



Forsvarsdepartementet

Postboks 8126 Dep

0032 OSLO

NATIONAL POLICE DIRECTORATE

Deres referanse:

2013/00552

Vår referanse:

201501983-20 008

Sted, Dato

Oslo, 25.08.2015

HØRINGSSVAR - FORSLAG TIL ENDRINGER I SIKKERHETSLOVEN

Politidirektoratet viser til Forsvarsdepartementets høringsbrev av 19. mai 2015 og avtale om utsatt frist til 4. september 2015.

Politidirektoratet har forelagt høringen for underliggende instanser. Vi har mottatt høringsuttalelser fra Kripos, Romerike, Asker og Bærum, Vestoppland og Oslo politidistrikt, som følger vedlagt i kopi. Uttalelsene er delvis innarbeidet i direktoratets høringsuttalelse.

Politidirektoratet har følgende merknader:

Bakgrunn for høringen

Departementet viser innledningsvis i høringsnotatet til et revisjonsarbeid som har "avdekket grunnleggende utfordringer når det gjelder oppfatninger av hva sikkerhetsloven bør regulere, herunder hvordan forholdet mellom sikkerhetsloven og annet sikkerhetsrelatert sektorregelverk bør være."

Politidirektoratet bemerker at informasjon som politiet forvalter i dagens IKT-portefølje frem til i dag i svært stor grad har falt utenfor sikkerhetslovens virkeområde. Som Kripos påpeker i sin høringsuttalelse faller politiregisterinformasjon i hovedsak under beskyttelsesinstruksens FORTROLIG og STRENGT FORTROLIG. Dette betyr at informasjon elektronisk skal beskyttes som sikkerhetslovens BEGRENSET så langt det passer. Etter Politidirektoratets vurdering er begrepet for diffust. Nasjonal sikkerhetsmyndighet (NSM) har ingen rolle i forvaltningen, rådgiving, veiledning eller tilsyn innenfor beskyttelsesinstruksens nedslagsfelt. Samtidig utveksler politiet informasjon med ulike samarbeidspartnere både nasjonalt og internasjonalt (EU) som pålegger politiet å sikre informasjon etter krav fra sikkerhetsloven.

Etter Politidirektoratets vurdering er det kompetanse- og ressurskrevende å forholde seg til ulike sektorregelverk når det gjelder sikring av IKT-løsninger. Det er ressurskrevende både for politiets interne kontrollenheter og for ulike tilsynsmyndigheter å få en oversikt over den sikkerhetsmessige tilstanden og etterlevelse av ulike regelverk. Politidirektoratet etterlyser en forenkling av forvaltningen av det sikkerhetsmessige sektorregelverket, slik at grensesnitt mellom lovgivning og IKT blir forenklet. Det vises bl.a. til arbeid som er gjort i Storbritannia

Politidirektoratet

POD

Post: Postboks 8051 Dep., 0031 Oslo

Besøk: Hammersborggata 12

Tlf: 23 36 41 00

Faks: 23 36 42 96

E-post:

politidirektoratet@politiet.no

Org. nr.: 982 531 950 mva

Giro:

www.politi.no

rundt "Government Security Classifications" som tilsynelatende ser ut til å forenkle regelverket ved å "slå sammen" klassifiseringer på tvers av sektorer.

§ 5 a Varslingsplikt mv. ved risiko for rikets selvstendighet og sikkerhet og andre vitale nasjonale sikkerhetsinteresser.

Departementet foreslår å innta en ny bestemmelse i sikkerhetsloven kapittel 2. Bestemmelsen skal regulere to forhold. For det første gir den Kongen i statsråd fullmakt til å fatte vedtak for å hindre planlagte eller pågående aktiviteter som innebærer en fare for rikets selvstendighet og sikkerhet og andre vitale nasjonale sikkerhetsinteresser. For det andre oppretter bestemmelsen en varslingsplikt for virksomheter som er underlagt sikkerhetsloven i tilfeller der det foreligger en ikke ubetydelig risiko for slik aktivitet.

Kripos støtter departementets forslag om innføring av ny § 5 a i sikkerhetsloven. Kripos fremholder i sin høringsuttalelse at varslingsplikten vil gi bedre oversikt over truende aktiviteter, og således kunne motvirke trusler mot rikets selvstendighet og sikkerhet og andre vitale nasjonale sikkerhetsinteresser

Politidirektoratet mener varslingsplikten bør utvides til også å omfatte virksomheter som eier kritisk infrastruktur, slik at olje- og energisektoren omfattes. Dette av hensyn til at sektoren har valgt å definere seg utenfor sikkerhetsloven, til tross for at andre skjermingsverdige objekter er kritisk avhengig av strøm for å opprettholde sine funksjoner. I tillegg er sektoren utsatt for etterretningsaktivitet, se vår merknad under § 29 a.

§ 6 a Gebyr

Departementet foreslår i § 6 a en klar hjemmel for å kunne kreve gebyr der en virksomhet utfører tjenester for en annen. Forslaget innebærer at det åpnes for nærmere å regulere i forskrift at det kan kreves gebyr for visse tjenester som, i medhold av bestemmelser gitt i sikkerhetsloven med underliggende forskrifter, utføres av en virksomhet for en annen.

Kripos fremholder i sitt hørings svar at det er riktig å kunne gi en rettslig adgang til å fastsette forskrift om gebyr. Kripos anser det som svært viktig at det i det videre arbeidet avveies hvilke tjenester det skal tas gebyr for, opp mot den økonomiske konsekvens som da tilkommer den enkelte virksomhet. Som eksempel viser Kripos til at prosessen for godkjenning av informasjonssystemer og kryptosystemer kan inneha stor økonomisk usikkerhet.

Oslo politidistrikt redegjør i sin uttalelse for distriktets erfaring med til dels store variasjoner mellom de ulike klareringsmyndigheter og saksbehandleres henvendelser. Distriktet vurderer at egenandelsvirkningen av et gebyr vil kunne bidra til å moderere innsynsbejæringene fra klareringsmyndighetene dersom politiet gis mulighet til å avkreve gebyr av klareringsmyndighetene, tilsvarende det klareringsmyndighetene vil kunne gjøre ut til de som anmoder om klarering.

Romerike politidistrikt anbefaler i sitt hørings svar at forslaget tas bort i sin helhet. Distriktet viser til at majoriteten av landets virksomheter er styrt etter økonomi og profitt, og at en ordning med gebyr trolig vil svekke sikkerhetstilstanden over tid. Distriktet antar at et gebyr vil gi konsekvenser for arbeidet med sikkerhetskulturen i virksomhetene.

