten op het gebied van Informatiebeveiliging aansluiting gevonden bij de Code voor Informatiebeveiliging.

- **SoGP**
  SoGP staat voor The Standard of Good Practice for Information Security. De norm is een belangrijke autoriteit op gebied van informatiebeveiliging. Het richt zich op
  informatiebeveiliging vanuit een zakelijk perspectief, waardoor een praktische basis voor de beoordeling van informatiebeveiliging in een organisatie wordt geregeld.
  De Standaard vertegenwoordigt een deel van de informatie van de ISF Information Security Forum), risicomanagement van producten en is gebaseerd op een schat aan materiaal, diepgaand onderzoek, en de uitgebreide kennis en praktische ervaring van de ISF leden wereldwijd.

- **NIST**
  NIST (National Institute of Standards and Technology) is een instituut die vooral in Amerika actief is. Men houdt zich o.a. bezig met standaarden om de commerciële handel met Europa te verbeteren, om transparantie te krijgen in technische voorschriften, wetten, beleid en procedures.

- **ISA – 99**
  ISA-99 biedt een actuele beoordeling van de veiligheidtools en technologieën die van toepassing zijn op de productie en Control Systems omgeving. Het beschrijft verschillende categorieën van beveiligingstechnologieën, de aard van de producten beschikbaar in deze categorieën, de voor- en nadelen van het gebruik van deze producten in het Manufacturing and Control Systems milieu, ten opzichte van de verwachte bedreigingen en bekende kwetsbaarheden; samen met de voorlopige aanbevelingen en richtlijnen voor het gebruik van deze beveiligingstechnologieën.

- **NERC**
  NERC (North American Electric Reliability corporation) is een programma ter bescherming van kritieke infrastructuur en coördineert alle inspanningen om de fysieke en cyberbeveiliging te verbeteren voor het bulk power systeem van Noord-Amerika als het gaat om betrouwbaarheid.
  Deze inspanningen omvatten de ontwikkeling van normen, naleving van handhaving, beoordeling van risico's en paraatheid, de verspreiding van kritische informatie via waarschuwingen aan de industrie en de bewustmaking van belangrijke kwesties.