TRANSMISSION

Routing line.....: RYFID;RYFIE

DISTRIBUTION

Distributed Action.:	FD 2-4	Automatic	04/09/18 16:41:00
	MSO FD	Automatic	04/09/18 16:41:00
	FST DUTY OFF	Automatic	04/09/18 16:41:00

MESSAGE

Action.....: FD
Info.....: FFT
From.....: E-TJENESTEN
SIC.....: UAJ
Message type..: Operation
Precedence.....: Routine
Identification.....: RYFIJ 2600 2471441
DTG.....: 041441Z SEP 18
Releaser.....: S=SAMBAND; O=RG-LUTEUH; A=FDN; C=NO;
Sent.....: 18/09/04 16:41:22
Received.....: 18/09/04 16:41:26
Subject.....: Kommentarer til høring - forskrifter til ny sikkerhetslov

Attachment [1]

FFT for Regelverksenheten

Attachment [2] - File_Transfer, 2018-08-27 (U) Kommentarer til høring - forskrifter til ny sikkerhetslov .pdf, 2 MB

ETTERRETNINGSTJENESTEN

Vår dato	Vår referanse	Deres/tidl. referanse
27.08.2018	2018/126-4	2015/3139-254/FD V 3/ENWA

Til
Forsvarsdepartementet

Att:

Høring - forskrifter til ny sikkerhetslov

Etterretningstjenesten (E-tjenesten) viser til Forsvarsdepartementets høringsbrev og høringsnotat av 2. juli 2018 om ovennevnte. I et ugradert høringssvar kan tjenesten på enkelte punkter ikke gi utdypende og detaljerte begrunnelser. Vi ser derfor gjerne at det gjennomføres et møte om saken, dersom departementet har behov for slike begrunnelser.

Generelle kommentarer
Det fremgår ikke direkte om forskriftene skal fastsettes ved kgl. res., eller av departementet etter forutgående delegasjon av Kongens forskriftskompetanse i loven. Gitt forskriftenes sektorovergripende karakter, samt det forhold at loven på enkelte områder har lagt forskriftskompetansen til Kongen i statsråd (§§ 1-2 annet ledd, 2-1 annet ledd, 2-5 fjerde ledd og 9-4 femte ledd), legger E-tjenesten til grunn at samtlige forskrifter skal fastsettes ved kgl. res. Dette åpner også for å kunne gi tilpassede regler i medhold av sikkerhetsloven § 1-2 annet ledd.

Inndelingen i tre forskrifter i tråd med høringsutkastet synes i utgangspunktet hensiktsmessig, herunder at reguleringen av myndighetenes roller og ansvar fastsettes i forskrifts form og ikke i instruks. De foreslåtte korttitler vurderes også hensiktsmessige, og bør innarbeides i forskriftsutkastene. Vi har likevel ikke motforestillinger til å samle alle bestemmelsene i én forskrift dersom dette vurderes å øke tilgjengeligheten av og sammenhengen i regelverket. Spesielt på personellsikkerhetsområdet mener vi at alle relevante bestemmelser burde som tidligere være samlet i en forskrift. Dette ikke minst av hensyn til den/de som omfattes av bestemmelsene og ønsker å sette seg inn i disse. Vi ser også enkelte fordeler ved én forskrift, bl.a. for å innarbeide elementene i myndighetsforskriften i de to øvrige forskriftene samt innarbeide myndighetsforskriften §§ 8-11 i klareringsforskriften.

E-tjenesten stiller seg positiv til at både lov og forskrift i større grad enn tidligere åpner for skjønnsmessige vurderinger, men basert på kunnskap om innsidetrusselen er vi bekymret for den åpningen forskriftene gir i adgangen til å sikkerhetsklarere utenlandske statsborgere. Det bemerkes i denne sammenheng at en risikovurdering og en sikkerhetsfaglig vurdering av trusselen ikke synes å være basisgrunnlaget for forskriftenes utforming.

