



Forsvarsdepartementet
Postboks 8126 Dep
0032 OSLO

VÅR REFERANSE
17/353

DERES REFERANSE
2015/3139-254/FD V
3/ENWA

DATO
27.09.2018

Forskrifter til ny sikkerhetslov - høringsuttalelse

1. Innledning

Det vises til Forsvarsdepartementets høringsbrev av 2. juli 2018 vedrørende forslag til forskrifter til ny sikkerhetslov. Forskriftene omhandler myndighetenes roller og ansvar for nasjonal sikkerhet (myndighetsforskriften), klarering av leverandører og personell (klareringsforskriften) og virksomhetens arbeid med forebyggende sikkerhet (virksomhetsforskriften).

Finanstilsynet gir i punkt 2 noen generelle merknader til forskriftsforslaget. I punkt 3 gis det nærmere merknader til bestemmelser i de tre forskriftene som kan medføre konsekvenser for Finanstilsynet og foretak i finanssektoren. Merknadene er tematisk organisert under de foreslåtte forskriftene, men kan også ha betydning for bestemmelser i de to andre forskriftene.

2. Generelle merknader

Forsvarsdepartementet har sendt på høring tre forskrifter til sikkerhetsloven. Det fremgår av høringsnotatet at departementet fortsatt vurderer om andre alternativer er mer hensiktsmessig og ber om tilbakemelding på dette fra høringsinstansene.

Etter Finanstilsynets vurdering er det utfordrende å finne frem i forskriftene. Det forhold at samme tema i flere tilfeller omhandles i flere forskrifter, gjør det utfordrende å få oversikt. Det er også til dels vanskelig å skjønne hvilken bestemmelse i sikkerhetsloven forskriftene refererer til. Det er mulig at en tematisk samling hadde vært enklere hvis alt ble samlet i én forskrift med gode henvisninger til sikkerhetsloven. Gode veiledninger med oversiktlige henvisninger mellom de forskjellige lovbestemmelsene og forskriftsbestemmelsene er også er mulighet.

Etter Finanstilsynets vurdering bør sektoransvarsprinsippet følges ved at ansvaret for forebyggende sikkerhet i sektoren tillegges det enkelte fagdepartement med underliggende sektormyndighet, jf. tilsynets høringsuttalelse til sikkerhetsloven. Den vedtatte sikkerhetsloven synes å gi bedre balanse mellom det overnasjonale, sikkerhetsmyndigheten og sektormyndighetene enn det som lå i det opprinnelige forslaget. Finanstilsynet vil understreke viktigheten av at sektoransvarsprinsippet også gjenspeiles i de underliggende forskriftene.

Det fremgår av sikkerhetslovens §1-3 at et departement, innenfor sitt ansvarsområde, kan fatte vedtak om at loven helt eller delvis skal gjelde. Det er Finanstilsynets forståelse at departementet også kan bestemme hvilke forskriftsbestemmelser som er relevante.

Finanstilsynet stiller seg positiv til at Nasjonal sikkerhetsmyndighet, som fagressurs, stiller til rådighet kompetanse som sektormyndighetene og foretakene kan trekke på ved behov.

3. Merknader til de enkelte forskriftsforslagene

3.1 Myndighetsforskriften

Myndighetsforskriften retter seg mot departementer, Nasjonal sikkerhetsmyndighet (NSM) og myndigheter med tilsynsansvar etter loven, og regulerer de overordnede roller, ansvar og oppgaver etter sikkerhetsloven. Finanstilsynet har ikke tilsynsansvar direkte etter sikkerhetsloven, men kan bli gitt et slik tilsynsansvar av Finansdepartementet.

