Bewaarplicht van telecommunicatiegegevens

en het toezicht door Agentschap Telecom

Onderdeel Ministerie van Economische Zaken

Inhoud

Begrippen en definities

1 Bewaarplicht
1.1 Om welke gegevens gaat het?
1.2 Wat regelt de Wet bewaarplicht?
1.3 Veilig bewaren, leveren en vernietigen
1.4 Wat is de rol van Agentschap Telecom?

2 Toezicht in de praktijk
2.1 De aanbieders
2.2 De behoeftestellers
2.3 De burgers

3 Voorkomen van overtredingen
3.1 Wat Agentschap Telecom doet
3.2 Wat aanbieders zelf kunnen doen

4 Overtredingen
4.1 Drie categorieën overtredingen
4.2 De instrumenten van Agentschap Telecom
4.3 De hoogte van boetes

5 Klachten
5.1 Over aanbieders en behoeftestellers
5.2 Over Agentschap Telecom

6 Fasering van de invoering van het toezicht

Over Agentschap Telecom

Begrippen en definities

In dit document worden specifieke begrippen en definities gebruikt. Om de informatie uit dit document goed te kunnen begrijpen, worden deze hieronder eerst uitgelegd.

Aanbieders: bedrijven en organisaties die telecomdiensten en telecomnetwerken aanbieden. Voorbeelden hiervan zijn telecomoperators en internet serviceproviders.

Behoeftestellers: overheidsinstanties die gegevens opvragen bij aanbieders. Dit zijn politie, justitie, inlichtingen- en veiligheidsdiensten. Ze gebruiken de gegevens om ernstige misdrijven en terrorisme te onderzoeken, opsporen en voorkomen.

Gegevens: informatie die via telecommunicatie wordt uitgewisseld. Voor de bewaarplicht gaat het specifiek om verkeers- en locatiegegevens. Dus wie belt met wie, wanneer, waar en hoe lang.

1 Bewaarplicht

Aanbieders van telecommunicatiediensten en –netwerken slaan gegevens op over telecomverkeer dat via hun netwerk of dienst verloopt. Dat moet veilig gebeuren, volgens de regels van de Wet bewaarplicht. Agentschap Telecom ziet erop toe dat die regels worden nageleefd.

1.1 Om welke gegevens gaat het?

Het gaat om verkeers- en locatiegegevens. Dit zijn gegevens als wie met wie belt, wanneer en waar, en voor hoe lang. Aanbieders van telecomdiensten en -netwerken (hierna 'aanbieders') slaan die gegevens op. Die gebruiken ze bijvoorbeeld voor de eigen bedrijfsprocessen. In principe is de inhoudelijke informatie die via telecommunicatie wordt uitgewisseld, alleen zaak van de boodschapper en van de ontvanger. Privacyregels beschermen de inhoud tegen oneigenlijk gebruik.

Criminaliteit en terrorisme zijn de redenen voor het instellen van de Wet bewaarplicht. De aanbieders kunnen helpen bij het voorkomen van misdrijven. Daarom zijn ze verplicht om gegevens te bewaren, te leveren en te vernietigen. Aanbieders moeten die gegevens op verzoek leveren aan politie, justitie, inlichtingen- en veiligheidsdiensten (hierna 'behoeftestellers'). De gegevens moeten op een veilige manier worden aangeleverd.

1.2 Wat regelt de Wet bewaarplicht?

Welke verkeers- en locatiegegevens mogen en moeten aanbieders bewaren? En op welke manier? Hoe moeten aanbieders gegevens aanleveren? De Wet bewaarplicht telecommunicatiegegevens (hierna 'Wet bewaarplicht') regelt hoe aanbieders verkeers- en locatiegegevens veilig moeten bewaren, beveiligen en leveren.

De Wet bewaarplicht is het gevolg van de Europese richtlijn voor dataretentie. De wet is onderdeel van hoofdstuk 13 van de Telecommunicatiewet. Het huidige hoofdstuk 13 gaat over bevoegd aftappen van communicatie. De Wet bewaarplicht gaat over historische gegevens, en is daarmee een goede aanvulling.

