

## Uppdatering av föreskrift om televerksamhetens informationssäkerhet (Kommunikationsverket 67 A/2015 M): Enkät om erfarenheter och utvecklingsidéer

Traficom/16241/09.09/2022

### Inledning

Med denna enkät kartlägger Transport- och kommunikationsverket Traficom synpunkter på hur skyldigheterna i nuvarande föreskrift Kommunikationsverket 67 A/2015 M fungerar gällande televerksamhetens informationssäkerhet samt eventuella behov av ändringar för det påbörjade föreskriftsprojektet.

### Bakgrund

Traficom har fattat beslut om att starta ett föreskriftsprojekt för att uppdatera Kommunikationsverkets föreskrift om televerksamhetens informationssäkerhet (Kommunikationsverket 67 A/2015 M) som trädde i kraft den 4 mars 2015.

Föreskriften granskas för alla kommunikationsnät och -tjänster men avsikten är att speciellt beakta nya arkitekturlösningar inom 5G-teknologin, nya användningsfall för mobilnät samt informationssäkerhetskrav som hänför sig till dem. För mobilnät och -tjänster kan det finnas eventuella preciseringsbehov på grund av den senaste utvecklingen som innebär bland annat tillträde till nya gränssnitt, virtualisering, användning av molntjänster samt att nätet och utrustningsutrymmena blivit allt mångformigare. I projektet beaktas även respons från intressentgrupper samt andra erfarenheter av uppdateringsbehov som man fått inom tillsyns- och inspektionsverksamheten.

Föreskriften gäller allmän televerksamhet och syftet med det är att:

- 1) främja informationssäkerheten i allmänna kommunikationsnät och kommunikationstjänster,
- 2) trygga den elektroniska kommunikationens konfidentialitet och värna om integritetsskyddet, och
- 3) säkerställa att informationssäkerheten genomförs i teleföretagen på ett övergripande, systematiskt och effektivt sätt.

### Målsättning

Målet med enkäten är att samla erfarenheter och utvecklingsidéer om den nuvarande versionen av föreskriften samt be om synpunkter på vissa nya punkter vars nödvändighet och innehåll man speciellt kommer att bedöma i samband med uppdateringen av föreskriften.

### Länkar

Föreskrift om televerksamhetens informationssäkerhet (Kommunikationsverket 67 A/2015 M): [https://www.finlex.fi/data/normit/44046/M67A\\_2015\\_SV.pdf](https://www.finlex.fi/data/normit/44046/M67A_2015_SV.pdf)

Motivering till och tillämpning av föreskrift 67:  
[https://www.finlex.fi/data/normit/44046/M67A\\_MPS\\_2015\\_SV.pdf](https://www.finlex.fi/data/normit/44046/M67A_MPS_2015_SV.pdf)

Information om informationssäkerheten i tjänster som genomförts i utlandet:  
[Suositus 205 2014 S SV.pdf](https://www.finlex.fi/data/normit/205_2014_S_SV.pdf)

Informationssäkerhetsbaserad filtrering av trafik till vissa kommunikationsportar i teleföretagens nät (Transport- och kommunikationsverkets rekommendation 312/2020 S): [Suositus3122020\\_SV.pdf \(traficom.fi\)](#)

## Tidtabell

Vänligen sänd svaren till Transport- och kommunikationsverket via [utlåtande.fi](#) **senast den 31 augusti 2022**.

## Svarsanvisningar

Enkäten följer huvudsakligen strukturen i den gällande föreskriften. I svaren kan man framföra utvecklings- eller ändringsbehov i anknytning till föreskriften både allmänt och för enskilda skyldigheter. Enkäten innehåller flera mer specifika frågor om behoven av utveckling av vissa punkter i föreskriften. För flera punkter i föreskriften efterfrågas synpunkter på eventuella utvecklingsbehov, men man önskar erfarenheter och nya utvecklingsidéer av de som svarar även för övriga punkter.

Vi önskar svar både allmänt om olika kommunikationsnät eller -tjänster och mer specifikt om speciella särdrag för vissa tjänster eller nätteknologier (såsom internetförbindelsetjänster eller 5G-mobilnät).

Transport- och kommunikationsverket ger er möjlighet att ge ett utlåtande i frågan antingen på finska eller på svenska. Ni kan även ge utlåtandet på engelska om ni vill.

Ge utlåtandet genom att svara på begäran om utlåtande som publicerats på [utlåtande.fi](#). Utlåtandet behöver inte skickas separat per e-post eller post till Traficoms registratorskontor.