Postadresse:
Postboks 193
Alnabru Bedriftssenter
N-0614 OSLO

Besøksadresse:
Lutvannsveien 60
N-0616 OSLO

Sivil telefon/telefaks:
+47 23 09 40 00
+47 23 09 44 66
Militær telefon/telefaks:
0510 4000 / 0510 4466

E-post/Internett:
post.etterretningstjenesten@mil.no
www.forsvaret.no
Organisasjonsnummer:
NO 974 7892 21

Vi har merket oss at ny sikkerhetslov, med nærmere detaljering i forskriftsutkastene, pålegger et relativt stort antall norske virksomheter å gjennomføre risikovurderinger, og at det i den forbindelse forutsettes at virksomhetene får tilgang til bl.a. trusselvurderinger. Selv om slik tilgang kan ivaretas på ulike måter, og til tross for at det uttales at det for mange virksomheter vil være tilstrekkelig med åpne trusselvurderinger, er det grunn til å tro at ordningen vil medføre et økt antall oppdrag til de to instanser som utarbeider trusselvurderinger knyttet til villede trusler (E-tjenesten og PST). Dette kan igjen medføre forventnings- og prioriteringsavklaringer.

Uavhengig av om et objekt etter vedtak er underlagt krav om (utvidet) adgangsklarering legger vi til grunn at objekteier selv vil kunne iverksette egnede adgangskontrolltiltak. Objekteier må herunder kunne nekte personer adgang til objektet etter en risikovurdering, uten begrunnelse overfor de(n) som nektes adgang, herunder i forhold til personer som innehar (utvidet) adgangsklarering. Dette burde etter vårt skjønn kommet tydeligere frem i høringsnotatet. Det samme gjelder at adgang til skjermingsverdig objekt i tillegg forutsetter autorisasjon og tjenstlig behov.

E-tjenesten mener det bør gis mulighet for å pålegge utplassering av VDI i virksomheter underlagt sikkerhetsloven, og mener modalitetene rundt dette burde vært fremmet som forslag i de foreliggende forskriftsutkastene. Pålegg om utplassering bør ikke kunne innføres uten etter høring basert på et konkret forslag til regulering.

Etter vår oppfatning bør NSM fortsatt være sentral myndighet for leverandørklarering. Det er etter vårt syn en fordel at klareringsmyndigheten for leverandørklareringer har et sektoroverskridende ansvar. At NSM forvalter sikkerhetsavtalene med andre land taler etter vårt syn også for videreføring av gjeldende ordning. Ved sikkerhetsgraderte anskaffelser i forsvarssektoren bør ansvarlig myndighet for leverandørklarering ha innsikt i særlige risiki og andre forhold i denne sektoren. I tillegg kommer at forsvarsindustrien i ikke ubetydelig utstrekning er gjenstand for leverandørklarering. At leverandørene er private rettssubjekter, tilsier etter vårt syn derfor ikke i seg selv at klareringsmyndigheten bør legges til Sivil klareringsmyndighet.

Kommentarer til utkast til forskrift om myndighetenes roller og ansvar for nasjonal sikkerhet (myndighetsforskriften)

Til § 2 første ledd fremstår det som noe uklart for oss om et vedtak om adgangsklarering kan differensiere mellom ulike persongrupper, eller om vedtak om adgangsklarering må gjelde enhver som skal ha adgang til objektet. Kan vedtaket f. eks. kun gjelde utenlandske statsborgere, eller gjøre unntak for ansattes samboere/ektefeller/barn? § 11 første ledd annet punktum taler vel for at vedtak etter § 2 kan innebære differensierte krav til adgangsklarering, men dette bør likevel etter vår vurdering tydeliggjøres. Etter vårt syn bør også § 11 første ledd annet punktum flyttes til § 2.

Til § 2 annet ledd kan det stilles spørsmål om et objekt eller en infrastruktur i det hele tatt kan være et mål for et «attentat».