1.3 Veilig bewaren, leveren en vernietigen

Gegevens bewaren, gegevens overdragen aan behoeftestellers als die erom vragen, en gegevens vernietigen: het moet veilig gebeuren, met oog voor de privacy en de bescherming van de persoonlijke levenssfeer van burgers en ook met oog voor het belang van de staat.

Datavernietiging in de wet
De huidige Telecommunicatiewet (met name de artikelen 11.5, 11.5a en 11.13) regelt al dat aanbieders verkeers- en locatiegegevens moeten vernietigen, met het oog op privacy van gebruikers. En ook welke gegevens aanbieders mogen gebruiken voor eigen doeleinden.

Veilig betekent: gegevens mogen niet in verkeerde handen komen. Veilig betekent ook dat alleen locatie- en verkeersgegevens worden opgeslagen, en dus niet ook de inhoud van de e-mail of het telefoongesprek. Veilig betekent tot slot dat de bewaarde gegevens na twaalf maanden op een adequate manier worden vernietigd.

Om behoeftestellers van dienst te kunnen zijn, moet de aanbieder ervoor zorgen dat de gegevens van voldoende kwaliteit zijn. En niet gemanipuleerd of gewijzigd. En, niet onbelangrijk: als om bepaalde gegevens wordt verzocht, zijn niet alleen de gevraagde gegevens staatsgeheim, maar ook het leveringsverzoek zelf. De aanbieder moet zijn pakket aan beveiligingsmaatregelen dus goed georganiseerd hebben.

In het kort: de verplichtingen van aanbieders

Bewaren en vernietigen
Aanbieders van telefoniediensten zijn verplicht verkeers- en locatiegegevens van het telecommunicatieverkeer twaalf maanden te bewaren. Niet korter en niet langer. Na twaalf maanden moeten de bewaarde gegevens op een adequate manier worden vernietigd. Deze regels gelden ook voor internet serviceproviders. In de zomer van 2009 is, onder druk van de Eerste Kamer, de bewaartermijn voor internetgegevens teruggebracht naar zes maanden. Daarom heeft het Kabinet een reparatiewetsvoorstel gemaakt dat voor advies naar de Raad van State is gezonden. Later zal het opnieuw worden ingediend bij de Tweede Kamer, die de verkorte termijn dan moet goedkeuren. Tot die tijd blijft de oorspronkelijke wet van kracht, met een bewaartermijn van 12 maanden.

Beveiligen
Al deze, vertrouwelijke, gegevens moeten goed beveiligd zijn. Zodat zij niet beschikbaar zijn voor onbevoegden. En zodat ze niet verloren kunnen gaan, of kunnen worden gewijzigd of gemanipuleerd. Ook moet de aanbieder voorkomen dat er gegevens worden bewaard die niet bewaard mogen worden.

Beschikbaar stellen
De aanbieder is verplicht de gegevens direct te overhandigen aan behoeftestellers wanneer zij daar om verzoeken. Behoeftestellers mogen zo'n leveringsverzoek niet zomaar doen: er is eerst toestemming nodig van de officier van justitie. Die geeft alleen toestemming als het gaat om zware misdrijven of terrorisme.

1.4 Wat is de rol van Agentschap Telecom?

Toezicht op naleving van de wetgeving rondom dataretentie en –vernietiging is belangrijk. Voor de privacy van burgers, en voor een effectievere bestrijding van ernstige criminaliteit. De Wet bewaarplicht geeft niet alleen regels, maar beschrijft ook hoe het toezicht wordt ingericht. Toezichthouder is Agentschap Telecom. Dit agentschap houdt ook toezicht op de naleving van de artikelen 11.5, 11.5a en 11.13 van de Telecommunicatiewet, die gaan over datavernietiging. En op de naleving van hoofdstuk 13 van de Telecommunicatiewet, over bevoegd aftappen.