För att kunna lämna sitt utlåtande ska svarpersonen registrera sig och logga in på [utlåtande.fi](#). Närmare anvisningar för att använda tjänsten finns på [utlåtande.fi](#) under Anvisningar > Bruksanvisning. Om ni behöver stöd för användningen kontakta [lausuntopalvelu.om@gov.fi](mailto:lausuntopalvelu.om@gov.fi).

Alla utlåtanden är offentliga och de publiceras på [utlåtande.fi](#). Om svaret innehåller uppgifter som företaget anser vara affärshemligheter eller annars sekretessbelagda ska sådana uppgifter lämnas in på en separat handling via säker e-post till Transport- och kommunikationsverkets registratorskontor på adressen [registrator@traficom.fi](mailto:registrator@traficom.fi). Förse svaret med diarienumret Traficom/16241/09.09/2022. Anvisningar för att skicka säker e-post finns på: <https://www.traficom.fi/sv/traficom/kontaktuppgifter/att-skicka-saker-e-post-till-traficom>

## Beredare

Ytterligare information ger:

Esa Fredriksson, specialsakkunnig, tfn 029 539 0330  
Marko Priiki, jurist, tfn 029 539 0596.

Transport- och kommunikationsverkets e-postadresser har formen  
[fornamn.efternamn@traficom.fi](mailto:fornamn.efternamn@traficom.fi)

## Begäran om utlåtande

### Allmänna bestämmelser (1 kap.)

#### Tillämpningsområde (2 §)

Borde kraven ställas på olika nivåer för (olika) teleföretag? Om svaret är ja, hur anser ni att indelningen borde genomföras?

#### Definitioner (3 §)

Har definitionerna varit tillräckligt täckande och fungerande?

### Allmänna krav för alla nät och tjänster (2 kap.)

#### Hänsynstagande till informationssäkerheten (4 §)

Anser ni att kraven är på en för allmän nivå? Om de är det, till vilka delar anser ni att de borde preciseras?

Skydd av trafik i nätet och av gränssnitt (anser ni att det är nödvändigt att förutsätta av teleföretag att skydda signalerings- och användartrafik genom att kryptera trafiken alltid när det tekniskt är möjligt?)

Genomförande av infrastrukturen för mobilnät i molntjänster (till exempel hur borde olika molntjänstlösningar beaktas i föreskriften?)

Beaktande av säkerheten hos underleverantörer (leveranskedjor, program, stödtjänster.)

Virtualisering av nätet (Trust domains, VNF åtskiljning, minimering av attackvektorer, nätadministration av virtualiseringsmiljö, HMEE, autentisering av pålitligheten för en plattform.)

Utökande och precisering av åtkomsthanteringskyldigheter (utökande av rättigheter för program/anordningar [SBA-säkerhet], automatisk nyckelhantering).

Lagring och skyddande av olika loggar.

Hur borde man i föreskriften beakta skyddande av edge computing-enheter?

Behörighetsregister: Utökande och precisering av upprätthållandet och dokumenteringsskyldigheten för behörigheter (som inkluderar sektorer [personer] som förutom teleföretaget har rätt att använda anordningar eller program som systemadministratör).

#### Riskhantering (5 §)

Borde uppföljningscykler för riskhantering helt eller delvis bestämmas till exempel för kritiska funktioner/system? (I nuläget kan ett teleföretag själv bestämma lämpliga uppföljningscykler.)

Borde man förutsätta dokumentering av riskhanteringsresultaten för flera behandlingsomgångar? (I nuläget krävs endast att den senaste behandlingsomgången dokumenteras.)

## Datamaterial (6 §)

Är kraven som gäller klassificeringssystem för datamaterial och hanteringsförfarandet uppdaterade? Medför till exempel molnlösningar nya utmaningar?

Anser ni att det är tydligt vilka datamaterial skyldigheten gäller?

## Trafik mellan hanteringsnät och hanteringsförbindelser (8 §)

Vilka behov anser ni förbättrar säkerhetskraven för trafiken i hanteringsnät och hanteringsförbindelser?

Anser ni att rekommendationen som gäller loggningen av inställningsändringar borde ändras och vara förpliktande? Borde lagringstiden enligt rekommendationen eller skyldigheten förlängas till exempel till ett år?

Borde rekommendationen som gäller åtskiljande av hanteringsnät eller trafik i arbetsstationer som används för näthantering ändras till förpliktande? Om ni svarade ja, vad borde skyldigheterna förutsätta?

Borde man i fortsättningen kräva centraliserad logghantering? Om ni svarade ja, för vilka funktioner?

Borde det i fortsättningen krävas upprättande och upprätthållande av logghanteringspolicy?

