



Forsvarsdepartementet  
Postboks 8126 Dep.  
0032 OSLO

Vår ref.:  
0905764-3 - 008

Vår dato:  
4.12.2009

FORSVARSDPARTEMENTET	
SAKNR. 07/ 00915 - 62	
08 DES 2009	
353 - spmp	
ARKBET:	Ugradert
KASSERES 5 ÅR	
KASSERES 30 ÅR	
BEVARES	

Dykkar ref.:  
2007/00915-51/FD I 4/BOE

Dykkar dato:  
14.10.2009

Saksbehandlar:  
Alexander Iversen

www.npt.no

## Høyringsssvar - forskrift om objektsikkerheit

Post- og teletilsynet (PT) viser til brev datert 14. oktober 2009 der Forsvarsdepartementet ber om merknadar til forslag til forskrift om objektsikkerheit (objektsikkerheitsforskrifta) og forslag til forskrift om endringar i forskrift om sikkerheitsadministrasjon.

PT ser positivt på at objektsikkerheitsforskrifta kjem på plass og gir tilslutnad til forskriftsutkastet, med dei merknadane som er gitt i dette brevet og under føresetnad at utkastet blir gjenstand for ein forskriftsteknisk gjennomgang.

I tillegg til tilsynet sine eigne merknadar så er aktørane som er underlagt sikkerheitslova innanfor post- og telesektoren gitt høve til å komme med innspel. PT har motteke skriftlege innspel frå Ventelo Networks AS (tidlegare BaneTele AS) og Telenor ASA, som er vedlagt dette brevet. Posten Norge AS hadde ingen merknadar.

### Merknad om klagegang

Høyringsbrevet ber om høyringsinstansane sitt syn på at det ikkje leggst opp til å gi tilgang til å klage på vedtak om klassifisering av skjermingsverdige objekt. Då vedtak etter sikkerheitslova vil kunne omfatte private rettssubjekt, følgjer det av forvaltingslova at desse vil kunne påklage eit slikt vedtak. I og med at slike vedtak fattast av departementet, vil klageorganet for private rettssubjekt vere Kongen i Statsråd. I kva grad dette er ei hensiktsmessig klageordning kan PT ikkje vurdere.

### Merknad til § 2-2 (klassifisering)

I § 2-2 tredje ledd står det at objekteigar skal ta omsyn til objektet si betydning for andre objekt. I høyringsbrevets merknad til § 2-2 tredje ledd står det derimot at «*gjensidig avhengighet til andre objekter eller andre virksomheter også må vurderes ved fastsetting av klasse.*». Denne merknaden legg til grunn andre premisser enn forskriftsteksta, slik som *gjensidig avhenge og andre virksomheter.*

PT føreset at ein ved klassifisering berre kan ta omsyn til objektet si betydning for andre objekt som det er gitt melding om, jf. referansen i § 2-1 femte ledd. Dette kan med fordel konkretiserast i forskriftsteksta, slik at § 2-2 tredje ledd vil lyde (endringar er understreka):

«*Ved klassifisering skal det tas hensyn til objektets betydning for andre objekter, jf. § 2-1 femte ledd.*»

I tillegg vil PT presisere at ved avhenge til andre sin IKT-infrastruktur så vil ein stort sett ha kjennskap til kva IKT-tenester ein er avhengig av, og ikkje objekt. Det er då tenestetilbydaren som best kan vurdere kva objekt som er kritiske for å levere desse tenestene.

#### **Merknad til § 3-1 (generelle krav til trygging)**

Når det gjeld eit skjermingsverdig objekt si avhenge til andre objekt bør det vere eit uttrykt mål at objekteigar søker å redusere slik avhenge som ledd i å trygge sitt objekt. I forhold til avhenge til IKT-infrastruktur vil dette vere tiltak som å etablere barrierar eller redundans. PT føreslår at redundans innarbeidast som eit muleg tryggingstiltak i § 3-1. Slik vil ein òg kunne unngå tilfeller der ein objekteigar som er avhengig av eit anna objekt i prinsippet kan skyve kostnader for tryggingstiltak over på den andre objekteigaren.