Agentschap Telecom opereert als een onafhankelijke toezichthouder. Het is onderdeel van het ministerie van Economische Zaken, en legt rechtstreeks verantwoording af aan de staatssecretaris van Economische Zaken. Agentschap Telecom zal ook optreden bij geschillen tussen aanbieder en behoeftesteller. Verder publiceert het agentschap onderzoeksresultaten over de naleving van de wet- en regelgeving en doet aanbevelingen.

Agentschap Telecom maakt gebruik van de registers van de Onafhankelijke Post- en TelecommunicatieAutoriteit (OPTA). Bij de OPTA zijn aanbieders van openbare diensten of netwerken geregistreerd. Het agentschap werkt ook samen met het College bescherming persoonsgegevens (CBP), toezichthouder van wetgeving over privacy en bescherming van de persoonlijke levenssfeer. Want het belang van de bestrijding van criminaliteit en het beschermen van de staatsveiligheid kan botsen met de bescherming van de persoonlijke levenssfeer. In beide gevallen gaat het om grondrechten.

Ook bestaat het gevaar van oneigenlijk gebruik wanneer aanbieders gegevens gebruiken voor bijvoorbeeld marketingdoeleinden. Daarom kent de Wet bewaarplicht waarborgen om de privacy van gebruikers te beschermen. Agentschap Telecom houdt daar toezicht op, in nauwe afstemming met het CBP.

Instrumenten van Agentschap Telecom

Voorlichting en ondersteuning
Het agentschap geeft voorlichting en ondersteuning via de website en via nieuwsbrieven. Het agentschap is ook telefonisch bereikbaar voor vragen en ondersteuning via zijn eigen klantcontactcentrum.

Controle en inspectie
Het beveiligingsplan van aanbieders moet voldoen aan wettelijke regels. Dat geldt ook voor bepaalde processen. Welke processen, dat staat in dit plan. Het agentschap controleert plan en processen. Bestaat het vermoeden dat regels niet (helemaal) worden nageleefd, dan inspecteert het agentschap ter plaatse.

Waarschuwing, last onder dwangsom, boete, strafrecht
Bij overtredingen grijpt het agentschap in en kunnen er sancties worden opgelegd.

2 Toezicht in de praktijk

Aanbieders moeten hun verkeers- en locatiegegevens veilig bewaren, beschikbaar stellen en tijdig vernietigen. In het belang van politie, justitie, veiligheids- en inlichtingendiensten. En in het belang van de privacy van gebruikers. Agentschap Telecom houdt daar toezicht op. Wat betekent het toezicht voor de verschillende partijen in de praktijk?

2.1 De aanbieders

Om de veiligheid van de opgeslagen gegevens te waarborgen, moet elke aanbieder maatregelen nemen. Die maatregelen volgen uit de Wet bewaarplicht telecommunicatiegegevens (de bewaarplicht), en bijvoorbeeld ook uit de Wet bescherming persoonsgegevens (WBP).

Elke aanbieder moet de getroffen maatregelen vastleggen in een beveiligingsplan. Agentschap Telecom controleert deze plannen. Dat verloopt zo: bij het ingaan van de bewaarplicht vraagt het agentschap bij elke aanbieder een kopie op van het beveiligingsplan. Als het nodig is, reageert het agentschap met adviezen ter verbetering. Eventueel wordt een voortgangscontrole aangekondigd, al dan niet gecombineerd met een waarschuwing. Op een waarschuwing volgt altijd een vervolgcontrole. En als daar bij een bepaalde aanbieder, of in het algemeen, aanleiding toe is, voert Agentschap Telecom ook bijzondere controles uit op bepaalde onderwerpen.

Opslag in het buitenland?
Grote aanbieders opereren vaak internationaal. Dan kan het zijn dat een Nederlandse aanbieder data in het buitenland opslaat. Dat kan bepaalde vraagstukken opleveren. Denk bijvoorbeeld aan belemmeringen voor fysiek toezicht. Maar: ook bij opslag in het buitenland blijft de Nederlandse wet- en regelgeving van kracht.

