Agentschap Telecom
Ministerie van Economische Zaken

Meting dataretentie 2013

Onderzoek naar de mate van naleving van de wet- en regelgeving

Colofon

Nummer	Versie 1.0
Datum	4 april 2014

Inhoud

Samenvatting

Aanbieders van openbare elektronische communicatienetwerken- en diensten (hierna: aanbieders) beschikken over diverse internet- en telefoniegegevens (NAW-, verkeers- en locatiegegevens) voor het overbrengen van communicatie. Deze gegevens dienen in beginsel te worden verwijderd zodra deze niet meer nodig zijn voor de normale bedrijfsvoering. Sinds september 2009 is de Wet bewaarplicht telecommunicatiegegevens (hierna: Wet bewaarplicht) van kracht. Hieruit vloeit de wettelijke verplichting voort om een gedeelte van de gegevens die worden gebruikt voor de normale bedrijfsvoering te bewaren voor opsporingsdoeleinden (dataretentie). De Wet bewaarplicht is opgenomen in hoofdstuk 13 van de Telecommunicatiewet (hierna: Tw). Het toezicht op de naleving van deze wet valt onder de bevoegdheden van Agentschap Telecom. Naast hoofdstuk 13 houdt Agentschap Telecom ook toezicht op hoofdstuk 11 van de Tw. Dit hoofdstuk bevat de wettelijke vereisten die worden gesteld aan het verwerken van een deel van de gegevens voor bedrijfsdoeleinden. Als onderdeel van het toezicht worden metingen gedaan. Agentschap Telecom heeft in het kader van dataretentie een 0- en een 1-meting uitgevoerd. De 'Meting dataretentie 2013' is de derde meting die door Agentschap Telecom hiervoor is uitgevoerd. Dit rapport geeft de resultaten weer van deze meting.

Voor de 'Meting dataretentie 2013' hebben de op dat moment bij de Autoriteit Consument & Markt (ACM) geregistreerde aanbieders een informatievordering ontvangen. De grote zes aanbieders zijn niet meegenomen. Deze aanbieders worden regelmatig gemonitord in (individuele) reguliere toezichtsactiviteiten. Als onderdeel van deze toezichtsactiviteiten wordt er aandacht besteed aan dataretentie en privacy. De overige 525 aanbieders hebben voor de meting een vragenlijst ontvangen. Deze groep aanbieders hebben samen circa 10% van alle telecomgebruikers in Nederland als klant. Dit betekent dat de grote zes aanbieders de overige circa 90% van alle telecomgebruikers in Nederland als klant hebben. Van de 525 bieden 337 aanbieders diensten aan welke gerelateerd kunnen worden aan het tapproces en/of het dataretentieproces. Deze 337 aanbieders zijn relevant voor de 'Meting dataretentie 2013'. Dit betekent dat in totaal minder dan 10% van de telecomgebruikers in de Nederland diensten afneemt bij deze 337 aanbieders.

Binnen deze groep van 337 aanbieders is onderzocht wat de stand van zaken is met betrekking tot de naleving van de wetgeving voor dataretentie en privacy in 2013. In deze meting is dieper ingegaan op de naleving van de wettelijke vereisten voor dataretentie en privacy.

Agentschap Telecom werkt informatie- en risicogericht. In haar toezicht hanteert Agentschap Telecom als uitgangspunt vertrouwen in zelfregulering door de aanbieders. Voor het verkrijgen van de informatie voor de meting is gebruik gemaakt van een informatievordering in de vorm van een vragenlijst. De resultaten uit de 'Meting dataretentie 2013' zijn gebaseerd op de informatie die de aanbieders door middel van de informatievordering hebben aangeleverd. De bevindingen van de meting worden hieronder weergegeven.

Bewaren

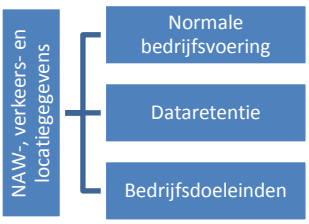
Ten behoeve van het onderzoeken, het opsporen en het vervolgen van ernstige misdrijven is het wettelijke verplicht dat een deel van de NAW-, verkeers- en locatiegegevens door de aanbieders voor een bepaalde termijn wordt bewaard. Uit de resultaten blijkt dat de verplichting tot het bewaren van de telefonie- en internetgegevens voor de duur van zes of twaalf maanden door 77 aanbieders (23%) gedeeltelijk wordt nageleefd, 24 aanbieders (7%) bewaren de gegevens niet en 236 aanbieders (70%) bewaren de gegevens en leven de wettelijke bewaarplicht na.

Vernietigen

Na afloop van de bewaartermijn zijn de aanbieders verplicht de gegevens onomkeerbaar binnen acht dagen te vernietigen. Uit de resultaten blijkt dat 101 aanbieders (30%) de gegevens gedeeltelijk vernietigen. 163 aanbieders (48%) geven aan de gegevens geheel te vernietigen en 73 aanbieders (22%) geven aan niet te vernietigen na afloop van de bewaartermijn. Een deel van deze aanbieders gebruikt de verkeers- en locatiegegevens voor bedrijfsdoeleinden die zijn opgenomen in hoofdstuk 11 Tw.

Privacy

Verkeers- en locatiegegevens moeten in beginsel, naast de wettelijk verplichte opslag voor dataretentie, worden verwijderd dan wel worden geanonimiseerd zodra deze gegevens niet langer nodig zijn ten behoeve van de overbrenging van communicatie. In hoofdstuk 11 van de Tw zijn vier bedrijfsdoeleinden opgenomen waarvoor de gegevens langer mogen worden bewaard dan noodzakelijk voor de overbrenging van de communicatie. Deze bedrijfsdoeleinden zijn facturering, marktonderzoek, verkoopactiviteiten met betrekking tot elektronische communicatiediensten en de levering van de diensten met toegevoegde waarde.



De resultaten laten zien dat 84 aanbieders (25%) de verkeers- en locatiegegevens, naast het gebruik voor de normale bedrijfsvoering en dataretentie, ook gebruiken voor deze doeleinden. Indien verkeers- en locatiegegevens voor bedrijfsdoeleinden worden gebruikt, zijn hieraan privacyregels verbonden. Afhankelijk van het bedrijfsdoel kan het gaan om het toestemmingsvereiste, de informatieplicht en het anonimiseren van de gegevens. Uit de meting blijkt dat het gebruik van

verkeers- en locatiegegevens voor bedrijfsdoeleinden, naast dataretentie en de normale bedrijfsvoering, is afgenomen. Van de aanbieders die de gegevens voor bedrijfsdoeleinden gebruiken, geven 50 aanbieders (60%) aan te voldoen aan de informatieplicht en 36 aanbieders (43%) geven aan te voldoen aan het toestemmingsvereiste. Het vereiste dat de verkeers- en locatiegegevens moeten worden geanonimiseerd dan wel worden verwijderd, indien deze niet meer noodzakelijk zijn voor de bedrijfsdoeleinden, wordt door 39 aanbieders (46%) nageleefd.

Beveiliging

Voor de beveiliging van de NAW-, verkeers- en locatiegegevens moeten de aanbieders maatregelen nemen. Deze maatregelen zijn weergegeven in het Besluit beveiliging gegevens telecommunicatie (Bbgt). 19 aanbieders (6%) verklaren gedeeltelijk passende technische en organisatorische maatregelen te hebben genomen, 48 (14%) aanbieders verklaren geen maatregelen te hebben genomen en 270 aanbieders (80%) verklaren wel passende technische en organisatorische maatregelen te hebben genomen. De maatregelen die uit dit besluit voortvloeien dienen te worden vastgelegd in een beveiligingsplan. Hier geven 185 aanbieders (55%) invulling aan.

Vergelijking vorige metingen

Voor zover mogelijk zijn de uitkomsten van de 0- en 1-meting met de uitkomsten van de ‘Meting dataretentie 2013’ vergeleken. Uit de vergelijking is af te leiden dat de naleving van de wettelijke verplichtingen is verbeterd met betrekking tot dataretentie. Voorts is af te leiden dat minder aanbieders gegevens verwerken voor bedrijfsdoeleinden met de daarvoor vereiste privacyverplichtingen (van 41% naar 25%). De naleving van de privacyvereisten die gelden voor het gebruik van de gegevens voor deze bedrijfsdoeleinden is nagenoeg gelijk gebleven.

Vervolgtraject

Agentschap Telecom werkt risicogericht en vertrouwt in de zelfregulering van de aanbieders. De resultaten van de informatievordering worden daarom gebruikt om het toezicht gerichter in te zetten. Dit betekent dat, naast het reguliere toezicht op alle aanbieders, de aanbieders die aangeven niet te voldoen in aanmerking komen voor een inspectie. Tegen aanbieders, die de wettelijke verplichtingen niet naleven, wordt handhavend opgetreden. Expliciete risicoaanvaarding van kleinere risico’s is daar een essentieel onderdeel van.

Naar aanleiding van de resultaten uit de ‘Meting dataretentie 2013’ gaat Agentschap Telecom zich voornamelijk richten op twee punten: de vernietiging van de NAW-, verkeers- en locatiegegevens, alsmede de naleving van de privacyvereisten die gelden voor de gegevens die voor de bedrijfsdoeleinden worden gebruikt. Het betreft de informatieplicht, het toestemmingsvereiste en het anonimiseren dan wel verwijderen van deze gegevens.

1. Inleiding

Elektronische communicatie neemt een steeds belangrijkere plaats in binnen de maatschappij. De NAW-, verkeers- en locatiegegevens die hierbij worden gegenereerd vanuit de normale bedrijfsvoering kunnen ten behoeve van het onderzoeken, het opsporen en het vervolgen van ernstige misdrijven van belang zijn. Om NAW-, verkeers- en locatiegegevens ter beschikking te kunnen stellen voor een opsporingsonderzoek moet een deel van deze gegevens voor een bepaalde termijn worden bewaard door aanbieders van elektronische communicatienetwerken en -diensten (hierna: aanbieders). Meer informatie over deze verplichtingen in het kader van dataretentie is te vinden op de website van Agentschap Telecom: www.agentschaptelecom.nl.

Meting dataretentie 2013

Agentschap Telecom is de toezichthouder voor dataretentie. Als onderdeel van het toezicht door Agentschap Telecom is de 'Meting dataretentie 2013' uitgevoerd. De meting is van start gegaan op 26 augustus 2013 en liep tot en met december 2013. De resultaten van deze meting worden in dit rapport besproken.[1]

Agentschap Telecom heeft voor dataretentie eerder metingen uitgevoerd. Dit heeft geresulteerd in de 0- en 1-meting.[2] In de 'Meting dataretentie 2013' wordt dieper ingegaan op de stand van zaken met betrekking tot de naleving van de Wet bewaarplicht telecommunicatiegegevens (hierna: Wet bewaarplicht) door de aanbieders. Met de uitkomsten van de 'Meting dataretentie 2013' is, voor zover mogelijk, een vergelijking gemaakt met de resultaten uit de 0- en 1-meting.[3]

Voor de meting zijn de op dat moment bij de Autoriteit Consument & Markt (ACM) geregistreerde aanbieders aangeschreven. Het betreft 525 aanbieders. De grote zes aanbieders zijn niet meegenomen in de meting. Deze aanbieders worden regelmatig gemonitord in individuele reguliere toezichtsactiviteiten door Agentschap Telecom.[4] Hierbij wordt tevens aandacht besteed aan dataretentie en privacy. De 525 aanbieders hebben voor de meting een vragenlijst ingevuld. Van de 525 aanbieders, zijn er 337 die diensten aanbieden welke gerelateerd kunnen worden aan het tapproces en/of het dataretentieproces. De resultaten van deze 337 aanbieders zijn verwerkt in dit rapport. Het aantal klanten in Nederland dat telecomdiensten afneemt bij deze 525 aanbieders is circa 10% van het totale aantal telecomgebruikers in Nederland. Dit betekent dat 90% van de telecomgebruikers klant is bij de grote zes aanbieders, die in deze meting buiten beschouwing zijn gelaten. Aangezien de antwoorden van de 337 aanbieders zijn opgenomen dit rapport, hebben de resultaten betekenis voor minder dan 10% van het totale aantal telecomgebruikers in Nederland.

---

[1] Een aantal totalen in het rapport komen niet precies uit op 100%. Dit komt doordat de aantallen in het rapport zijn afgerond op gehele getallen en er op een aantal vragen in de vragenlijst meerdere antwoorden mogelijk waren.

[2] Zie voor de resultaten van de 0-meting het rapport: Eindrapport Nulmeting Wet bewaarplicht telecommunicatiegegevens. Een onderzoek naar de stand van zaken betreffende de naleving van de Wet bewaarplicht bij Internet Service Providers. 3 mei 2010. Zie voor de resultaten van de 1-meting het rapport: Toezicht Dataretentie en het verwerken van persoons- en locatiegegevens voor bedrijfsdoeleinden. De 1-meting. 26 april 2012.

[3] De opzet van de drie metingen is niet identiek. In de 0-meting is gekeken naar de Internet Service Providers die op dat moment in 2009 bij de ACM waren geregistreerd. Voor de 1-meting zijn alle op dat moment bij de ACM geregistreerde aanbieders van openbare elektronische communicatienetwerken en/of –diensten meegenomen in de meting.

[4] *Handelingen II* 2013/14, nr. 13, item 6 <https://zoek.officielebekendmakingen.nl/h-tk-20132014-13-6.html>.

