Eindrapport Nulmeting Wet bewaarplicht telecommunicatiegegevens

Een onderzoek naar de stand van zaken betreffende de naleving van de Wet bewaarplicht bij Internet Service Providers.

Nummer : Versie 1.1

Datum : 3 mei 2010

Copyright : Agentschap Telecom ©2010

Inhoudsopgave

1 Management Samenvatting. 4
2 Inleiding en leeswijzer. 6
3 Inhoud en aanpak onderzoek. 7
3.1 Onderzoeksvraag. 7
3.2 Aanpak onderzoek. 8
3.2.1 Vragenlijst / enquête. 8
3.2.2 Audits. 8
3.2.3 Verwerken resultaten 10
4 Bevindingen. 11
4.1 Huidige situatie bewaren noodzakelijke gegevens. 11
4.2 Huidige situatie beveiligen noodzakelijke gegevens. 12
4.3 Huidige situatie vernietigen gegevens. 15
4.4 Lopende ontwikkelingen aanbieders. 16
4.5 Gewenste situatie bereikt. 17
4.6 Investeringskosten aanbieders. 17
4.7 Bevindingen audits. 18
4.8 Overige bevindingen. 20
5 Conclusies. 21

Bijlagen

Bijlage 1 Vragenlijst zoals verstuurd aan de ISP's 23

Bijlage 2 Onderwerpen zoals behandeld tijdens de audits van de ISP's 24

1 Management Samenvatting.

Naar aanleiding van een toezegging door de Minister aan de Eerste Kamer tijdens de behandeling van de Wet bewaarplicht telecommunicatiegegevens, is door Agentschap Telecom een onderzoek uitgevoerd. Het onderzoek is uitgevoerd in de periode tussen 1 september 2009 en 28 februari 2010. Dit onderzoek betrof de huidige stand van zaken bij de Internet Service Providers waar het de invoering van noodzakelijke maatregelen en de naleving van de wet en het impliciete Besluit beveiliging gegevens telecommunicatie betreft.

Dit rapport van bevindingen is het resultaat van een enquête, bestaande uit 138 volledig ingevulde reacties, alsmede het uitvoeren van 25 audits bij een deel van de populatie. Hierbij is gericht aandacht besteed aan de vragen uit de Eerste Kamer naar de volgende onderwerpen:

- de stand van zaken betreffende de invoering van de bewaarplicht, in het bijzonder de opgeslagen gegevens inclusief de vernietiging daarvan, en de lopende ontwikkelingen in de markt betreffende de invoering;
- de waarborgen voor de beveiliging van de opgeslagen gegevens conform het Besluit beveiliging gegevens telecommunicatie;
- de mate waarin investeringskosten voor de Internet Service Providers reden kunnen zijn om niet te voldoen aan de verplichtingen van de wet.

De bevindingen met betrekking tot de genoemde en onderzochte onderwerpen kunnen samengevat als volgt worden weergegeven:

- Slechts een zeer klein deel van de partijen bewaart op dit moment alle noodzakelijke gegevens. Echter de meeste aanbieders bewaren een deel van de noodzakelijke gegevens. Dit zijn meestal de gegevens die nodig zijn voor facturatie. Voor vrijwel alle partijen die nog niet alle noodzakelijke gegevens bewaren, is het nog ontbreken van de technische specificaties de belangrijkste reden. Dit laatste in combinatie met de mogelijkheid van een nog te verschijnen Algemene Maatregel van Bestuur waarin de wijze van levering kan worden opgelegd.
- Het vernietigen van de opgeslagen gegevens is bij vrijwel alle partijen opgenomen in een project dat dient om te gaan voldoen aan alle verplichtingen. Vrijwel alle aanbieders geven hier nog geen prioriteit aan, vanwege het feit dat het vernietigen pas vanaf 1 september 2010 actueel wordt (dit is 12 maanden, de verplichte bewaartermijn, na inwerkingtreding van de wet).
- Vrijwel alle aanbieders die nog niet volledig voldoen aan de wet hebben een project dat dient om volledig te gaan voldoen aan de wet en nadere regelgeving. Voor alle aanbieders ligt de einddatum van het project (het moment waarop volledig wordt voldaan aan de wet en nadere regelgeving) voor het einde van 2010.
- De beveiliging van de opgeslagen gegevens is over het algemeen geregeld, echter vrijwel nergens is volledig aan de specifieke eisen zoals gesteld in het Besluit beveiliging gegevens telecommunicatie voldaan. Bovendien hebben nog niet alle partijen de beveiliging opgenomen in het verplichte beveiligingsplan.
- De Internet Service Providers voorzien een investering voor het bouwen van een systeem voor de opslag van de noodzakelijke gegevens die bedrijfseconomisch gezien geen belemmering vormt om aan de wet te voldoen. Wel verwachten de partijen hoge operationele kosten om het systeem up-to-date te houden. Bovendien verwachten de kleine aanbieders dat de financiële lasten, mede door het geringe aantal vorderingen en verzoeken, aanzienlijk zullen stijgen.
- Het merendeel van de aanbieders heeft de intentie om de verplichtingen na te leven zoals die opgelegd worden door de Wet bewaarplicht telecommunicatiegegevens en het Besluit beveiliging gegevens telecommunicatie. Slechts bij een enkeling is geconstateerd dat er onwil bestaat om te voldoen aan de wet.

Tijdens het onderzoek is een tendens waargenomen dat naarmate de aanbieder groter is, er een aanzienlijk beter begrip van de wet en nadere regelgeving aanwezig is. Met name bij de kleine aanbieders is regelmatig een situatie aangetroffen waarbij er veel onduidelijkheden gesignaleerd zijn.

Naast de bevindingen met betrekking tot de gestelde onderzoeksvragen hebben de marktpartijen nog frequent aandacht voor de volgende onderwerpen gevraagd:

- Deze specificaties voor de opslag van de noodzakelijke gegevens zijn voor de aanbieder gelijk aan de specificaties van de levering van die gegevens aan de behoeftestellers. Het ontbreken van de door de overheid op te geven technische specificaties van de noodzakelijke gegevens levert een vertraging in de realisatie van hun systemen op. De belangrijkste reden hiervoor is dat de aanbieder niet wil investeren in een systeem, dat mogelijk weer aangepast moet worden wanneer de specificaties vanuit de overheid opgelegd worden.
- De marktpartijen beschouwen het hoge beveiligingsniveau waar aan voldaan moet worden, niet in lijn met de wijze waarop sommige vertegenwoordigers van opsporingsdiensten met vorderingen en verzoeken om inlichtingen omgaan.
- De informatievoorziening door de overheid met betrekking tot de verplichtingen van de Wet bewaarplicht telecommunicatiegegevens, wordt vooralsnog door de aanbieders als ontoereikend beschouwd. Met name een intensievere dialoog met meerdere partijen die de totale markt vertegenwoordigen (inclusief middelgrote en kleine aanbieders) en een uitgebreidere voorlichting hadden dit in hun ogen kunnen voorkomen.

In het rapport staan de beschrijving van de aanpak van het onderzoek en de afzonderlijke bevindingen in detail weergegeven.

2 Inleiding en leeswijzer.

Vanuit de Europese Commissie is een Europese Richtlijn Dataretentie uitgevaardigd die in de lidstaten geïmplementeerd moet worden. In Nederland is dit gedaan middels de Wet bewaarplicht telecommunicatiegegevens (verder Wet bewaarplicht) die de noodzakelijke aanpassingen doet aan hoofdstuk 13 van de Telecommunicatiewet. Tijdens de behandeling van het wetsvoorstel in de Eerste Kamer is, door de Minister van Justitie, de uitvoering van een nulmeting toegezegd.

Aanleiding voor deze toezegging was de discussie die in de Eerste Kamer is gevoerd over:

- de mate waarin de aanbieders aan de wettelijke verplichtingen voldoen,
- de waarborgen voor de beveiliging van opgeslagen gegevens en vorderingen van inlichtingen- en opsporingsdiensten en
- de investeringen die de aanbieders van telecommunicatienetwerken en telecommunicatiediensten hiervoor moeten doen.

In de periode tussen 1 september 2009 en 28 februari 2010 is door Agentschap Telecom, op verzoek van het Ministerie van Economische Zaken, een onderzoek uitgevoerd in het kader van deze Nulmeting Wet bewaarplicht.

Het uitgevoerde onderzoek (op basis van de vragen zoals geformuleerd in paragraaf 3.1) bestond uit drie delen:

- Een inventarisatie van de situatie in de markt op basis van een schriftelijke vragenlijst, die door de betreffende marktpartijen is beantwoord.
- Een bezoek aan een deel van de aanbieders ter verificatie en verdieping van de gegeven antwoorden.
  Van alle bezoeken is een audit rapport opgemaakt, dat door de betreffende aanbieders is geverifieerd en ondertekend is geretourneerd. Hiermee geven de aanbieders aan dat de weergave in het audit rapport conform hetgeen besproken is.
- Rubricering en verwerking van de antwoorden op de vragenlijst.