Een aanbieder kan zijn beveiligingsplan wel op orde hebben, maar in de praktijk niet (goed) uitvoeren. Bij een gerichte verdenking voert Agentschap Telecom een grondige inspectie uit. Worden er overtredingen geconstateerd, dan leidt dat waarschijnlijk tot sancties (meer daarover in hoofdstuk 4). Ook doet Agentschap Telecom jaarlijks een reeks steekproeven bij aanbieders. Dit om de actualiteit en de naleving van de beveiligingsplannen te controleren. Het agentschap kan bijvoorbeeld vragen om inzage in logbestanden, die bepaalde processen hebben geregistreerd.

2.2 De behoeftestellers

Politie, justitie, veiligheids- en inlichtingendiensten kunnen gegevens opvragen bij aanbieders. De Wet bewaarplicht regelt niet welke gegevens in welke gevallen opgevraagd mogen worden. De bevoegdheden van behoeftestellers zijn vastgelegd in andere wetgeving: in het Wetboek van Strafvordering. Aan die bevoegdheden is met de komst van de Wet bewaarplicht niets veranderd.

In de praktijk ziet Agentschap Telecom erop toe dat aanbieder én behoeftesteller de benodigde voorbereidingen hebben getroffen voor een veilige gegevensoverdracht. Dat is van groot belang. Want de taak van de behoeftestellers maakt dat zowel het leveringsverzoek als de gegevens zelf, staatsgeheim is. Bij conflicten tussen beide partijen speelt het agentschap een bemiddelende rol.

Een klacht van een behoeftesteller over een aanbieder kan aanleiding zijn voor het agentschap om een bijzondere controle of een inspectie uit te voeren bij die aanbieder.

2.3 De burgers

Voor burgers geldt het grondrecht van privacy en bescherming van de persoonlijke levenssfeer. Met name het CBP houdt toezicht op wetgeving op dat gebied. Ook de bewaarplicht raakt de privacy van burgers. Want verkeers- en locatiegegevens geven informatie over de persoonlijke levenssfeer: ze geven inzicht in wie met wie belde, waar en voor hoe lang.

De bewaarplicht stelt daarom duidelijke beperkingen aan de tijdsduur en het soort gegevens dat bewaard mag worden. Dat verhoogt het gevoel van veiligheid bij burgers, en vormt zo een bescherming van de persoonlijke levenssfeer.

3 Voorkomen van overtredingen

Voorkomen is beter dan genezen. Dit is een belangrijk uitgangspunt van Agentschap Telecom. Daarom steekt het agentschap veel energie in voorlichting en ondersteuning. Pas daarna komen er instrumenten als inspectie, boetes, bestuursdwang en – in het uiterste geval – strafrecht.

3.1 Wat Agentschap Telecom doet

Langs verschillende kanalen kunnen aanbieders rekenen op informatie en communicatie over de bewaarplicht. De website www.agentschap-telecom.nl bevat structurele informatie over het onderwerp.

Regelmatige e-mails informeren over nieuwe ontwikkelingen en bijzondere onderwerpen, zoals vernietiging en privacy. Op de website staan handige checklists voor aanbieders. Ook staan er richtlijnen voor beveiligingsplannen die aanbieders kunnen gebruiken bij het opstellen van hun beveiligingsplannen.

Agentschap Telecom zal regelmatig met vertegenwoordigers van aanbieders, belangengroepen en het ministerie van Economische Zaken van gedachten wisselen over ontwikkelingen en ervaringen. Ook voor de behoeftestellers is er regelmatig gelegenheid om ervaringen uit te wisselen.

Verschillen tussen aanbieders
De behoefte aan informatie en ondersteuning is niet bij elke aanbieder even groot. Want aanbieders verschillen onderling enorm. In aantallen gebruikers en in (aantallen) producten en diensten. Vooral bij kleine aanbieders kan de bewaarplicht een grote impact hebben. Het agentschap ondersteunt hen doormiddel van voorlichting en het aanbieden van richtlijnen voor beveiligingsplannen.

3.2 Wat aanbieders zelf kunnen doen

1 Informatie vergaren over ontwikkelingen
De aard van de dienstverlening van aanbieders is privacygevoelig. Met of zonder Wet bewaarplicht. Het is dus zaak voor aanbieders om zich te blijven informeren. Het agentschap stelt zich op als kenniscentrum op dit terrein. De website is een centraal informatiepunt. Ook wordt een informatiepakket voor aanbieders ontwikkeld.