Verkeers- en locatiegegevens kunnen door de aanbieders, naast dataretentie en de normale bedrijfsvoering, ook gebruikt worden voor bedrijfsdoeleinden. Agentschap Telecom is ook toezichthouder voor de naleving van de wettelijke privacyvereisten die hiervoor gelden.

Wetgeving

Om te kunnen voldoen aan de vraag van de behoeftesteller voor het onderzoeken, het opsporen en het vervolgen van ernstige misdrijven is sinds 2009 de Wet bewaarplicht van kracht. In deze wet staan verplichtingen waar aanbieders aan moeten voldoen met betrekking tot het bewaren, vernietigen en beveiligen van internet- en telefoniegegevens. Het gaat hierbij om NAW-, verkeers-, en locatiegegevens ten behoeve van communicatie en niet om de inhoud van deze communicatie. De Wet bewaarplicht is onderdeel geworden van hoofdstuk 13 van de Telecommunicatiewet (Tw). Agentschap Telecom is, naast toezichthouder op de naleving van de verplichtingen van aanbieders voor het bewaren, vernietigen en het beveiligen van deze gegevens, ook toezichthouder voor de verplichtingen uit hoofdstuk 11 van de Tw. Hoofdstuk 11 bevat de verplichtingen die gelden voor het verwerken van verkeers- en locatiegegevens voor bedrijfsdoeleinden.
In het Besluit beveiliging gegevens telecommunicatie (Bbgt) zijn de verplichte beveiligingsmaatregelen ten aanzien van gegevens betreffende het aftappen en opnemen van telecommunicatie opgenomen. Hierin staat beschreven welke maatregelen de aanbieders moeten treffen om te voldoen aan de vereiste beveiliging.

Aanbieders

De verplichtingen uit hoofdstuk 11 en 13 van de Tw gelden voor alle aanbieders van openbare telecommunicatienetwerken en/of -diensten, welke gerelateerd kunnen worden aan het tapproces en/of het dataretentieproces. De aanbieders die hebben aangegeven geen aanbieder te zijn in deze zin, zijn niet meegenomen in dit onderzoek.

Missie Agentschap Telecom

De missie van Agentschap Telecom is dat het agentschap de beschikbaarheid van moderne en betrouwbare telecommunicatie in en voor Nederland waarborgt.

Uitgangspunten van het toezicht

Agentschap Telecom werkt eraan minder last en meer effect te bewerkstelligen. De aandacht voor de vermindering van lastendruk komt tot uiting in het informatiegestuurd en risicogericht toezicht houden.
Daarnaast is het toezicht erop gericht om spontane naleving zoveel mogelijk te stimuleren. Zelfregulering en vertrouwen in een goed presterende markt zijn uitgangspunten in het toezicht. Dit zorgt voor een gelijk speelveld en een effectieve aanpak. Effectief toezicht impliceert dat in sommige gevallen de gewenste beïnvloeding van de doelgroep een harde aanpak rechtvaardigt, maar meestal zal in eerste instantie een zachte aanpak gehanteerd kunnen worden om het doel te bereiken.

Maatschappelijk belang centraal

Bij het uitvoeren van de missie van Agentschap Telecom staat het maatschappelijk belang centraal. Voor opsporingsonderzoeken en de Staatsveiligheid is het van belang dat de NAW-, verkeers- en locatiegegevens kunnen worden opgevraagd.

Sturingsfilosofie

Toezicht sluit aan op de laatste ontwikkelingen in het werkveld en op de beleidsprioriteiten van de Minister van Economische Zaken.

Daarom houdt Agentschap Telecom toezicht vanuit de volgende sturingsfilosofie:

- Toezicht is verantwoordelijk voor het inspectietoezicht en draagt daarmee bij aan het stelsel;
- Toezicht heeft aandacht voor lastendrukvermindering en draagt hieraan bij door selectief en slagvaardig te zijn;
- Toezicht heeft vertrouwen in zelfregulering;
- Toezicht is toegankelijk;
- Toezicht is expliciet voor risico-aanvaarding;
- Er is aandacht voor scheiding toezicht/uitvoering en toezicht/sanctionering;
- De nationale en supranationale dimensie worden gelijkgeschakeld.

Agentschap Telecom als toezichthouder

Agentschap Telecom streeft naar betrouwbare netwerken en/of diensten. In haar rol als toezichthouder vormt zowel regelconformiteit als beleidsconformiteit een belangrijk middel. Regelconformiteit is onder meer het toezien op de naleving van de gestelde regels en het eventueel sanctioneren van de overtreder. Concreet betekent dit dat Agentschap Telecom erop toeziet of daadwerkelijk de NAW-, verkeers- en locatiegegevens worden bewaard, vernietigd en beveiligd. Het betekent ook dat Agentschap Telecom erop toeziet of privacymaatregelen worden genomen voor de verkeers- en locatiegegevens die, naast dataretentie en de normale bedrijfsvoering, worden verwerkt voor bedrijfsdoeleinden.

Beleidsconformiteit betekent dat Agentschap Telecom een signalerende en adviserende functie vervult bij het realiseren van beleidsdoelstellingen. Hierbij wordt gekeken of de aanbieders in de praktijk voldoen aan de verplichtingen voor het bewaren, het vernietigen, het beveiligen en de privacy van de desbetreffende gegevens. Het agentschap doet dit door middel van inspecties waarbij niet alleen gekeken wordt naar de strikte naleving van de regels. Met name wordt gekeken naar de praktijk van de aanbieder. Daarmee wordt getoetst of de aanbieders daadwerkelijk voldoen aan de verplichtingen. Relevante bevindingen in algemene zin kunnen onderwerp van gesprek zijn met de beleidskern van het Ministerie van Economische Zaken.

Informatiegestuurd toezicht

Toezicht houden is het verzamelen van informatie over de vraag of een handeling of zaak voldoet aan de daaraan gestelde eisen, het zich daarna vormen van een oordeel daarover en het eventueel naar aanleiding daarvan interveniëren.[5] Door informatiegestuurd toezicht te houden wordt getracht de beschikbare gegevens te verzamelen en systematisch te analyseren. Het

[5] Begrippenkader Rijksinspecties, IR 2012/07/10b.

verzamelen van informatie is de eerste fase van het proces van toezicht. Voor de 'Meting dataretentie 2013' is informatie gevorderd in de vorm van een vragenlijst. De informatie die de aanbieders hebben aangeleverd door middel van de informatievordering, wordt meegenomen in het toezicht van Agentschap Telecom.

Risicogericht toezicht

Naast het informatiegestuurd toezicht houdt Agentschap Telecom toezicht op basis van risicoanalyses. Het toezicht richt zich op activiteiten die de hoogste risico's voor het te beschermen belang vormen.

Toezicht in de praktijk

Agentschap Telecom kan bij het toezicht de volgende instrumenten inzetten:

- Voorlichting;
- Onderzoek;
- Administratieve controles;
- Inspecties.

Onafhankelijke positie

Als toezichthouder verzamelt Agentschap Telecom informatie en brengt hiermee zijn oordeel tot stand, onafhankelijk van andere partijen. Op deze wijze levert het agentschap een bijdrage aan de doelstellingen voor dataretentie. Agentschap Telecom stelt zelfstandig haar prioriteiten in het toezicht vast en acht dit van groot belang om onafhankelijk te zijn bij het interveniëren en bij publicatie van onderzoeksresultaten over de naleving met betrekking tot het bewaren, het vernietigen, het beveiligen en de privacy.

Leeswijzer

In dit rapport is de nadruk gelegd op dataretentie. Dit betekent dat hoofdstuk 13 van de Tw van toepassing is. Naast dit hoofdstuk speelt hoofdstuk 11 ook een belangrijke rol met betrekking tot de privacy.

Het rapport bestaat uit 10 hoofdstukken. Hoofdstuk 1 is de inleiding. Hoofdstuk 2 geeft de onderzoeksvragen en de methodiek van de meting weer. Hierna volgt in hoofdstuk 3 een toelichting op het doel en het vervolg van de meting. In hoofdstuk 4 komt het verloop van de meting aan bod. Hoofdstuk 5 gaat in op de verschillende bewaardoeleinden van de NAW-, verkeers-, en locatiegegevens. Hoofdstuk 6 gaat in op het bewaren van de gegevens. Het vernietigen komt aan bod in hoofdstuk 7. Hoofdstuk 8 gaat in op de privacy van de gegevens. De resultaten van de beveiliging van de gegevens worden behandeld in hoofdstuk 9. Hoofdstuk 10 sluit af met enkele conclusies.

2. Onderzoeksvragen en methodiek

In dit hoofdstuk komen de onderzoeksvragen en methodiek van de 'Meting dataretentie 2013' aan bod.

2.1 Onderzoeksvragen

Voor de uitvoering van de 'Meting dataretentie 2013' is informatie gevorderd in de vorm van een vragenlijst. De informatievordering bestaat voornamelijk uit gesloten vragen en deze sluiten in de basis aan bij de vragen uit de 1-meting. In de 'Meting dataretentie 2013' is dieper ingegaan op de naleving van de wettelijke vereisten. Hiervoor zijn meer bewijstechnische vragen gesteld om de gegeven antwoorden in de informatievordering, voor zover mogelijk, op aantoonbaarheid te kunnen toetsen.

De volgende onderzoeksvraag is geformuleerd:
"Wat is de mate van naleving van de Wet bewaarplicht door openbare aanbieders van telecommunicatienetwerken en/of –diensten in het jaar 2013?"

Om tot de beantwoording van deze onderzoeksvraag te komen zijn onder meer de volgende subvragen in de informatievordering opgenomen:

- Bewaren de aanbieders de gegenereerde NAW-, verkeers-, en locatiegegevens voor de duur van zes of twaalf maanden?
- Vernietigen de aanbieders de gegenereerde NAW-, verkeers-, en locatiegegevens onomkeerbaar binnen acht dagen na afloop van de bewaartermijn?
- Bewaren de aanbieders de gegenereerde verkeers- en locatiegegevens voor een ander doel dan dataretentie?
- Wordt er voor het gebruik van deze gegevens voldaan aan de plicht de gebruikers te informeren?
- Wordt voor het bewaren van deze gegevens toestemming aan de gebruikers gevraagd?
- Zijn er passende technische en organisatorische maatregelen genomen om de opgeslagen gegevens te beveiligen?
- Beschikt de aanbieder over een beveiligingsplan dat voldoet aan de wettelijke vereisten?[6]

2.2 Methodiek

Bepalen van de doelgroep
De door Agentschap Telecom samengestelde doelgroep heeft een informatievordering ontvangen. De doelgroep bestaat uit nagenoeg alle aanbieders die samen een aandeel hebben

[6] Zie voor de volledige vragenlijst bijlage II.

van circa 10% van alle telecomgebruikers in Nederland. Zoals aangegeven in de inleiding worden de zes grote aanbieders, die circa 90% van de markt bedienen, regelmatig gemonitord in individuele reguliere toezichtsactiviteiten, waarbij dataretentie en privacy onder andere aan bod komen.[7] Op basis van het register van de ACM en de bij Agentschap Telecom bekende gegevens is de doelgroep van de meting geselecteerd. In totaal zijn er 525 ACM-geregistreerde aanbieders aangeschreven.[8]

Informatievordering

Op 26 augustus 2013 is de informatievordering met begeleidende brief verstuurd naar de geselecteerde aanbieders. De informatievordering bestaat uit 39 vragen. Voorts is er in de informatievordering verzocht om het beveiligingsplan van de aanbieder mee te sturen, indien Agentschap Telecom deze nog niet in het bezit heeft. De beantwoording van de vragenlijst was niet vrijblijvend. Op grond van art. 18.7 Tw is de aanbieder verplicht de gevraagde informatie te verstrekken.

[7] *Handelingen II* 2013/14, nr. 13, item 6 <https://zoek.officielebekendmakingen.nl/h-tk-20132014-13-6.html>.

[8] De ACM hanteert drie categorieën waarin de aanbieders zijn onderverdeeld naar grootte van de omzet: kleine aanbieders voor organisaties met een omzet tot 2 miljoen euro per jaar, middelgrote aanbieders voor organisaties met een omzet van 2 tot 20 miljoen euro per jaar en grote aanbieders voor organisaties met een omzet van 20 miljoen euro of meer per jaar. Voor ons rapport is hierin geen onderscheid gemaakt.

3. Doel en vervolg van dit rapport

3.1 Doel van dit rapport

Door middel van de 'Meting dataretentie 2013' is er onder de aanbieders onderzoek gedaan naar de mate van naleving van de wet- en regelgeving met betrekking tot dataretentie, privacy en beveiliging.

De 'Meting dataretentie 2013' is een meting waaruit blijkt wat de stand van zaken in 2013 is met betrekking tot de naleving van de wetgeving en waarbinnen het accent ligt op de aantoonbaarheid van de naleving door de aanbieders.
Reeds eerder hebben er metingen plaatsgevonden, de 0- en 1-meting. Op specifieke deelonderwerpen wordt er een vergelijking gemaakt tussen de uitkomsten van de 0- en 1-meting met de 'Meting dataretentie 2013'. Uit deze vergelijking blijkt welke verschuivingen er binnen de naleving hebben plaatsgevonden.