Til § 6 legges til grunn at E-tjenesten etter vedtak og på vegne av NSM kan få ansvar for å gjennomføre TSU, penetrasjonstesting, monitoring og annen testing av sikkerhetstiltak for å sikre ivaretakelse av E-tjenestens særskilte skjermingsbehov. Tjenestens skjermingsbehov er betydelig større enn i andre deler av den offentlige forvaltning, og krever tilpassede permanente påbygningstiltak ut over grunnsikring, herunder hurtig iverksettelse av nevnte § 6-tiltak i inn- og utland av hensyn til oppdukkende behov. E-tjenesten har egen spisskompetanse på området, en betydelig sikkerhetsorganisasjon, omfattende erfaring og en god sikkerhetskultur. Vi anfører at dette også synes å være i tråd med lovens og forskriftenes intensjon om i større utstrekning enn i dag å overlate til den enkelte virksomhet å definere et nødvendig og forsvarlig sikkerhetsnivå basert på virksomhetsspesifikke helhetlige risikovurderinger, kombinerte tiltak, kostnadseffektivitet og omstendighetene for øvrig. I den utstrekning § 6-tiltak i forhold til E-tjenesten helt eller delvis likevel skal gjennomføres av andre enn tjenesten selv, tilsier sikkerhetsmessige hensyn at E-tjenesten ikke vil kunne gi samtykke til tiltak dersom NSM velger å sette bort gjennomføringen til en offentlig eller privat tredjepart.

E-tjenesten forvalter i dag kryptomateriell mottatt fra fremmede stater. Vi ber om at denne praksisen kan videreføres uavhengig av det som bestemmes om NSMs rolle i § 7 første ledd.

Til § 8 bemerkes at E-tjenesten har behov for å videreføre ordninger som hindrer at tjenestens ansatte lar seg identifisere i det nasjonale registeret over alle klareringsavgjørelser. Vi legger til grunn at § 8 ikke vil være til hinder for dette.

Til § 9 ber vi om at gjeldende praksis videreføres knyttet til at tjenesten i enkelte tilfeller selv fører register over egne sikkerhetsgraderte anskaffelser.

Til § 10 bemerkes at E-tjenesten i dag selv utsteder klareringsbevis for eget personell. Vi legger til grunn at § 10 første ledd ikke innebærer at dette heretter må gjøres av NSM.

Vi foreslår at det i § 11 første ledd første punktum presiseres at unntak fra krav om sikkerhetsklarering og autorisasjon kun kan treffes når det er særlig behov for det «...*og virksomhetens leder ber om det,..*». Det synes urimelig at NSM kan dispensere fra et sikkerhetskrav i strid med virksomhetens ønsker.

Overskriften i kapittel 3 bør justeres til «Responsfunksjon og varslingssystem for digital infrastruktur», i tråd med overskriften i sikkerhetsloven § 2-4. E-tjenesten er generelt skeptisk til begrepet «nasjonalt» i denne sammenheng, og peker på at bl.a. et eventuelt DGF i langt større grad enn VDI vil være et reelt nasjonalt varslingssystem. Sikkerhetsloven § 2-4 bruker imidlertid begrepene «nasjonal responsfunksjon» og «nasjonalt varslingssystem» om NSM NorCERT og VDI. Av den grunn foreslår vi ikke endringer i paragrafteksten. Vi er også motstander av å bruke begrepet «digitale angrep» om digital etterretning og annen aktivitet i det digitale rom som ikke har til hensikt å påvirke informasjon, systemer eller personer i form av ødeleggelse, forstyrrelser, skade, manipulasjon eller andre påvirkninger. Også her tar vi imidlertid til etterretning at sikkerhetsloven benytter begrepet «digitale angrep».

I § 13 første ledd foreslås «*og avtale er inngått etter virksomhetsforskriften § 56 andre ledd*» strøket. Virksomhetsforskriften § 56 (som for øvrig ikke har et andre ledd) gjelder kun VDI-avtaler. Deling av informasjon fra NSM til partene i FCKS kan gjelde annen informasjon enn VDI-

informasjon, og under enhver omstendighet er VDI-avtale i seg selv ikke tilstrekkelig hjemmel for å kunne utlevere VDI-informasjon.