2 Goede beveiligingsplannen maken en uitvoeren
Juist vanwege de privacygevoeligheid van hun dienstverlening hebben veel aanbieders al een beveiligingsplan. Met als doel aftappen door onbevoegden te voorkomen en het bevoegde aftappen op een veilige manier mogelijk te maken.

Anderen hebben nog geen, of nog geen volledig plan. Die groep aanbieders moet dus alsnog zorgen voor een correct beveiligingsplan. Agentschap Telecom ondersteunt hen daarbij door richtlijnen aan te bieden voor beveiligingsplannen.

Bewaarplicht: bedrijfsbelangen vs. privacy
Aanbieders kunnen de bewaarplicht als een last ervaren. Veilig databeheer kan immers geld kosten en levert geen (direct) financieel belang op. Maar de dienstverlening van de aanbieders betekent dat ze over grote hoeveelheden privacygevoelige informatie beschikken. Dat brengt verantwoordelijkheid met zich mee. De bewaarplicht helpt de aanbieder die verantwoordelijkheid waar te maken door regels te stellen voor het veilig bewaren en vernietigen van gegevens. De bedrijfsbelangen van de aanbieder lopen hier dus in feite parallel met de privacybelangen van de burger.

3 Sancties voorkomen
De strategie van Agentschap Telecom is: eerst voorlichten en waarschuwen. Pas als dat niet werkt, komen bestuurlijke sancties en strafrecht in beeld.

4 Overtredingen

Met toezicht op dataretentie wil Agentschap Telecom het risico op incidenten en mogelijke schade door overtredingen zo klein mogelijk houden. Het agentschap beschikt daarbij over verschillende instrumenten: van waarschuwing tot strafrecht.

4.1 Drie categorieën overtredingen

Overtredingen van de wet- en regelgeving rond de bewaarplicht worden onderscheiden in drie categorieën: lichte, middelzware en zware overtredingen. Daarbij gaat het telkens om de vraag of er een incident optreedt, en of daar vervolgens schade uit ontstaat.

Welk instrument gebruikt Agentschap Telecom bij een overtreding? Dat hangt – naast de overtreding – af van het soort aanbieder. Uit een doelgroepanalyse van het agentschap komen drie doelgroepen: netwerkaanbieders, dienstenaanbieders zonder eigen netwerk en kleine(re) aanbieders die het grootste deel van hun bedrijfsvoering inkopen. Deze doelgroepen zijn gedefinieerd op basis van aantallen gebruikers en (aantallen) producten en diensten. Ook speelt mee of de bedrijfsvoering gedeeltelijk in het buitenland plaatsvindt.

Lichte overtredingen

Een lichte overtreding is een overtreding van de wet- en regelgeving die niet direct tot een incident heeft geleid. Een aanbieder heeft bijvoorbeeld een steek laten vallen bij de autorisatie van de eigen medewerkers. Dat is dus een overtreding. Als de verkeerde autorisaties geen gevolgen hebben, is er geen sprake van een incident.

Hoe opsporen
Een lichte overtreding kan aan het licht komen bij controle van de beveiligingsplannen. Of bij een inspectie.

Hoe optreden
Zeker in het eerste jaar dat de bewaarplicht ingaat (zie hoofdstuk 5), zal het agentschap volstaan met voorlichting of een waarschuwing. Als dat niet werkt, bij onwil van de aanbieder, kan een last onder dwangsom of een boete worden opgelegd.

Middelzware overtredingen

Een middelzware overtreding is ernstiger: de overtreding leidt wel tot een incident. Maar dat incident leidt niet tot schade. Een voorbeeld: een aanbieder heeft de autorisatie niet goed geregeld. Een van de medewerkers maakt daar misbruik van, door onbevoegd gegevens van klanten in te zien. Dat is een incident. Maar de medewerker schaadt de belangen van die klanten niet; er is dan geen sprake van schade.