#### **Merknad til § 3-3 (tilrettelegging for trygging av IKT-infrastruktur)**

I § 3-3 er det lagt opp til tryggingstiltak mot logiske angrep via Internett. PT meiner at IKT-infrastruktur må fortolkast som meir enn Internett, og at trugsmål mot IKT-infrastrukturen kan omfatte meir enn logiske angrep. PT har i dag varslingsrutinar for fysiske hendingar som medfører utfall av elektronisk kommunikasjon (ekom). Dette varslingsystemet omfattar kritisk ekominfrastruktur.

PT meiner at § 3-3 ikkje bør vere avgrensa til berre å gjelde logiske angrep på Internett, men skildre varslingsystemet på ein meir generalisert måte som inkluderer både logiske og fysiske angrep.

#### **Merknad til § 3-4 (Tiltak mot EMP og HPM)**

I høyringsbrevets merknad til § 3-4 er plikta til å vurdere trugselnivå for EMP/HPM lagt til objekteigar. Etter det PT kjenner til er Politiets tryggingsteneste det organet som har kompetanse til å vurdere trugselnivå, ikkje objekteigar eller sektormyndigheit. Vidare bør Nasjonalt tryggingorgan (NSM) bidra til ei overordna, sektorovergripande risikovurdering for å harmonisere vurderingane i den einskilde sektor.

Der ei overordna risikovurdering ligg til grunn ser PT det som fornuftig at den enkelte objekteigar/sektormyndigheit vurderer kva som kan akseptast av EMP/HPM-risiko, slik det er foreslått i høyringsbrevet.

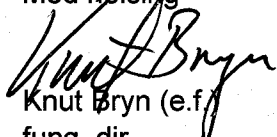
#### **Merknad til § 4-1 (iverksetting av tiltak - kostnader og dispensasjon)**

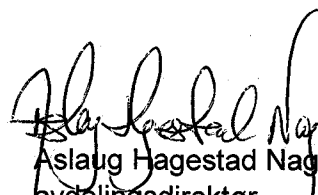
I § 4-1 er det lagt opp til at den einskilde verksemd skal dekkje utgiftene ved eventuelle tiltak. I lov om elektronisk kommunikasjon (ekomlova) § 2-10 fjerde ledd er derimot staten pålagt å kompensere meirkostnader for trygging- og beredskapstiltak hos ekomtilbydarar, det vil seie kostnader som går utover rein kommersiell tilpassing:

*Tilbyder skal i utgangspunktet dekke kostnader ved sikkerhets- og beredskapstiltak [...]. Tilbyderes reelle merkostnader forbundet med levering av sikkerhets- og beredskapstiltak, skal kompenseres av staten [...]. Med merkostnad menes kostnad som vil falle bort uten pålegget, utover kostnaden ved en ren kommersiell tilpassing.*

For objekteigarar som er underlagt sikkerhetslova og ekomlova vil difor desse to føresegnene kunne virke mostridande. PT gir likevel sin tilslutnad til at objekteigar sjølv dekkjer kostnader som følgje av krav heimla i objektsikkerhetsforskrifta. Ekomlova § 2-10, som er meint å supplere sikkerhetslova jf. Ot.prp. nr. 58 (2002-2003), vil parallelt kunne heimle andre krav om sikkerheits- og beredskapstiltak som faller under, og eventuelt ved sida av, objektsikkerhetsforskrifta.

Med helsing

  
Knut Bryn (e.f.)  
fung. dir.

  
Aslaug Hagestad Nag  
avdelingsdirektør

**Fra:** Svartvadet Jan Olav [jan.olav.svartvadet@ventelo.no]  
**Sendt:** 27. november 2009 13:27  
**Til:** Iversen, Alexander  
**Kopi:** Olsen Per Magne  
**Emne:** FORSKRIFT OM OBJEKTSIKKERHEIT - INNSPEL TIL HØYRING

**Kategorier:** Rød kategori

**DocumentIsArchived:** 0

Ref. PTs brev 0905764-2-008 av 031109.

