



Agentschap Telecom  
Ministerie van Economische Zaken

# Regels

voor openbare aanbidders



Als aanbieder van openbare telecommunicatienetwerken en/of -diensten, bijvoorbeeld (mobiele) telefonie en internettoegang moet u aan een aantal verplichtingen voldoen. Deze verplichtingen zijn opgenomen in de Telecommunicatiewet en de daarbij horende besluiten en regelingen.

## Waar u aan moet voldoen

In de Telecommunicatiewet staan de volgende regels beschreven:

- aftapbaar maken van uw netwerk of dienst;
- bewaren, vernietigen en beschikbaar stellen van telecomgegevens;
- beveiligen van telecomgegevens;
- privacy;
- verwijderen of anonimiseren van verkeers- en locatiegegevens;
- waarborgen van de bereikbaarheid van 112.

---

## De rol van Agentschap Telecom

Agentschap Telecom opereert als een onafhankelijke toezichthouder. De organisatie is onderdeel van het ministerie van Economische Zaken en legt rechtstreeks verantwoordelijkheid af aan de Minister van Economische Zaken.

Agentschap Telecom zal ook optreden bij geschillen tussen aanbieder en behoefte-steller. Toezicht op naleving van de wetgeving is belangrijk. Telecommunicatiegegevens dragen bij aan de bestrijding van criminaliteit en terrorisme.

---

## Registreren bij de OPTA

Voor het houden van toezicht wordt onder andere de registratielijst van de Onafhankelijke Post- en Telecommunicatie Autoriteit (OPTA) gehanteerd. Bij de OPTA

zijn aanbieders van openbare diensten of netwerken geregistreerd. Wanneer u dus aanbieder bent, moet u zich aanmelden bij de OPTA.



## Bevoegd aftappen

Bevoegd aftappen is het beluisteren en/of opnemen van telecommunicatieverkeer voor opsporingsonderzoeken en voor de Staatsveiligheid. Het speelt een belangrijke rol bij de bestrijding van georganiseerde en zware criminaliteit, terrorismebestrijding en bij de zorg voor de Staatsveiligheid. Alleen onder strikte voorwaarden mag op verzoek van behoeftestellers worden getapt. De vordering of het verzoek aan u om te leveren komt via de Officier van Justitie of het hoofd van de AIVD.

De vereisten voor bevoegd aftappen vindt u in hoofdstuk 13 van de Telecommunicatiewet.

### Waar moet u aan voldoen?

Om uw netwerk of dienst aftapbaar te maken en houden, is het noodzakelijk dat u voorzieningen in uw netwerk inbouwt. Wanneer behoeftestellers daarom vragen, is het essentieel dat u hen alle gegevens verstrekt die hen in staat stellen hun bevoegdheden op het gebied van aftappen uit te oefenen. Denk ook aan de naam, het adres en de woonplaats die bij een bepaald telefoonnummer behoren. Verdere uit-

werking van de regels voor aftappen vindt u in het Besluit en de Regeling aftappen openbare telecommunicatienetwerken en –diensten.

### Centraal Informatiepunt Onderzoek Telecommunicatie (CIOT)

Het CIOT is een organisatie die tussen u en de aanvragers van telecommunicatiegegevens staat. Het CIOT beheert een geautomatiseerd informatiepunt (het CIOT-informatiesysteem) en draagt zo bij aan zorgvuldige opslag en gebruik van de informatie. Het CIOT heeft zelf geen inzage in de gegevens. (Bijzondere) opsporings-, inlichtingen- en veiligheidsdiensten zijn bevoegd om gegevens in het informatiesysteem op te vragen als dat nodig is voor strafvordering, inlichtingenverzameling of hulpverlening in noodsituaties.

Verdere uitwerking van de regelgeving voor het aanleveren van gegevens aan het CIOT vindt u in het Besluit verstrekking gegevens telecommunicatie.

# Bewaarplicht telecommunicatiegegevens

Sinds 1 september 2009 is de Wet bewaarplicht telecommunicatiegegevens (hierna: Wet bewaarplicht) van kracht. Met de Wet bewaarplicht worden aanbieders van openbare telecommunicatienetwerken en/of -diensten (internettoegang, e-mail en (internet-) telefonie) verplicht tot het bewaren van verkeers- en locatiegegevens van gebruikers voor een periode van twaalf maanden. Het gaat hierbij niet om de inhoud van de communicatie. Het bewaren van verkeers- en locatiegegevens is van belang voor de opsporing en vervolging van (ernstige) misdrijven. Meer informatie over de Wet Bewaarplicht vindt u in hoofdstuk 13 van de Telecommunicatiewet.

## Waar moet u aan voldoen?

### Bewaren

Er zijn drie categorieën gegevens die moeten worden opgeslagen:

- verkeersgegevens.
- locatiegegevens;
- naam, adres en woonplaats van de klant zoals die waren op het moment van de betreffende communicatie.

Een overzicht hiervan vindt u in de bijlage van artikel 13.2a van de Telecommunicatiewet.

Van groot belang is dat de opgeslagen gegevens authentiek zijn. Dit betekent dat de gegevens die u levert aan de behoefte-stellers precies dezelfde zijn als die in uw systeem.