Hoe opsporen
Een middelzware overtreding kan aan het licht komen bij controle van de beveiligingsplannen. Of bij een inspectie. Krijgt het agentschap een klacht binnen over een mogelijk incident, dan krijgt de opsporing daarvan prioriteit.

Hoe optreden
Het agentschap zal een last onder dwangsom of een boete opleggen.

Zware overtredingen

wat
De overtreding leidt tot een incident waarbij de belangen van burgers, behoeftestellers of de overheid direct worden geschaad.

hoe opsporen
Overtredingen van deze categorie hebben hoge prioriteit bij Agentschap Telecom. Het agentschap voert met name preventieve controles uit op punten waar volgens de risicoanalyses de kans op deze overtredingen het grootst is.

hoe optreden
Als de mogelijkheid tot herstel bestaat, legt het agentschap in principe een last onder dwangsom op. Bij verwijtbaar handelen door de aanbieder volgt (ook) een boete. De doelgroepanalyse geeft aan welke interventie hier het meest effectief is.

4.2 De instrumenten van Agentschap Telecom

Agentschap Telecom heeft vier instrumenten om op te treden bij overtredingen. In toenemende zwaarte: waarschuwing, last onder dwangsom, boete en strafrecht.

Waarschuwing
Bij een waarschuwing krijgt de aanbieder de mogelijkheid om de situatie te verbeteren of te herstellen. Er wordt nog geen boete opgelegd. Na een voortgangscontrole besluit het agentschap of er verdere stappen ondernomen moeten worden.

Last onder dwangsom
De aanbieder krijgt de mogelijkheid de overtreding binnen een vastgestelde tijd te herstellen. Doet hij dat niet, dan moet hij de dwangsom betalen, en alsnog de overtreding tenietdoen.

Boete
Als waarschuwing en dwangsom niet werken, of als er sprake is van onwil, dan kan het agentschap een boete opleggen.

Strafrecht
Is de overtreding een strafbaar feit, dan kunnen de politie en het openbaar ministerie strafrechtelijke stappen ondernemen.

4.3 De hoogte van boetes

De hoogte van boetes is in principe afhankelijk van de ernst van de overtreding. Voor lichte overtredingen is het basisbedrag € 250, bij middelzware overtredingen is dat € 500 en bij zware € 1000.

Bij de bepaling van de boete speelt ook de omvang van de aanbieder een rol: overtredingen door grote aanbieders hebben immers meer impact dan bij kleine. Er worden vier categorieën onderscheiden. Naar de bruto omzet: onder € 200.000, onder € 2 miljoen, onder € 20 miljoen, en daarboven. Boven de € 200.000 omzet worden de basisbedragen verhoogd. Het resultaat staat hieronder.

De boetes per overtreding, afhankelijk van de omzet
(de bedragen gelden per 1 januari 2009)

	minder dan € 200.000	€ 200.000 - € 1.999.999	€ 2.000.000 - € 19.999.999	€ 20.000.000 en meer
licht	€ 250	€ 1.250	€ 6.250	€ 62.500
middel	€ 500	€ 2.500	€ 12.500	€ 125.000
zwaar	€ 1.000	€ 5.000	€ 25.000	€ 250.000

5 Klachten

5.1 Over aanbieders en behoeftestellers

Aanbieders slaan verkeersgegevens op, behoeftestellers kunnen deze opvragen. De belangen van beide partijen hoeven niet altijd gelijk te lopen, waardoor geschillen ontstaan. Partijen kunnen het agentschap vragen om een uitspraak. Het agentschap kan daarbij een externe partij om advies vragen.

5.2 Over Agentschap Telecom

Het kan ook zijn dat een aanbieder een klacht heeft over Agentschap Telecom. Deze kunnen schriftelijk worden ingediend. Vervolgens nemen wij eerst telefonisch contact op met de aanbieder om de klacht te bespreken. Afhankelijk van de aard en omvang van de klacht zal Agentschap Telecom een reactie opstellen en eventuele aanpassingen in de werkwijze doorvoeren.

