Agentschap Telecom
Ministerie van Economische Zaken en Klimaat

Biedt u openbare telefonie, internettoegang en/of een netwerk aan?

Biedt u openbare [1)] telefonie, internettoegang en/of een netwerk [2)] aan? Aanbieders [3)] van deze netwerken of diensten [4)] hebben op grond van de Telecommunicatiewet een aantal verplichtingen. In deze folder leest u hier meer over. Achterin deze folder staat een lijst waarin een aantal begrippen wordt uitgelegd.

Biedt u openbare telefonie, internettoegang en/of een netwerk aan?

Waar moet u aan voldoen

In de Telecommunicatiewet staan de volgende verplichtingen voor het mogen aanbieden van openbare telefonie, internettoegang en een netwerk:

1. U treft een voorziening die het mogelijk maakt dat uw netwerk en/of dienst kan worden afgetapt door de hiertoe bevoegde instanties;
2. U voldoet aan de regels omtrent de beveiliging van telecommunicatiegegevens;
3. U draagt zorg voor het voorkomen van uitval van het netwerk en/of de dienst. Grote storingen meldt u bij het Loket Meldplicht Telecomwet;
4. U houdt zich aan de privacyregels; u verwijdert of anonimiseert de verkeers- [5] en locatiegegevens [6] volgens de regels in de wet. U houdt zich aan de informatieplicht en u vraagt toestemming aan uw abonnee of gebruiker voor het gebruik van de eerdergenoemde gegevens (indien dit wettelijk is voorgeschreven).

In deze folder staat wat deze verplichtingen voor u betekenen. In de tekst wordt enkele keren verwezen naar de Telecommunicatiewet en de bijbehorende besluiten en regelingen*. De relevante wetteksten zijn te vinden op www.wetten.overheid.nl.

TIP: Beheert u beroepshalve een net dat in de ondergrond ligt of legt u een glasvezelnetwerk aan? Dan moet u dit net aanmelden bij het Kadaster. Hierdoor wordt uw net beschermd tegen beschadiging door graafactiviteiten. (www.kadaster.nl/netbeheerders)

**Daarnaast registreert u zich bij de Autoriteit Consument en Markt. Voor Radio en TV-omroepdiensten en/of -netwerken gelden alleen de continuïteitsverplichtingen.*

De rol van Agentschap Telecom

Agentschap Telecom is een onafhankelijke toezichthouder en ziet erop toe dat aanbieders de verplichtingen uit de Telecommunicatiewet naleven. Bij niet naleving van deze verplichtingen kan Agentschap Telecom optreden met bijvoorbeeld waarschuwingen, lasten onder dwangsom [7] en/of bestuurlijke boetes.

Het agentschap is onderdeel van het Ministerie van Economische Zaken en Klimaat.

1. Bevoegd aftappen

Bevoegd aftappen is het realtime beluisteren en/of opnemen van telecommunicatieverkeer door opsporings- of inlichtingendiensten. Het speelt een belangrijke rol bij de bestrijding van zware criminaliteit, terrorisme en bij de zorg voor de staatsveiligheid. Alleen onder strikte voorwaarden mag op bevel van een officier van justitie worden getapt. Ook de hoofden van de AIVD en MIVD kunnen opdracht geven deze gegevens te leveren. De verplichtingen rond bevoegd aftappen staan in hoofdstuk 13 van de Telecommunicatiewet.

Waar moet u aan voldoen?

Om uw netwerk en/of dienst aftapbaar te maken en te houden, is het noodzakelijk dat er voorzieningen in het netwerk worden ingebouwd, waarvoor u zelf verantwoordelijk bent (denk hierbij aan tapapparatuur). Wanneer behoeftestellers [8)] daarom vragen, is het essentieel dat u hen alle gegevens verstrekt, zodat zij kunnen aftappen. Denk bijvoorbeeld aan de naam, het adres en de woonplaats die bij een bepaald telefoonnummer horen. Verdere uitwerking van de regels voor aftappen vindt u in het Besluit en de Regeling aftappen openbare telecommunicatienetwerken en -diensten.

Centraal Informatiepunt Onderzoek Telecommunicatie (CIOT)

Het Centraal Informatiepunt Onderzoek Telecommunicatie (CIOT) is een 'doorgeefluik' tussen opsporings- en inlichtingendiensten die informatie nodig hebben en de aanbieders die deze informatie kunnen leveren. Het CIOT beheert een geautomatiseerd informatiepunt (het CIOT-informatiesysteem).