Politidirektoratet stiller seg kritisk til at det innføres gebyr for tjenester som utføres med hjemmel i sikkerhetsloven. Sikkerhetsklarering av personell, godkjenning av kryptosystemer, monitoring, inntrengningstesting av informasjonssystemer og tekniske sikkerhetsundersøkelser

nevnes som eksempler på tjenester det kan være aktuelt å kreve gebyr for. Disse tjenestene står etter Politidirektoratets vurdering sentralt i arbeidet med å forbedre den forebyggende sikkerhetstjenesten. Det er ressurskrevende å følge sikkerhetslovens plikter med forebyggende sikkerhetstjeneste, hvilket vil kunne være motivasjon for at enkelte virksomheter bevisst prøver å definere seg utenfor sikkerhetsloven. Formålet med sikkerhetsloven er å verne om nasjonale sikkerhetsinteresser. Politidirektoratet mener det blir lite formålstjenlig å gebyrlegge virksomheter som ønsker å bidra til dette nasjonale formålet, fremfor å tenke egne økonomiske besparelser og konkurransedyktighet. Direktoratet tiltrer Kripos' påpekning av viktigheten av å avveie hvilke tjenester det skal tas gebyr av dersom forslag til § 6a ikke utgår.

§ 9 Nærmere om oppgavene

Departementet foreslår at virksomheten som i dag utøves av NSM gjennom VDI- og NorCERT-funksjonene lovfestes i § 9 som en del av NSMs oppgaver.

I høringsnotatet, på side 13, fremheves at NSM skal "koordinere håndteringen av alvorlige IKT-hendelser..". Politidirektoratet mener denne setningen er egnet til å skape forvirring knyttet til våre nasjonale beredskapssystemer, da setningen antyder at NSM har et større ansvar enn de i realiteten har.

I henhold til politiloven § 2 skal politiet "beskytte person, eiendom og fellesgoder og verne om all lovlig virksomhet". Det er politiet som er samfunnets sivile maktapparat og som har anledning til å gripe inn overfor borgerne med hjemmel i politiloven § 7 og straffeprosessloven. Vi viser i denne forbindelse til høringsuttalelsene fra Kripos og Oslo politidistrikt.

Kripos uttaler i sitt hørings svar at de er enig i å lovfeste varslingssystemet for digital infrastruktur (VDI) og nasjonal responsfunksjon for alvorlige dataangrep mot samfunnskritisk infrastruktur (NorCERT). Videre bemerker Kripos at de er oppmerksom på det Digitale sårbarhetsutvalgets kommende utredning av sårbarheter innen kritiske samfunnsfunksjoner og kritisk infrastruktur. Kripos har bidratt inn i dette arbeidet, hvor det i mandatet ligger at de også skal se på sivil-militært samarbeid og samarbeid mellom offentlige og private aktører.

Politidirektoratet motsetter seg ikke lovfesting av ansvaret til NorCERT-funksjonen, men bemerker at lovfesting kan bidra til å forsterke de uklarheter som allerede eksisterer rundt hvilke myndigheter som har ansvar for hva knyttet til alvorlige IKT-hendelser. Forarbeidene bør etter direktoratets vurdering derfor klargjøre at det er politiet som har ansvar for krisehåndtering i sivil sektor. Som Kripos påpeker, kan arbeidet i Det digitale sårbarhetsutvalget frembringe nye momenter knyttet til ansvarsforholdene.

Videre viser vi til uttalelsen fra Oslo politidistrikt, der distriktet "stiller spørsmål til hvorvidt departementet i stor nok grad har redegjort for hensiktsmessigheten av at NSM som tilsynsmyndighet også skal tillegges det operative ansvaret for den nasjonale cyber- og informasjonssikkerheten. Videre i hvilken grad en slik innretning kommer i konflikt med uavhengighetsprinsippet mellom utførende og kontrollerende funksjoner."

I initialfasen av alvorlige IKT-hendelser kan det være uklart hva som er motivet og hvem som står bak. Selv om endringene i sikkerhetsloven ikke direkte omhandler dette, vil direktoratet peke på at det kan være en svakhet at håndteringen skjer uten det ordinære politiets deltakelse.

Justis- og beredskapsdepartementet har gitt politiet i oppgave å etablere en Justis- CSIRT for å kunne varsle på tvers av departementets underliggende etater. Det er nærliggende at denne må revitaliseres og styrkes dersom et slikt samarbeid skal være effektivt og gi merverdi.

§ 10a – behandling av personopplysninger

Departementet foreslår en ny § 10 a som klargjør NSMs adgang til å behandle personopplysninger. I bestemmelsens første ledd etableres det et klart hjemmelsgrunnlag for NSMs behandling av personopplysninger i forbindelse med drift av VDI- og NorCERT-funksjonene. Bestemmelsen tar sikte på å forsterke hjemmelsgrunnlaget for den behandlingen av personopplysninger som skjer i dag.

Kripos støtter i sin høringsuttalelse departementets forslag til ny § 10. Kripos bemerker imidlertid at den foreslåtte ordlyden fremstår som uklar, all den tid departementet legger til grunn at personopplysningslovens bestemmelser kommer til anvendelse på behandlingen av personopplysninger i denne forbindelse, inkludert de aktuelle unntaksbestemmelsene. Kripos fremholder det som mer hensiktsmessig å fastslå det rettslige grunnlaget for behandlingen av personopplysninger i ny § 10a og deretter innta en henvisning til personopplysningsloven, dette for å unngå visse unøyaktigheter i ordlyden slik den fremstår i forslaget.

§ 13 a Sikkerhetsmessig overvåking av godkjente informasjonssystemer

Departementet foreslår en ny bestemmelse i sikkerhetsloven om virksomhetens egen adgang til sikkerhetsmessig overvåking av godkjente informasjonssystemer.

Kripos tiltrer i sin høringsuttalelse departementets forslag om innføring av ny § 13 a i sikkerhetsloven. Kripos viser til at både den teknologiske og samfunnsmessige utviklingen tilsier en mulighet for økte sårbarheter med dertil behov for å avdekke og håndtere eventuelle angrep eller uregelmessigheter som kan true sikkerheten i godkjente informasjonssystemer. Kripos bemerker at den typen overvåking av informasjonssystemene som det legges opp til i den foreslåtte bestemmelsen, hvor blant annet trafikk- og innholdsdata kan lagres for å avdekke sikkerhetstruende hendelser, vil kunne være kontrolltiltak av en til dels inngripende karakter for den enkelte. Selv om bestemmelsen i all hovedsak er en videreføring av dagens § 5-2 i informasjonssikkerhetsforskriften, og denne dermed også kunne utvides til omfatte innholdsdata, mener Kripos det fremstår som en god løsning å regulere virksomheters egen adgang til sikkerhetsmessig overvåking tydeligere, som foreslått i ny § 13 a hvor også hensynet til ansattes personvern ivaretas tilfredsstillende.