Naar aanleiding van de verstuurde vragenlijst is bij 24 bedrijven een bestuursrechtelijk traject gestart. Deze bedrijven hebben niet of niet tijdig gereageerd op het verzoek om inlichtingen.

Het rapport bestaat uit de volgende onderdelen:

- In hoofdstuk 3 is de onderzoeksvraag weergegeven en de wijze waarop het onderzoek is ingericht en uitgevoerd.
- In hoofdstuk 4 zijn de bevindingen weergegeven, zoals die uit de antwoorden op de vragenlijst en uit de bezoeken naar voren zijn gekomen.
- In hoofdstuk 5 zijn de hoofdlijnen van de bevindingen als conclusie weergegeven.

In de bijlagen bij het rapport zijn detailgegevens opgenomen zoals die in het onderzoek naar voren zijn gekomen. Tevens is in de bijlage de uitwerking van de onderzoeksaanpak opgenomen.

3 Inhoud en aanpak onderzoek.

Agentschap Telecom heeft opdracht gekregen om een nulmeting uit te voeren met betrekking tot de invoering van de Wet bewaarplicht telecommunicatiegegevens (verder Wet bewaarplicht). Basis voor hiervoor is de toezegging van de Minister van Justitie aan de Eerste Kamer[1] om een onderzoek uit te voeren naar de huidige situatie bij de aanbieders van internet, email en telefonie. De nadruk ligt hierbij op de Internet Service Providers (ISP's). De aanbieders van telefonie, zowel de traditionele draadgebonden telefonie als de mobiele telefonie, zijn in de nulmeting niet expliciet meegenomen.

Als toezichthouder op de naleving van deze nieuwe wet, had Agentschap Telecom al het voornemen om een nulmeting over de gehele breedte van de markt uit te voeren. Hierbij zouden alle relevante wetsartikelen aan de orde komen, van belang voor het toezicht door het agentschap. De uitgevoerde nulmeting heeft een beperkte scope en is gericht op de beantwoording van de vragen uit de Eerste Kamer. Bovendien is het onderzoek uitgevoerd binnen een aanzienlijk kortere tijdspanne dan oorspronkelijk was gepland.
In dit rapport zijn geen conclusies of bevindingen opgenomen die gericht zijn op traditionele telefonie, zowel via een vaste verbinding als mobiel. Dit behoort wel tot het toezicht van Agentschap Telecom, maar valt buiten de scope van het onderzoek. Ook het aanbieden van netwerken valt buiten de scope van de opdracht. De rapportage over de dienstverlening van de ISP's betreft dan ook alleen de onderwerpen "internet toegang", "email" en "internettelefonie".

3.1 Onderzoeksvraag.

Voorafgaand aan het onderzoek zijn, door de opdrachtgever[2], de onderzoeksvragen als volgt geformuleerd:

1. Wat is de "IST-situatie" bij de ISP's qua realisatie van de bewaarplicht en wat zijn de lopende ontwikkelingen door de providers zelf. Wanneer is de SOLL-situatie bereikt?
2. Is de beveiliging van de gegevens (conform het eveneens impliciet aangenomen Besluit beveiliging gegevens telecommunicatie) dan gewaarborgd?
3. Breng in kaart welke ISP's aangeven dat disproportionele investeringskosten (in relatie tot de bedrijfsomvang en het aantal bevragingen) de reden is waarom zij niet voldoen of binnen redelijke termijn gaan voldoen aan de eisen. En wel zodanig dat op basis van deze bevindingen er eventueel een gericht vervolgonderzoek gedaan kan worden naar de omvang en de legitimiteit van deze bezwaren.

Hiermee wordt beoogd een beeld te geven van:

- de huidige situatie bij de aanbieders met betrekking tot de verplichte opslag van gegevens[3];
- de huidige situatie met betrekking tot de genomen beveiligingsmaatregelen, zowel de beveiliging van de opgeslagen gegevens als de beveiliging van de ontvangen vorderingen, inclusief het daarbij behorende antwoord;
- de ontwikkelingen waar aanbieders mee bezig zijn op het gebied van dataretentie en beveiliging;
- het moment waarop de markt een situatie heeft bereikt waarbij gesproken kan worden van een correcte opslag van gegevens en voldoende beveiliging conform wet- en regelgeving;
- de mate waarin de investeringskosten zullen leiden tot het niet naleven van de wettelijke verplichtingen.

[1] Zie Handelingen 2008-2009 Eerste Kamer, nr. 40, pag. 1839-1862.
[2] Ministerie van Economische Zaken.
[3] Het betreft de door de aanbieder gegenereerde noodzakelijke gegevens, zoals beschreven in de bijlage bij de Wet bewaarplicht. Deze worden verder in het document aangeduid als "noodzakelijke gegevens".

3.2 Aanpak onderzoek.

Uitgangspunt voor de aanpak van het onderzoek is geweest, de mate waarin wordt voldaan aan wet- en regelgeving zoals opgenomen in de Wet bewaarplicht en het Besluit beveiliging gegevens telecommunicatie (Bbgt). Immers de wet, inclusief het Bbgt, betreft de opslag van gegevens, de beveiliging van de gegevens en de tijdige vernietiging daarvan.
Tevens geeft deze onderzoeksopzet een stabiel kader waarmee in een later stadium vervolgmetingen gedaan kunnen worden. Deze vervolgmetingen maken deel uit van het toezicht door Agentschap Telecom.

3.2.1 Vragenlijst / enquête.

Teneinde een correcte weergave van de huidige situatie te kunnen geven, is er voor gekozen om alle geregistreerde aanbieders die onder de Wet bewaarplicht vallen te bevragen. Zo is een enquête ontwikkeld met onderzoeksvragen. In bijlage 1 vindt u de vragen welke specifiek gericht zijn op het beantwoorden van de onderzoeksvraag. De beantwoording van deze vragen heeft de onderzoekers een eerste indruk gegeven van de huidige situatie bij de ISP's en de relevante toekomstige ontwikkelingen. Tevens geeft het de onderzoekers een eerste indruk van het moment waarop men denkt de SOLL-situatie (de gewenste situatie) te bereiken, te weten "het in beginsel voldoen aan de wet".

De enquête is aan 322 marktpartijen verstuurd. Deze aanbieders staan allen ingeschreven bij de OPTA in het register van openbare aanbieders.
Van deze 322 partijen zijn 138 volledig ingevulde vragenlijsten retour ontvangen die, vervolgens door de onderzoekers, voor nader onderzoek zijn gebruikt.
Op basis van de antwoorden kunnen de 138 partijen die de vragenlijst volledig ingevuld retour hebben gestuurd, aangemerkt worden als openbaar aanbieder die aan de Wet bewaarplicht moeten voldoen. Deze partijen vormen de volledige populatie voor de nulmeting.

24 Partijen hebben niet of niet tijdig gereageerd. Van de overige aanbieders is een antwoord ontvangen dat ofwel niet volledig was (een klein deel van de aanbieders) waardoor het niet verwerkt kon worden, ofwel hebben partijen aangegeven geen aanbieder te zijn onder hoofdstuk 13 van de Telecommunicatiewet. Door Agentschap Telecom worden deze overige geregistreerde aanbieders nader onderzocht. Zij vallen vooralsnog buiten de nulmeting.

De 138 onderzochte bedrijven zijn ingedeeld naar grootte op basis van de categorie-indeling van de OPTA[4]. Dit leidt tot de volgende verdeling van de markt:

- 18 grote aanbieders,
- 44 middelgrote aanbieders en
- 76 kleine aanbieders.

Een uitgebreide analyse van de antwoorden op de vragen heeft plaatsgevonden. Hierbij zijn de binnengekomen reacties bestudeerd en gescoord naar de verschillende onderwerpen.

Van de aangeschreven partijen hebben wij in 24 gevallen geen reactie ontvangen binnen de termijn (inclusief twee rappellen). Bij deze bedrijven is een bestuursrechtelijk traject gestart, waarbij een boete wordt aangekondigd voor het niet of niet tijdig reageren. Daarnaast worden deze bedrijven na afloop van de nulmeting, als eerste door Agentschap Telecom bezocht voor een inspectie.

3.2.2 Audits.

Om een beter inzicht in de antwoorden te krijgen en een verdieping te bereiken, is vervolgens een deel van de ISP's bezocht voor een audit. Deze ISP's zijn geselecteerd op basis van de criteria:

- omvang en
- geschat risico op basis van de antwoorden op de vragen.

[4] De OPTA hanteert drie categorieën op basis van de gerealiseerde omzet: kleine aanbieders hebben een omzet tot € 2.000.000,- per jaar, middelgrote aanbieders hebben een omzet tussen € 2.000.000,- en € 20.000.000,- per jaar en grote aanbieders hebben een omzet van € 20.000.000,- of meer per jaar.