Ventelo Networks AS (VN) har gått gjennom tilsendt dokumentasjon ift. vårt eierskap av kritisk infrastruktur og mtp. at Forskrift om objektsikkerhet med stor sannsynlighet vil påvirke og stille krav til oss. Vi har ikke sett forhold eller momenter som krever forslag til radikal endring, men kan oppsummere høringen i følgende punkter:

- det henvises til Sikkerhetsloven §17 for den pålagte klassifiseringen. Tross gitte kriterier finner vi fortsatt rom for subjektive oppfatninger og vurderinger av hva som er skjermingsverdig og vi vil be om at f.eks. PT for telesektoren gjør en utdypning av disse utvelgelseskriteriene.
- vi finner det sannsynlig at pålagt objektsikring kan medføre større økonomiske belastninger enn det vi som operatør ville gjennomført i ren kommersiell interesse og vi påpeker at dette derfor bør omfatte støtteordninger og tildelinger, på linje med Spesielle samfunnsplagte oppgaver (SSO).
- forslaget til ny forskrift omtaler hvilke informasjonssystemer, herunder kryptosystemer, som skal håndtere sikkerhetsgradert informasjon. Ventelo Networks AS er en videreføring av BaneTele AS og vi betegner oss fortsatt som underlagt Sikkerhetsloven, men har aldri praktisert sivilt beredskapssystem med anskaffelse av krypterte kommunikasjonsmidler.

Med vennlig hilsen

**Jan Olav Svartvadet**  
*Sikkerhetssjef*

**Mobil:** 90 75 76 15  
**Sentralbord:** 21 55 00 00  
**E-post:** jan.olav.svartvadet@ventelo.no  
**Web:** www.ventelo.no



**Ventelo**

Rolfsbuktveien 4, Postboks 1, 1330 Fornebu

**Ventelo har som mål å gi den beste kundeopplevelsen.**

Du kan forvente at jeg:

*Følger deg i mål - Gjør det enkelt - Tar ansvar - Viser respekt - Tør å tenke nytt*

Post- og teletilsynet  
Postboks 93  
4791, Lillesand

Att.: Aslaug Hagestad Nag

Vår dato  
30.11.2009

Vår referanse  
GR.050.3/11/09/TD

Deres dato  
03.11.2009

Deres referanse  
0905764-2 - 008

Vår saksbehandler  
T.Danielsen, tlf.: 992 48 058/678 92 721

## FORSKRIFT OM OBJEKTSIKKERHET INNSPILL TIL HØRING

Vi viser til Post- og teletilsynets brev datert 3. november 2009, der Telenor blir invitert til å gi innspill til Forsvarsdepartementets høring om ny Forskrift om Objektsikkerhet. I det følgende er Telenors kommentarer til forslaget.

### Generelt om endringene i Sikkerhetsloven og forskriftsutkastet

Forsvarsdepartementet valgte ikke å sende høringsbrevet til samme adressater som ved høringen i 2003, med begrunnelse om at forslaget om å utvide sikkerhetslovens virkeområde til også å omfatte privat virksomhet ikke ble fulgt opp ved lovendringen vedtatt i mars 2008. Når forslaget til Objektsikkerhetsforskriften vurderes er det viktig å ta hensyn til at det allerede er private virksomheter, som med bakgrunn i viktige samfunnsfunksjoner, er underlagt Sikkerhetsloven.

Den allerede vedtatte endringen i Sikkerhetslovens § 17, som ennå ikke er iverksatt, slår fast at det ved utvelgelse skal tas objektets betydning for kritisk funksjoner for det sivile samfunn, akseptabel tidsperiode for funksjonssvikt og betydning for andre objekter. Dette vil i stor grad være tilfelle for elektronisk kommunikasjon. Kartlegging av disse punktene vil kreve et betydelig kartleggingsarbeid og samarbeid mellom forskjellige sektorer. Det stiller krav til gode retningslinjer fra de sektoransvarlige myndigheter.