Anser ni att loggarnas precisionsnivå borde bestämmas?

## Särskilda krav för gränssnitt (3 kap.)

Borde man förutsätta skyddande av signalgränssnitt av teleföretagen (till exempel SS7, Diameter & HTTP/2)? Om ni svarade ja, vilka åtgärder borde man förutsätta?

## Hindrande av IP-trafik i samtrafikgränssnitt (11 §)

Borde kravet preciseras till exempel med gränsroutrar (BGP) för krav som gäller skyddande av sessioner, förpliktande att ta i bruk RPKI eller filtreringsskyldighet vad beträffar för noggranna ruttannonseringar, förfalskade ruttannonseringar och reserveringar av adressrymder för särskild användning?

## Särskilda krav för internetaccess tjänster (4 kap.)

### Åtskiljande av trafik i internetaccess tjänster (13 §)

Motsvarar motiveringarna av kravet nuläget? Finns det nya metoder för att åtskilja trafik? Anser ni att skyldigheten borde utvidgas så att den är oberoende av tjänsten?

Nätverksskivning (till exempel åtskiljning av skivor, åtkomsthantering av vertikaler.) Hur anser ni att man borde beakta skivningens säkerhetsfrågor i föreskriften?

## Dirigering av e-posttrafik från konsumentabonnemang (14 §)

Anser ni att det även i fortsättningen är nödvändigt att begränsa SMTP-trafiken på det sätt som beskrivs i föreskriften? (motivera er synpunkt)

Om inte, hur anser ni att begränsningen borde ändras? Borde begränsningen tas bort helt eller delvis?

Anser ni det vara motiverat att utveckla föreskriften så att teleföretag borde ta bort begränsningen från abonnemanget på begäran av konsumenten?

Anser ni det vara motiverat att utvidga begränsningen i föreskriften även till andra än konsumentabonnemang?

## Allmän skyldighet att filtrera skadlig trafik (15 §)

Anser ni att skyldigheten borde utvidgas så att den är oberoende av tjänsten eller utvidgas även till andra tjänster (såsom SMS/MMS)?

Anser ni det nödvändigt att precisera skyldigheten om avvärjning av överbelastningsangrepp? Vad anser ni skyldigheten för skyddande av kommunikationsnät mot överbelastningsangrepp ska innehålla? (observation och avvärjning av nätet internt och externt)

Anser ni att portfiltreringen är den rätta i nuläget? Borde några av filtreringarna i rekommendationen finnas i föreskriften? Motivera er synpunkt. (Se även rekommendation 312/2020 S.)

Hur anser ni att filtreringsskyldigheten borde utvecklas för att bättre motsvara nuvarande utmaningar i synnerhet för krypterad trafik? (DNS over HTTPS med mera)

Ökande av skyldigheten av filtreringsförmågan för SMS/MMS?

## Bortkoppling av internetaccess-tjänster (16 §)

Motsvarar motiveringarna av kravet nuläget?

Borde man ge närmare bestämmelser om lindrigare åtgärder än bortkoppling än i nuläget?

Borde man i skyldigheten (bortkoppling och lindrigare åtgärder än det) beakta situationer där skadlig trafik inte ännu har observerats, men utnyttjande är möjligt på grund av en sårbarhet i en apparat eller ett program som anslutits till ett kundabonnemang?

## Särskilda krav för e-posttjänster (5 kap.)

Den nuvarande föreskriften innehåller knappt några krav gällande allmän datasäkerhet för e-posttjänster eller förbättrande av pålitlighet och integritet för förmedling av e-post. Åtgärder har emellertid presenterats i föreskriftens motiveringspromemoria.

Vad anser ni om att några av dessa krav borde inkluderas i den nya versionen av föreskriften, till exempel genom att förplikta användning av protokoll, metoder eller standarder som förbättrar säkerheten såsom DMARC, DKIM, SPF, DANE eller MTA-STS?

## **Särskild skyldighet att filtrera e-posttjänster (18 §)**

Har det uppstått speciella utmaningar av filtreringsåtgärderna?

I föreskriftens motiveringspromemoria har det ingående presenterats olika metoder för att genomföra e-postfiltrering, fattas det något?

## **Information till kunderna (6 kap.)**

### **Allmän skyldighet att ge information om åtgärder som ska vidtas i fråga om informationssäkerheten (21 §)**

Anser ni att det behövs en uppdatering av Kommunikationsverkets rekommendation Information om informationssäkerheten i tjänster som genomförs i utlandet? (205/2014 S).

## **Ert allmänna utlåtande om föreskriften**

Här kan ni ge eventuella kommentarer om föreskriften eller tillämpningen av den.