Eveneens is besloten om aan de groep te bezoeken aanbieders nog een aantal bedrijven expliciet toe te voegen. Dit zijn:

- bedrijven waarvan op basis van de antwoorden op de vragenlijst en op basis van eerdere ervaring van Agentschap Telecom, het beeld bestaat dat zij "best in class"[5] zijn. Hiermee is de invulling van een referentiekader mogelijk, aan de hand waarvan getoetst kan worden of de aanbieders het momenteel maximaal haalbare gedaan hebben om te voldoen aan de wet- en regelgeving.
- bedrijven die zelf hebben aangegeven geen aanbieder te zijn, maar waarbij op grond van de door hen ingestuurde antwoorden op de vragen, gerede twijfel bij Agentschap Telecom is ontstaan of zij daadwerkelijk geen aanbieder zijn.

Binnen bovenstaand kader zijn 25 aanbieders bezocht. Bij deze ISP's is een audit uitgevoerd waarmee een verificatie- en verdiepingsslag heeft plaatsgevonden op de verstrekte informatie.

De inhoud van de audit betrof de inhoud van de Wet bewaarplicht met de bijlage en het Bbgt met bijlage, tegen de achtergrond van de gestelde vragen. Meer specifiek zijn de volgende vragen en thema's met de betreffende bedrijven doorgenomen[6]:

- De bekendheid met de wet- en regelgeving.
  Bij partijen die aangeven onduidelijkheden te ervaren met de wet- en regelgeving of zich hier nog niet in verdiept hebben, kunnen niet in staat geacht worden aan de voorschriften te voldoen. Dit wordt versterkt door de uiterst specifieke eisen die gesteld worden aan de beveiliging van de gegevens van de vorderingen en verzoeken.
- Welke producten en diensten worden door de betreffende partij aangeboden.
  Wat doet de aanbieder hierbij zelf en wat is uitbesteed aan derden.
  Deze gegevens zijn (mede)bepalend wat de aanbieder aan gegevens moet vastleggen en of er eventueel sprake is van een verplichte schriftelijke overeenkomst met die derden.
- Welke gegevens worden bewaard en welke termijn wordt hierbij gehanteerd.
  In de bijlage van de wet is opgenomen welke gegevens bewaard moeten worden. Daarnaast is bij vrijwel alle marktpartijen bekend dat er een wetsvoorstel in behandeling is om de bewaartermijn van de verkeersgegevens voor email en internet terug te brengen tot zes maanden. In ieder geval moet de aanbieder maatregelen genomen hebben voor een passende bewaartermijn.
- Waarborgen van de beveiliging van gegevens.
  Aan de hand van de eisen zoals gesteld in het Bbgt en in dat kader aan het beveiligingsplan, zijn de aanbieders bevraagd. Hierbij zijn alle punten (voor zover van toepassing voor de betreffende aanbieder[7]) aan de orde geweest.

Tijdens het auditgesprek is aandacht besteed aan het moment waarop de betreffende aanbieder volledig zal voldoen aan de Wet bewaarplicht. Hierover zijn ter plaatse afspraken gemaakt, vooral om te bevorderen dat de betreffende aanbieder een realistische inschatting maakt.

Daarnaast zijn tijdens de audit, de omzet van het bedrijf en de verwachte investeringskosten om te kunnen voldoen aan de wet, opgevraagd. Eveneens is getoetst of de hoogte van de investering een belemmering is om aan de wet te voldoen. Deze toets heeft plaatsgevonden door de aanbieder zelf te laten verklaren hoe hierover geoordeeld wordt.

Alle bezochte partijen zijn in de gelegenheid gesteld om op grond van een concept auditrapport op feitelijke onjuistheden te reageren. In de rapporten zijn deze onjuistheden in onderling overleg gecorrigeerd. De correcties betroffen geen essentiële punten.

[5] Het begrip "best in class" geeft het prestatie niveau aan binnen een industrie, dat gehanteerd wordt als een standaard of als een norm die gehaald of overtroffen moet worden.
[6] In bijlage 2 is een volledig overzicht van de tijdens de audit behandelde onderwerpen en vragen opgenomen.
[7] Niet alle voorschriften zijn altijd van toepassing. Indien de aanbieder bijvoorbeeld een deel van zijn dienstverlening / product heeft uitbesteed aan een derde, hoeft deze aanbieder niet zelf aan alle verplichtingen te voldoen. Echter de aanbieder heeft dan wel de verplichting om een schriftelijke overeenkomst met deze derde te sluiten waarin de verplichtingen van deze derde geregeld worden.

3.2.3 Verwerken resultaten

Door het uitvoeren van de audits is een verificatieslag uitgevoerd van de ingestuurde antwoorden en tevens een verdiepingsslag met betrekking tot de inhoud van de antwoorden.

De audits hebben eveneens inzicht gegeven in het rubriceren van de antwoorden op de vragen. Vervolgens zijn, op basis van de geformuleerde antwoordrubrieken, de reacties op de vragen ingedeeld.

De bevindingen zijn in kaart gebracht op basis van de volgende vragen:

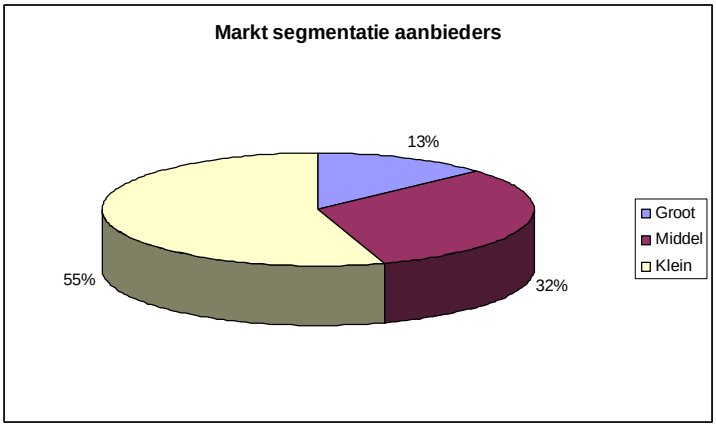
- Huidige situatie (IST):
    - Worden alle noodzakelijke gegevens bewaard per aangeboden product of dienst of betreft het slechts een gedeelte dan wel wordt er (vrijwel) niets bewaard?
    - Zijn de opgeslagen gegevens adequaat beveiligd?
    - Worden (in de toekomst) alle opgeslagen gegevens na afloop van de bewaartermijn adequaat vernietigd?
    - Zijn de “systemen” met betrekking tot het opvragen van de gegevens op basis van een vordering of verzoek adequaat beveiligd, inclusief de daarbij behorende procedures en voorwaarden?
- Wat doet de aanbieder om te gaan voldoen aan de wet- en regelgeving, voorzover die aanbieder nog niet gereed is?
- Wanneer is volgens opgave van de aanbieder de gewenste situatie (SOLL) bereikt?
- Wat verwacht de aanbieder aan noodzakelijke investeringen te moeten doen en is dit voor de aanbieder een belemmering om aan de wet te (gaan) voldoen?
- Overige bevindingen die uit de antwoorden op de vragen en uit de audits naar voren zijn gekomen.

4 Bevindingen.

In dit hoofdstuk zijn de bevindingen van de meting weergegeven. Hierbij zijn de bevindingen uit de audits gehanteerd als verificatie en verdieping van de antwoorden op de vragenlijst. De bevindingen worden per onderwerp uit de onderzoeksopdracht weergegeven.

Bij de weergave van de bevindingen is telkens, naast het totaal, een onderscheid weergegeven naar de grootte van de aanbieder volgens de categorieën die de OPTA hiervoor hanteert. Hiermee wordt het mogelijk om specifieke situaties voor deze categorieën duidelijk te maken.
De onderverdeling van de 138 verwerkte aanbieders naar deze categorieën is hierna weergegeven.

Overzichten marktsegmentatie aanbieders



	Totaal	Groot	Middel	Klein
Aantal aanbieders	138	18	44	76
In procenten	100	13%	32%	55%

Tijdens het onderzoek is duidelijk geworden dat er verschillen in de onderzoeksresultaten zijn, afhankelijk van de grootte van de aanbieder. Deze verschillen zijn wellicht te verklaren doordat grote organisaties meer capaciteit hebben om aanpassingen naar aanleiding van de Wet bewaarplicht te realiseren, dan kleine organisaties. Duidelijk is geconstateerd dat een beperkt aantal grote partijen op basis van hun betrokkenheid bij het implementatietraject van de Europese richtlijn in de Nederlandse wetgeving, anders scoren dan partijen die niet direct betrokken zijn geweest. Dit lijkt logisch gezien de voorsprong die de genoemde grote partijen hebben. Echter om een beeld van de gehele markt te verkrijgen zijn alle waarnemingen in het rapport verwerkt. Wel is het onderscheid tussen grote, middelgrote en kleine aanbieders overal weergegeven.