Politidirektoratet støtter forslaget om innføring av § 13 i sikkerhetsloven, da dette er et viktig tiltak for å kjenne til den sikkerhetsmessige statusen til et (sikkerhetsgodkjent) informasjonssystem.

Politidirektoratet antar at politiets IKT-infrastruktur med påliggende systemportefølje (også kalt politinett og nødnett) faller inn under samfunnskritisk infrastruktur da politiets oppgaver bl.a. er å bidra til befolkningens trygghet. Deler av selve den fysiske IKT-infrastrukturen faller inn under sikkerhetsloven med forskrift om objektsikkerhet, mens informasjonssystemene politinett og nødnett ikke er sikkerhetsgodkjent for å behandle informasjon gradert etter sikkerhetsloven.

Politiet har som ovenfor nevnt lite informasjon som pr i dag faller inn under sikkerhetsloven. Det er derfor få sikkerhetsgodkjente informasjonssystemer i politiets portefølje. Det er enkelte mindre systemer, men disse er ikke knyttet sammen, eller til politiets nasjonale IKT-system

(politinett). Direktoratet antar at kapasiteter for sikkerhetsmessig overvåking av informasjonssystemer vil gjelde for systemer som har en viss størrelse og kapasitet, og ikke små dedikerte systemer. Dersom dette ikke er tilfelle, vil det etter direktoratets vurdering kreve tilførsel av kompetanse og kapasitet for å vurdere konsekvensen av denne endringen.

Direktoratet viser for øvrig til bestemmelsens femte ledd, som lyder: "Informasjon som nevnt i første og andre ledd skal kun benyttes til formål om å håndtere sikkerhetstruende hendelser." Politidirektoratet forstår bestemmelsen slik at den avskjærer muligheten til å benytte informasjonen fra overvåkningen av informasjonssystemet til en etterfølgende straffesaksbehandling. Et alvorlig IKT-angrep mot godkjente informasjonssystemer vil kunne medføre betydelig skade på viktige samfunnsinteresser. Bestemmelsen omhandler kun godkjente informasjonssystemer, altså tilhørende virksomheter underlagt sikkerhetsloven, herunder hensynet til rikets sikkerhet. Politidirektoratet stiller derfor spørsmål ved at viktig bevismateriale fra overvåking med sikkerhetsgraderte informasjonssystemer ikke kan benyttes til strafferettslig formål.

§ 23 Autorisasjonsansvarlig og klareringsmyndighet

Bestemmelsens andre ledd foreslår å redusere antall klareringsmyndigheter til én for sivil sektor og én for forsvarssektoren, i tillegg til Etterretnings- og sikkerhetstjenestene.

Vestoppland politidistrikt uttaler i sitt hørings svar at de anser en vesentlig reduksjon av antall klareringsmyndigheter som hensiktsmessig for å sikre en enhetlig og godt faglig forankret praksis. Distriktet tiltrer forslaget om at det opprettes to klareringsmyndigheter, samt forslaget om en sentral sivil klareringsmyndighet underlagt Justis- og beredskapsdepartementet.

Kripos anser forslaget til reduksjon av antall klareringsmyndigheter som fornuftig. Kripos viser til at de etter politiregisterforskriften del 11 er behandlingsansvarlig for 17 av 19 av politiets sentrale registre. I henhold til forskrift om personellsikkerhet § 3-4 kan NSM eller klareringsmyndigheten kreve å få utlevert opplysninger og utfyllende opplysninger fra disse registrene i forbindelse med personkontroll. En reduksjon i antall klareringsmyndigheter vil etter Kripos vurdering sikre at denne typen informasjon behandles mer enhetlig og tilfredsstillende sikkert.

Politidirektoratet deler oppfatningen om at antallet klareringsmyndigheter må reduseres betydelig for å oppnå formålet om mer robuste kompetansemiljøer og en mer ensartet praksis, herunder styrking av rettssikkerheten til den enkelte som skal sikkerhetsklareres. En reduksjon til kun to klareringsmyndigheter vil imidlertid gi den sivile klareringsmyndigheten et betydelig større saksomfang. Dette vil etter direktoratets vurdering trolig medføre en "flaskehals" som sannsynligvis vil innebære at saksbehandlingstiden vil øke, hvilket vil være svært uheldig for de berørte virksomhetene.

Det følger av sikkerhetsloven § 21 tredje ledd 3. punktum at "Sikkerhetssamtale skal gjennomføres der dette ikke anses som åpenbart unødvendig." Direktoratet forstår begrunnelsen til lovforslaget § 23 slik at det er nødvendigheten av sikkerhetssamtale som krever en selvstendig begrunnelse, mens lovteksten synes å kreve at det er det åpenbart unødvendige som krever begrunnelse. Lovteksten forstått slik vil med andre ord alltid kreve sikkerhetssamtale dersom unnlattelse av dette ikke kan begrunnes tilstrekkelig som åpenbart unødvendig. Dersom aktuell bestemmelse skal forstås slik at det alltid må gjennomføres sikkerhetssamtale med mindre det kan begrunnes som åpenbart unødvendig, vil dette

underbygge sannsynligheten for økt saksbehandlingstid ved en reduksjon til kun to klareringsmyndigheter.

Lovforslaget begrunnes blant annet med at mange klareringsmyndigheter har få saker og liten kompetanse. Politidirektoratet behandler årlig et høyt antall klareringssaker¹. Størrelsen på politietaten og antall årlige klareringer bør derfor begrunne et behov for å ha en egen klareringsmyndighet. Politidirektoratet er av den oppfatning at de største sivile klareringsmyndigheter på størrelse med Norsk kommunikasjonskontroll og Politidirektoratet bør opprettholdes for at det sivile klareringsinstituttet ikke skal bli for sårbart.

§ 29 a Anskaffelser til kritisk infrastruktur

Departementet foreslår en ny bestemmelse som gir Kongen i statsråd kompetanse til å nekte en anskaffelse til norsk kritisk infrastruktur gjennomført, dersom det foreligger en ikke ubetydelig risiko for rikets selvstendighet og sikkerhet eller andre vitale nasjonale sikkerhetsinteresser. Det gis også hjemmel til å sette vilkår for enkelte anskaffelser. Bestemmelsen vil supplere dagens regler om sikkerhetsgraderte anskaffelser, og er ment å være en sikkerhetsventil. Bestemmelsen vil kunne komme til anvendelse på kritisk infrastruktur som ikke tilfredsstillere kriteriene for å bli utpekt som skjermingsverdig objekt. Bestemmelsen pålegger også virksomhetene en varslingsplikt.