Het Directoraat-Generaal Energie, Telecom en Markten van het Ministerie van Economische Zaken en het Ministerie van Veiligheid en Justitie worden door dit rapport geïnformeerd omtrent de naleving. De telecommarkt is voortdurend in beweging door nieuwe technische, maatschappelijke en politieke (Europese) ontwikkelingen. Dit brengt rechten, plichten en risico's met zich mee. Het is van maatschappelijk belang dat de beleidsmakers op de hoogte zijn van de mate van naleving, opdat kan worden gecontroleerd of de naleving overeenkomt met de beleidsdoeleinden en deze indien nodig kunnen worden aangepast.

De gegevens van de aanbieders in dit rapport zijn geanonimiseerd. Door middel van de publicatie krijgen de aanbieders inzicht in de mate van naleving van de wet- en regelgeving met betrekking tot het bewaren, het vernietigen, de beveiliging en de privacy door de telecomsector.

3.2 Vervolg van dit rapport

De uitkomsten van de 'Meting dataretentie 2013' vormen voor Agentschap Telecom een belangrijke basis in de risicogerichte aanpak tegen het niet naleven van de wet- en regelgeving met betrekking tot het bewaren, het vernietigen, de beveiliging en de privacy van de gegevens. Aanbieders die niet (volledig) aan de wetgeving voldoen komen in aanmerking voor handhavende acties. Agentschap Telecom kiest er in haar aanpak in principe voor om in te zetten op acties die gericht zijn op de grootste risico's. Expliciete risicoaanvaarding van kleinere risico's is daar een essentieel onderdeel van.

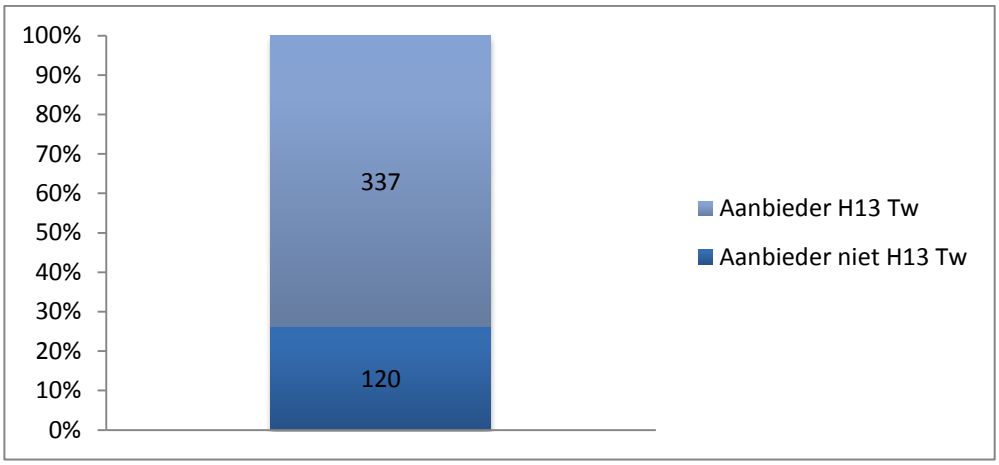
Agentschap Telecom heeft naar aanleiding van de resultaten uit de 1-meting de aanbieders bezocht die hoog scoorden op het niet naleven van de wetgeving. Tijdens de inspecties zijn er afspraken gemaakt met de aanbieders met betrekking tot de te nemen acties om de naleving te verhogen. Deze afspraken zijn nagekomen door de bezochte aanbieders. Voorts zijn er ook inspecties uitgevoerd bij aanbieders, die hebben aangegeven geen aanbieder te zijn waarop

hoofdstuk 13 van toepassing is, maar waarbij er een vermoeden bestond dat deze aanbieders wel dienen te voldoen aan de hieruit voortvloeiende verplichtingen.

4. Verloop van de meting

De meting dataretentie is op 26 augustus 2013 van start gegaan. In totaal zijn er 525 ACM geregistreerde aanbieders aangeschreven om te voldoen aan de vordering om informatie aan te leveren.

Van het totaal van deze 525 aanbieders zijn er 68 aanbieders (13%) die niet langer hoeven te voldoen aan de vordering tot informatie. Redenen hiervoor zijn onder andere faillissement van de aanbieder en/of beëindiging van de organisatie.

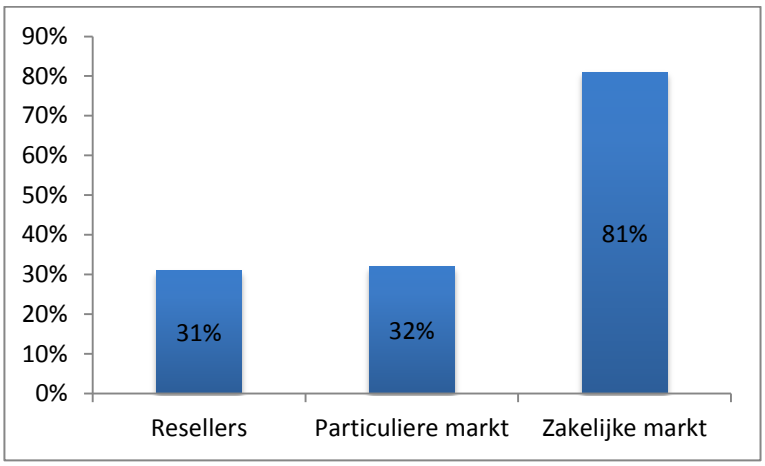


Figuur 1: onderverdeling in aanbieder en geen aanbieder waarop hoofdstuk 13 Tw van toepassing is.

Van de 457 aanbieders hebben 337 aanbieders (74%) aangegeven een aanbieder van openbare telecommunicatienetwerken en/of openbare telecommunicatiediensten te zijn in de zin van art. 1.1 Tw, waarvan de diensten gerelateerd kunnen worden aan het tapproces en/of het dataretentieproces. Van de 337 aanbieders geven 110 aanbieders (33%) aan een nieuwe aanbieder te zijn. Dit betekent voor de 'Meting dataretentie 2013' dat zij zich tussen 1 november 2010 en 1 augustus 2013 hebben ingeschreven bij de ACM. Van de 457 aanbieders hebben 120 aanbieders (26%) aangegeven 'anders' te zijn.

Van de 120 aanbieders die hebben aangegeven 'anders' te zijn zal nader worden onderzocht in hoeverre de aangeboden diensten vallen onder hoofdstuk 13 van de Tw. Indien blijkt dat deze aanbieders alsnog moeten voldoen aan wet- en regelgeving voor het bewaren, het vernietigen, de beveiliging en de privacy zal Agentschap Telecom hierop gericht actie ondernemen.

De aanbieders kunnen de diensten aanbieden op meerdere markten. Dit betekent voor de 337 aanbieders uit deze meting het volgende:



Figuur 2: onderverdeling markten.

Van de 337 aanbieders geven 104 aanbieders (31%) aan wholesalepartij te zijn, 275 aanbieders (81%) geven aan diensten aan te bieden op de zakelijke markt en 107 aanbieders (32%) geven aan diensten aan te bieden op de particuliere markt.

5. Bewaardoeleinden gegevens

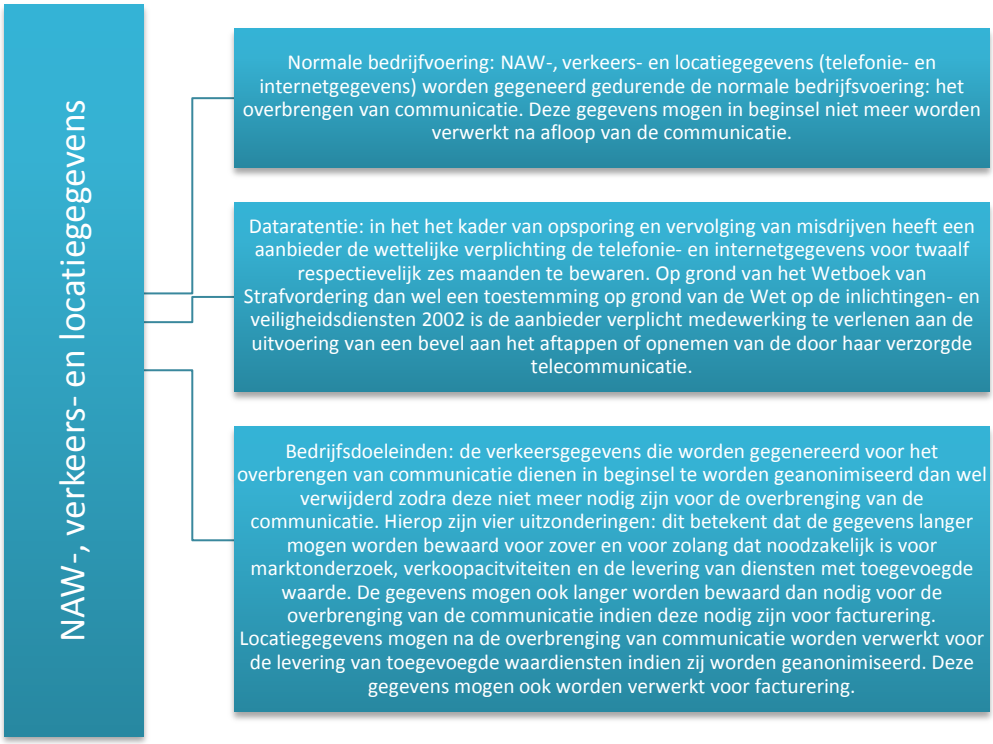
De 'Meting dataretentie 2013' concentreert zich op hoofdstuk 11 en 13 van de Tw. In dit hoofdstuk zal de regelgeving met betrekking tot die hoofstukken worden toegelicht. De overige regelgeving waar aanbieders zich aan dienen te houden wordt voor deze meting buiten beschouwing gelaten.

Het bewaren, vernietigen en anonimiseren dan wel verwijderen van NAW-, verkeers- en locatiegegevens dient verschillende doeleinden. Dit betekent dat voor ieder doel er andere, in de Tw geregelde, verplichtingen gelden.

In beginsel mogen de verwerkte verkeers- en locatiegegevens met betrekking tot de abonnees en gebruikers niet worden verwerkt voor andere doeleinden indien deze gegevens niet langer nodig zijn voor het overbrengen van de communicatie. Op deze hoofdregel wordt een uitzondering gemaakt met betrekking tot dataretentie (art. 11.13 Tw) en de vier bedrijfsdoeleinden opgenomen in art. 11.5 en art. 11.5a van de Tw.

In het kader van dataretentie is een aanbieder verplicht een deel van de NAW-, verkeers- en locatiegegevens, voor zover deze in het kader van de aangeboden netwerken of diensten worden gegenereerd of verwerkt, voor een bepaalde termijn te bewaren ten behoeve van het onderzoeken, opsporen en vervolgen van ernstige misdrijven (art. 13.2a lid 2 Tw). Na afloop van de bewaartermijn van zes of twaalf maanden dienen de gegevens binnen acht dagen te worden vernietigd.

Naast het moeten bewaren van de gegevens in het kader van dataretentie voor het onderzoeken, opsporen en vervolgen van ernstige misdrijven en de normale bedrijfsvoering, mogen aanbieders een deel van de verkeers- en locatiegegevens op grond van art. 11.5, 11.5a en 11.11 van de Tw (art. 11.13 Tw) voor andere doeleinden (facturering, verkoopactiviteiten, marktonderzoek en de levering van diensten met toegevoegd waarde) verwerken. Voor de verwerking dient wel te worden voldaan aan de privacyvereisten die volgen uit art. 11.5 en art. 11.5a van de Tw.



5.1 Verkeersgegevens

De aanbieder die verkeersgegevens verwerkt en opslaat ten behoeve van de overbrenging van communicatie, dient deze gegevens te verwijderen dan wel te anonimiseren zodra deze gegevens niet langer nodig zijn voor de overbrenging van de communicatie (art. 11.5 lid 1 Tw). Indien deze gegevens worden gebruikt voor facturering, marktonderzoek, verkoopactiviteiten met betrekking tot elektronische communicatiediensten of voor de levering van diensten met toegevoegde waarde zijn ander regels van kracht (art. 11.5 lid 2 en 3 Tw).
De aanbieder die verkeersgegevens (die niet langer nodig zijn voor het overbrengen van communicatie) verwerkt voor de facturering, mag deze gegevens verwerken tot het einde van de wettelijke termijn waarbinnen de factuur in rechte kan worden betwist of de betaling in rechte kan worden afgedwongen (art. 11.5 lid 2 Tw).
Het verwerken van verkeersgegevens (die niet langer nodig zijn voor het overbrengen van communicatie) voor marktonderzoek, verkoopactiviteiten met betrekking tot elektronische communicatiediensten of voor de levering van diensten met toegevoegde waarde, is toegestaan voor zolang dit noodzakelijk is (art. 11.5 lid 3 Tw).

Informatieplicht
Voor verkeersgegevens die voor facturering, marktonderzoek, verkoopactiviteiten met betrekking tot elektronische communicatiediensten of voor de levering van diensten met toegevoegde waarde worden gebruikt, dient de aanbieder de abonnee of gebruiker in kennis te stellen van het soort verkeersgegevens dat wordt verwerkt en de duur van deze verwerking. (art. 11.5 lid 2 en 3 jo. art. 11.5 lid 4 Tw).