Vi vil også vise til §§ 17 a og b, som omtaler klassifisering og plikt til å beskytte skjermingsverdige objekter. Hvis Telenors objekter klassifiseres etter disse paragrafene vil det kreves utvidede sikkerhetstiltak og økt behov for samarbeid og koordinering med myndighetene. Ressursbehov vil i forbindelse med implementering av disse kravene være stor, spesielt med tanke på fristen som er satt til to år.

Høringsbrevet inviterer til å kommentere det faktum at det ikke er tatt med noen bestemmelse om klageadgang. Utpeking av objekter kan føre til restriksjoner for kommersiell bruk for objekteier. Dette kan i sin tur medføre økonomiske kostnader og tap. Det bør derfor være mulig å klage på vedtak når dette vil få urimelige følger for objekteier.

Det sies i høringsbrevet at antallet klassifiserte objekter skal holdes lavt. For ekomsektoren vil dette ikke uten videre være tilfelle, da både avhengigheten for brukerne og infrastrukturens oppbygging kan medføre at lokale objekter kan være av vital betydning for systemets totale funksjonsevne.

Viktigheten av klare retningslinjer fra sektoransvarlig departement vil derfor være viktig før arbeidet med utpeking av objekter iverksettes. Retningslinjene må i tillegg til å gi prinsipper for utvelgelse også gi føringer for kostnadsdekning slik at eiere av egen infrastruktur ikke blir pålagt kostnader som vil være konkurransevridende.

Høringsbrevet fastslår at den enkelte virksomhet skal dekke utgiftene ved tiltak etter de omtalte lov- og forskriftsendringene. Dette er ikke i samsvar med Ekomlovens § 2-10, som fastslår at for å oppfylle nasjonale behov for kommunikasjonssikkerhet skal reelle merkostnader for sikringstiltak utover rent kommersielle, dekkes av staten. Telenor forutsetter at dette vil være tilfelle for å oppfylle eventuelle krav som følger av Objektsikkerhetsforskriften.

### **Merknader til de enkelte bestemmelsene**

#### **Til § 2**

Telenor har en rekke objekter som inneholder deler av infrastruktur som må være operativ for å opprettholde leveranser både lokalt og over større områder. Arbeidet med å dokumentere skadevurdering kan derfor bli ganske omfattende. Før dette arbeidet iverksettes må det derfor utarbeides underlag og retningslinjer fra sektoransvarlig myndighet.

Av merknadene til de enkelte bestemmelsene tolker vi det slik at også logiske systemer og tilknytning til den samfunnskritiske funksjonen kan være grunnlag for klassifisering. Vi er av den oppfatning at logisk tilgang til systemer, selv om disse ikke er graderte, vil kunne utsette våre systemer for sabotasje av like stor alvorlighet som fysisk tilgang til objektene. Dette fremgår ikke tydelig av forskriftsutkastet, men vi forventer at dette blir adressert i de sektorvise retningslinjene for klassifisering av objekter.

Forskriftens tekst legger ikke begrensninger med hensyn til avhengighet overfor andre objekter. Merknadene til det samme punktet fastslår at man snakker om eksterne objekteiere. Leverandører av elektrisk kraft er eksempler på objekteiere som Ekomtilbyderne er avhengige av for å levere sine tjenester. Her vil det også kunne være snakk om gjensidig avhengighet. Det vil kreve utstrakt koordinering mellom forskjellige objekteiere før det er mulig å fastslå behovet for å klassifisere et objekt.

Endringer i nettstruktur kan endre avhengigheten mellom objekter. Større grad av redundans vil kunne medføre reduserte skadefølger for de avhengige objektene og dermed behov for reklassifisering, igjen med koordinering med andre objekteiere.

Det er viktig ikke å undervurdere behovet for ressurser til å gjennomføre dette arbeidet.

Forslaget om å klassifisere bare skjermingsverdige deler av et objekt vil være vanskelig, da det er totaliteten av anleggene som gjør det i stand til å levere tjenester. Dagens sikring er også basert på at hele anlegget skal beskyttes og kravene for selvstendig adgang til anlegg krever samme klarering og autorisasjon som adgang til enkelte deler av anleggene.

Vi vil igjen understreke viktigheten av klare føringer før arbeidet iverksettes.