Iverksettelse av inntrengningstesting, kommunikasjons- og innholdskontroll og testing av sikkerhetstiltak

Myndighetsforskriften § 3 har bestemmelser om at NSM kan iverksette ulike typer av testing, slik som inntrengningstesting, kommunikasjons- og innholdskontroll og testing av sikkerhetstiltak. Dette kan skje når virksomhetens ledelse i et foretak som har et skjermingsverdig objekt, ber om det. Bestemmelsen kan ha betydning for foretak under tilsyn. Etter Finanstilsynets mening bør det innføres et krav om at myndigheter med sektoransvar varsles i rimelig tid før iverksettelse av slike tester, slik at sektormyndighetene er informert dersom det skulle oppstå en hendelse med bakgrunn i testingen.

NSM kan også iverksette tekniske undersøkelser. PST skal varsles om slike undersøkelser. Finanstilsynet mener at myndigheter med sektoransvar også her bør varsles om omfang, innhold og eventuell risiko med samme begrunnelse som ved testing.

Finanstilsynet mener at krav om varsel til sektormyndighet bør fremgå av forskriften.

Eierkontroll

Forskriften § 20 inneholder en bestemmelse om hvilke opplysninger en melding om erverv av kvalifiserte eierandeler i foretak som er underlagt sikkerhetsloven, skal inneholde. Dette er opplysninger om erververs styre, daglig ledelse, eierstruktur, kapitalforhold, konsolidering m.m. Forsvarsdepartementet har bedt høringsinstansene om innspill til utformingen av bestemmelsen og om det er behov for ytterligere bestemmelser om eierskapskontroll.

Bestemmelsen krever i all hovedsak samme type informasjon som ved erverv av kvalifiserte eierandeler i finansforetak mv. Finanstilsynet har derfor ingen merknader til utformingen, og mener at det heller ikke er behov for ytterligere regulering av kvalifisert eierskap siden eierskapet skal godkjennes både etter sikkerhetsloven og finanslovgivningen.

3.2 Klareringsforskriften

Klarering av personell

Det er foreslått en bestemmelse i klareringsforskriftens § 4 om at det bare er virksomhetens autorisasjonsansvarlige som kan be klareringsmyndigheter om klarering av personell. Det fremgår av kommentaren til bestemmelsen at dette kan delegeres ved behov. Der hvor personell skal klareres som en del av leverandørklaringsprosessen, er det fastsatt at det er oppdragsgiver som skal be klareringsmyndigheten om klarering. Finanstilsynet forstår forslaget slik at autorisasjonsansvarlige i et direktorat kan be om sikkerhetsklarering også av samarbeidspartnere som ikke er ansatt i virksomheten. For eksempel kan Finanstilsynet i dag be om klarering av ansatte i foretak under tilsyn. Finanstilsynet mener at delegeringsadgangen bør tydeliggjøres i forskriften.

Tilbakekall av leverandørklarering

Klareringsforskriften § 34 åpner for at en klarering kan kalles tilbake dersom det oppdages avvik fra sikkerhetskravene etter at klareringen er gitt. Klareringsmyndighetene kan fastsette en rimelig frist for retting av avvikene. Bestemmelsen er en videreføring av gjeldende regelverk.

Tilbakekall av klarering kan ha store konsekvenser for foretak under tilsyn som har leveranser utført av en leverandør som omfattes av sikkerhetsloven. Et eksempel på dette kan være hvis en bank blir pålagt å flytte sine driftstjenester fra en etablert driftsleverandør som opererer fra India. Dette vil være en krevende og kostbar prosess. Det vil også kunne utgjøre en risiko for ustabilitet i tjenester for grunnleggende nasjonal funksjonalitet.

Finanstilsynet mener det vil være viktig at foretak med tjenester underlagt sikkerhetsloven blir informert av klareringsmyndigheten tidligst mulig om et eventuelt tilbakekall, slik at foretaket kan iverksette sin avviklings plan og finne alternative løsninger før tilbakekall inntreffer. Det er også viktig at sektormyndigheten blir informert. Et tilbakekallsvedtak bør ikke treffes før konsekvensene er utredet i samråd med berørte sektormyndigheter og foretak. Dette bør fremgå av forskriften.