4.1 Huidige situatie bewaren noodzakelijke gegevens.

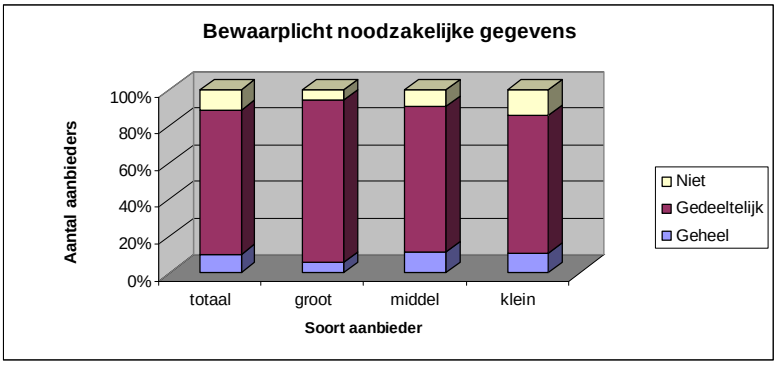
Als eerste is in beeld gebracht in hoeverre de aanbieders de noodzakelijke gegevens in de huidige situatie bewaren. Bij de bestudering van de antwoorden is een onderscheid gemaakt naar de volgende drie categorieën antwoorden:

- Geheel.
  De aanbieder bewaart alle gegenereerde gegevens per aangeboden product of dienst conform de bijlage van de wet.
  Dit betekent dat de aanbieder hiermee op het onderdeel “bewaren” voldoet aan de wet.
- Gedeeltelijk.
  De aanbieder bewaart slechts een gedeelte van de gegevens zoals die opgenomen zijn in de bijlage van de wet. Het betreft dan bijvoorbeeld de “billing-gegevens”. Deze zijn niet volledig, afgezet tegen hetgeen opgenomen is in de bijlage van de wet. Hierbij is rekening gehouden met het genereren van de gegevens.

Immers gegevens die niet gegenereerd worden hoeven ook niet bewaard te worden. Dit betekent dat de aanbieder op het onderdeel “bewaren” niet volledig voldoet aan de wet.

- Niet.
  De aanbieder bewaart de verplichte gegevens (nog) niet.
  Dit betekent dat de aanbieder op dit punt (nog) niet voldoet aan de wet.

Overzichten “bewaren gegevens” op basis van vragenlijst, in procenten.



	Totaal	Groot	Middel	Klein
Geheel	10,9%	11,1%	11,4%	10,5%
Gedeeltelijk	77,5%	83,3%	79,5%	75,0%
Niet	11,6%	5,6%	9,1%	14,5%

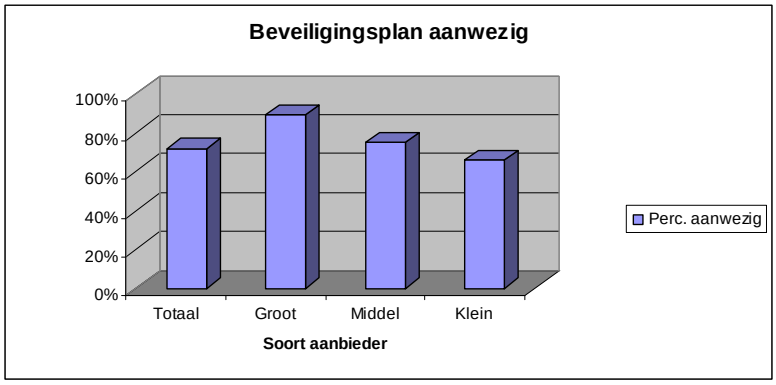
De score kan tot de conclusie leiden dat het bewaren van noodzakelijke gegevens (nog) niet goed ingevoerd is. Zowel uit de reacties op de vragenlijst als uit de audits blijkt dat de belangrijkste reden hiervoor is, de onduidelijkheid die de marktpartijen nog ervaren met betrekking tot de technische specificaties van de gegevens. In het bijzonder wordt aangegeven dat nog onvoldoende duidelijk is in welk technisch formaat de gegevens opgeslagen (en geleverd) moeten worden. Zolang dit niet duidelijk is wil men nog geen definitieve beslissing nemen over de realisatie. Immers in geval men de verkeerde beslissing neemt, moet er op een later moment nog een keer gebouwd / geïnvesteerd worden. Het kan dan namelijk zo zijn dat de opgeslagen gegevens, eerst geconverteerd moeten worden naar het formaat dat de behoeftesteller wil ontvangen. Dit zou een dubbele investering betekenen.

4.2 Huidige situatie beveiligen noodzakelijke gegevens.

Aanbieders zijn verplicht een beveiligingsplan te hebben waarin vastgelegd is hoe de beveiliging binnen de eigen organisatie is georganiseerd. Het Bbgt kent specifieke eisen waar het beveiligingsplan en dus de beveiliging aan moet voldoen. Het onderzoek naar de beveiliging van de noodzakelijke gegevens is gesplitst naar deze onderdelen.

Wat betreft het beveiligingsplan is onderzoek gedaan naar de aanwezigheid van het plan. Bovendien moet het beveiligingsplan opgezet zijn conform de eisen uit het Bbgt. De bevindingen op dit punt zijn als volgt:

Overzichten aanwezigheid “beveiligingsplan conform Bbgt” op basis van vragenlijst, in procenten.



	Totaal	Groot	Middel	Klein
Perc. aanwezig	72%	89%	75%	66%

Uit deze gegevens blijkt een trend dat, naarmate de aanbieder groter is, deze beter ingesteld is op het inrichten van een beveiligingsplan conform het Bbgt.

De conclusie dat het ontbreken van het voorgeschreven beveiligingsplan betekent dat de beveiliging niet gewaarborgd is, is onjuist. Echter, het is wel een indicatie of er maatregelen genomen zijn zoals die in het Bbgt zijn voorgeschreven.

Naast de aanwezigheid van een beveiligingsplan, moet de aanbieder, om de gegevens adequaat te beveiligen, voldoen aan de eisen zoals opgenomen in het Bbgt. Deze eisen zijn meegenomen in de audit en staan als zodanig verwoord in bijlage 2.
Hiervoor zijn de reacties verdeeld over de volgende rubrieken:

- Conform Bbgt.
  De aanbieder heeft ten behoeve van de beveiliging van de gegevens alle maatregelen zoals beschreven in het Bbgt in essentie genomen.
- Standaard of gedeeltelijk beveiligd.
  De beveiliging van de aanbieder voldoet slechts gedeeltelijk aan de eisen uit het Bbgt. Voorbeelden hiervan zijn een beveiligingsniveau dat voldoet aan het Bbgat[8], de ISO 27001 norm voor informatiebeveiliging, een proactieve inrichting van de beveiligingsmogelijkheden die het gebruikte platform en systeem kent.
- Onvoldoende beveiligd.
  De beveiliging van de aanbieder gaat niet verder dan de standaardbeveiliging die het platform biedt. Hier wordt niet op een proactieve manier mee omgegaan.

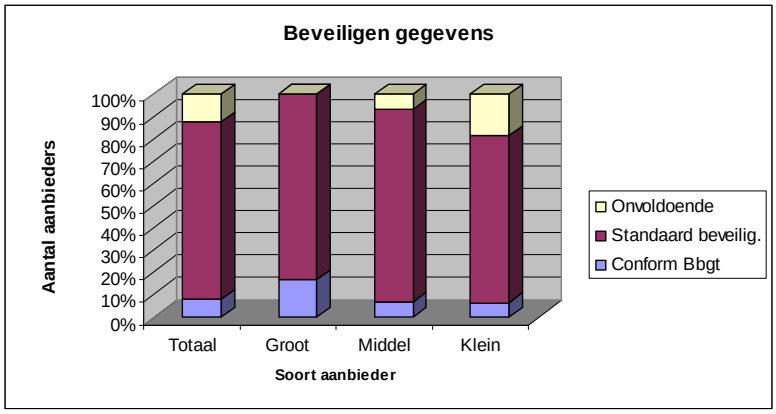
Het merendeel van de bedrijven heeft de beveiliging op een “standaard” wijze gerealiseerd. Zoals aangegeven betekent dit een beveiliging conform het Bbgat, de ISO 27001 norm voor informatiebeveiliging of een proactieve wijze van omgaan met de beveiligingsmogelijkheden die meegeleverd worden met het geïnstalleerde platform. Dit laatste wil zeggen dat de beveiligingsmogelijkheden zoals die door de leverancier van het platform of de softwareomgeving worden aangeboden, nadrukkelijk zijn ingesteld door de aanbieder. Hiermee wordt een aanzienlijk hoger beveiligingsniveau gerealiseerd dan wanneer dit niet proactief gebeurt.

Partijen die voldoen aan het Bbgt hebben, ten opzichte van beveiliging volgens het Bbgat, tevens geregeld dat de tijdelijke bestanden die binnen hun organisatie ontstaan naar aanleiding van een vordering of verzoek, voldoen aan de daaraan gestelde beveiligingseisen. Daarnaast is bij deze bedrijven geregeld dat de opgeslagen noodzakelijke gegevens binnen acht dagen na de voorgeschreven bewaartermijn onomkeerbaar worden vernietigd.

[8] Bbgat staat voor het “Besluit beveiliging gegevens aftappen telecommunicatie”, de voorloper van het Bbgt.