NSM vil ikke sjelden ha mottatt informasjon fra E-tjenesten eller E-tjenestens partnere om fare for alvorlige digitale hendelser. I enkelte tilfeller er informasjonen klausulert. NSM kan i slike tilfeller ikke uten videre informere berørte aktører om trusler, sårbarheter og mulige tiltak. Vi anbefaler derfor at § 13 annet ledd endres til å lyde: «*Ved fare for alvorlige hendelser skal Nasjonal sikkerhetsmyndighet så langt mulig...*»

Til kapittel 4 om tilsyn merker E-tjenesten seg og slutter seg til departementets uttalelse i høringsnotatet s. 16 om videreføring av dagens instruksbaserte ordning knyttet til NSMs overordnede og systemrettede tilsyn med tjenesten.

Etter § 16 kan NSM avtale med sektormyndigheten at sistnevnte kan føre tilsyn med leverandører. Tilsvarende bør etter vårt syn også kunne avtales med E-tjenesten i særskilte tilfeller.

Til § 18 tredje ledd forutsetter vi at tilsynsrapporter etter NSMs tilsyn i E-tjenesten ikke kan gjøres tilgjengelig for PST (eller andre) uten etter uttrykkelig forutgående samtykke fra E-tjenesten.

Kommentarer til utkast til forskrift om virksomhetens arbeid med forebyggende sikkerhet (virksomhetsforskriften)
Til § 5 bemerkes at det for E-tjenesten neppe vil være praktikabelt eller formålstjenlig at kontroll av styringssystemet utføres av andre enn de som har styrende eller utøvende oppgaver i det forebyggende sikkerhetsarbeidet. Vi legger til grunn at dagens praksis kan videreføres, jf. «om mulig» i § 5 tredje ledd.

Det bemerkes en skrivefeil i § 11 annet ledd («for å» gjentatt to ganger etter hverandre).

Til §§ 13 og 54 bemerkes at utplassering og bruk av sikringsstyrker fra Forsvaret eller politiet ikke reguleres av sikkerhetsloven og således heller ikke er et påbyggingstiltak etter § 13. Overskriften til § 54 bør derfor endres til å lyde: «Tilrettelegging for bruk av sikringsstyrker» og «som et påbygningstiltak» bør strykes i paragrafen.

§§ 15 og 16 passer ikke fullt ut for E-tjenestens operative virksomhet. Vi legger til grunn at dagens praksis kan videreføres.

E-tjenesten har en bekymring knyttet til § 20, som vi oppfatter legger opp til et endret regime for oppbevaring og behandling av lavgradert informasjon (BEGRENSET). Hvordan virksomhetene skal oppbevare og behandle BEGRENSET informasjon skal, slik vi tolker det, risikovurderes av virksomheten som eier informasjonen. Forskriften åpner for å kunne utøve større grad av skjønn enn tidligere, selv om det presiseres at uautorisert personell ikke med enkle midler skal få tilgang til informasjon som er sikkerhetsgradert. Man kan tenke seg at en oppmykning som foreslått betyr at E-tjenestens sin informasjon som kun er BEGRENSET, vil bli håndtert mer uforsiktig av enkelte andre, herunder våre leverandører, og ikke i like stor grad oppbevares og behandles i beskyttet eller sperret område slik kravet er i dag. Det kan også bli mer krevende

for oss å sikre oss at mottaker behandler og oppbevarer lavgradert informasjon sikkert nok. Det er derfor en risiko for at informasjon som vi nå verdivurderer til å være BEGRENSET, vil bli gradert KONFIDENSIELT i fremtiden fordi man ønsker å beholde skjermingen som oppbevarings- og behandlingskravene til dette graderingsnivået ivaretar ved spredning utenfor tjenesten. I lang tid fremover anser vi også at det endrede sikkerhetsnivået kan volde ikke uvesentlige overgangsutfordringer, fordi «gammel» BEGRENSET er verdivurdert ut fra en visshet om at informasjonen kun vil behandles i beskyttet eller sperret område. «Ny» BEGRENSET og «gammel» BEGRENSET vil trolig verdivurderes forskjellig som følge av at «ny» BEGRENSET har et lavere sikkerhetsnivå. Vi anmoder derfor om at departementet vurderer om kapittel 5 også bør inneholde noen ytterligere minimumssikkerhetsregler av ufravikelig karakter for informasjon gradert BEGRENSET.

E-tjenesten er bekymret for at standarden «forsvarlig sikkerhetsnivå», jf. § 20, for skjermingsverdig ugradert informasjon i for stor grad åpner for skjønn og ulik praksis.