Toestemmingsvereiste
Voor verkeersgegevens die worden gebruikt voor marktonderzoek, verkoopactiviteiten met betrekking tot elektronische communicatiediensten of de levering van diensten met toegevoegde waarde, dient de abonnee of de gebruiker waarop de verkeersgegevens betrekking hebben, voorafgaand aan de verwerking hiervan, toestemming te geven voor dit gebruik. De abonnee of gebruiker kan de gegeven toestemming te allen tijde intrekken (art. 11.5 lid 3 sub b Tw). Dit betekent dat de gegevens in dat geval voor deze doeleinden niet meer mogen worden gebruikt en dienen te worden verwijderd dan wel geanonimiseerd.

5.2 Locatiegegevens

De verwerking van locatiegegevens van een abonnee of gebruiker van openbare elektronische communicatienetwerken of -diensten, anders dan bedoeld in art. 11.5 Tw, is slechts toegestaan indien deze gegevens zijn geanonimiseerd dan wel de abonnee of gebruiker voor de verwerking van deze gegevens toestemming heeft gegeven voor de verwerking van deze gegevens ten behoeve van de levering van een dienst met toegevoegde waarde (art. 11.5a lid 1 Tw).[9] Deze toestemming kan te allen tijde worden ingetrokken (art. 11.5a lid 4 Tw).

Voor het verwerken van de locatiegegevens ten behoeve van de levering van een toegevoegde waardedienst, is naast het toestemmingsvereiste, de informatieplicht van toepassing. De aanbieder dient voorafgaand aan het verkrijgen van de toestemming de abonnee of gebruiker te informeren over de soort locatiegegevens dat wordt verwerkt, de doeleinden van die verwerking, de duur van de verwerking en of de gegevens aan een derde zullen worden verstrekt ten behoeve van de levering van de dienst met toegevoegde waarde (art. 11.5a lid 2 Tw).

De aanbieder mag slechts de locatiegegevens gebruiken voor zover en voor zolang dat noodzakelijk is voor de levering van de dienst met toegevoegde waarde (art. 11.5a lid 3 Tw). Een uitzondering op deze termijn is van toepassing op de locatiegegevens die noodzakelijk zijn voor het opstellen van een factuur. De locatiegegevens mogen in dat geval worden verwerkt tot het einde van de wettelijke termijn waarbinnen de factuur in rechte kan worden betwist of de betaling in rechte kan worden afgedwongen (art. 11.5a lid 3 jo art. 11.5 lid 2 Tw).

Het verwijderen dan wel anonimiseren van de telefonie- en internetgegevens dienen op een dusdanige wijze te geschieden dat deze redelijkerwijs niet meer zijn te herleiden tot individuele natuurlijke personen en/of rechtspersonen.[10]

In hoofdstuk 6, 7 en 8 zal verder worden ingegaan op de desbetreffende wettelijke kaders met betrekking tot de verschillende doeleinden.

[9] T&C Telecommunicatie- en privacyrecht, art.11.5a Tw, aant. 4, p.409.
[10] T&C Telecommunicatie- en privacyrecht, art.11.5 Tw, aant. 2, p.405.

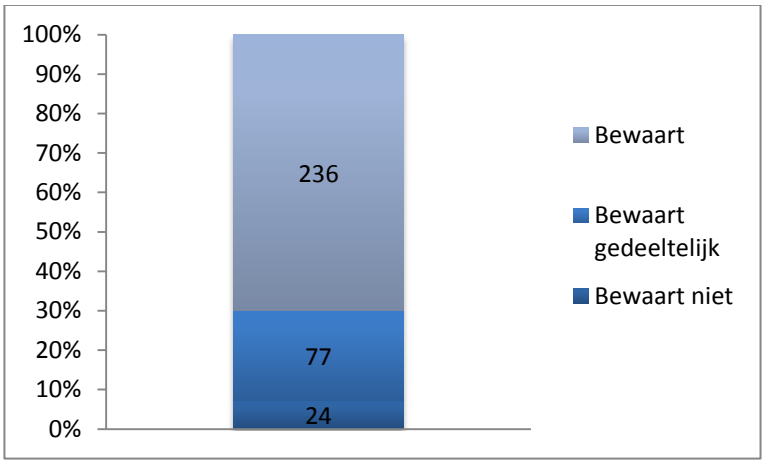
6. Bewaren

In het kader van dataretentie moeten NAW-, verkeers- en locatiegegevens voor een wettelijk vastgestelde periode worden bewaard.

De bewaartermijn voor gegevens in verband met telefonie bedraagt twaalf maanden. De bewaartermijn voor de gegevens in verband met internettoegang, e-mail en internettelefonie bedraagt zes maanden (art. 13.2a lid 3 Tw). De gegevens die dienen te worden bewaard zijn opgenomen in de bijlage behorende bij art. 13.2a van de Tw.[11]

Resultaten meting

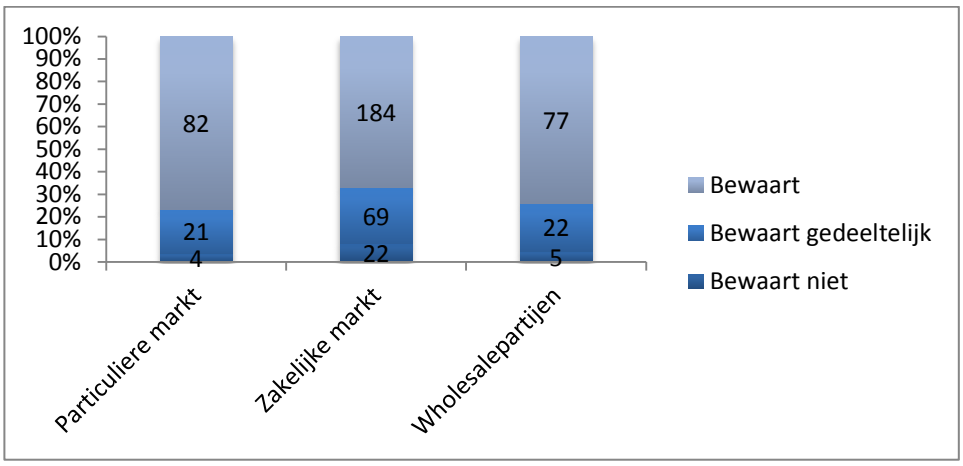
In de informatievordering is gevraagd of de aanbieders de gegevens bewaren.



Figuur 3: resultaten met betrekking tot het bewaren van NAW-, verkeers- en locatiegegevens.

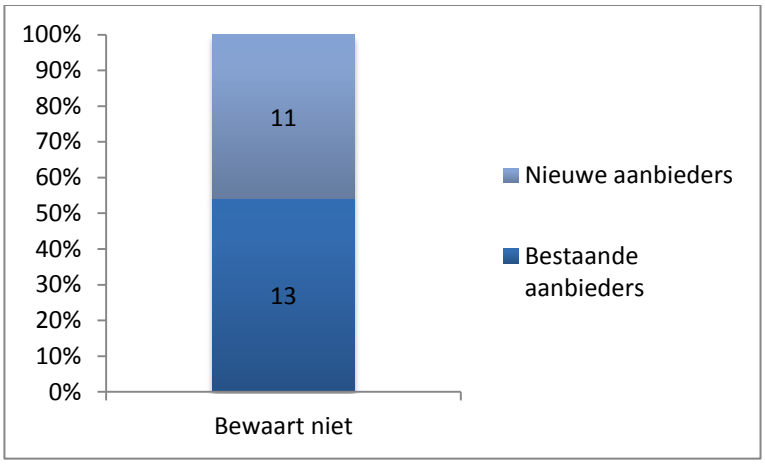
Van de 337 aanbieders geven 236 aanbieders (70%) aan de bij de dienstverlening gegenereerde gegevens te bewaren, 77 aanbieders (23%) geven aan gedeeltelijk de gegevens te bewaren en 24 aanbieders (7%) geven aan dit niet te doen.

[11] Zie bijlage III.



Figuur 4: onderverdeling bewaren per markt.

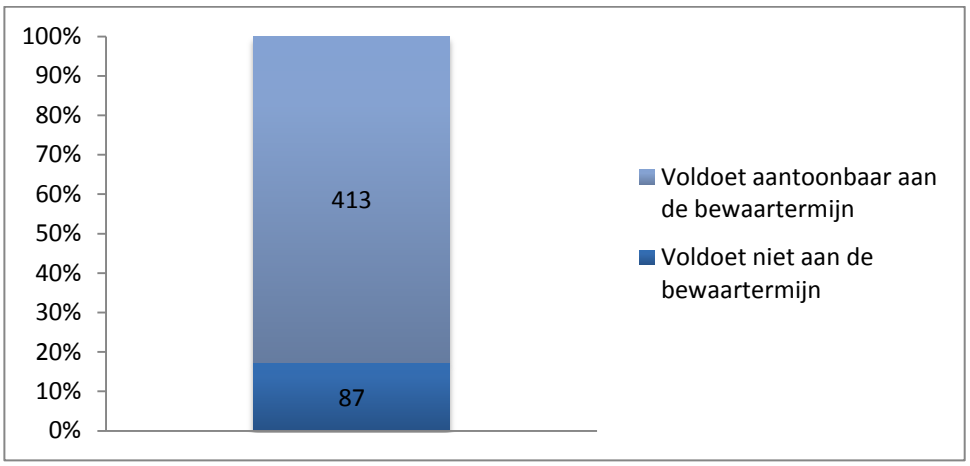
Er zijn 24 aanbieders die aangeven geen gegevens te bewaren. Hiervan bestaat ongeveer de helft uit nieuwe aanbieders.



Figuur 5: onderverdeling van de groep aanbieders die niet bewaart.

In de informatievordering is gevraagd of de aanbieders die de gegevens bewaren zich houden aan de bewaartermijn van zes of twaalf maanden en dit ook kunnen aantonen.[12]

[12] De gegevens die worden bewaard kunnen onder eigen beheer, in beheer bij een derde partij of zowel onder eigen beheer als in beheer bij een derde partij worden bewaard. Dit verklaart dat de uitkomst hoger is dan het aantal aanbieders dat relevant is voor deze meting (337).



Figuur 6: bewaartermijn

Van de aanbieders verklaart 83% aan te kunnen tonen de gegevens te bewaren voor de vereiste bewaartermijn. De groep aanbieders die niet voldoet aan de wettelijke bewaartermijn, bestaat uit aanbieders die niet voldoen aan de vereiste bewaarduur of aanbieders die niet kunnen aantonen dat de gegevens worden bewaard.

Vergelijking met vorige metingen

In vergelijking met de 0-meting is een stijging te zien in het geheel opslaan van de gegevens, voor het gedeeltelijk bewaren van de gegevens en het niet bewaren van de gegevens is een afname te zien.

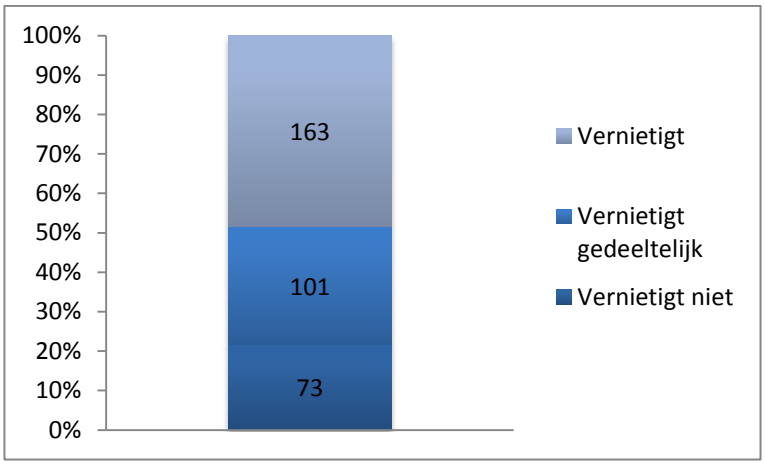
In vergelijking met de 1-meting is een stijging te zien in het bewaren van de desbetreffende gegevens. Bij de 1-meting voldeed 59% van de totale groep aanbieders aan het bewaren van de vereiste gegevens. Uit deze meting blijkt dat 70% van de aanbieders de gegevens opslaat. Er is een klein verschil in de resultaten met betrekking tot het niet bewaren van de gegevens of het gedeeltelijk bewaren van de gegevens.

7. Vernietigen

De NAW-, verkeers- en locatiegegevens die in het kader van dataretentie dienen te worden bewaard, dienen na afloop van de bewaartermijn van zes of twaalf maanden onverwijld, doch uiterlijk binnen acht dagen na afloop van de termijn te worden vernietigd (art. 13.2a lid 2 Tw jo art. 5 Bbgt).[13]

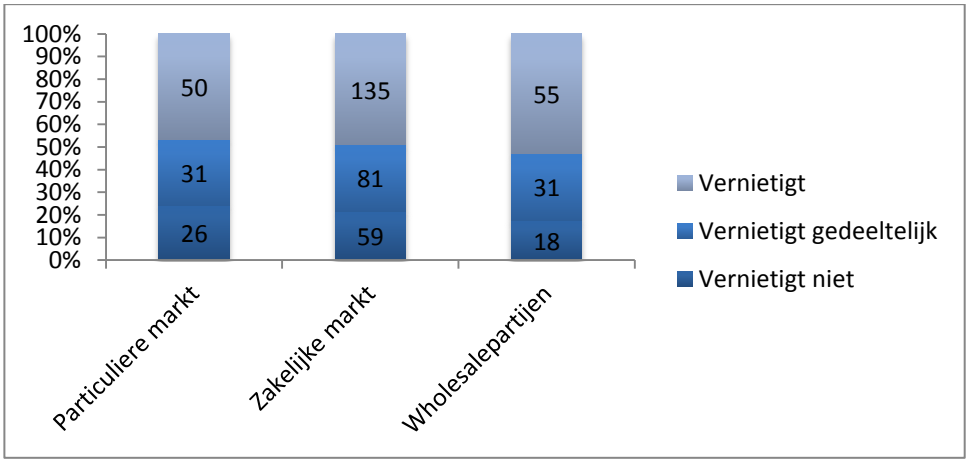
Resultaten meting

In de meting is gevraagd naar de mate van vernietiging.