Som forvalter av samfunnskritisk infrastruktur støtter Politidirektoratet endringsforslaget. Det er behov for en hjemmel for anskaffelser til kritisk infrastruktur som ikke faller inn under graderte anskaffelser så lenge politiets nasjonale IKT-system (både nødnett og politinett) i dag er ugradert. Det påpekes dog at informasjon om politiets IKT-infrastruktur kan være gradert selv om infrastrukturen i seg selv ikke behandler gradert informasjon.

Politidirektoratet mener det er viktig at eier av kritisk infrastruktur ilegges en varslingsplikt dersom en anskaffelse til kritisk infrastruktur kan innebære en sikkerhetsmessig risiko på nasjonalt nivå. Det fremgår av hovedpunktene i forslaget under punkt 2.7.2 at bestemmelsen vil kunne komme til anvendelse på kritisk infrastruktur som ikke tilfredsstillere kriteriene for å bli utpekt som skjermingsverdig objekt. Sett i lys av at en viktig sektor som olje- og energi fortsatt definerer seg utenfor sikkerhetsloven, er dette en viktig bestemmelse. Direktoratet viser til PSTs åpne trusselvurdering 2015, herunder forventet etterretningsaktivitet. Som følge av dette er det grunn til å tro at fremtidige offentlige anskaffelser knyttet til kritisk infrastruktur vil kunne gi verdifull informasjon for en etterretningsaktør.

Politidirektoratet mener imidlertid at det er av stor betydning at også andre enn virksomheten selv gis adgang til å varsle det ansvarlige departement for virksomheten. Årsaken ligger i at virksomheten selv kan ha økonomisk interesse i å unnlate å varsle om en slik risiko ved anskaffelsen, og dermed ta en kalkulert risiko med at departementet ikke av eget initiativ finner grunn til å undersøke anskaffelsen nærmere. Oslo politidistrikt bemerker i sitt høringssvar risiko for ulik forståelse av loven på dette punktet, og redegjør nærmere for dette på side 3 i høringsuttalelsen.

Videre finner Politidirektoratet det nødvendig å understreke behovet for at "kritisk infrastruktur" defineres i § 3, i likhet med andre sentrale begreper i loven. Det vises her til

¹ 2010: 724 saker, 2011: 714 saker, 2012: 920 saker, 2013: 941 saker, per 1.halvår 2014: 464 saker

NOU 2006:6 Når sikkerheten er viktigst. (Beskyttelse av landets kritiske infrastrukturer og kritiske samfunnsfunksjoner.)

Oslo politidistrikt skriver i sitt høringssvar at det bør vurderes hvorvidt hele eller deler av politiets IKT-infrastruktur bør defineres som kritisk infrastruktur. Videre skriver distriktet følgende:

"Oslo politidistrikt bifaller departementets formål om å etablere et rettslig grunnlag for å stille sikkerhetsmessige krav til kritisk infrastruktur som p.t. faller utenfor sikkerhetsloven. Oslo politidistrikt ser imidlertid at lovforslaget kan gi implikasjoner for forvaltning av politiets IKT-infrastruktur. Oslo politidistrikt overlater i lys av dette til Politidirektoratet å vurdere lovforslagets betydning for politiet i sin helhet, herunder i hvilken grad IKT-infrastrukturen i politiet vil måtte redefineres som en del av nasjonal kritisk infrastruktur jfr. sikkerhetsloven"

Politidirektoratet ser at det kan være nødvendig å vurdere om hele eller deler av politiets nasjonale IKT-system faller inn under sikkerhetsloven gitt politiets oppgave i å opprettholde befolkningens trygghetsfølelse, slik Oslo politidistrikt påpeker i sitt høringssvar. Politidirektoratet ser at det kan være nødvendig å vurdere om hele eller deler av politiets nasjonale IKT-system faller inn under sikkerhetsloven gitt politiets oppgave i å opprettholde befolkningens trygghetsfølelse, slik Oslo politidistrikt påpeker i sitt høringssvar. Det er kjent at det er et behov for nasjonale løsninger for behandling og kommunikasjon av sikkerhetsgradert informasjon. Det vil imidlertid kreve en beslutning i samarbeid mellom politiet, som en betydelig informasjonseier, og departement dersom dagens nasjonale IKT-infrastruktur skal redefineres til å behandle og kommunisere sikkerhetsgradert informasjon.

Dersom det besluttes at et nasjonalt IKT-system for å imøtekomme de kommuniserte behovene skal sikkerhetsgodkjennes etter sikkerhetsloven, vil dette medføre betydelige kostnader, endring av teknologivalg, kompetanse, og betydelige organisatoriske og fysiske endringer.

Med hilsen



Knut Smedsrud
avdelingsdirektør



Kari-Grethe Stave
seksjonssjef

Vedlegg:

- Uttalelse av 02.07.15 fra Romerike politidistrikt
- Uttalelse av 10.07.15 fra Asker og Bærum politidistrikt
- Uttalelse av 30.07.15 fra Vestoppland politidistrikt
- Uttalelse av 03.08.15 fra Kripos
- Uttalelse av 06.08.15 fra Oslo politidistrikt

Kopi:

Justis- og
beredskapsdepartementet
Postboks 8005 Dep,
0030 Oslo



Politidirektoratet
Postboks 8051 Dep.
0031 OSLO

ROMERIKE POLICE DISTRICT

Deres referanse:
2013/00552-260/FD V 3/GCB/PAF

Vår referanse:
201503030-2 340

Sted, Dato
Lillestrøm, 02.07.2015

HØRINGSUTTALELSE

Forslag til endringer i lov 20. mars 1998 nr. 10 om forebyggende sikkerhetstjeneste (sikkerhetsloven)

Det vises til forsvarsdepartementets høringsnotat av 19. mai 2015:

Forslagene for å ivareta nye sikkerhetsmessige behov i §§ 5a, 10a, 13a og 29a, anses fornuftige og i tråd med samfunnsutviklingen. Dette anses også å gjelde forslag om endring i §§ 2, 9, 23 og 28.

Forslag om ny § 6a - åpner for å kunne gebyrfeste sikkerhetstjenester som utføres med hjemmel i loven.

Kommentarer - § 6a Gebyr

Majoriteten av landets virksomheter er styrt etter økonomi og profitt. En ordning med gebyr vil trolig svekke sikkerhetstilstanden over tid. Gebyr antas å gi konsekvenser for arbeidet med sikkerhetskulturen i virksomhetene.

Forslaget i § 6a anbefales tatt bort i sin helhet.

Med hilsen

Bjørn Vandvik
Politimester

Einar Svensen
Sikkerhetsleder

Romerike politidistrikt

Administrativ enhet
Post: Postboks 354, N-2001 Lillestrøm
Besøk: Jonas Liesgt 20

Tlf: 64 84 20 00
Faks: 64 84 20 01
E-post:
post.romerike@politiet.no

Org. nr.:
Giro: 7694.05.07959
www.politi.no



Politidirektoratet
Postboks 8051 Dep.