I høringsnotatet fremheves det at § 23 er en videreføring av informasjonssikkerhetsforskriften § 3-2. Som eksempel vises til at det vil forekomme tilfeller hvor EOS-tjenestene må dele etterretningsinformasjon med andre land av hensyn til nasjonale sikkerhetsinteresser. Informasjonssikkerhetsforskriften krever ikke at utlevering i slike tilfeller, uten at det foreligger en sikkerhetsavtale, må treffes på departementsnivå. Utkast til § 23 fastsetter imidlertid at Forsvarsdepartementet og Justis- og beredskapsdepartementet kan gjøre unntak fra kravet til sikkerhetsavtale. Dette vil i så fall være en endring av dagens praksis, som ikke er drøftet i høringsnotatet. Vi mener at dagens praksis, som for E-tjenesten innebærer at vi vurderer dette selv, bør videreføres. Forsvarsdepartementet godkjenner nye samarbeidsrelasjoner og avtaler forbundet med disse, men det vil verken være praktisk eller nødvendig at departementet skal treffe vedtak i hvert enkelt tilfelle hvor informasjon deles med etablerte partnere.

E-tjenesten forvalter i dag kryptomateriell mottatt fra fremmede stater. Vi ber om at denne praksisen kan videreføres uavhengig av bestemmelsen om at NSM skal bestemme hvilket materiell som kan brukes til å kryptere informasjon gradert KONFIDENSIELT eller høyere, jf. § 25 fjerde ledd annet punktum.

Til § 27 bemerkes at E-tjenesten er av den prinsipielle oppfatning at kildeinformasjon ikke bør ha tidsbegrenset gradering, men som hovedregel være tidsubestemt. Det er et viktig signal om konfidensialitet til og livsvarig beskyttelse av eksisterende og fremtidige kilder.

E-tjenesten går imot regelen i § 29 om at NSM – i strid med virksomhetens skadevurdering – skal kunne om-/avgradere informasjon. Slik myndighet bør kun ligge hos overordnet nivå i linjen.

E-tjenesten behandler omfattende mengder høygradert informasjon, og praktiserer i forståelse med NSM enkelte særordninger, bl.a. for internt utlån av H-dokumenter, jf. utkastet til § 41 første ledd. Vi ber om at gjeldende praksis kan videreføres.

Til § 47 bemerkes at E-tjenesten har skjermingsverdige informasjonssystemer hvis eksistens og funksjon ikke kan røpes overfor NSM eller andre tredjeparter. E-tjenesten har herunder skjermingsverdige informasjonssystemer som omfattes av § 47 tredje ledd, og som er godkjent

av E-tjenesten etter en risikovurdering. E-tjenesten har egen spisskompetanse på området. Etter vårt syn er gjeldende ordninger forsvarlige og bør videreføres, hvilket formodentlig krever at det i § 47 åpnes for å gjøre unntak og tilpasninger i forhold til E-tjenestens informasjonssystemer. Vi anfører at dette også synes å være i tråd med lovens og forskriftenes intensjon om i større utstrekning enn i dag å overlate til den enkelte virksomhet å definere et nødvendig og forsvarlig sikkerhetsnivå basert på virksomhetsspesifikke helhetlige risikovurderinger, kombinerte tiltak, kostnadseffektivitet og omstendighetene for øvrig. Unntak og tilpasninger utelukker selvsagt ikke en videreføring av dagens faglige samarbeid med NSM om sikring av informasjonssystemer.

Overskriften til kapittel 8 bør endres til å lyde «Varslingssystem for digital infrastruktur», jf. merknad til myndighetsforskriften kapittel 3.

Kommentarer til utkast til forskrift om klarering av leverandører og personell (klareringsforskriften)
E-tjenesten anser at § 2 bokstav d kan utgjøre en hjemmelsutfordring. Dersom omspurte oppgir en person som omspurte anser å ha en nær relasjon til (og som ikke er «nærstående»), så utløser dette en mulighet for personkontroll av vedkommende uten at denne nødvendigvis har kjennskap til opplysningen om relasjonen eller mulighet til å motsette seg påstanden om dette. Vi anser at dette kan etter omstendighetene kan være juridisk betenkelig, da den som det blir opplyst om kan ha en helt annen oppfatning om relasjonens art enn omspurte har.