6 Fasering van de invoering van het toezicht

Op dit moment is er nog weinig bekend over hoe aanbieders omgaan met dataretentie. En ook niet hoe het staat met de naleving van – bestaande - regelgeving voor datavernietiging. Daarom kiest Agentschap Telecom voor een gefaseerde invoering van het toezicht.

De start van het toezicht (najaar 2009)
In het najaar van 2009 start Agentschap Telecom met het toezicht op de Wet bewaarplicht. Dit begint met nulmeting. Deze moet inzicht geven in hoeverre bestaande en nieuwe regels in de praktijk worden nageleefd. Centraal in dit eerste jaar staan voorlichting en ondersteuning. Bovendien moeten alle aanbieders het agentschap voorzien van een exemplaar van hun beveiligingsplan. Het agentschap zal daarop reageren met adviezen, aanbevelingen, waarschuwingen enzovoort.

Het eerste volledige toezichtsjaar (2010)
De ervaringen uit 2009 vormen de input van een nieuwe risicoanalyse, waarmee het toezicht verder wordt aangescherpt. Daardoor kan Agentschap Telecom zich dit tweede jaar meer richten op categorieën aanbieders waar de grootste risico’s zijn te verwachten. Het jaar wordt afgesloten met een uitgebreide evaluatie van het toezicht, de effecten en de risico's.

Daarna
Het streven is om 20% van de aanbieders met het hoogste risico jaarlijks te controleren. De overige 80% komt eens in de twee jaren aan bod. Op basis van de eerste twee toezichtsjaren komt Agentschap Telecom met aanbevelingen voor aanpassingen in de (nieuwe) wet- en regelgeving rondom dataretentie.

Agentschap Telecom

Minder last, meer effect
Dat is de overheidsbrede visie op toezicht. Die visie brengt Agentschap Telecom in praktijk. Met toezicht dat zich laat omschrijven als:
Selectief: gericht toezicht, gebaseerd op analyse en onderzoek
Slagvaardig: toezicht op maat, door een geschikt scala aan instrumenten
Samenwerkend: taken en informatie delen daar waar het kan
Onafhankelijk: directe verantwoording aan de minister
Transparant: duidelijk zijn over toezicht
Professioneel: werken met professionele, ervaren toezichthouders

Over de organisatie
Agentschap Telecom maakt deel uit van het ministerie van Economische Zaken. Het ministerie heeft – ook namens de ministers van Binnenlandse Zaken, Justitie en Defensie – het agentschap de taak gegeven om toezicht te houden op de naleving van de Wet bewaarplicht.

De markt voor elektronische communicatie heeft een zekere technische regulering nodig. Agentschap Telecom stelt kaders die technische innovaties en economische ontwikkeling mogelijk maken. Daarbij willen we zo min mogelijk beperken en maximaal faciliteren. Zo stellen we frequentieruimte beschikbaar waarbinnen bedrijven zoveel mogelijk vrij kunnen innoveren. Omdat het frequentiespectrum schaars is, moet het gebruik ervan doelmatig zijn. Dit maakt dat Agentschap Telecom meer en meer de *technical regulator* van Nederland wordt.

De toezichtstaken strekken zich uit over een breed gebied: zo houdt het agentschap ook toezicht op de handel in elektrische apparaten of telecommunicatieapparaten, bevoegd aftappen, de beschikbaarheid van netwerken. Nieuwe toezichtstaken hebben we op het gebied van de Wet Ruimtevaartactiviteiten, de Grondroerdersregeling en de bereikbaarheid van het alarmnummer 112.

Meer informatie

Dit document is bedoeld om een algemeen inzicht te geven in het toezicht van Agentschap Telecom rond de Wet bewaarplicht telecommunicatiegegevens. Meer informatie vindt u op de www.agentschap-telecom.nl. En in de Wet zelf: kijk daarvoor op www.wetten.nl.

Dit document komt niet in plaats van de wet- en regelgeving rond de bewaarplicht. U kunt er daarom geen rechten aan ontlenen.

Agentschap Telecom
Emmasingel 1
9726 AH Groningen
T 050 587 74 44
E agentschaptelecom@at-ez.nl
www.agentschap-telecom.nl