Bovendien is bij deze bedrijven geregeld dat de ontvangen vorderingen, verzoeken inclusief de antwoorden daarop binnen de daarvoor gestelde termijn op de voorgeschreven wijze vernietigd worden.

Overzichten “beveiligen gegevens” op basis van vragenlijst, in procenten.



	Totaal	Groot	Middel	Klein
Conform Bbgt	8%	17%	7%	7%
Standaard beveilig.	80%	83%	86%	75%
Onvoldoende	12%	0%	7%	18%

ISO 27001 betreft een internationale standaard voor informatiebeveiliging. In de standaard wordt beschreven hoe informatiebeveiliging procesmatig ingericht kan worden, om de beveiligingsmaatregelen uit de ISO/IEC 17799 norm te effectueren.
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.

Wanneer een aanbieder in de bedrijfsvoering van zijn gehele organisatie of de noodzakelijke delen daarvan, rekening heeft gehouden met de Wet bewaarplicht, hoeft zij weliswaar niet te voldoen aan de eisen zoals gesteld aan het beveiligingsplan, maar kunnen de genomen beveiligingsmaatregelen wel voldoende zijn.
Ook hier geldt dus dat gezien het specifieke karakter van de eisen in het Bbgt en het voorgeschreven beveiligingsplan, het beeld dus niet wil zeggen dat de partijen die hier conform Standaard beveiliging scoren, niets hebben gedaan aan beveiliging. Echter, zij voldoen niet aan de specifiek gestelde eisen.

4.3 Huidige situatie vernietigen gegevens.

Aanbieders zijn verplicht de gegevens binnen acht dagen na de bewaartermijn te vernietigen. De reacties zijn verdeeld over de volgende mogelijkheden:

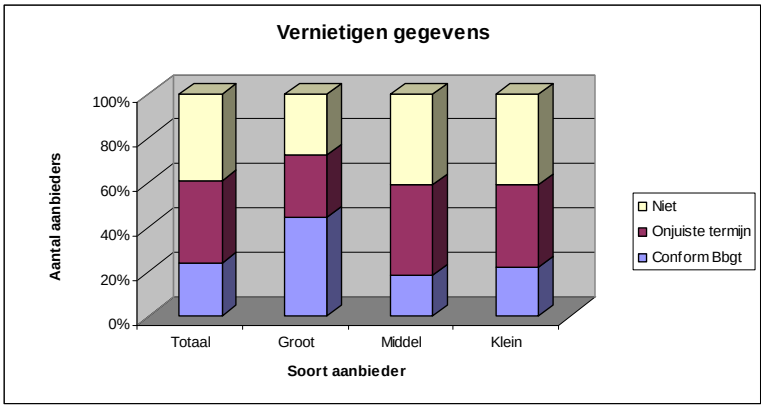
- Conform Bbgt.
  De aanbieder heeft alles geregeld om, conform het Bbgt, de gegevens binnen acht dagen na de bewaartermijn onomkeerbaar te vernietigen.
- Onjuiste termijn.
  De aanbieder vernietigt de gegevens wel, maar doet dit niet binnen de termijn van acht dagen na afloop van de bewaartermijn. Hierbij is zowel “te vroeg” als “te laat” vernietigen opgenomen.
- Niet.
  De aanbieder vernietigt de gegevens niet.

Uit de audits komt nadrukkelijk naar voren dat de aanbieders het onderwerp vernietiging van de opgeslagen gegevens wel in hun project / planning hebben opgenomen. Echter omdat vernietigen van de opgeslagen gegevens pas speelt vanaf 1 september 2010, hebben veel aanbieders dit nog niet geregeld. De datum 1 september 2010 is gerelateerd aan de datum van inwerkingtreding van de wet (1 september 2009) en de verplichte bewaartermijn van één jaar. In de nulmeting is op dit onderdeel geen rekening gehouden met het voorliggende wetsvoorstel waarin de bewaartermijn voor internet wordt verkort tot zes maanden.

Een aantal aanbieders hanteert een andere termijn voor de vernietiging. Hierbij is vrijwel altijd sprake van een verbinding met andere wetgeving. Vaak is gesignaleerd dat bijvoorbeeld op grond van fiscale wetgeving, de bewaartermijn door de aanbieders op zeven jaar is ingesteld.

Voor het vernietigen van de gegevens betreffende de door de aanbieder ontvangen vorderingen en verzoeken, is tijdens de audits geconstateerd dat dit beter geregeld is dan het vernietigen van de opgeslagen gegevens. Echter er is vrijwel geen enkele aanbieder die hierover de verplichte rapportage aan de behoeftesteller stuurt. Tevens wordt hier door de aanbieders over opgemerkt dat de behoeftestellers daar ook niet naar vragen.

Overzichten “vernietigen gegevens” op basis van vragenlijst, in procenten.



	Totaal	Groot	Middel	Klein
Conform Bbgt	24%	44%	18%	22%
Onjuiste termijn	37%	28%	41%	37%
Niet	39%	28%	41%	41%

Als bezwaar tegen de vernietiging van de vorderingen, maar vooral de vernietiging van de op basis hiervan verstuurde gegevens naar de behoeftesteller, wordt gemeld dat aanbieders deze gegevens willen bewaren vanwege juridische aspecten.
Het gaat hierbij om:

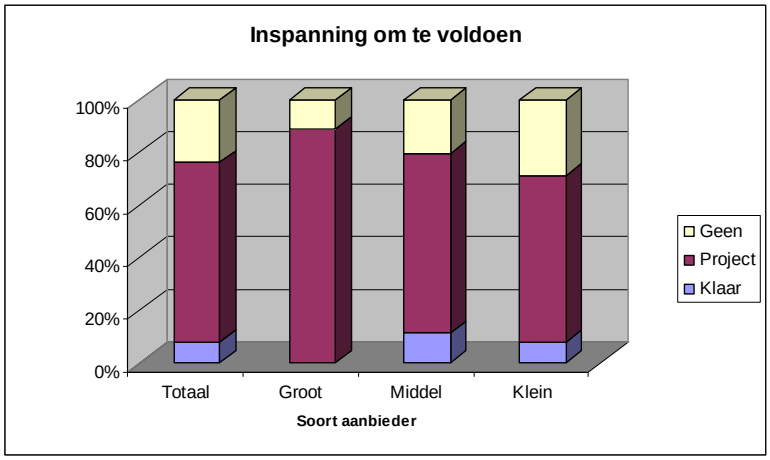
- "onduidelijke communicatie van de behoeftesteller met betrekking tot de ontvangst van de opgevraagde gegevens".
  Zolang de aanbieder geen bevestiging van ontvangst heeft gekregen en daarmee heeft voldaan aan zijn wettelijke verplichting, houdt deze aanbieder uit voorzorg voor een herhaalde vraag de gegevens vast.
- "juridische aspecten naar de klant"
  Idem als voorgaande maar dan ter bescherming van de eigen organisatie richting de klant.

4.4 Lopende ontwikkelingen aanbieders.

De meeste aanbieders zijn al enige tijd bezig met de invoering van maatregelen in hun organisatie om te (gaan) voldoen aan de Wet bewaarplicht. Uit het onderzoek blijken verschillende stadia waar aanbieders in zitten. De volgende onderverdeling van de reacties is gehanteerd:

- Conform Wet en Bbgt.
  Dit betekent dat de aanbieder voldoet aan de Wet bewaarplicht en het Bbgt.
- Aanbieder heeft een lopend project.
  De aanbieder voldoet nog niet aan de wet. De aanbieder heeft wel een project in uitvoering met als gedefinieerd projectresultaat: "voldoen aan de wet". Dit project kent een duidelijke opleverdatum.
- Nog geen actie.
  De aanbieder voldoet niet aan de wet en heeft ook nog geen actie ondernomen om te gaan voldoen.

Overzichten "lopende ontwikkelingen" op basis van vragenlijst, in procenten.



	Totaal	Groot	Middel	Klein
Conform Wet & Bbgt	8%	0%	11%	8%
Project	68%	89%	68%	63%
Geen	24%	11%	20%	29%

De grote aanbieders zijn voorzichtiger in hun uitspraken over de status van hun voorbereidingen dan de middelgrote en de kleine aanbieders. Tijdens de audits zijn grote partijen bezocht die vrijwel geheel voldoen. Voor deze aanbieders is de aanduiding "vrijwel", voldoende om aan te geven dat zij nog niet gereed zijn. Kleine aanbieders zijn eerder genegen om te verklaren dat zij gereed zijn.

Inhoudelijk geven aanbieders aan dat zij, naast maatregelen om de noodzakelijke gegevens te gaan bewaren, ook maatregelen nemen m.b.t. de beveiliging.
Veel aanbieders die gebruik maken van ketenpartners waar zij delen van hun dienstverlening inkopen, hebben nog niet goed begrepen wat zij dan wel moeten regelen. Het sluiten van een inhoudelijk goede, schriftelijke overeenkomst waarin de ketenpartner aangeeft “aan de wet en Bbgt te voldoen” is slechts bij een beperkt aantal partijen daadwerkelijk gerealiseerd.
De projecten omvatten daarnaast ook het inrichten van een beheersorganisatie, noodzakelijk om het “systeem” binnen hun organisatie blijvend goed te laten functioneren. Aan de investeringskant komt dit telkens terug.