Til § 3 viser vi til våre generelle kommentarer ovenfor om at virksomheten etter omstendighetene må kunne sette høyere krav for adgang til skjermingsverdig objekt eller infrastruktur, eller helt eller delvis nekte adgang når det fremstår saklig og forsvarlig.

Til § 6 tredje og fjerde ledd bemerkes at E-tjenesten finner det betenkelig at nærstående ikke skal ha betydning for adgangsklarering når det er definert at dette først og fremst er et tiltak for å redusere risikoen for terror mot kritiske og meget kritiske objekter. Fjerde ledd reiser videre etter vårt syn spørsmål om det er tilstrekkelig begrunnet at andre nærstående kun inngår i sikkerhetsklarering for SH dersom foreliggende opplysninger gir grunn til å anta at disse kan påvirke personens pålitelighet, lojalitet eller dømmekraft, mens andre nærstående alltid skal inngå i personkontrollen ved utvidet adgangsklarering dersom det skal gis tilgang til MEGET KRITISK objekt (eller infrastruktur?).

Etter vår oppfatning er oppramsing av temaer som skal besvares i skjema til bruk i en klareringsprosess, jf. § 7, unødvendig og heller ikke hensiktsmessig. For å unngå unødvendige begrensninger for klareringsmyndighetene, og for å ivareta behov for revisjoner og endringer av lov og forskrifter i takt med samfunnsutviklingen, burde det være tilstrekkelig å beholde første ledd og heller fastsette at «*Den som skal sikkerhetsklareres for KONFIDENSIELT eller høyere skal på skjema fastsatt av Nasjonal sikkerhetsmyndighet gi sitt samtykke til gjennomføring av personkontroll og opplyse om de spørsmål som følger av fastsatt skjema og veiledning*». Vi anser at det er lite hensiktsmessig å definere disse spørsmålene i forskrift. Vi vil også bemerke ordlyden i bokstav i som foreligger i forslaget, hvor det overlates til den enkelte å vurdere hvilke land som kan ha betydning for klareringsavgjørelsen. Dette kan etter vårt syn ikke overlates til den enkelte. Det samme gjelder bokstav n, hvor den enkelte skal vurdere hvilke helseopplysninger eller medikamentbruk som kan ha betydning for egen dømmekraft.

E-tjenesten mener at § 8 burde ha samme ordlyd som forslaget ovenfor til § 7, f.eks. slik: «*Den som skal gis adgangsklarering eller utvidet adgangsklarering skal opplyse om den informasjonen som det spørres om i skjema utarbeidet av Nasjonal sikkerhetsmyndighet.*» Dersom ordlyden besluttes beholdes bør bokstav b (opplysninger om statsborgerskap), da dette etter omstendighetene kan være av vesentlig betydning.

Det gis verken i loven, forskriften eller i høringsnotatet noen informasjon om hvilke egne registre NSM besitter og hvilke opplysninger som kan innhentes og lagres i slike registre, jf. §§ 9 og 10, jf. også sammenhengen med sikkerhetsloven § 8-5 sjette ledd om opplysninger fra «andre kilder» enn relevante registre. Fra et forutberegnelighets- og rettssikkerhetsperspektiv bør dette etter vår vurdering tydeliggjøres og reguleres nærmere. Det samme gjelder for «klareringsmyndighetens egne registre» i § 32 bokstav g.

Til § 14 fjerde ledd bemerkes at dersom slike unntakseksempler skal benyttes, bør det etter vårt syn tilføyes at det kan legges vekt på at utenlandsoppholdet relaterer seg til land som utgjør svært lav sikkerhets- og etterretningsmessig trussel mot Norge. Begrepet «en norsk virksomhet» fremstår som noe utydelig, da dette også vil kunne inkludere enkeltmannsforetak eller AS, noe som ikke utelukker en sterk tilknytning til aktuell stat. Det bør videre fremkomme at dersom unntakshjemmelen skal benyttes, bør/skal det gjennomføres sikkerhetssamtale som et kompenserende tiltak.