Figuur 7: resultaten vernietiging van de NAW-, verkeers- en locatiegegevens.

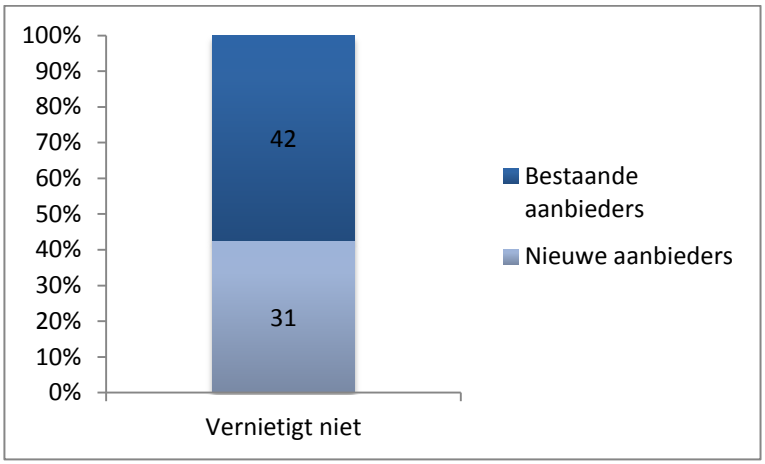
Van de 337 aanbieders geven 163 aanbieders (48%) aan de desbetreffende gegevens geheel te vernietigen, 101 aanbieders (30%) geven aan de gegevens gedeeltelijk te vernietigen en 73 aanbieders (22%) geven aan de gegevens niet te vernietigen.



Figuur 8: onderverdeling vernietigen per markt.

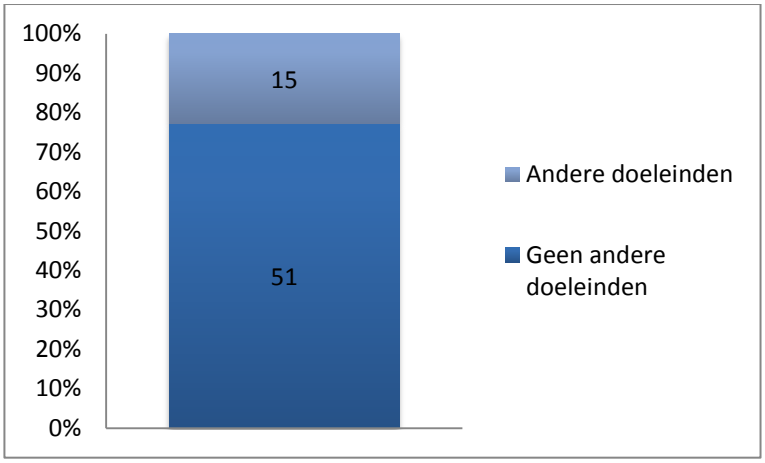
[13] *Stb.* 2009, 350, p.7.

Van de 73 aanbieders die niet vernietigen zijn 31 nieuwe aanbieders.



Figuur 9: niet vernietigen.

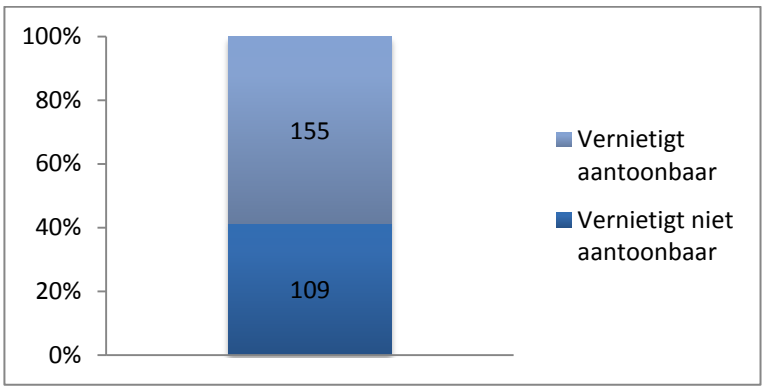
Voorts is onderzocht of de aanbieders die niet vernietigen de gegevens bewaren voor bedrijfsdoeleinden.



Figuur 10: niet vernietigen van gegevens voor gebruik bedrijfsdoeleinden.

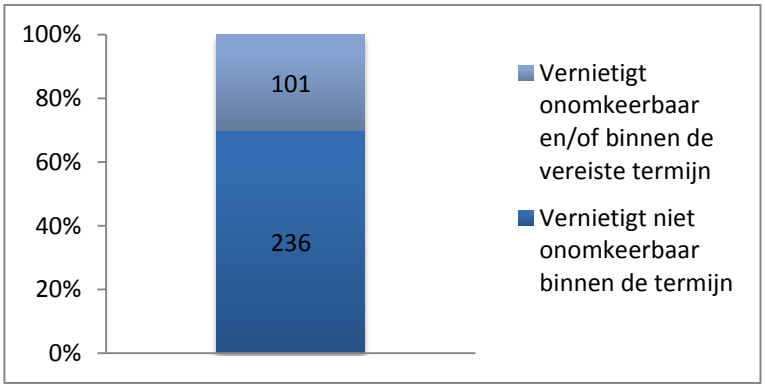
Aan de aanbieders die aangeven de gegevens geheel of gedeeltelijk te vernietigen, is gevraagd of zij dit ook kunnen aantonen.[14]

[14] De gegevens die worden vernietigd kunnen onder eigen beheer, in beheer bij een derde partij of zowel onder eigen beheer als in beheer bij een derde partij worden vernietigd. Dit verklaart dat de uitkomst hoger is dan het aantal aanbieders dat relevant is voor deze meting (337).



Figuur 11: aantoonbaar vernietigen.

Aan de aanbieders is voorts gevraagd of zij de gegevens ook binnen acht dagen na de bewaartermijn van zes of twaalf maanden onomkeerbaar vernietigen.[15]



Figuur 12: vernietigtermijn.

De groep aanbieders die aangeeft de gegevens niet binnen acht dagen na zes of twaalf maanden onomkeerbaar te vernietigen, kan bestaan uit aanbieders die de gegevens voor een ander wettelijk toegestaan doel bewaren of zich niet aan de bewaartermijn houden.

Vergelijking met vorige metingen

In vergelijking met de 0-meting is een stijging zichtbaar van het totaal aantal aanbieders dat voldoet aan het onomkeerbaar vernietigen van de gegevens binnen de vereiste termijn van art. 13.2a lid 2 Tw jo art. 5 Bbgt.

In vergelijking met de 1-meting blijkt 78% van de aanbieders de gegevens geheel of gedeeltelijk te vernietigen. Dit is een stijging in vergelijking met de 49% van de 1-meting. Voorts blijkt dat 19% van de aanbieders vernietigt buiten de gestelde termijn en 4% van de aanbieders niet onomkeerbaar vernietigt. Ook dit is gestegen.

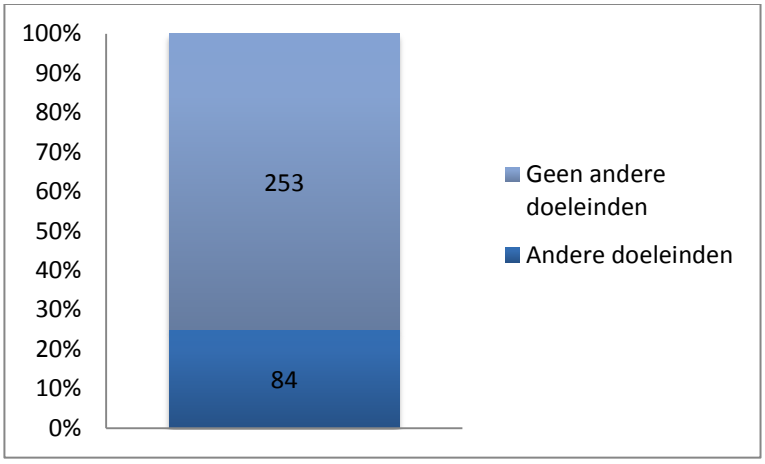
[15] De gegevens die worden vernietigd kunnen onder eigen beheer, in beheer bij een derde partij of zowel onder eigen beheer als in beheer bij een derde partij worden vernietigd. Dit verklaart dat de uitkomst hoger is dan het aantal aanbieders dat relevant is voor deze meting (337).

8. Privacy

In hoofdstuk 5 is aangegeven dat een deel van de NAW-, verkeers- en locatiegegevens, naast de normale bedrijfsvoering en de verplichte verwerking in het kader van dataretentie ook kunnen worden gebruikt voor bedrijfsdoeleinden (facturering, marktonderzoek, verkoopactiviteiten en diensten met toegevoegde waarde). Indien deze gegevens voor deze bedrijfsdoeleinden worden gebruikt, zijn er vanuit de Tw wettelijke bepalingen opgesteld voor de privacy van deze gegevens en gelden de wettelijke vereisten voor die doeleinden met betrekking tot het mogen bewaren, het verwijderen dan wel het anonimiseren van deze verkeers- en locatiegegevens (art. 11.5, 11.5a en 11.13 Tw).[16] Hier zal in dit hoofdstuk verder op worden ingegaan.

Resultaten meting

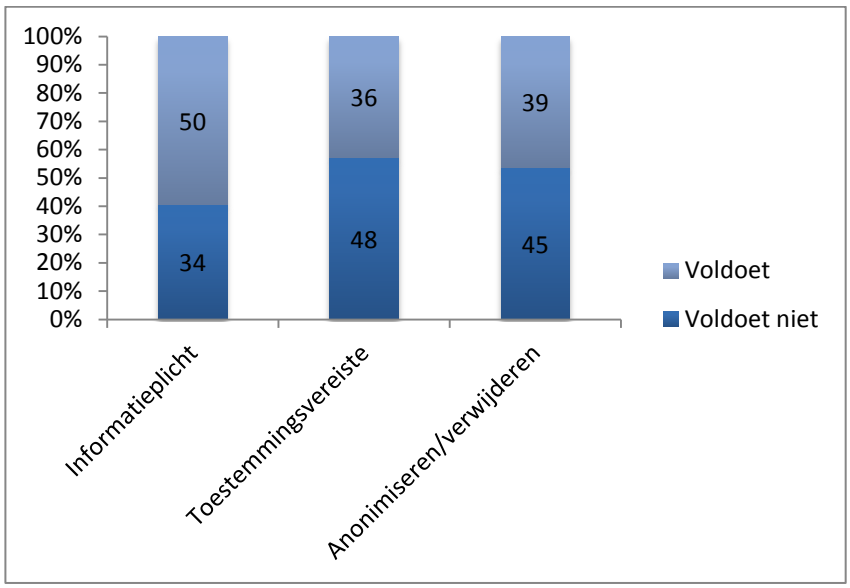
Van de 337 aanbieders geven 84 aanbieders (25%) aan verkeers-, en locatiegegevens ook voor een ander doel dan dataretentie te gebruiken.



Figuur 13: andere doeleinden

Binnen deze groep van 84 aanbieders is onderzocht of de aanbieders voldoen aan de informatieplicht, het toestemmingsvereiste en de regelgeving met betrekking tot het anonimiseren of verwijderen van de desbetreffende gegevens.

[16] *Stb.* 2009, 350, p.7.



Figuur 14: naleving wettelijke vereisten privacy.

Van de 84 aanbieders geven 50 aanbieders (60%) aan te voldoen aan de informatieplicht en 36 aanbieders (43%) verklaren te voldoen aan het toestemmingsvereiste. Dit betekent dat de klanten wel worden geïnformeerd omtrent het soort gegevens dat wordt verwerkt en de duur van het gebruik, echter dat niet in alle gevallen hiervoor ook toestemming wordt gevraagd aan de klanten.
Van de 84 aanbieders verklaren 39 aanbieders (46%) te kunnen aantonen de gegevens te anonimiseren of verwijderen, zodra deze niet meer noodzakelijk zijn voor het doel waarvoor deze werden bewaard.

Vergelijking met vorige metingen
In vergelijking met de 1-meting is de naleving van de privacyvereisten met betrekking tot de informatieplicht en het vragen om toestemming nagenoeg gelijk gebleven.

9. Beveiliging opgeslagen gegevens

De NAW-, verkeers- en locatiegegevens dienen te worden bewaard in het kader van dataretentie. In verband met de privacygevoeligheid van deze gegevens is het van belang dat de gegevens beveiligd worden opgeslagen, opdat kennisneming door onbevoegden wordt voorkomen. Uit het Bbgt vloeit voort welke wettelijke vereisten er zijn gesteld met betrekking tot de beveiliging van deze gegevens. Uit de regelgeving vloeit voort dat er technische en organisatorische maatregelen dienen te worden genomen om de opgeslagen gegevens te beveiligen en dat een aanbieder in het bezit dient te zijn van een beveiligingsplan.