ASKER OG BÆRUM POLICE DISTRICT

0031 OSLO

(sendes også på e-post til postmottak POD)

Deres referanse:
2015/01983

Vår referanse:
201500847-2 008

Sted, Dato
Sandvika, 10.07.2015

HØRINGSUTTALELSE - FORSLAG TIL ENDRING I SIKKERHETSLOVEN

Det vises til direktoratets e-post 1. juni d.å., med Forsvarsdepartementets brev av 19. juni d.å. som bilag.

Asker og Bærum politidistrikt har gjennomgått de foreliggende forslag til endringer i sikkerhetsloven, og vi har følgende merknader:

Forslag til ny § 9 e – om VDI og NorCert funksjonene

Internett og IKT-avhengighet utgjør en sårbarhet i samfunnet generelt, og spesielt i forhold til kritisk infrastruktur og kritiske samfunnsfunksjoner (KIKS). Dette er noe Direktoratet for Samfunnssikkerhet og Beredskap blant annet peker på gjennom Nasjonalt Risikobilde 2014.

For å ivareta disse funksjonene mener vi det er viktig at det er noen som innehar en totaloversikt og kan avdekke og se de gjensidige avhengighetene. Utkastet peker på at VDI-systemet som hovedregel skal være basert på frivillighet, men at det bør være muligheter for å kreve dette gjennom forskrift. Nytt lovverk bør gi myndighetene muligheter for å kunne pålegge eiere/ innehavere av KIKS å være knyttet til VDI-systemet der risikobildet gjør dette påkrevet. Det samme bør være gjeldene for de avhengigheter knyttet til systemet.

Skjermingsverdige objekter utgjør bare en del av den samlede summen med KIKS objekter. På samme måte vil sårbarheter og gjensidige avhengigheter i samfunnet være mer omfattende enn de som er definert som skjermingsverdige objekter. Det er for totalbilde sin del, viktig at det sees i sammenheng. Vi mener derfor det er positivt at ny bestemmelse også vil omfatte slik kritisk infrastruktur og kritiske samfunnsfunksjoner, som ikke er omhandlet og definert som et skjermingsverdig objekt i dag.

Asker og Bærum politidistrikt

Politimesteren
Post: Postboks 415, 1302 Sandvika
Besøk: Kjørboveien 33

Tlf: 67 57 60 00
Faks: 67 54 86 34
E-post:
post.askerogbaerum@politiet.no

Org. nr.: 947 131 613
Giro:
www.politi.no

På samme måte er det viktig å se helheten i forhold til anskaffelser til KIKS nevnt i forlag til ny § 29a.

Med hilsen

Terje Nybøe
Politimester

Saksbehandler:
Henrik Hartmann
politioverbetjent

Kopi til:
june.kristin.bellika@politiet.no



Politidirektoratet
P.b. 8051 Dep.
0031 OSLO

VESTOPPLAND POLICE DISTRICT

Deres referanse:
201501983

Vår referanse:
201500867-2 008

Sted, Dato
Gjøvik, 30.07.2015

HØRING - FORSLAG TIL ENDRINGER I SIKKERHETSLOVEN.

Det vises til e-post av 1. juni 2015 fra Politidirektoratet med henvisning til Forsvarsdepartementets brev av 19. mai 2015.

Etter gjennomgang av de nærmere begrunnelsene for behovet for endringer sikkerhetsloven, er det ikke nødvendig herfra å komme med noen innsigelser eller tillegg til de konkrete lovforslagene. Forsvarsdepartementets synspunkt om at dagens utvikling innen teknologi og andre utviklingstrender, som økt globalisering, internasjonalisering, tverrsektorielle avhengigheter representerer nye sikkerhetsutfordringer for vårt samfunn tiltres.

Det er av viktighet at sikkerhetsloven er tilpasset de sikkerhetsbehov som ikke minst revisjonsarbeidet har avdekket. De lovendringer og nye bestemmelser som er foreslått fremstår som hensiktsmessige for å tilpasse aktuelle og mer fremtidige sikkerhetsbehov. I tillegg er det positivt at norsk lovgivning på sikkerhetsområdet harmonerer med andre lands lovverk, som vi ønsker å sammenlikne oss med. Forslagene støttes i sin helhet.

En vesentlig reduksjon av antall klareringsmyndigheter fremstår som særlig hensiktsmessig for å sikre en enhetlig og godt faglig forankret praksis. At det foreslås opprettet to klareringsmyndigheter, en for militær sektor og en for sivil sektor, støttes. Videre tiltres forslaget om en sentral sivil klareringsmyndighet underlagt Justis- og Beredskapsdepartementet.

Med hilsen

J. Martin Welhaven
politimester

Vestoppland politidistrikt

Vestoppland politidistrikt
Post: Postboks 54, 2801 Gjøvik
Besøk: Ibsensgate 1, 2821 Gjøvik

Tlf: 61151300
Faks:
E-post:

Org. nr.:
Giro:
www.politi.no



Politidirektoratet
Postboks 8051 Dep.
0031 OSLO

NCIS Norway

Deres referanse:
201501983

Vår referanse:
201501153

Sted, dato
Oslo, 3.8.2015

HØRINGSUTTAELSE – FORSLAG TIL ENDRINGER I SIKKERHETSLOVEN

Kripos viser til høringsbrev fra Forsvarsdepartementet av 19. mai 2015 vedrørende endringer i sikkerhetsloven, samt e-post fra Politidirektoratet av 1. juni 2015. I høringsnotatet foreslås det endringer i gjeldende bestemmelser i sikkerhetsloven, samt enkelte nye bestemmelser. Høringsfrist til Politidirektoratet er satt til 3. august 2015.

Innledende kommentarer

Det fremgår av side 2 i høringsnotatet at bakgrunnen for høringen er en evalueringsrapport utarbeidet av en flerdepartemental gruppe ledet av Forsvarsdepartementet. Revisjonen har avdekket behov for revisjon av sikkerhetsloven på flere områder, hvorav denne høringen ivaretar endringer i lovgivningen som det anses behov for å få raskt på plass.

Kripos imøteser det videre revisjonsarbeidet av sikkerhetslovgivningen og ønsker i den forbindelse allerede nå å peke på de utfordringer man i justissektoren erfarer knyttet til svak harmonisering av norsk regelverk opp mot EU-gradering av tilsvarende informasjon, ref. Norges avtale med EU¹. Videre viser beskyttelsesinstruksens § 12 til sikkerhetslovens forskrifter for krav til elektronisk behandling av dokumenter. Politiet behandler store mengder informasjon som graderes etter instruksens beskyttelsesgrader. Kravene som fremkommer i forskriftene kan synes rigide opp mot beskyttelsesinstruksens anvendelsesområde. Kripos legger til grunn at en bedret harmonisering vil bli omhandlet av det eksterne utvalget som er nedsatt med tanke på en mer omfattende revisjon av dagens regelverk.