Aanbieders moeten zich hierop aansluiten en via dit informatiesysteem elke 24 uur een actueel digitaal bestand leveren met gegevens van hun abonnees die horen bij IP-adressen, telefoonnummers en e-mailadressen. Het CIOT heeft zelf geen inzage in deze gegevens. Zie ook het Besluit verstrekking gegevens telecommunicatie. Verdere informatie over het CIOT kunt u vinden op de website van het CIOT (www.ciot.nl).

2. Beveiligen telecommunicatie-gegevens

Een goede beveiliging van telecommunicatiegegevens (o.a. rondom een vordering) is noodzakelijk. Dit voorkomt dat deze beschikbaar komen voor onbevoegden, verloren gaan, gewijzigd of gemanipuleerd worden. Daarom wordt van u verwacht dat u een beveiligingsplan heeft.

Beveiligingsplan

Het doel van het beveiligingsplan is dat u inzichtelijk maakt hoe u de gegevens o.a. rondom een vordering beveiligt. Opsporings- en inlichtingendiensten kunnen deze opvragen. De minimale eisen voor een beveiligingsplan staan beschreven in het Besluit beveiliging gegevens telecommunicatie.

3. Continuïteit

Burgers en bedrijven vertrouwen op de beschikbaarheid van telecomdiensten en netwerken. Telecom- en ICT-storingen kunnen zowel economische als maatschappelijke gevolgen hebben. Daarom is het belangrijk om voorzorgsmaatregelen te treffen. Zo kunt u de continuïteit en de beschikbaarheid van uw dienst(en) en/of netwerken beschermen. Dit is zowel in uw belang als in het belang van uw klanten.

Zorgplicht

Maatregelen die u moet nemen
Om de beschikbaarheid van uw diensten en/of netwerken te waarborgen én om risico's van uitval te beheersen, moet u passende maatregelen nemen. 'Passend' betekent dat de kosten van de maatregelen van technische en organisatorische aard in redelijke verhouding staan tot de risico's. Bent u aanbieder van openbare telefoniediensten en/of netwerken waar openbare telefoniediensten over worden afgehandeld, dan geldt de verplichting om bij een technische storing of bij uitval van het elektriciteitsnetwerk, alle noodzakelijke maatregelen te treffen om de dienstverlening zo snel mogelijk te herstellen. U bent wettelijk verplicht deze maatregelen vast te leggen in een continuïteitsplan.

Continuïteitsplan
Dit plan bevat in ieder geval de maatregelen die u heeft genomen om de continuïteit van uw dienstverlening te waarborgen. Bijvoorbeeld hoe u de risico's op inbreuken van de veiligheid en integriteit van uw netwerk en dienst beheerst inclusief een actuele risicoanalyse. Wie binnen uw organisatie de verantwoordelijke continuïteitsfunctionaris is en meldfunctionaris is. Daarnaast kennen de werknemers die betrokken zijn bij de veiligheid en integriteit van uw netwerk, het plan en kunnen ze erbij als dat nodig is en is uw netwerk of dienst fysiek en digitaal beveiligd.

De minimale eisen voor een continuïteitsplan vindt u op de website van Agentschap Telecom. Zie ook het Besluit continuïteit openbare elektronische communicatienetwerken en –diensten.

Meldplicht

Mocht er ondanks de door u getroffen (voorzorgs)maatregelen toch een deel van uw netwerk en/of dienst uitvallen, dan bent u verplicht om grote storingen te melden. Dit doet u bij het Loket Meldplicht Telecomwet van Agentschap Telecom.

Melden, hoe gaat dat?
Een melding doet u via www.meldplichttelecomwet.nl. U vindt hier het formulier voor het melden van continuïteitsverstoringen. Na het insturen van dit internetformulier krijgt u van Agentschap Telecom een meldingsnummer. Kunt u nog niet meteen alle benodigde informatie aanleveren, stuur dan alvast de wel beschikbare informatie. De ontbrekende gegevens kunt u later nog aanvullen tot uiterlijk vier weken na het einde van het incident. Vermeld daarbij het meldingsnummer dat u bij de eerste melding heeft ontvangen. U kunt meldingen ook telefonisch doen, 24 uur per dag via 0900 - 70 70 701.