Een grote groep aanbieders is bezig met een derde om hun systeem en organisatie op orde te krijgen. Uit het onderzoek blijkt dat deze partijen de uitvoering van de maatregelen zoveel mogelijk bij deze tussenpersoon leggen. Het grootste deel van deze groep geeft weliswaar aan bezig te zijn met een project, maar laat dit project in praktijk geheel door de tussenpersoon uitvoeren.
Op basis van de gegeven antwoorden (inclusief ontvangen beveiligingsplannen) is er gerede twijfel bij Agentschap Telecom of deze aanbieders de overeenkomst met de derde adequaat geregeld hebben.

4.5 Gewenste situatie bereikt.

De aanbieders is gevraagd om op te geven wanneer zij volledig denken te voldoen aan Wet- en regelgeving. Een grote groep aanbieders geeft hierbij geen termijn aan wanneer zij gereed zijn. Overigens geeft deze groep wel aan ergens in 2010 te gaan voldoen.

Van de aanbieders die wel een termijn noemen geeft het overgrote deel aan vóór de zomer van 2010 gereed te zijn. Hierbij dient wel opgemerkt te worden dat de bezochte bedrijven hun planning naar aanleiding van de audit hebben aangepast. Dit betreft in het bijzonder de kleine en middelgrote aanbieders. Tijdens de audits zijn er afspraken gemaakt, vooral om de door hen genoemde datum zo realistisch mogelijk vast te stellen. Het effect hiervan is geweest dat de data naar achteren zijn geschoven, waarbij de einddatum wel nog steeds in 2010 valt.

Bij veel partijen wordt de planning duidelijk beïnvloed door de onduidelijkheid die de aanbieders ervaren met betrekking tot de “technische invulling van de te bewaren en te leveren gegevens”. De meeste bezochte aanbieders geven desondanks een datum af waarop zij verwachten te voldoen aan de wet- en regelgeving.

4.6 Investeringskosten aanbieders.

Uit het onderzoek is gebleken dat de aanbieders onderscheid maken uit de volgende te maken kosten(posten) om te (gaan) voldoen aan de wet:

- Investeringskosten betreffende een systeem om de noodzakelijke gegevens te bewaren;
- Investeringskosten betreffende een systeem om de ontvangen vorderingen en verzoeken te kunnen beantwoorden;
- Exploitatiekosten om de eerdergenoemde systemen in een zodanige staat van onderhoud te houden dat voldaan kan worden aan het onverwijld antwoorden op een vordering of verzoek;
- Exploitatie- en administratiekosten om te voldoen aan een feitelijke vordering of verzoek.

Vrijwel alle bezochte bedrijven geven aan slechts het eerste gedeelte van de investering op dit moment te kunnen overzien. Vanwege het ontbreken van duidelijkheid over de technische specificaties met betrekking tot het aanleveren van de gegevens aan een behoeftesteller, kan alleen een schatting gegeven worden over de investering om een systeem te bouwen voor het bewaren van de gegevens. Deze investering wordt door de aanbieders niet als een belemmering gezien om te voldoen aan de wet.

De investering die gedaan moet worden om de vorderingen en verzoeken te beantwoorden kan vanwege de onduidelijkheid over de technische specificaties nog niet goed geschat worden.

Vrijwel alle aanbieders maken hierbij een voorbehoud. Dit is tevens van invloed op de planning van het project waarmee de aanbieders zullen gaan voldoen.

Vanwege de mogelijkheid om de inhoudelijke kant van de levering van de gegevens met een Algemene Maatregel van Bestuur te regelen en vanwege het lopende dataretentieproject binnen het Ministerie van Justitie, wachten veel aanbieders op invulling van de technische specificaties om maar één keer een ICT-systeem te hoeven ontwerpen en bouwen.

Naast de investeringskosten geven de aanbieders aan, hoge operationele kosten te verwachten om het systeem goed te kunnen laten functioneren (exploitatiekosten, m.u.v. de daadwerkelijke kosten voor de beantwoording van vorderingen en verzoeken). Deze mening van de aanbieders is nog niet verder onderzocht.

De kleine aanbieders verwachten over het geheel te maken te krijgen met een grotere financiële belasting dan door hen was voorzien. Dit wordt vooral veroorzaakt door het voorgaande in combinatie met het geringe aantal vorderingen en verzoeken die zij verwachten te krijgen. Zij gaan er vanuit extra kosten te moeten maken, zowel m.b.t. de afschrijving van hun investering als operationele kosten om het systeem up-to-date te moeten houden, waar onvoldoende dekking tegenover zal staan. Ook deze mening van de aanbieders is niet verder onderzocht.

4.7 Bevindingen audits.

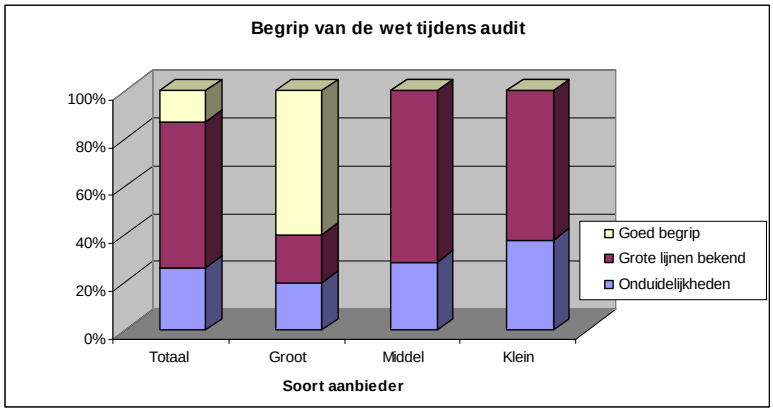
Tijdens de audits zijn nog specifieke bevindingen gedaan, waaruit extra inzichten zijn af te leiden. Vooral de kennis en het begrip van de Wet bewaarplicht en het Bbgt blijken medebepalend te zijn voor de score van de aanbieder.

Tijdens de bezoeken is specifiek gevraagd naar de mate van kennis van de wet en het Bbgt en hoe die is opgedaan. Ook is tijdens de bezoeken ingegaan op het begrip dat de aanbieder heeft van de materie. Dit is gedaan door tijdens het gesprek regelmatig het begrip te toetsen.
In deze rapportage wordt onderscheid gemaakt tussen:

- Goed.
  De aanbieder beheerst de wet en het Bbgt zodanig, dat verwacht mag worden dat de aanbieder zonder veel extra kennis en / of begrip op een juiste wijze zal voldoen aan de wet en het Bbgt.
- Grote lijnen bekend.
  De kennis en het begrip van de aanbieder m.b.t. de wet en het Bbgt zijn in grote lijnen aanwezig. Op specifieke punten is nog extra kennis / inzicht noodzakelijk om de mate van naleving goed te kunnen noemen.
- Onduidelijkheden.
  De aanbieder heeft een duidelijke achterstand in kennis en begrip van de wet en het Bbgt. Hij ervaart nog meerdere onduidelijkheden. Betreffende organisaties mogen dan ook niet in staat worden geacht om, zonder extra ondersteuning, te voldoen aan de wet en het Bbgt.

Tijdens de bezoeken is nadrukkelijk aan de orde geweest dat de aanbieders nog wachten op meer duidelijkheid betreffende de definitie van vast te leggen gegevens en de wijze waarop de aanbieders de opgeslagen gegevens moeten gaan aanleveren.

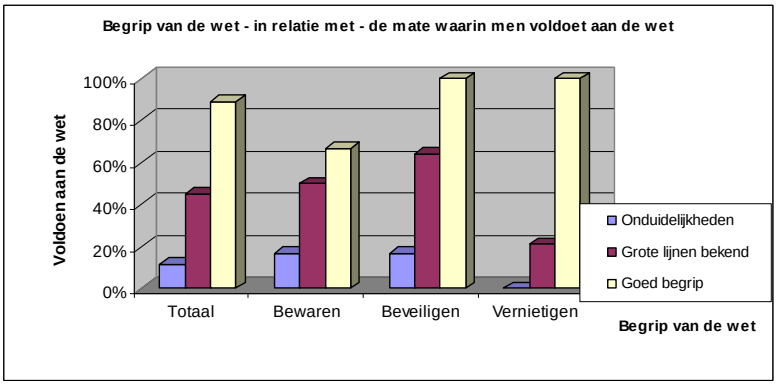
Overzichten “begrip van de wet” in relatie tot grootte op basis van audits, in procenten.