Kripos har kommentarer til flere av de foreslåtte bestemmelsene som nå er på høring. Merknadene fremgår under.

¹ Nasjonal sikkerhetsmyndighet dok.nr. 200300338-28 310: "Agreement between the Kingdom of Norway and the European Union on security procedures for the exchange of classified information", signert 22.11.2004.

Kripos/

Ny § 13 a – sikkerhetsmessig overvåking av godkjente informasjonssystemer

Kripos støtter departementets forslag om innføring av ny § 13 a i sikkerhetsloven. Både den teknologiske og samfunnsmessige utviklingen tilsier en mulighet for økte sårbarheter med dertil behov for å avdekke og håndtere eventuelle angrep eller uregelmessigheter som kan true sikkerheten i godkjente informasjonssystemer.

Kripos ser at den typen overvåking av informasjonssystemene som det legges opp til i den foreslåtte bestemmelsen, hvor blant annet trafikk- og innholdsdata kan lagres for å avdekke sikkerhetstruende hendelser, vil kunne være kontrolltiltak av en til dels inngripende karakter for den enkelte. Selv om bestemmelsen i all hovedsak er en videreføring av dagens § 5-2 i informasjonssikkerhetsforskriften, og denne dermed også kunne utvides til omfatte innholdsdata, fremstår det som en god løsning å tydeligere regulere virksomheters egen adgang til sikkerhetsmessig overvåking som foreslått i ny § 13a hvor også hensynet til ansattes personvern ivaretas tilfredsstillende.

Endringer i § 9 – nærmere om oppgavene

Kripos ser seg enig i å lovfeste varslingsystemet for digital infrastruktur (VDI) og nasjonal responsfunksjon for alvorlige dataangrep mot samfunnskritisk infrastruktur (NorCERT). Disse to funksjonene er tett knyttet sammen og anses i økende grad nødvendig for å kunne ha et helhetlig sanntidsbilde over sårbarheter og trusler mot digitalt baserte samfunnskritiske funksjoner.

Kripos er oppmerksom på det Digitale sårbarhetsutvalgets kommende utredning av sårbarheter innen kritiske samfunnsfunksjoner og kritisk infrastruktur. Kripos har bidratt inn i dette arbeidet. I mandatet ligger at det også skal se inn i sivil-militært samarbeid og samarbeid mellom offentlige og private aktører. Resultatet fra dette arbeidet antas å kunne gi strategiske momenter vedrørende endringsforslaget for § 9.

Ny § 10a – behandling av personopplysninger

Kripos støtter departementets forslag til ny § 10. En klar rettslig regulering av Nasjonal sikkerhetsmyndighets behandling av personopplysninger vil skape en langt bedre forutberegnelighet for den enkelte og samtidig klargjøre adgangen til behandlingen av informasjon i langt større grad enn at det må foretas en skjønnsmessig vurdering etter personopplysningsloven § 8f.

All den tid departementet legger til grunn at personopplysningslovens bestemmelser kommer til anvendelse på behandlingen av personopplysninger i denne forbindelse, inkludert de aktuelle unntaksbestemmelsene, fremstår imidlertid den foreslåtte ordlyden som noe uklar. Etter Kripos' vurdering fremstår det som mer hensiktsmessig å fastslå det rettslige grunnlaget for behandlingen av personopplysninger i ny § 10a og deretter innta en henvisning til personopplysningsloven, dette for å unngå visse unøyaktigheter i ordlyden slik den fremstår i forslaget.

Endringer i § 23 – autorisasjonsansvarlig og klareringsmyndighet

Kripos er etter politiregisterforskriftens del 11 behandlingsansvarlig for 17 av 19 av politiets sentrale registre. I henhold til forskrift om personellsikkerhet § 3-4 kan NSM eller klareringsmyndigheten kreve å få utlevert opplysninger og utfyllende opplysninger fra disse registrene i forbindelse med personkontroll.

En reduksjon i antall klareringsmyndigheter vil etter Kripos vurdering sikre at denne typen informasjon behandles mer enhetlig og tilfredsstillende sikkert. Forslaget til reduksjon av antall klareringsmyndigheter fremstår for Kripos som et fornuftig tiltak i så måte.

Kripos vil i denne sammenheng også bemerke at vi finner personellsikkerhetsforskriften for å være for generell og vidtrekkende, noe vi antar det er mulig å komme tilbake til i forbindelse med den bredere gjennomgang av sikkerhetsloven.

Ny § 6a – gebyr

Kripos mener det er riktig å kunne gi en rettslig adgang til å fastsette forskrift om gebyr. I det videre arbeidet anser Kripos det svært viktig å avveie hvilke tjenester det skal tas gebyr for opp mot den økonomiske konsekvens som da tilkommer den enkelte virksomhet. Som eksempel kan prosessen for godkjenning av informasjonssystemer og kryptosystemer inneha stor økonomisk usikkerhet.

Ny § 5a – varslingsplikt mv. ved risiko for rikets selvstendighet og sikkerhet og andre vitale nasjonale sikkerhetsinteresser

Kripos støtter departementets forslag om innføring av ny § 5 a i sikkerhetsloven. Dette vil være med å gi bedre oversikt over truende aktiviteter og kunne motvirke trusler mot rikets selvstendighet og sikkerhet og andre vitale nasjonale sikkerhetsinteresser.

Med hilsen

Ketil Haukaas

Saksbehandlere:
Stein Damman
informasjonssikkerhetsleder
Telefon: + 4723208011

Christine Ask Ottesen
seniorrådgiver
Telefon: +4723208227



POLITIET

OSLO POLITIDISTRIKT

Politidirektoratet

OSLO POLICE DISTRICT

Deres referanse:
201501983

Vår referanse:
201504168-5 008

Sted, Dato
Oslo, 6.8.2015

HØRINGSUTTALELSE FRA OSLO POLITIDISTRIKT AD FORSLAG TIL ENDRINGER I LOV AV 20. MARS 1998 NR. 10 OM FOREBYGGENDE SIKKERHETSTJENESTE (SIKKERHETSLOVEN)

BAKGRUNN

Det vises til epost fra politidirektoratet av 1. juni 2015 med henvisning til høringsnotat av 19. mai 2015 om forslag til endringer i lov av 20. mars 1998 nr. 10 om forebyggende sikkerhetstjeneste (sikkerhetsloven).