9.1 Beveiliging

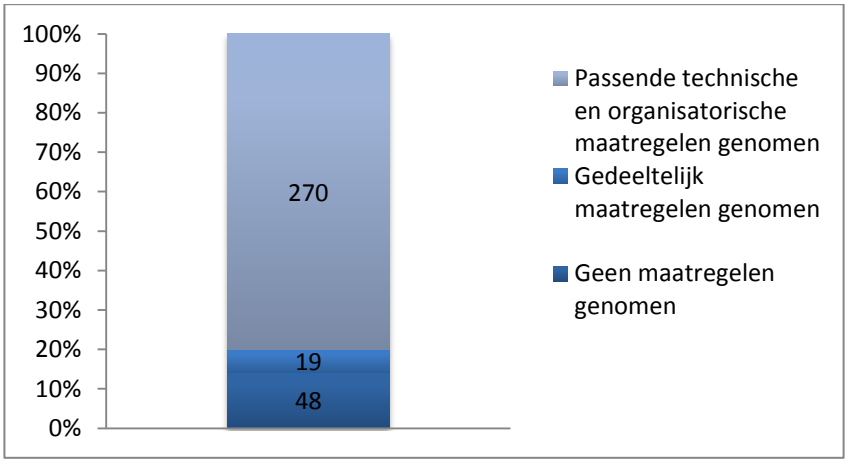
De technische en organisatorische maatregelen waaraan moet zijn voldaan, zijn opgenomen in de bijlage bij art. 2 lid 3 Bbgt. Het gaat om beveiliging ten aanzien van:

- Personeel, fysieke beveiliging en beheer van communicatie;
- Beheer van communicatie- en bedieningsprocessen;
- Toegangsbeveiliging van geautomatiseerde informatiesystemen;
- Ontwikkeling, onderhoud en reparatie van geautomatiseerde informatiesystemen.

Om inzicht te krijgen in de wijze waarop invulling is gegeven aan de beveiliging van de opslag van de gegevens is in de informatievordering aandacht besteed aan de plaats waar de gegevens worden opgeslagen en of de toegang door middel van codes is beveiligd.

Resultaten meting

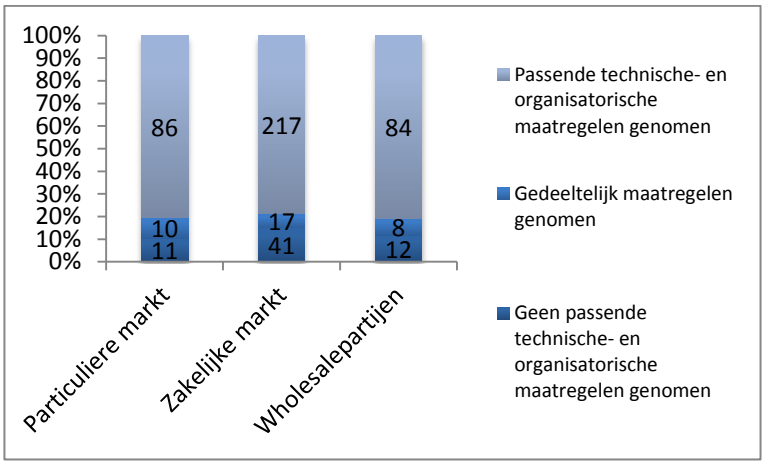
Voor de beveiliging is het van belang dat de aanbieders technische en organisatorische maatregelen nemen.



Figuur 15: resultaten passende technische en organisatorische maatregelen.

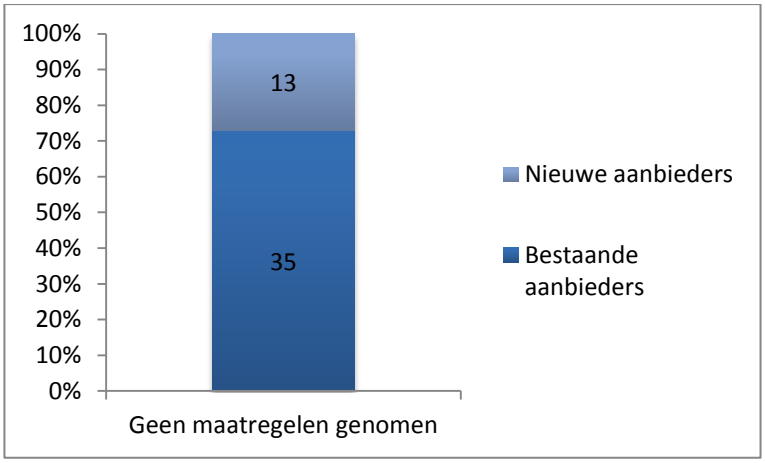
Van de 337 aanbieders geven 270 aanbieders (80%) aan dat zij aantoonbare passende technische en organisatorische maatregelen hebben genomen om de betreffende gegevens te

beveiligen, 19 aanbieders (6%) verklaren aan te kunnen tonen gedeeltelijk passende technische en organisatorische maatregelen te hebben genomen en 48 aanbieders (14%) geven aan geen passende technische en organisatorische maatregelen te hebben genomen of kunnen dit niet aantonen.
Deze verdeling is hieronder per markt weergegeven.



Figuur 16: maatregelen per markt

De groep van 48 aanbieders, die heeft aangeven geen passende technische- en organisatorische maatregelen te hebben genomen of dit niet kan aantonen, bestaat deels uit nieuwe aanbieders (13).



Figuur 17: bestaande aanbieders versus nieuwe aanbieders.

9.2 Beveiligingsplan

Op grond van art. 2 Bbgt moeten aanbieders alle noodzakelijke maatregelen treffen om kennisneming van de gegevens door onbevoegden te voorkomen.
Een maatregel hiervoor is het zorg dragen voor een beveiligingsplan (art. 3 Bbgt). In dit beveiligingsplan dient de aanbieder te beschrijven welke maatregelen hij heeft genomen om de gegevens te beveiligen. De aanbieder moet in het beveiligingsplan in elk geval aangeven op

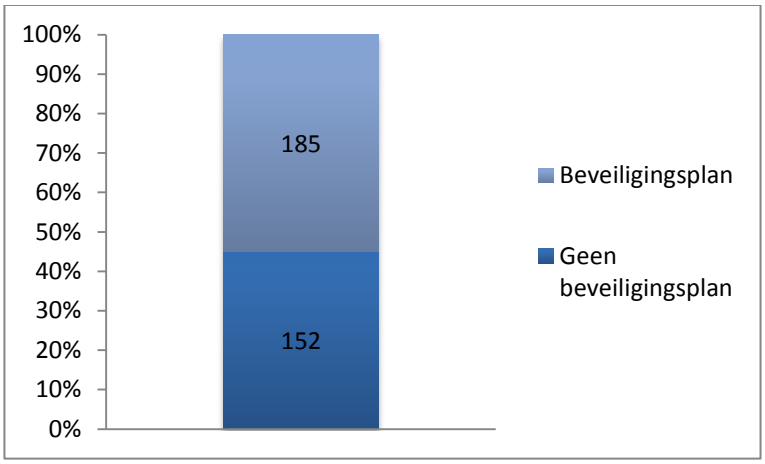
welke wijze hij uitvoering heeft gegeven aan zijn beveiligingsplicht ten aanzien van personeel, fysieke beveiliging, beveiliging van de omgeving, beheer van communicatie- en bedieningsprocessen, toegangsbeveiliging, ontwikkeling, onderhoud en reparatie van geautomatiseerde informatiesystemen.[17]

Verplichting inzage beveiligingsplan

Naast de verplichting dat de aanbieder ervoor dient te zorgen dat er een beveiligingsplan is opgesteld waarin uitvoering is gegeven aan zijn beveiligingsplicht, is de aanbieder tevens verplicht op verzoek van een behoeftesteller inzage te verlenen in het beveiligingsplan (art. 3 lid 2 Bbgt).

Resultaten meting

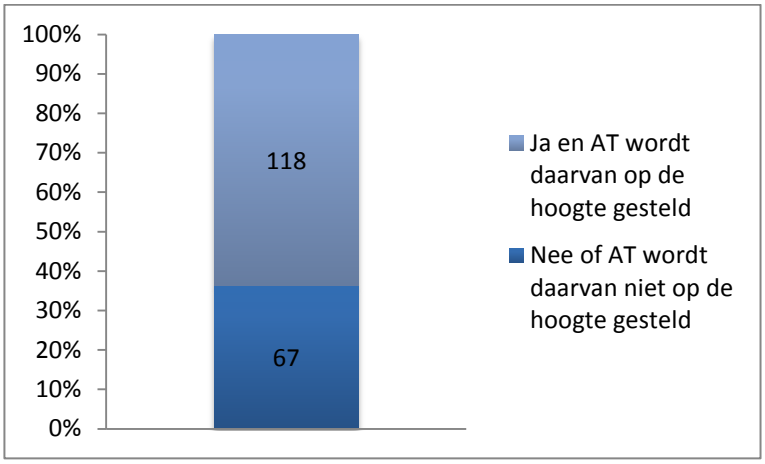
In de onderstaande grafiek worden de resultaten weergegeven van de aanbieders die in het bezit zijn van een beveiligingsplan.



Figuur 18: beveiligingsplan.

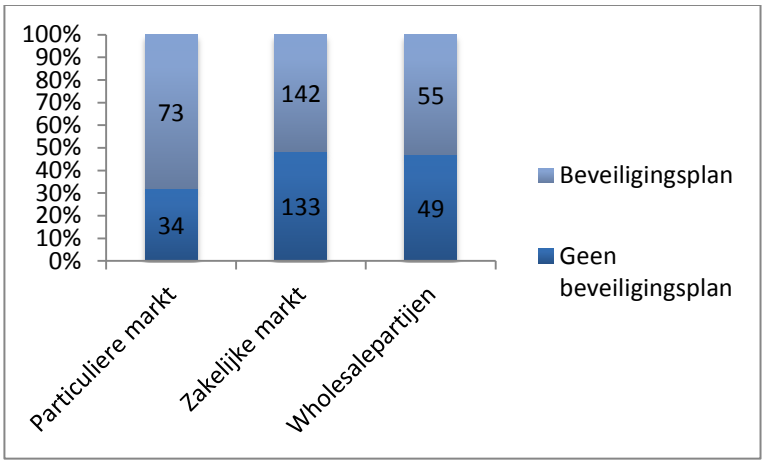
Van de 337 aanbieders beschikken 185 aanbieders (55%) over een beveiligingsplan dat voldoet aan alle vereisten uit art. 3 Bbgt. Hiervan geven 170 aanbieders (92%) aan het beveiligingsplan aan te passen als er zich wijzingen binnen de organisatie voordoen, die van invloed zijn op de gegevens in het plan. 118 aanbieders geven aan Agentschap Telecom op de hoogte te stellen van de wijzigingen.

[17] Zie bijlage Bbgt.



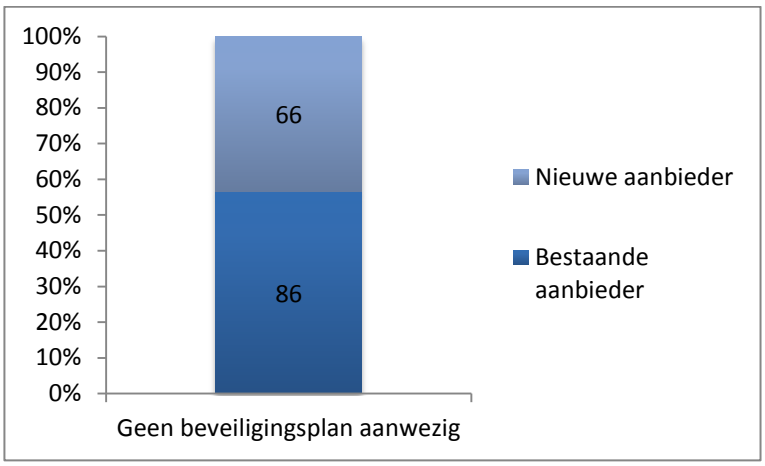
Figuur 19: Agentschap Telecom wordt op de hoogte gesteld.

Het hebben van een beveiligingsplan is onderverdeeld naar de markt waarop de diensten worden aangeboden.



Figuur 20: beveiligingsplan per markt.

Van de 152 aanbieders die niet in het bezit zijn van een beveiligingsplan, bestaat bijna de helft uit nieuwe aanbieders.



Figuur 21: nieuwe aanbieder versus bestaande aanbieder

Vergelijking met vorige metingen

Uit de 'Meting dataretentie 2013' blijkt dat het percentage aanbieders dat in het bezit is van een beveiligingsplan conform art. 3 Bbgt lager ligt dan in de 0-meting.

In vergelijking met de 1-meting is het percentage aanbieders dat in het bezit is van een beveiligingsplan nagenoeg gelijk gebleven.

10. Conclusie

In dit rapport zijn de resultaten weergegeven van de 'Meting dataretentie 2013'. In deze meting zijn de resultaten van de informatievordering weergegeven, die door 337 aanbieders is ingevuld. Deze aanbieders hebben samen minder dan 10% van alle telecomgebruikers in Nederland als klant. De overige 90% van de gebruikers is klant bij de grote zes aanbieders. Deze aanbieders zijn niet meegenomen in deze meting, aangezien zij regelmatig worden gemonitord in reguliere individuele toezichtsactiviteiten. Met de resultaten uit het rapport 'Meting dataretentie 2013' kan de onderzoeksvraag worden beantwoord: "Wat is de mate van naleving van de Wet bewaarplicht door openbare aanbieders van telecommunicatienetwerken en/of -diensten in het jaar 2013?". Er is onderzocht of de aanbieders voldoen aan de verplichtingen uit hoofdstuk 11 (privacy) en hoofdstuk 13 (dataretentie) van de Tw.