### Beschikbaar stellen

Wanneer behoefte-stellers, zoals Justitie of inlichtingen- en veiligheidsdiensten, daarom vragen, bent u verplicht om de gegevens direct te overhandigen. Behoefte-stellers mogen zo'n leveringsverzoek niet zomaar doen: er is eerst toestemming nodig van de Officier van Justitie. Deze geeft alleen toestemming als het gaat om zware misdrijven of terrorisme.

### Vernietigen

Na twaalf maanden moeten de bewaarde gegevens op een adequate manier worden vernietigd. De wet zegt dat dit 'onverwijld' moet gebeuren. Dit houdt in dat binnen acht dagen na het verlopen van de bewaartermijn de gegevens onomkeerbaar moeten zijn vernietigd. Als de gegevens geheel of gedeeltelijk worden gebruikt voor bedrijfsdoeleinden, zoals voor markt-onderzoek of verkoopactiviteiten, dan mag u deze gegevens bewaren zolang dat nodig is mits u toestemming heeft van de abonnee.



## Beveiligen telecommunicatiegegevens

U kunt zich voorstellen dat goede beveiliging van al deze vertrouwelijke gegevens noodzakelijk is. Zodat zij niet beschikbaar zijn voor onbevoegden, niet verloren kunnen gaan, kunnen worden gewijzigd of gemanipuleerd.

### Beveiligingsplan

Het doel van het beveiligingsplan is dat u inzichtelijk maakt hoe u de beveiliging waarborgt. Beschikt u nog niet over een beveiligingsplan? Zorgt u er dan voor dat u deze zo snel mogelijk opstelt. De minimale inhoud van een beveiligingsplan is beschreven in het Besluit beveiliging gegevens telecommunicatie (Bbgt).



## Houd de privacy in acht

Voor het afhandelen van de communicatie genereert u verkeers- en locatiegegevens. Deze zijn privacygevoelig en moeten dus beschermd worden. Daarom zijn hier regels voor opgesteld. Deze vindt u in de artikelen 11.5, 11.5a en 11.13 van de Telecommunicatiewet. Agentschap Telecom houdt toezicht op het naleven van deze regels. Zij werkt hierbij nauw samen met het College Bescherming Persoonsgegevens.

Voor verkeersgegevens geldt dat wanneer zij niet langer nodig zijn voor het overbrengen van de communicatie, zij moeten worden verwijderd dan wel geanonimiseerd.

Uitzonderingen:

- wettelijke verplichtingen;
- verkeersgegevens voor facturatie;
- verkeersgegevens voor bedrijfsdoeleinden.

Voorwaarde voor de laatste twee uitzonderingen is dat u de abonnee

of gebruiker op de hoogte stelt van de periode waarin de gegevens worden verwerkt en welke verkeersgegevens het betreft. Voor gebruik van gegevens voor bedrijfsdoeleinden heeft u toestemming nodig van de gebruiker of abonnee. Deze mag de toestemming op ieder gewenst moment intrekken. Bovenstaande geldt ook voor locatiegegevens. Daarnaast moet het mogelijk zijn om de toegevoegde waarde dienst kosteloos en eenvoudig (tijdelijk) te stoppen.

Bovenstaande regels gelden niet:

- bij het belang van de nationale veiligheid of het voorkomen, opsporen en vervolgen van strafbare feiten;
- bij onderzoek naar hinderlijke of kwaadwillige oproepen bij een abonnee.

Deze verkeersgegevens mag u tot maximaal drie maanden na het beëindigen van een onderzoek bewaren. Na afloop van deze periode moet u de verkeersgegevens verwijderen.

# Verwijderen of anonimiseren van verkeers- en locatiegegevens

Voor verkeers- en locatiegegevens geldt dat wanneer zij niet langer nodig zijn voor het overbrengen van de communicatie, zij moeten worden verwijderd dan wel geanonimiseerd. Anonimiseren is het volledig en onomkeerbaar verwijderen van persoonsidentificerende kenmerken.

## Hoe kunt u anonimiseren?

Er zijn gegevens die direct weergeven om

welke persoon het gaat. Het verwijderen van direct identificerende kenmerken, zoals een telefoonnummer of IP-adres is echter niet altijd voldoende. Soms bevat een bestand gegevens van een abonnee die door het koppelen van verkeers- en locatiegegevens kunnen leiden tot identificatie van een persoon. Deze gegevens moeten dan worden verwijderd.

---

## Bereikbaarheid 112

De bereikbaarheid van het alarmnummer 112 is van levensbelang. Zorgt u er daarom voor dat alarmnummers onder alle omstandigheden bereikbaar zijn. Dit is wettelijk vastgelegd in artikel 7.7, derde lid van de Telecommunicatiewet.

Is er sprake van 'opstoppingen' in het telefoonnetwerk, zoals op oudejaarsavond? Zorgt u er dan voor dat u alle noodzakelijke maatregelen treft om de bereikbaarheid van alarmnummers te blijven waarborgen. Dit noemt men 'congestievoorziening'.



Agentschap Telecom – afdeling Toezicht  
Ministerie van Economische Zaken  
Postbus 1671 | 3800 BR | Amersfoort

T +31 (0)50 5877 444 (ma t/m vrij 8.30 – 17.00)  
informatieveiligheid@at-ez.nl  
[www.agentschap-telecom.nl](http://www.agentschap-telecom.nl)

September 2010