Oslo politidistrikt forstår at denne høringen tilhører første fase av en mer omfattende revisjon av sikkerhetsloven. I denne fasen foreslår Forsvarsdepartementet endringer i § 2, § 9, § 23 og § 28, samt forslag til innføring av fem nye bestemmelser gjennom ny § 5 a, ny § 6 a, ny § 10 a, ny § 13 a og ny § 29 a. Oslo politidistrikt forstår videre at regjeringen har oppnevnt et sikkerhetsutvalg som skal utrede nytt lovgrunnlag for forebyggende nasjonal sikkerhet gjennom en NOU ila høsten 2016.

DRØFTING

Generelt

Oslo politidistrikt er på generelt grunnlag positiv til at lovens formål og virkeområde oppdateres i takt med utviklingen i teknologi og samfunn med de nye sikkerhetsutfordringer som følger av dette. Oslo politidistrikt er eier av verdier og funksjoner som er gradert og/eller klassifisert iht. sikkerhetsloven m/ forskrifter. I tillegg vurderer Oslo politidistrikt at det kan være relevante sikkerhetsutfordringer i politiet som ikke entydig kan besvares av dagens sikkerhetslov. Om angjeldende verdier og funksjoner kan ha direkte eller indirekte påvirkning på nasjonal sikkerhet og beredskap bør vurderes i forbindelse med nevnte utredning av nytt lovgrunnlag. Oslo politidistrikt bifaller derfor det arbeidet som nå er startet med å regulere og forbedre forholdet mellom sikkerhetsloven og andre sikkerhetsrelaterte regelverk.

Når det gjelder de forslag som omfattes av nåværende høringsrunde, vurderer Oslo politidistrikt at lovendringene ikke synes å få vesentlig betydning for distriktets funksjonsevne

Post:
Besøk:

Tlf:
Faks:
E-post:

Org. nr.:
Giro:
www.politi.no

eller virksomhetsutøvelse, med forbehold av hva som vil følge av forskrifter. Oslo politidistrikt velger likevel å knytte særskilte merknader til følgende punkter:

Ad forslag til ny § 6 a: Om gebyr

Departementet foreslår innføring av gebyr for tjenester som utføres med hjemmel i sikkerhetsloven:

"Kongen kan fastsette nærmere forskrift om gebyr for tjenester som utføres med hjemmel i denne lov. Gebyret må være formålstjenlig, og gebyret skal ikke overstige kostnadene ved ytelsen."

Departementet beskriver at formålet er å gi dagens bestemmelse i forskrift om informasjonssikkerhet § 5-24 andre ledd (gebyr ved godkjenning av informasjonssystemer) en sterkere forankring ved lov. Departementet opplyser at det ikke har tatt standpunkt til hvilke eventuelle øvrige tjenester som det kan være aktuelt å kreve gebyr for, men nevner at sikkerhetsklarering av personell eller leverandører kan være tjenester hvor dette kan bli vurdert.

Departementet oppgir videre ytterligere to formål med en gebyrordning; *"...kunne bidra til at virksomheter som ber om en tjeneste i større grad foretar en reell vurdering av det aktuelle behovet for tjenesten.."* (egenandelsvirkning), samt at *"...den tjenesteytende virksomhet tilføres økte ressurser ved økt saksmengde"* (behovsbasert ressursinndekning).

Oslo politidistrikt får regelmessig henvendelser fra klareringsmyndigheter om utlevering av registeropplysninger og/eller straffesaksdokumenter ifm sikkerhetsklareringer. Sikkerhetsloven § 20 fjerde ledd: *"Registeransvarlig plikter å utlevere registeropplysninger uten hinder av taushetsplikt"*, jf. forskrift om personellsikkerhet § 3-3, 2. ledd: *"Dersom opplysninger nevnt i første ledd ikke gir tilstrekkelig grunnlag for en klareringsavgjørelse, kan NSM eller klareringsmyndigheten kreve å få utfyllende opplysninger fra den behandlingsansvarlige for registeret"*.

Ved slike henvendelser opplever Oslo politidistrikt til dels store variasjoner mellom de ulike klareringsmyndigheter og saksbehandlere om hvilke saker det anmodes utlevering av. Enkelte anmodninger er rettet spesifikt mot enkeltsaker som klareringsmyndigheten av erfaring vurderer å ha betydning, mens anmodninger fra andre kan omfatte det totale antall saker registrert på personen. Dette uavhengig lengde på rulleblad, og til tross for at negativ klareringsavgjørelse antakeligvis vil kunne konkluderes ut fra kun et begrenset utvalg av straffesakene alene. Dette medfører for ofte unødvendig stort ressursbeslag for å innhente, kopiere, saksbehandle, ekspedere, samt å tilbakeføre den totale dokumentmengde til arkiv. Selv om Oslo politidistrikt forstår at innsynsbehovet vil kunne variere for den enkelte klareringsanmodning, stiller vi spørsmål til de sterkt varierende behov for innsyn som de ulike klareringsmyndigheter/saksbehandlere oppgir, og hvorvidt behovene for utfyllende opplysninger alltid er reelle mht. å fremskaffe et tilstrekkelig vurderingsgrunnlag.

Oslo politidistrikt vurderer at egenandelsvirkningen av et gebyr vil kunne bidra til å moderere innsynsbegjæringene fra klareringsmyndighetene dersom politiet gis mulighet til å avkreve gebyr av klareringsmyndighetene, tilsvarende det klareringsmyndighetene vil kunne gjøre ut til de som anmoder om klarering. Videre vil inntektsvirkningen ved økt saksmengde enklere kunne bidra til tilføring av ressurser. Ved å få tilgang til tilstrekkelige ressurser til å respondere

effektivt også ved økt saksmengde, vil politiet kunne bidra til å redusere den samlede tid en klareringsprosess tar. Således kan en gebyrordning isolert sett gi positiv samfunnsøkonomisk effekt. På den andre siden bør politidirektoratet vurdere nærmere de prinsipielle sidene ved at politiet skal fakturere klareringsmyndigheter eller andre virksomheter for slike tjenester. Dette også sett opp mot behandling av tilsvarende innsynsbegjæringer hjemlet i øvrig lovverk (fra domstoler, advokater, etc.).

Ad forslag til endringer i § 9: Om Nasjonal sikkerhetsmyndighets oppgaver

Departementet foreslår å utvide Nasjonal sikkerhetsmyndighets (NSM) lovfestede ansvar til også å omfatte operativ virksomhet:

"e. drive en nasjonal responsfunksjon for alvorlige dataangrep mot samfunnskritisk infrastruktur og et nasjonalt varslingsystem for digital infrastruktur."