Naleving algemeen
De resultaten tonen aan dat de wettelijke vereisten uit hoofdstuk 13 op het gebied van het bewaren van NAW-, verkeers- en locatiegegevens en de beveiliging van deze gegevens over het algemeen worden nageleefd door de aanbieders.
Naar aanleiding van deze resultaten zal Agentschap Telecom zich vooral richten op twee elementen. De naleving van de wettelijke vereisten uit hoofdstuk 11 voor de privacy van de verkeers- en locatiegegevens als deze gegevens voor bedrijfsdoeleinden worden gebruikt, naast de normale bedrijfsvoering en dataretentie. Voorts betreft het de wettelijke vereisten uit hoofdstuk 13 voor het vernietigen van de NAW-, verkeers- en locatiegegevens.

Bewaren
Uit de resultaten blijkt dat de verplichting tot het bewaren van de telefonie- en internetgegevens voor de duur van zes of twaalf maanden gedeeltelijk wordt nageleefd door 77 aanbieders (23%) aanbieders, 24 aanbieders (7%) bewaren de gegevens niet en 236 aanbieders (70%) bewaren de gegevens en leven deze wettelijke bewaarplicht na.
Van de 24 aanbieders (7%) die de gegevens niet bewaren, bestaat de helft uit nieuwe aanbieders.

Vernietigen
Uit de resultaten blijkt dat 101 aanbieders (30%) de gegevens gedeeltelijk vernietigen en 163 aanbieders (48%) geven aan de gegevens geheel te vernietigen. 73 aanbieders (22%) geven aan niet te vernietigen na afloop van de bewaartermijn. Een deel van deze aanbieders gebruikt verkeers- en locatiegegevens voor bedrijfsdoeleinden. Agentschap Telecom zal zich vooral richten op de aanbieders die niet vernietigen. Van de 73 aanbieders die niet vernietigen is 42% nieuwe aanbieder.

Privacy
De resultaten tonen aan dat 84 aanbieders (25%) verkeers- en locatiegegevens, naast dataretentie, tevens gebruiken voor andere doeleinden in het kader van art. 11.5, 11.5a en 11.13 Tw. Binnen deze groep moeten de aanbieders voldoen aan de informatieplicht, het

toestemmingsvereiste en dienen zij de gegevens te anonimiseren dan wel te verwijderen zodra deze niet meer noodzakelijk zijn voor het doel waarvoor deze werden bewaard. Uit de meting is gebleken dat het gebruik van verkeers- en locatiegegevens voor bedrijfsdoeleinden, naast de normale bedrijfsvoering en dataretentie, is afgenomen. Van de aanbieders die de gegevens voor bedrijfsdoeleinden gebruiken geven 50 aanbieders (60%) aan te voldoen aan de informatieplicht en 36 aanbieders (43%) geven aan te voldoen aan het toestemmingsvereiste. Het vereiste dat de verkeers- en locatiegegevens moeten worden geanonimiseerd dan wel worden verwijderd, indien deze niet meer noodzakelijk zijn voor de bedrijfsdoeleinden, wordt door 39 aanbieders (46%) nageleefd. Agentschap Telecom zal zich ook met name richten op de groep aanbieders die niet voldoet aan de informatieplicht, het toestemmingsvereiste of het anonimiseren dan wel verwijderen van de gegevens.

Beveiliging

Voor wat betreft de beveiliging van gegevens kan uit de resultaten van de meting de conclusie worden getrokken dat 270 aanbieders (80%) verklaren aantoonbaar passende technische en organisatorische maatregelen te hebben genomen om opgeslagen gegevens te beveiligen, 19 aanbieders (6%) geven aan gedeeltelijk passende technische en organisatorische maatregelen te hebben genomen en 48 aanbieders (14%) geven aan geen maatregelen te hebben genomen. Voor wat betreft de verplichting om te beschikken over een beveiligingsplan dat voldoet aan de wettelijke vereisten van art. 3 Bbgt verklaren 185 aanbieders (55%) hieraan te voldoen. Het beveiligingsplan is geen statisch document. Bijna iedere aanbieder (92%) voert wijzigingen binnen de organisatie door in het beveiligingsplan.

Vergelijking vorige metingen

Uit de vergelijking tussen de ‘Meting dataretentie 2013’ en de 0- en 1-meting is, voor zover mogelijk, af te leiden dat over het algemeen de naleving van de wettelijke verplichtingen is verbeterd met betrekking tot dataretentie. Van de 337 aanbieders geeft 25% aan de NAW-, verkeers- en locatiegegevens langer te bewaren dan nodig voor de overbrenging van communicatie, omdat zij de gegevens gebruiken voor bedrijfsdoeleinden (marktonderzoek, verkoopactiviteiten, facturering en diensten met toegevoegde waarde). Dit is een daling in vergelijking met de 0- en 1-meting. De naleving van de privacyvereisten waar de aanbieders aan dienen te voldoen als zij de gegevens voor deze vier bedrijfsdoelen gebruiken, is nagenoeg gelijk gebleven.

Afkortingen

Aanbieder	Aanbieder van openbare elektronische communicatiediensten en/of -netwerken
ACM	Autoriteit Consument & Markt
Bbgt	Besluit beveiliging gegevens telecommunicatie
Tw	Telecommunicatiewet
Wet bewaarplicht	Wet bewaarplicht telecommunicatiegegevens

Bijlage I: aanbiedingsbrief 'Meting dataretentie 2013'

> Retouradres Postbus 1671 3800 BR Amersfoort

Piet Mondriaanlaan 54
3812 GV Amersfoort
Postbus 1671
3800 BR Amersfoort
T (033) 460 08 00
F (033) 460 08 50
www.agentschaptelecom.nl

Contactpersoon

T

E informatieveiligheid@
agentschaptelecom.nl

Ons kenmerk
AT-EZ/

Uw kenmerk
-

Bijlagen
1

Datum
Betreft Meting dataretentie 2013

Geachte heer, mevrouw,

Agentschap Telecom is belast met het toezicht op de naleving van de telecommunicatiewetgeving in het kader van dataretentie (opslag en vernietiging van telefonie- en internetgegevens). Deze wetgeving is van toepassing op aanbieders van openbare telecommunicatienetwerken en/of openbare telecommunicatiediensten (hierna: aanbieder). Ik vraag uw medewerking aan de meting dataretentie 2013 die Agentschap Telecom als toezichthouder uitvoert. De meting wordt uitgevoerd door middel van een enquête.

Niet vrijblijvend
De beantwoording van de enquêtevragen is niet vrijblijvend. Agentschap Telecom is gerechtigd namens de Minister deze inlichtingen te vorderen voor haar toezichtactiviteiten. Ingevolge artikel 18.7 Telecommunicatiewet (hierna: Tw) bent u verplicht uw medewerking te verlenen aan de meting dataretentie 2013. De gegevens die u verstrekt zullen vertrouwelijk worden behandeld. Tijdens inspecties en audits kan de feitelijke situatie worden vergeleken met de door u ingevulde antwoorden.

Meting dataretentie 2013
Het doel van de meting is te inventariseren of u als aanbieder voldoet aan de wettelijke vereisten voor dataretentie. Na een bepaalde periode gaat het agentschap met een volgende meting na of er verschuivingen optreden in de mate waarin de aanbieders deze verplichtingen naleven.

Op grond van het register van Autoriteit Consument & Markt blijkt dat uw organisatie binnen de reikwijdte van deze wetgeving valt. Mocht u van mening zijn dat uw organisatie niet aan de verplichtingen voor dataretentie hoeft te voldoen, dan kunt u dit aangeven in de enquête en verzoeken wij u tevens het formulier te retourneren.

Regelgeving
De voor u relevante artikelen zijn opgenomen in hoofdstuk 11 en 13 van de Tw, alsmede het Besluit beveiliging gegevens telecommunicatie. De Tw regelt onder meer de bewaartermijn voor internet- en telecommunicatiegegevens.
Naast de bewaartermijn is ook bepaald dat de bewaarde gegevens beveiligd en binnen een vastgestelde termijn vernietigd moeten worden. Voor het bewaren van gegevens die nodig zijn voor zakelijke doeleinden van aanbieders, zoals het overbrengen van communicatie, facturering en verkoopactiviteiten, geldt geen verplichting tot bewaring, maar wel tot verwijderen of anonimiseren. Deze gegevens mogen niet langer bewaard worden dan noodzakelijk voor de bedrijfsvoering van de aanbieder.

Enquête
In de bijlage treft u de enquête aan. Ik verzoek u de ingevulde enquête binnen drie weken na dagtekening van deze brief per e-mail of per post te retourneren.

- Per e-mail naar informatieveiligheid@agentschaptelecom.nl, o.v.v. 'meting dataretentie 2013';
- Per post naar Agentschap Telecom, t.a.v. afdeling Veiligheid, antwoordnummer 7234, 3800 TE Amersfoort.

Mocht u naar aanleiding van deze brief nog vragen hebben, dan vernemen wij dit graag van u.

Hoogachtend,

De Minister van Economische Zaken,
namens deze,

A.C. van Emous
Hoofd Veiligheid afdeling Toezicht
Agentschap Telecom

Bijlage II: enquête 'Meting dataretentie 2013'

Enquête meting dataretentie 2013 inzake de mate van naleving van de Twging in het kader van dataretentie[18].

De beantwoording van de vragen in deze enquête is niet vrijblijvend. De informatie wordt namens de Minister van Economische Zaken opgevraagd op basis van art. 18.7 van de Tw (Tw).

* *Bij vragen met een sterretje zijn meerdere antwoorden mogelijk.*

Vestigings- en contactgegevens

Ondernemingsnaam:
Straat:
Postcode:
Plaats:

Postadres:
Postbus:
Postcode:
Plaats:

Algemeen telefoonnummer vestiging:

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

Omvang van uw onderneming naar omzetgegevens

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

□ 0 - 2 miljoen euro
□ 2 - 20 miljoen euro
□ 20 miljoen euro of meer

Dienstverlening

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

□ Aanbieder van openbare telecommunicatienetwerken en/of openbare telecommunicatiediensten, welke gerelateerd kunnen worden aan het tapproces en/of het dataretentieproces.
□ Anders (wanneer u deze optie aankruist behoeft u de vragen 3 t/m 39 niet te beantwoorden).

[18] De volgende wetgeving is van toepassing op dataretentie: de Telecommunicatiewet (Tw) en het Besluit beveiliging gegevens telecommunicatie (Bbgt). De verplichtingen die volgen uit deze wetgeving worden aangeduid met de term 'dataretentie'.

3. Welke diensten worden er geleverd?*

□ Internettoegang
□ Telefoniedienst SIP, VOIP of vast
□ Mobiele telefonie
□ Prepaid
□ Wholesale internettoegang
□ Wholesale telefonie
□ Anders, namelijk…

Wholesale: het aanbieden van telecommunicatiediensten tot wederverkoop door resellers

4. Aan wie worden deze diensten geleverd?*

□ Particulieren (ga naar vraag 12)
□ Zakelijke markt (ga naar vraag 12)
□ Resellers (ga naar vraag 5)

Reseller: inkoper van telecommunicatiediensten met als doel deze weder te verkopen

5. Is er een overeenkomst met de reseller waarin vermeld wordt dat uw onderneming de gegevens bewaart voor de reseller in het kader van dataretentie?

□ Ja
□ Nee (ga naar vraag 12)

6. Is in de overeenkomst vastgelegd dat de wholesalepartij de, door de klanten van de reseller, gegenereerde verkeers- en locatiegegevens, bewaart?

Meer informatie over de te bewaren gegevens kunt u vinden op www.agentschaptelecom.nl/onderwerpen/veiligheid en in artikel 13.2a Tw.

□ Ja
□ Nee
□ Gedeeltelijk

7. Wie slaat de NAW-gegevens op?

□ Wholesale partij
□ Reseller

In vraag 8 tot en met 11 wordt met de term 'gegevens' bedoeld, de gegevens die u bewaart zoals u heeft aangegeven in vraag 6 en 7.

8. Is in de overeenkomst vastgelegd dat de opgeslagen gegevens voor de verplichte duur van zes of twaalf maanden worden bewaard?

□ Ja
□ Nee

Bewaartermijn:

- 6 maanden voor gegevens in verband met internettoegang, e-mail en internettelefonie
- 12 maanden voor gegevens in verband met telefonie over een vast of mobiel netwerk
- 12 maanden voor prepaid telefoniediensten en prepaid internetdiensten

Meer informatie over de bewaartermijn kunt u vinden op www.agentschaptelecom.nl/onderwerpen/veiligheid en in de artikelen 13.2a en 13.4 Tw.

9. Is in de overeenkomst vastgelegd dat de opgeslagen gegevens na de wettelijke bewaartermijn van zes of twaalf maanden binnen 8 dagen na de termijn onomkeerbaar moeten worden vernietigd?

□ Ja
□ Nee

Meer informatie over het vernietigen kunt u vinden op www.agentschaptelecom.nl/onderwerpen/veiligheid en in artikel 5 Besluit beveiliging gegevens telecommunicatie (Bbgt).