Bekendheid wet	Totaal	Groot	Middel	Klein
Onduidelijkheden	26%	20%	29%	38%
Grote lijnen bekend	61%	20%	71%	62%
Goed begrip	13%	60%	0%	0%

In onderstaand overzicht is weergegeven de relatie tussen het begrip van de wet inclusief het Bbgt en het effect daarvan op de mate waarin men voldoet. Hieruit blijkt dat naarmate de wet en het Bbgt beter begrepen worden, de mate van naleving ook toeneemt. Deze tendens werd waargenomen tijdens het afnemen van de audits. De percentages in onderstaande diagram en tabel, hebben alleen betrekking op de partijen die door de onderzoekers zijn bezocht.
De bedrijven die weinig of geen kennis hebben van wet- en regelgeving, scoren beduidend slechter op de onderwerpen bewaren van gegevens en op de beveiliging.

Overzichten “begrip van wet en Bbgt” in relatie tot de mate van voldoen, op basis van audits.



N.a.v. audits	*Percentage aanbieders dat aan de wet voldoet*			
Bekendheid wet	Totaal	Bewaren	Beveiligen	Vernietigen
Onduidelijkheden	11%	17%	17%	0%
Grote lijnen bekend	45%	50%	64%	21%
Goed begrip	89%	67%	100%	100%

4.8 Overige bevindingen.

Tijdens de bezoeken is aan de aanbieders gevraagd welke onderwerpen zij nog aan de orde wilden stellen, voor zover niet in de vragenlijst en de auditvragen aan de orde zijn gekomen. Hiervan is door de aanbieders in de meeste gevallen gebruik gemaakt. De volgende onderwerpen zijn hierbij aan de orde gekomen:

- Onduidelijkheid in wet- en regelgeving.
  Hiermee wordt bedoeld dat het de aanbieder niet duidelijk is op welke wijze de gegevens opgeslagen moeten worden (in technische zin). Het doel is duidelijkheid te krijgen over de wijze waarop de gegevens geleverd moeten worden aan de behoeftestellers.
  Een eventuele conversie bij de aanbieder van het eigen opslag formaat naar het gewenste formaat voor levering, is voor de aanbieder een risico voor hogere (investerings-)kosten dan gewenst en nodig. Vanwege de bestaande onduidelijkheid over deze technische specificaties zijn veel aanbieders nog niet gereed met het bouwen van hun systeem voor dataretentie. Dit is voor de aanbieders een belangrijk gegeven met betrekking tot de naleving en vooral, met betrekking tot de te maken kosten / investering. Een enkeling heeft de oplossing al gebouwd, maar is daarbij uitgegaan van de eigen interpretatie van de wet- en regelgeving. Zie ook de tekst van paragraaf 4.6 Investeringskosten aanbieders.
  Dit onderwerp is door bijna 65% van de bezochte aanbieders genoemd. Dit getal ligt voor alle respondenten van de vragenlijst boven de 50% en wordt dus door het overgrote deel van de markt genoemd.

- (On)zorgvuldigheid omgang met vorderingen en verzoeken door behoeftestellers.
  In 20% van de bezoeken is door de aanbieder op een of andere manier gerefereerd aan de handelwijze van behoeftestellers betreffende het indienen van een vordering of verzoek bij de aanbieder. De marktpartijen die dit hebben genoemd, hebben allen ervaring met een onzorgvuldige wijze waarop het verzoek bij hen terecht is gekomen. Zo zijn er partijen waar bijvoorbeeld een vordering of verzoek op een centrale fax binnenkomt zonder dat hier van te voren contact over is geweest, of zelfs terwijl er duidelijke afspraken gemaakt zijn met betreffende behoeftesteller over de wijze van indienen.
  Deze partijen hebben hier allen aanmerkelijk bezwaar tegen, mede vanwege de eisen die gesteld worden aan de aanbieders met betrekking tot de waarborgen van de beveiliging van de vorderingen en verzoeken.

- Dialoog met de overheid / meer informatie.
  Eveneens heeft 20% van de bezochte aanbieders aangegeven last te hebben van een “informatieachterstand”. Hierbij wordt zowel gerefereerd aan de bijzondere positie van de deelnemers aan het “Overleg grote aanbieders” als aan de informatieverstrekking van de overheid in het algemeen.
  Een aantal partijen geeft aan graag eerder betrokken te zijn geweest in een dialoog met de overheid, iets dat voorbehouden is geweest aan de vijf grote aanbieders die betrokken zijn geweest bij de invoering van de Europese richtlijn in het Overleg grote aanbieders”.
  Hierdoor zijn in hun ogen specifieke problemen en mogelijke oplossingen van middelgrote en kleine aanbieders onvoldoende meegenomen in het proces.
  Daarnaast hebben deze partijen aangegeven een informatietekort te hebben ervaren van de zijde van de overheid. De informatiestroom is volgens deze aanbieders te laat op gang gekomen en vooralsnog onvolledig.

- Valt mijn product / dienst wel onder de Wet bewaarplicht.
  In 16% van de bezoeken is de vraag aan de orde gekomen of een product of dienst onder de Wet bewaarplicht valt. Hierbij zijn deze vragen ofwel gericht op de gehele aanbieder (bijvoorbeeld als een aanbieder onder eigen label producten of diensten verkoopt, maar deze of een gedeelte inkoopt bij een andere aanbieder), ofwel gericht op een specifiek onderdeel zoals bijvoorbeeld WiFi access points.

5 Conclusies.

De hoofdlijnen van de bevindingen kunnen als volgt weergegeven worden:

1. Het merendeel van de aanbieders heeft de intentie om de verplichtingen na te leven zoals die opgelegd worden door de Wet bewaarplicht en het Besluit beveiliging gegevens telecommunicatie. Slechts bij een enkeling is geconstateerd dat er onwil bestaat om te voldoen aan de wet.

2. In de huidige situatie zijn vrijwel alle partijen bezig met de voorbereidingen om te komen tot naleving. Een zeer grote groep wacht hierbij op de technische specificaties.

3. Gevolg van punt 2 is dat de meeste partijen op dit moment nog niet alle noodzakelijke gegevens bewaren. Het bewaren van alle noodzakelijke gegevens is wel in de planning van de aanbieders opgenomen.

4. Bedrijven die op dit moment nog niet alle noodzakelijke gegevens bewaren, hebben meestal wel een gedeelte van de gegevens opgeslagen. Het betreft dan vrijwel altijd gegevens voor facturatie.

5. Met betrekking tot de beveiliging van de gegevens en het proces moeten de meeste bedrijven nog gaan voldoen aan de specifieke eisen van het Besluit beveiliging gegevens telecommunicatie (Bbgt). Het grootste deel van de aanbieders heeft wel enige mate van actieve beveiliging ingericht, maar moet nog een slag maken om te voldoen aan de strikte eisen van het Bbgt.

6. Vernietiging van de opgeslagen gegevens moet nog geregeld worden. Dit is vrijwel overal een punt van aandacht en als zodanig opgenomen in de planning, maar wordt voor de aanbieders pas actueel in september 2010. Dat is immers het eerste moment waarop vernietiging aan de orde is (één jaar na invoering van de Wet bewaarplicht op 1 september 2009).

7. Naar eigen zeggen verwacht de markt dat de gewenste situatie voor het eind van 2010 bereikt zal zijn. Dit wordt mede bepaald door de snelheid waarmee duidelijkheid komt over het technische formaat waarin de gegevens opgeslagen (en geleverd) moeten worden.
   Hierbij kan nog een voorbehoud gemaakt worden voor de tijdige afronding van de functionaliteit met betrekking tot de vernietiging van de gegevens. Het is niet automatisch gegarandeerd dat ook deze functionaliteit in 2010 daadwerkelijk gereed zal zijn.

8. De investeringen die aanbieders moeten doen om een systeem voor “het bewaren van de noodzakelijke gegevens” te ontwikkelen, vormen vooralsnog geen belemmering om aan de wet te voldoen.

9. Op het gebied van investeringen maakt de markt zich zorgen over het ontbreken van de technische specificaties. Partijen willen niet investeren voordat duidelijk is op welke wijze de overheid (lees de inlichtingen- en opsporingsdiensten) de gegevens vastgelegd en geleverd willen hebben.

10. De markt maakt zich daarnaast zorgen over de extra operationele kosten die gemaakt moeten worden om het systeem te laten functioneren en daarmee gereed te zijn voor het onverwijld leveren in geval van een eventuele vordering of verzoek, zeker als dit wordt gezien in relatie tot een beperkt aantal vorderingen en verzoeken.

11. De markt beschouwt de informatievoorziening en de voorlichting vanuit de overheid met betrekking tot de wet als onvoldoende. Een betere voorlichting en een intensievere dialoog, vooral met meer partijen, had volgens de markt dit gevoel kunnen voorkomen.

12. De markt heeft af en toe moeite met de wijze waarop opsporingsdiensten omgaan met hun vorderingen en verzoeken tot het leveren van gegevens. Zeker als dit wordt beschouwd in relatie tot het zware beveiligingsniveau dat aan de marktpartijen wordt opgelegd.

Bijlagen

Bijlage 1 Vragenlijst zoals verstuurd aan de ISP’s.

Bijlage 2 Onderwerpen zoals behandeld tijdens de audits van de ISP’s.

Bijlage 1 Vragenlijst zoals verstuurd aan de ISP's.