Bereikbaarheid 112

De bereikbaarheid van het alarmnummer 112 is van levensbelang. Als aanbieder bent u verplicht voorzieningen te treffen die noodzakelijk zijn om de ononderbroken toegang tot alarmnummers te waarborgen (denk hierbij aan een extra lijn of het reserveren van bandbreedte). Voor mobiele telefonie geldt wel dat daarvoor dekking aanwezig moet zijn van het mobiele netwerk.

Maatregelen
Is er sprake van 'congestie' in het telefoonnetwerk, bijvoorbeeld op oudejaarsavond of bij grote evenementen? Dan neemt u alle noodzakelijke maatregelen om de bereikbaarheid van het alarmnummer 112 te waarborgen. Deze maatregelen noemen we 'congestievoorzieningen'. Naast deze voorzieningen neemt u ook maatregelen om de bereikbaarheid van het alarmnummer te waarborgen bij een technische storing of uitval van het elektriciteitsnetwerk.

4. Houd de privacy in acht

Verkeers- en locatiegegevens zijn privacygevoelig en moeten worden beschermd. Dit betekent dat u de verkeers- en locatiegegevens verwijdert of anonimiseert wanneer deze niet langer nodig zijn voor het overbrengen van de communicatie.

Uitzonderingen zijn:
- wettelijke verplichtingen;
- verwerken van verkeers- en locatiegegevens voor bedrijfsdoeleinden.

Wilt u de verkeers- en locatiegegevens gebruiken voor bedrijfsdoeleinden, zoals facturatie? Dat mag, onder voorwaarde dat u de abonnee of gebruiker op de hoogte stelt van de periode waarin de verkeers- en locatiegegevens worden verwerkt en welke gegevens u bewaart voor dit doel. Voor gebruik van gegevens voor een aantal bedrijfsdoeleinden, zoals marktonderzoek, heeft u voorafgaand toestemming nodig van de abonnee of gebruiker. Deze mag de toestemming op elk gewenst moment intrekken. Daarnaast moet het mogelijk zijn om een dienst waarbij locatiegegevens worden gebruikt kosteloos en eenvoudig (tijdelijk) te stoppen.

Voor een onderzoek naar kwaadwillende en hinderlijke oproepen, bijv. stalking of bedreiging, is het toegestaan om op verzoek van een klant verkeersgegevens op te slaan.

De regels voor het beschermen van verkeers- en locatiegegevens staan in de artikelen 11.5, 11.5a en 11.13 van de Telecommunicatiewet. Agentschap Telecom houdt toezicht op het naleven van deze regels en werkt hierbij nauw samen met de Autoriteit Persoonsgegevens.

Begrippen en definities

In deze folder worden specifieke begrippen en definities gebruikt. Om de informatie goed te kunnen begrijpen, worden deze hieronder uitgelegd. De definities uit de Telecommunicatiewet of de onderliggende besluiten zijn echter altijd leidend.

1) Openbaar: voor het publiek beschikbaar.

2) Netwerk: een elektronisch communicatienetwerk of een telecommunicatienetwerk.

3) Aanbieders: bedrijven en organisaties die openbare telefonie, internet-toegang en/of een netwerk aanbieden.

4) Diensten: een elektronische communicatiedienst of een telecommunicatiedienst.

5) Verkeersgegevens: gegevens die worden verwerkt voor het overbrengen van communicatie over een elektronisch communicatienetwerk of voor de facturering ervan.

6) Locatiegegevens: gegevens waarmee de geografische positie van de apparatuur van een gebruiker wordt aangegeven.

7) Last onder dwangsom: bij een last onder dwangsom kan de overtreder een verplichting worden opgelegd (de zogenaamde 'last') om een overtreding ongedaan te maken of te beëindigen. Als de overtreder daar niet aan voldoet, moet de persoon of het bedrijf in kwestie een bepaald bedrag (per geconstateerde overtreding) betalen (de zogenaamde 'dwangsom').

8) Behoeftestellers: overheidsinstanties die gegevens opvragen bij aanbieders. Dit zijn politie, justitie, opsporings –en inlichtingendiensten. Zij gebruiken de gegevens om zware criminaliteit en terrorisme te onderzoeken, op te sporen en te voorkomen.

Voor meer informatie kunt u terecht op onze website
www.agentschaptelecom.nl

Agentschap Telecom – hoofdafdeling Toezicht
Ministerie van Economische Zaken en Klimaat
Postbus 1671 | 3800 BR | Amersfoort

T +31 (0)50 5877 444 (ma t/m vrij 8.30 – 17.00)
informatieveiligheid@agentschaptelecom.nl

December 2017