10. Is er overeengekomen dat de gegevens in het kader van dataretentie worden opgeslagen in een aparte database?

□ Ja
□ Nee

11. Zijn in de overeenkomst de vereiste technische en organisatorische maatregelen, waaraan moet zijn voldaan om de opgeslagen gegevens te beveiligen, vastgelegd?

□ Ja
□ Nee
□ Gedeeltelijk

Er moeten beveiligingsmaatregelen worden genomen ten aanzien van: a. personeel, fysieke beveiliging en beveiliging van de omgeving; b. beheer van communicatie- en bedieningsprocessen; c. toegangsbeveiliging van geautomatiseerde informatiesystemen; d. ontwikkeling, onderhoud en reparatie van geautomatiseerde informatiesystemen. Meer informatie kunt u vinden op www.agentschaptelecom.nl/onderwerpen/veiligheid en in artikel 2 Bbgt.

Bewaren

In vraag 12 tot en met 20 wordt met de term 'gegevens' bedoeld de NAW-, verkeers-, en locatiegegevens.

12. Worden alle bij uw dienstverlening gegenereerde gegevens bewaard?

Zie toelichting vraag 6

□ Ja
□ Nee
□ Gedeeltelijk

13. Worden alle binnen uw onderneming gegenereerde gegevens onder eigen beheer bewaard?

□ Ja (ga naar vraag 14)
□ Nee (ga naar vraag 16)
□ Gedeeltelijk (ga naar vraag 14)

14. Worden de in eigen beheer opgeslagen gegevens door uw onderneming bewaard voor de verplichte duur van zes of twaalf maanden?

Zie toelichting vraag 8

□ Ja, en dit is aantoonbaar
□ Ja, en dit is *niet* aantoonbaar
□ Nee

15. Worden de gegevens, opgeslagen in het kader van dataretentie, bewaard in een aparte database?

□ Ja
□ Nee

16. Worden de gegevens die niet onder eigen beheer worden bewaard door een derde partij opgeslagen?

□ Ja
□ Nee (ga naar vraag 21)
□ Gedeeltelijk

17. Worden de door een derde partij opgeslagen gegevens bewaard voor de verplichte duur van zes of twaalf maanden?

Zie toelichting vraag 8

□ Ja, en dit is aantoonbaar
□ Ja, en dit is *niet* aantoonbaar
□ Nee

18. Worden de gegevens, opgeslagen in het kader van dataretentie, door de derde partij bewaard in een aparte database?

□ Ja
□ Nee

19. Is er een overeenkomst waarin vermeld staat dat een derde partij de gegevens voor u bewaart?

□ Ja
□ Nee

20. Bij welke partij worden de te bewaren gegevens geheel of gedeeltelijk opgeslagen?

□ _____

Vernietigen

In vraag 21 tot en met 27 wordt met de term 'gegevens' bedoeld de NAW-, verkeers-, en locatiegegevens.

21. Worden alle bij uw dienstverlening gegenereerde gegevens vernietigd?

□ Ja
□ Nee
□ Gedeeltelijk

22. Worden de binnen uw onderneming gegenereerde gegevens onder eigen beheer vernietigd?

□ Ja (ga naar vraag 23)
□ Nee (ga naar vraag 24)
□ Gedeeltelijk (ga naar vraag 23)

23. Worden de in eigen beheer opgeslagen gegevens door uw onderneming na afloop van de bewaartermijn van zes of twaalf maanden binnen 8 dagen onomkeerbaar vernietigd?

Zie toelichting vraag 9

□ Ja
□ Nee
□ De gegevens worden onomkeerbaar vernietigd, echter niet binnen 8 dagen na de wettelijke bewaartermijn
□ De gegevens worden wel na de wettelijke bewaartermijn vernietigd, echter nog niet onomkeerbaar
□ Gedeeltelijk
□ De gegevens worden op basis van een ander wettelijk toegestaan doel bewaard
□ Onbekend, opslag bij derden

24. Worden de gegevens die niet onder eigen beheer worden bewaard door een derde partij vernietigd?

□ Ja
□ Nee (ga naar vraag 27)
□ Gedeeltelijk
□ Onbekend (ga naar vraag 27)

25. Is er tussen uw onderneming en de derde partij die de gegevens voor u bewaart overeengekomen dat deze de gegevens vernietigt?

□ Ja, en dit is aantoonbaar
□ Ja, en dit is *niet* aantoonbaar
□ Nee
□ Onbekend

26. Worden de door een derde partij opgeslagen gegevens onomkeerbaar vernietigd binnen 8 dagen na afloop van de bewaartermijn van zes of twaalf maanden?

Zie toelichting vraag 9

□ Ja
□ Nee
□ De gegevens worden onomkeerbaar vernietigd, echter nog niet binnen 8 dagen na de wettelijke bewaartermijn
□ De gegevens worden wel na de wettelijke bewaartermijn vernietigd, echter nog niet onomkeerbaar
□ Gedeeltelijk
□ De gegevens worden op basis van een ander wettelijk toegestaan doel bewaard
□ Onbekend

27. Kunt u aantonen dat de gegevens, zoals aangegeven in vraag 22 en 24, daadwerkelijk geheel of gedeeltelijk worden vernietigd?

□ Ja
□ Nee

Privacy

In vraag 28 tot en met 31 wordt met de term 'gegevens' bedoeld de verkeers-, en locatiegegevens.

Het is mogelijk dat de bij uw dienstverlening gegenereerde verkeers- en locatiegegevens door uw onderneming voor een mogelijk ander doel dan dataretentie worden bewaard. Er is geen bewaarplicht voor deze gegevens, echter wel een toestemmingsvereiste door uw gebruikers voor een aantal doelen en de plicht tot het anonimiseren dan wel verwijderen van de gegevens.

Meer informatie over privacy kunt u vinden op www.agentschaptelecom.nl/onderwerpen/veiligheid en in de artikelen 11.5, 11.5a en 11.13 Tw.

28. Bewaart u de desbetreffende gegevens voor een ander doel dan dataretentie?

□ Ja
□ Nee (ga naar vraag 32)

29. Informeert u uw gebruikers van de soorten verkeersgegevens die worden verwerkt en de duur van de verwerking voor de doeleinden ingevolge art. 11.5 Tw?

□ Ja
□ Nee

30. Vraagt u toestemming aan uw gebruikers voor het bewaren van de gegevens ten behoeve van marktonderzoek, verkoopactiviteiten en de levering van toegevoegde waardediensten?

□ Ja
□ Nee

31. Anonimiseert of verwijdert u de gegevens zodra deze niet meer noodzakelijk zijn voor het doel waarvoor deze werden bewaard, ingevolge art. 11.5, 11.5a en 11.13 Tw?

□ Ja, de gegevens worden geanonimiseerd en dit is aantoonbaar
□ Ja, de gegevens worden verwijderd zodra deze niet meer noodzakelijk zijn en dit is aantoonbaar
□ Ja, de gegevens worden geanonimiseerd en dit is *niet* aantoonbaar
□ Ja, de gegevens worden verwijderd zodra deze niet meer noodzakelijk zijn en dit is *niet* aantoonbaar
□ Nee

Beveiliging

In vraag 32 tot en met 35 wordt met de term 'gegevens' bedoeld de NAW-, verkeers-, en locatiegegevens.

32. Zijn er passende technische en organisatorische maatregelen genomen om de opgeslagen gegevens te beveiligen?

Zie toelichting vraag 11

□ Ja, en dit is aantoonbaar
□ Ja, en dit is *niet* aantoonbaar
□ Nee
□ Gedeeltelijk, en dit is aantoonbaar
□ Gedeeltelijk, en dit is *niet* aantoonbaar

33. Waar worden de desbetreffende gegevens opgeslagen?

□ Binnen een eigen digitale werkomgeving
□ Binnen een *on*beveiligde cloud
□ Binnen een beveiligde cloud
□ Anders, namelijk…

34. Worden de gegevens opgeslagen in Nederland?

□ Ja
□ Nee, in het buitenland
□ De gegevens worden niet opgeslagen
□ Onbekend

35. Is de toegang tot de gegevens beveiligd door speciale inloggegevens?

□ Ja
□ Nee

Beveiligingsplan

36. Beschikt u over een beveiligingsplan dat voldoet aan alle vereisten van art. 3 Bbgt?

□ Ja
□ Nee

37. Past u het beveiligingsplan aan indien er zich wijzigingen voordoen binnen uw onderneming, die van toepassing zijn op de gegevens in het plan, en stelt u Agentschap Telecom daarvan op de hoogte? *Indien Agentschap Telecom nog niet in het bezit is van uw beveiligingsplan, verzoeken wij u deze mee te sturen.*

□ Ja, en Agentschap Telecom wordt daarvan op de hoogte gesteld
□ Ja, en Agentschap Telecom wordt daarvan *niet* op de hoogte gesteld
□ Nee

Naleving

38. Voldoet u aan alle vereisten inzake dataretentie?

□ Ja (einde enquête)
□ Nee

39. Indien u niet voldoet aan alle vereisten inzake dataretentie, geef dan aan wanneer u denkt wel volledig te voldoen?

□ Binnen één maand □ Binnen zes maanden

□ Binnen drie maanden

Evaluatie

De volgende vragen zijn vrijblijvend. Met deze vragen willen wij onze dienstverlening evalueren en verbeteren.

40. Is er naar aanleiding van de gegeven informatie in de aanbiedingsbrief en de enquête duidelijk wat er van u verwacht wordt?

□ Ja
□ Nee

41. Vindt u het praktisch dat het toezicht door Agentschap Telecom wordt uitgevoerd in de vorm van een enquête?

□ Ja
□ Nee

42. Op welke manier zou u in de toekomst door Agentschap Telecom benaderd willen worden?

□ Schriftelijk
□ Elektronisch
□ Persoonlijke afspraak

43. Deze ruimte is bestemd voor overige aanbevelingen voor Agentschap Telecom:

□ _____

Dit is het einde van de enquête. Bedankt voor uw medewerking.

Bijlage III: bijlage behorende bij art. 13.2a van de Tw

In deze bijlage wordt verstaan onder:

- a. telefoondienst: oproepen (met inbegrip van spraak, voicemail, conference call of call-gegevens), aanvullende diensten (met inbegrip van call forwarding en call transfer), messaging- en multimediadiensten (met inbegrip van short message service (SMS), enhanced media service (EMS) en multimedia service (MMS);
- b. gebruikersidentificatie: een unieke identificatie die aan een persoon wordt toegewezen wanneer deze zich abonneert op of registreert bij een internettoegangsdienst of internetcommunicatiedienst;
- c. celidentiteit (Cell ID): de unieke code van een cel van waaruit een mobiele telefoonoproep werd begonnen of beëindigd.

In deze bijlage worden als gegevens, bedoeld in art. 13.2a van de wet, aangewezen de volgende gegevens:

- A. Bij telefonie over een mobiel of een vast netwerk:
  - a. het telefoonnummer van de oproeper en het telefoonnummer (de telefoonnummers) die werden opgeroepen en, in het geval van aanvullende diensten zoals call forwarding of call transfer, het nummer (de nummers) waarnaar de verbinding is doorgeleid.
  - b. namen en adressen van de betrokken abonnees of geregistreerde gebruikers;
  - c. datum en tijdstip van aanvang en einde van de verbinding;
  - d. de gebruikte telefoondienst;
  - e. bij mobiele telefonie:
  - – de International Mobile Subscriber Identity (IMSI) van de oproepende en van de opgeroepen deelnemer;
  - – de International Mobile Equipment Identity (IMEI) van de oproepende en de opgeroepen deelnemer;
  - – in geval van vooraf betaalde anonieme diensten, datum en tijdstip van de eerste activering van de dienst en aanduiding (Cell ID) van de locatie waaruit de dienst is geactiveerd;
  - – de locatieaanduiding bij het begin van de verbinding;
  - – gegevens voor het identificeren van de geografische locatie van cells middels referentie aan hun locatieaanduidingen gedurende de periode dat communicatiegegevens worden bewaard.

- B. Bij internettoegang, e-mail over het internet en internettelefonie:
  - a. de toegewezen gebruikersidentificatie(s) en de gebruikersidentificatie of telefoonnummer van de beoogde ontvanger(s) van een internettelefoonoproep;

- b. de gebruikersidentificatie en het telefoonnummer toegewezen aan elke communicatie die het publieke telefoonnetwerk binnenkomt;
- c. naam en adres van de abonnee of de geregistreerde gebruiker aan wie het IP-adres, de gebruikersidentificatie of het telefoonnummer was toegewezen op het tijdstip van de communicatie en naam (namen) en adres (adressen) van de abonnee(s) of de geregistreerde gebruiker(s) en de gebruikersidentificatie van de beoogde ontvanger van communicatie;
- d. datum en tijdstip van de log-in en log-off van een internetsessie gebaseerd op een bepaalde tijdzone, samen met het IP-adres, hetzij statisch, hetzij dynamisch, dat door de aanbieder van een internettoegangsdienst aan een communicatie is toegewezen, en de gebruikersidentificatie van de abonnee of geregistreerde gebruiker;
- e. datum en tijdstip van de log-in en log-off van een e-maildienst over het internet of internettelefoniedienst gebaseerd op een bepaalde tijdzone;
- f. de gebruikte internetdienst;
- g. het inbellende nummer voor een inbelverbinding;
- h. de digital subscriber line (DSL) of ander eindpunt van de initiatiefnemer van de communicatie.