Vragen

1. Kenmerkt uw organisatie/bedrijf zich als Internet Service Provider of als aanbieder van openbare telecommunicatiediensten? Zo nee, waarom niet?

2. Omschrijft u de omvang van uw organisatie als groot, middel of klein? Licht uw keuze toe.

3. Worden de bij uw dienstverlening gegenereerde verkeers- en locatiegegevens, zoals bedoeld in de Telecommunicatiewet, door uw organisatie opgeslagen? Zo ja, geef per dienst aan welke gegevens dit zijn? (zie voor bedoelde verkeers- en locatiegegevens bijlage 1).

4. Welke typen gegenereerde verkeers- en locatiegegevens worden nog niet opgeslagen en wat is de reden daarvoor? Wanneer denkt uw organisatie deze gegevens wel te kunnen opslaan? Licht uw antwoord toe.

5. Met welke maatregelen of procedures wordt zeker gesteld dat de opgeslagen gegevens na de gestelde bewaartermijn worden vernietigd?

6. Wat zijn bij uw organisatie de technische en/of organisatorische ontwikkelingen om te voldoen aan de wet bewaarplicht en op welke termijn verwacht uw organisatie hieraan (volledig) te voldoen?

7. Hoe heeft uw organisatie de beveiliging van verkeersgegevens gewaarborgd? Hoe is dit vastgelegd?

8. Kunt u aangeven wat de impact is van deze wetgeving op uw organisatie? Geef een overzicht van de kosten die uw organisatie denkt te maken om aan de bewaarplicht te voldoen. (graag uitsplitsen naar inzet van menskracht en techniek)

9. Is er een beveiligingsplan[9], zoals bedoeld in het Besluit beveiliging gegevens telecommunicatie of zoals bedoeld in het al bestaande Besluit beveiliging gegevens aftappen telecommunicatie? (zie bijlage 2)
   Ik verzoek u een afschrift of actualisatie van uw beveiligingsplan aan Agentschap Telecom toe te zenden.

10. Ik vraag u een actueel organogram van uw organisatie op te sturen. Wilt u hierbij ook aangeven welke ketenpartners eventueel bijdragen aan het verzorgen van uw telecommunicatiediensten en welke rol deze in het proces hebben?

[9] Aanbieders van openbare telecommunicatienetwerken en/of -diensten zijn op basis van de Wet bewaarplicht verplicht in het bezit te zijn van een beveiligingsplan.

Bijlage 2 Onderwerpen zoals behandeld tijdens de audits van de ISP's.

Vragen / onderwerpen per onderdeel

Bekendheid met wet- en regelgeving

- Hoe bent u erachter gekomen dat er een nieuwe wet is?
- Bent u bekend met de nadere regelgeving, het BBGT?
- Begrijpt u de wet, het BBGT en de bijlagen?
- Heeft u de vragenlijst, naar uw eigen mening, volledig kunnen invullen? Wilt u de door u gegeven antwoorden nog verder verduidelijken?

Aanbod van ISP inclusief bewaren gegevens

- Welke diensten en/of producten biedt u aan
- Wat levert u daarbij zelf en wat is uitbesteed aan ketenpartner(s)
- Per aangeboden dienst / product:
    - Worden de noodzakelijke gegevens bewaard
    - Welke bewaartermijn wordt gehanteerd

Beveiligingsplan

I. Beveiligingseis algemeen
Er is een functionaris, belast met het toezicht op de uitvoering en naleving van de beveiligingsmaatregelen, de security officer. Deze dient regelmatig controles uit te voeren en de resultaten vast te leggen.

II. Beveiligingseisen ten aanzien van personeel

a. In de functiebeschrijving van personeel dat in aanraking komt met de informatie en gegevens, wordt de verantwoordelijkheid voor de beveiliging daarvan beschreven.
b. Er dient een geheimhoudingsverklaring te zijn voor personeel dat in aanraking komt met de informatie en gegevens.
c. Uitsluitend personeel dat overeenkomstig de functiebeschrijving belast is met de verwerking van de informatie en gegevens heeft toegang tot de informatie en de gegevens.

III. Fysieke beveiliging en beveiliging van de omgeving

a. De informatie en de gegevens voortvloeiende uit een vordering worden zoveel mogelijk binnen één ruimte geconcentreerd.
b. De ruimte waarbinnen de informatie en de gegevens voortvloeiende uit een vordering aanwezig zijn is deugdelijk fysiek beveiligd.
c. De fysieke beveiliging is zodanig ingericht dat ongeautoriseerde toegang en pogingen worden gedetecteerd. Daarnaast dient men tijdig hierop te reageren.
d. Enkel geautoriseerde personen mogen indien noodzakelijk toegang hebben tot de ruimte waar de gegevens of de informatie zich bevindt.
e. Het binnentreden en verlaten van de ruimte dient individueel te worden gelogd en achteraf herleidbaar te zijn.
f. Er dienen deugdelijke beveiligde opbergmiddelen gebruikt te worden voor de documenten of verwisselbare gegevensdragers waar de informatie en de gegevens zichtbaar zijn.
g. Eigen personeel begeleidt derden met onderhoud- en reparatiewerkzaamheden in de ruimte waarin de informatie en de gegevens zich bevinden.

IV. Beheer van communicatie- en bedieningsprocessen

a. Er dient een rubricering (staatsgeheim of vertrouwelijk) te worden aangebracht aan vordering.
b. De vordering mag alleen worden gereproduceerd door daartoe geautoriseerde persoenen.
c. De vordering mag niet buiten de normale werkruimte gebracht. Wanneer dit wel gebeurd dient men dit te registreren.

d. De verwijdering en vernietiging van de vordering moet onomkeerbaar zijn. Hiervan word een rapport opgemaakt, met een afschrift aan de bevoegde autoriteit wie het aangaat dan wel een door deze aangewezen instantie.

V. Toegangsbeveiliging van geautomatiseerde informatiesystemen
a. Het systeem waarin de informatie en gegevens worden verwerkt dient op deugdelijke wijze te worden beveiligd. Onder meer door middel van persoonsgebonden authenticatie.
b. De beveiliging van het systeem wordt zodanig ingericht dat ongeautoriseerde toegang en pogingen daartoe worden gedetecteerd. Daarnaast dient men hier tijdig op te reageren.
c. Het aantal foutieve inlogpogingen is beperkt tot drie, hierna dient blokkering plaats te vinden. Deze blokkering mag alleen door de beveiligingsfunctionaris worden opgeheven. Met uitzondering van de systeembeheerder.
d. Men mag het systeem niet eerder verlaten voordat de computer gelockt (handmatig dan wel automatisch) is.
e. De handelingen met betrekking tot de verwerking van informatie en gegevens dienen persoongebonden te worden gelogd.
f. Enkel geautoriseerd personeel heeft toegang tot het systeem.
g. De toegangsrechten van de gebruikers worden periodiek geëvalueerd.
h. De autorisaties van alle gebruikers worden vastgelegd.

VI. Ontwikkeling, onderhoud en reparatie van geautomatiseerde informatiesystemen
a. De aanbieder moet alle de wijzigingen in apparatuur, software of procedures die de beveiliging van de gegevens en informatie kunnen beïnvloeden beoordelen. Tevens moet de wijziging controleerbaar zijn.
b. Het onderhouden van de systemen vindt op locatie plaats.
c. Bij onderhoud op afstand moet er toestemming zijn van de beveiligingsfunctionaris. Tevens moeten er voldoende aantoonbare waarborgen zijn voor het beveiligingsniveau van informatie en gegevens.
d. Reparatie aan het geautomatiseerde van het systeem vindt op locatie plaats. Tenzij de informatie en gegevens zijn verwijderd en niet te achterhalen zijn.

<u>Overige eisen Bbgt</u>
- Er dienen maatregelen te zijn in geval van calamiteiten.
- Voor personeelsleden die in aanraking komen met een vordering of de verwerking van een vordering dient minimaal een Verklaring Omtrent het Gedrag (VOG) te liggen.
- De gegevens voortvloeiende uit een vordering dienen binnen acht dagen onomkeerbaar vernietigd te worden.
- Wanneer er inbreuk is gemaakt ten tijde de verwerking van een vordering dient dit te worden gelogd en te worden gerapporteerd aan de bevoegde autoriteit dan wel een door deze aangewezen instantie.

<u>Algemene indruk over de waarborgen van de beveiliging van de gegevens</u>.
- Aantoonbaarheid maatregelen; zijn de genomen maatregelen aantoonbaar.
- Hoe is het risicomanagement geregeld.
- Is er sprake van de implementatie van “continue verbetering” (plan – do – check – act)

<u>Investeringen om te kunnen voldoen aan de wet en regelgeving</u>.
- Welke kosten / investeringen zijn nodig om aan wet en regelgeving te voldoen / gaan voldoen.
- Wat is de hoogte van de huidige omzet.
- Wat is de geschatte hoogte van de kosten in relatie tot de omzet van het bedrijf.
- Wat is het effect op de “business case” van het bedrijf.

<u>Afsluiting audit</u>
Herhaling van gemaakte afspraken.