#### **Til § 3**

Sektormyndighetene må gi nærmere retningslinjer for hvilke sikkerhetstiltak som skal iverksettes. Det blir viktig at spesielt risikovurderinger ivaretas gjennom systemer som er felles for alle innen samme sektor. Alternativt må det tydeliggjøres hvilke faktorer som skal legges til grunn for vurderingene.

Objekteiere er avhengig av informasjon om hvilke risikoelementer som skal legges til grunn for vurdering og valg av EMP-beskyttende tiltak. Myndighetene må gi nærmere retningslinjer om risiko og trussel, og hvilke sikringsnivåer og tekniske løsninger som da skal benyttes. EMP-/HPM-tiltak må bygges inn ved valg av byggteknisk konstruksjon eller som del av grunnlagsspesifikasjonen for teknisk utstyr. Det er derfor viktig å få på plass kravene raskt slik at det ikke kreves ekstra kostnader for å oppnå beskyttelseskravene i ettertid.

Kravet til å tilrettelegge for sikringsstyrker er helt nødvendig for at private virksomheter skal oppnå kravene som er gitt i Sikkerhetslovens § 17, b. Dette vil medføre kostnader til organisering, bygningsmessige tiltak og rutinemessig øvelser som forutsettes dekket etter Ekomloven.

Til § 4.

Implementering av sikringstiltak i Telenors anlegg skjer på grunnlag av kommersielle behov. Tiltak utover kommersielle behov forventes dekket av myndighetene. § 4-1 bør derfor ha en referanse til at kostnader kan dekkes i henhold til sektorvise lover og forskrifter.

Til § 5.

Etter at forskriften er godkjent, må den enkelte sektor utarbeide retningslinjer/bestemmelser for hvordan sektoren skal praktisere regelverket. Fristene som er satt må i første omgang rettes mot de sektoransvarlige for etablering av utdypende retningslinjer og regelverk. Når det er på plass, kan frister overfor objekteier defineres.

Eventuelle fysiske tiltak vil måtte planlegges og gjennomføres i de årlige budsjettprosesser eventuelt fordelt over flere år. Dette vil kunne medføre problemer med å nå de tidsfrister som er satt i § 5-2. Administrative tiltak kan iverksettes så snart utfyllende retningslinjer er på plass.

### **Merknader til endringer i forskrift om sikkerhetsadministrasjon**

Til § 2-6, tredje ledd.

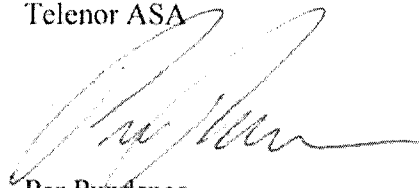
Avhengigheten fysiske objekter i ekomsektoren har til informasjonssystemer for drift og overvåkning vil være vital selv om informasjonssystemet ikke er gradert. En sikkerhetsgradering av tilbydernes interne nett vil kunne medføre store kostnader til sikring og begrense mulighetene til effektiv drift. Viktigheten av slike systemer kan ikke overses men det må etableres en tilnærming slik at dette håndteres på både en sikkerhetsmessig og kostnadmessig god måte. Hvordan dette skal ivaretas må avtales mellom objekteier og sektoransvarlige myndigheter.

### **Konklusjon**

Telenor ser positivt på at Objektsikkerhetsforskriften kommer på plass. Det er nødvendig for å få en felles tilnærming for beskyttelse av kritisk infrastruktur. Det er viktig at sektoransvarlige myndigheter kommer med retningslinjer og krav til de tiltak som skal gjennomføres innen egen sektor.

Det forventes av innføring av nye sikkerhetstiltak for å oppfylle denne forskriften gjøres etter Ekomlovens § 2-10, som definerer at kostnader til denne type tiltak skal dekkes av myndighetene. Frist for iverksettelse av objekteiers sikringstiltak må tilpasses sektoransvarlige myndigheters utarbeidelse av definerte retningslinjer.

Med hilsen  
Telenor ASA



Per Pundsnes  
Vice president  
Group Risk