I vurderingen av utvidet adgangsklarering, jf. § 15 annet ledd, mener vi klareringsmyndigheten i tillegg bør kunne vektlegge forhold som nevnt i loven § 8-4 fjerde ledd bokstav c, g og o.

Det anses uryddig og uheldig at § 17 opererer med et annet begrep (klareringsintervju) enn loven (sikkerhetssamtale), når begrepene har samme meningsinnhold. Dersom begrepet sikkerhetssamtale av enkelte oppfattes misvisende, bør dette kunne avhjelpes med skriftlig informasjon om samtalens formål mv. ved innkalling til samtalen. Vi anbefaler derfor at begrepet sikkerhetssamtale videreføres, jf. sikkerhetsloven § 8-4 hvor dette begrepet blir brukt. Klareringsintervju er dessuten en misvisende betegnelse som kan være i konflikt med samtalens intensjon. Dette kan i verste fall medføre sosialt ønskverdig besvarelser, og ikke gi valide svar på spørsmålene. Begrepet tilbakeholder informasjon om samtalens alvorlighetsgrad.

Annet ledd i § 17 bør endres eller utgå. En sikkerhetssamtale har som formål å innhente opplysninger som belyser en persons sikkerhetsmessige skikkethet, og forholdene i § 8-4 fjerde ledd som det her henvises til, er for snever.

Til § 19 bemerkes at vi mener at begrepet «karantene» er lite treffende, og at det eksisterende begrepet «observasjonstid» beskriver intensjonen bedre.

Bestemmelsen i § 21 første ledd forstås å gjelde opplysninger som ikke omfattes av loven § 8-13 annet ledd.

Paragraf 22 annet ledd er uklar. Vi antar det bør komme klarere frem at innsyn i lydopptak eller audiovisuelt opptak kun kan skje hos klareringsmyndigheten. Ordlyden nå kan også tolkes

dithen at man kan få med seg kopi av opptak ved å møte frem hos klareringsmyndigheten, hvilket vi legger til grunn ikke har vært meningen.

Til § 24 bemerkes at E-tjenesten er underlagt særlige arkivregler som bl.a. unntar tjenesten fra avleveringsplikt. Vi legger til grunn at særreglene går foran generelle regler fastsatt av NSM i medhold av § 24.

Vi reiser spørsmål om § 26 første ledd første punktum kan strykes, all den tid bestemmelsen ikke synes å tilføre noe materielt nytt sett i forhold til § 26 første ledd annet punktum.

E-tjenesten mener klagerett bør avskjæres i saker om autorisasjon av utenlandske statsborgere for BEGRENSET etter reglene i kapittel 4. En viser til forskjellen mellom autorisasjonsavgjørelser og avgjørelser om klarering.

Til § 29 bør det klargjøres hva som menes med henholdsvis norske og utenlandske leverandører, herunder hva det vil si å «holde til» i Norge. For eksempel legger vi til grunn at et utenlandsk selskap med en filial i Norge skal anses som en norsk leverandør dersom anskaffende virksomhet forholder seg til representanter for filialen i Norge i spørsmål som gjelder den sikkerhetsgraderte anskaffelsen, og sikkerhetsgradert informasjon skal behandles og oppbevares i Norge.

Vi har for øvrig merket oss at det i høringsnotatet pkt. 4.6.2 varsles en veiledning som vil gjøre det enklere å se sammenhengen mellom anskaffelsesregelverket og sikkerhetsloven med forskrifter. I den anledning er det ønskelig fra vår side med en klargjøring av hva som i forskrift om offentlige anskaffelser § 2-2 ligger i begrepene «erklært hemmelige» og «særlige sikkerhetstiltak». Det er også ønskelig å klargjøre i hvilken utstrekning anskaffelsesregelverket tillater kvalifikasjons- eller tildelingskriterier som vektlegger mulighet for kontroll av komponenter fra tiltrodd tredjepart.

Morten Haga Lunde
Generalløytnant
Sjef Etterretningstjenesten

Kopimottakere:
Forsvarets fellestjenester/Regelverksenheten