3.3 Virksomhetsforskriften

Virksomhetens ledelse

Forskriften stiller flere krav til "virksomhetens leder" for arbeidet med sikkerhetsstyring, blant annet til fastsettelsen av styringsdokumenter. Forsvarsdepartementet understreker i høringsnotatet at bruken av begrepet "virksomhetens leder" ikke er ment å gjøre inngrep i ansvarsforholdene som følge av selskapsretten eller annen organisasjonsrett. Det betyr at styret har ansvaret hvis ansvaret ikke er delegert til daglig leder. Finanstilsynet mener at det bør fremgå av virksomhetsforskriften at sektorregleverkets bestemmelser om ansvarsfordeling innad i foretak skal gjelde.

Sikkerhetsmål

Av forslaget til forskriftens § 4 følger det at foretak som er underlagt sikkerhetsloven, f.eks. større banker, skal planlegge hvordan kravene til et forsvarlig sikkerhetsnivå skal oppfylles, og hvordan foretaket skal evaluere om kravene er oppfylt. Dette vil blant annet innebære tiltak for å sikre at skjermingsverdig informasjon ikke kommer på avveie, endres, går tapt eller ikke er tilgjengelig. Videre må det følges opp at systemene er sikret, og at det er etablert varslingssystemer for avdekking av uønskede aktiviteter og oppfølging av slik aktivitet. Forsvarsdepartementet har bedt

høringsinstansene om innspill på hvordan et foretak kan beskyttet sine skjermingsverdige verdier på en slik måte at kravet til forsvarlig sikkerhetsnivå oppnås.

Hva som er forsvarlig sikkerhetsnivå, vil variere avhengig av hva som til enhver tid er skjermingsverdig. Foretakene skal først vurdere risikoen. Med bakgrunn i denne vurderingen skal foretakene finne mulige passende sikkerhetstiltak, fastsette hvilke av disse som skal benyttes, samt iverksette og evaluere tiltakene. Finanstilsynet mener at den risikobasert tilnærmingen som er foreslått, er hensiktsmessig.

Skadevurdering – skjermingsverdige objekter og infrastruktur

I forslag til virksomhetsforskrift § 52 stilles det krav til en virksomhets skadevurderinger. Skadevurderingen skal inneholde informasjon om hvilke konsekvenser sikkerhetsrelaterte hendelser kan medføre for grunnleggende nasjonale funksjoner, krav til gjenopprettingstid, muligheter for gjenoppretting eller erstatning, og i hvilken grad rettstridig overtakelse kan påvirke befolkningens grunnleggende sikkerhet. Det stilles også krav om at ny skadevurdering skal gjennomføres ved endringer i definerte forhold. Skadevurderinger skal oversendes berørt departement eller NSM.

Finanstilsynet mener at denne type skadevurdering er viktig informasjon i Finanstilsynets tilsynsarbeid og at forskriften derfor bør inneholde en bestemmelse om at utarbeidet skadevurdering også skal oversendes sektormyndigheten.

Pålegg om tilknytning til varslingsystem for digital infrastruktur

Det foreslås i forskriften § 56, tilknytning til varslingsystem for digital infrastruktur, en videreføring av dagens bestemmelse om frivillig tilknytning til varslingsystem for digital infrastruktur. Forsvarsdepartementet vurderer imidlertid om NSM bør kunne pålegge slik tilknytning og har bedt om høringsinstansenes syn på saken.

Flere foretak i finanssektoren er i dag frivillig tilknyttet varslingssystemet. Finanstilsynet stiller imidlertid spørsmål ved nytteverdien av et pålegg. Det er Finanstilsynets oppfatning at foretak som i dag er tilknyttet varslingsystemet, er delte i sine syn på effekten av tilknytningen. Dersom foretakene opplever at ordningen ikke bidrar positivt til foretakets sikkerhetsarbeid, kan et pålegg virke mot sin hensikt. Det kan også være en risiko for at foretakene i for stor grad lener seg på informasjon fra NSM i sitt arbeid med å etablere sikkerhetstiltak relatert til trusler mot nasjonens sikkerhet. Hvis det innføres adgang til å gi pålegg om tilknytning til varslingsystem, mener Finanstilsynet at dette bør kunne gis av sektormyndighetene og fremgå av forskriften.

Foretak har et selvstendig ansvar for å etablere et sikkerhetsnivå som er i tråd med sikkerhetsloven, uavhengig av informasjonen som innhentes gjennom varslingsystemet. NSM må forventes å fokusere på trusler som kan true nasjonens sikkerhet, mens foretak under tilsyn av Finanstilsynet hovedsakelig har oppmerksomheten rettet mot digital kriminalitet som kan resultere i blant annet svindel. Det kan være behov for at foretak i finanssektoren i større grad, basert på veiledning fra NSM, retter fokus på trusler som utgjør en risiko for nasjonal sikkerhet i eget sikkerhetsarbeid. For eksempel kan relevant personell hos foretakene og dens leverandører instrueres i hvordan aktører som utgjør en trussel opererer, hvordan informasjonen som mottas fra NSM skal håndteres, og hvilke sikkerhetstiltak som skal iverksettes.

Finanstilsynet mener NSM sitt ansvar for informasjonsutveksling og veiledning knyttet til varslingsystem for digital infrastruktur bør tydeliggjøres i myndighetsforskriftens § 13.

Personellsikkerhet

Forskriftens kapittel 9 definerer krav til sikkerhetsklarering, adgangsklarering og autorisasjon. Personer som skal autoriseres for tilgang til informasjon gradert "konfidensiell" eller høyere, skal sikkerhetsklareres. Personell med tilgang til skjermingsverdige objekter og infrastruktur må ha gyldig adgangserklæring. Ansvarlig departement kan fatte vedtak om krav til adgangsklarering. Klarering foretas av klareringsmyndighet.

Den autorisasjonsansvarlige hos virksomheten kan gi autorisasjon uten klarering der det foreligger sikkerhetstiltak som reduserer risikoen. Det kan være krevende for virksomhetene å vurdere hva som er tilstrekkelig risikoreduserende tiltak. Etter Finanstilsynets vurdering bør dette fremgå tydeligere av forskriften. Det kan for eksempel gjøres ved at det henvises til virksomhetsforskriften § 4 om sikkerhetsmål, der det henvises til sikkerhetslovens bestemmelser om sikkerhetstiltak som er nødvendig for å gi et forsvarlig sikkerhetsnivå og redusere risikoen knyttet til sikkerhetstruende virksomhet.

Autorisasjon av utenlandske statsborgere

Virksomhetsforskriften § 61 og klareringsforskriften kapittel 4 krever særskilt behandling av sikkerhetsklarering av personell med utenlandsk statsborgerskap som skal ha tilgang til sikkerhetsgradert informasjon. En særskilt behandling kan omfatte en vurdering av hjemlandets sikkerhetsmessig betydning, personens tilknytning til hjemlandet og tilknytning til Norge.

Tilsvarende særskilt behandling er ikke et uttrykkelig krav når det gjelder adgangsklarering til skjermingsverdige objekter og infrastruktur. Sikkerhetsloven regulerer bestemmelser for klarering av personer med utenlandsk statsborgerskap, og Finanstilsynet oppfatter at dette omfavner både sikkerhetsklarering og adgangsklarering. Dette bør tydeliggjøres i virksomhetsforskriften § 61 og klareringsforskriften kapittel 4.

For Finanstilsynet

Morten Baltzersen
finansstilsynsdirektør

Per Mathis Kongsrud
Direktør for digitalisering og analyse

Dokumentet er godkjent elektronisk og har derfor ikke håndskrevne signaturer.