Oslo politidistrikt stiller spørsmål til hvorvidt departementet i stor nok grad har redegjort for hensiktsmessigheten av at NSM som tilsynsmyndighet også skal tillegges det operative ansvaret for den nasjonale cyber- og informasjonssikkerheten. Videre i hvilken grad en slik innretning kommer i konflikt med uavhengighetsprinsippet mellom utførende og kontrollerende funksjoner. Det legges riktignok opp til at VDI og NorCERT skal underlegges EOS-utvalgets kontroll, men vi kan ikke se at departementet i sine vurderinger har gjort betraktninger mht EOS-utvalgets forutsetninger samt evne til reell kontroll på dette virksomhetsnivået; f.eks. hvorvidt kompetansespennet kan bli uhenksommessig langt mellom utførende og kontrollerende funksjoner.

Oslo politidistrikt har ingen forutsetninger til nærmere å vurdere legitimiteten til det eksplisitte endringsforslag, men ønsker på et generelt grunnlag å bemerke de prinsipielle komplikasjoner som følger av å lovfeste en organisatorisk innretning som kan oppfattes å komme i konflikt med sikkerhetslovens egen *forskrift om sikkerhetsadministrasjon, § 2-4 fordeling av oppgaver*. Prinsippet om separasjon mellom utførende og kontrollerende funksjoner gjenspeiles også i øvrige deler av sikkerhetsloven, underbygges av internasjonale standarder, og står svært sentralt i forståelsen av hvordan sikkerhetsarbeidet bør organiseres. For virksomheter underlagt sikkerhetsloven kan endringsforslaget til lovens § 9 fremstå som et paradoks til egen forskrift, bidra til en utilsiktet økning av tolkningsrommet for hva som er akseptabel og hensiktsmessig organisering av sikkerhetsarbeidet, derav devaluere betydningen av bestemmelsen.

Ad forslag til endringer i § 23: Om autorisasjonsansvarlig og klareringsmyndighet

Departementet foreslår å redusere antall klareringsmyndigheter betydelig:

"Kongen utpeker to klareringsmyndigheter, en for forsvarssektoren og en for sivil sektor..."

Vi har gjennom våre bemerkninger ad forslag om ny § 6 a, om gebyr (se dette), redegjort for våre erfaringer som følger av ulik praksis i klareringsmyndighetenes innsynsanmodninger til politiet. Oslo politidistrikt vurderer at forslaget om reduksjon i antall klareringsmyndigheter kan forbedre standardisering og kompetanse om reelt innsynsbehov i straffesaksregistrene, øke kvalitet og effektivitet på kildeinnhenting, bedre ivareta hensynet til personvern, samt bidra til å redusere den samlede behandlingstiden for klareringssaker.

Forslaget har videre formål om å sikre objektiviteten i vurderingsgrunnlaget for sikkerhetsklareringer. I dag er politidirektoratet egen klareringsmyndighet og sikkerhetsklarerer, med visse unntak, for alt personell i politiet. Oslo politidistrikt er opptatt av at klareringsinstituttets integritet gis de beste forutsetninger for å opprettholdes gjennom bl.a. tilstrekkelig avstand mellom klareringsmyndigheten og de personer som skal klareres. Forslaget vil ytterligere bygge opp om prinsippet om avstand mellom aktørene i sikkerhetsklaringsprosessen. Oslo politidistrikt støtter derfor forslaget om å redusere antall klareringsmyndigheter til to; én for forsvarssektoren og én for sivil sektor.

Ad forslag til ny § 29 a: Om anskaffelser til kritisk infrastruktur

Sikkerhetsloven inneholder bestemmelser som gir myndighetene adgang til å stille sikkerhetsmessige krav ved visse leveranser til norsk kritisk infrastruktur. Forutsetningen er at leveransen faller inn under lovens definisjon av sikkerhetsgraderte anskaffelser iht lovens § 3 jfr. forskrift om sikkerhetsgraderte anskaffelser § 2-1. Definisjonen av sikkerhetsgradert anskaffelse er knyttet opp mot at leverandøren vil kunne få tilgang til eller tilvirke sikkerhetsgradert informasjon, få tilgang til skjermingsverdig objekt, eller om informasjon om anskaffelsen i seg selv må sikkerhetsgraderes.

Lovens virkeområde fører imidlertid til at ikke alle anskaffelser til kritisk infrastruktur fanges opp av nåværende regler for sikkerhetsgraderte anskaffelser. Departementet foreslår derfor en utvidelse av lovens kapittel 7 sikkerhetsgraderte anskaffelser, til også å omfatte kritisk infrastruktur.

Endringer av lovens omfang og implikasjoner for politiet:

Departementet definerer i denne sammenhengen kritisk infrastruktur som *"anlegg og systemer som er helt nødvendig for å opprettholde samfunnets kritiske funksjoner og befolkningens trygghetsfølelse"*, og *"Med samfunnets kritiske funksjoner menes funksjoner som er absolutt nødvendig for å ivareta befolkningens grunnleggende behov"*. Videre listes en rekke eksempler som "nasjonal sikkerhet", "styring og kriseledelse", "trygghet for liv og helse", "lov og orden", m.fl.

Disse er alle områder som politiet er gitt et særlig oppgaveansvar for å lede og/eller bidra til ivaretagelse av; både i fredstid og i deler av konfliktspenning for øvrig. Per i dag er f.eks. verken nødnett eller "politinet" eksplisitt fanget av sikkerhetslovens bestemmelser, til tross for den sentrale understøttelsen begge infrastrukturene har til politiets operative funksjoner og ledelsesevne i beredskapssammenheng. I den utstrekning politiets IKT-infrastruktur vurderes å utgjøre en kritisk innsatsfaktor for politiets funksjonsevne, bør det samtidig vurderes hvorvidt hele eller deler av politiets IKT-infrastruktur bør defineres som kritisk infrastruktur jfr. sikkerhetsloven. Dette vurderes spesielt relevant i de tilfeller hvor infrastruktur understøtter bistandsressurser klassifisert som skjermingsverdige objekter jfr. samme lov m/ forskrifter.

Oslo politidistrikt bifaller departementets formål om å etablere et rettslig grunnlag for å stille sikkerhetsmessige krav til kritisk infrastruktur som p.t. faller utenfor sikkerhetsloven. Oslo politidistrikt ser imidlertid at lovforslaget kan gi implikasjoner for forvaltning av politiets IKT-infrastruktur. Oslo politidistrikt overlater i lys av dette til politidirektoratet å vurdere lovforslagets betydning for politiet i sin helhet, herunder i hvilken grad IKT-infrastrukturen i politiet vil måtte redefineres som en del av nasjonal kritisk infrastruktur jfr. sikkerhetsloven.

Vedr. krav til varsling

Departementet foreslår ny § 29 a som gjør en virksomhet pliktig til å varsle ansvarlig fagdepartement "...dersom en anskaffelse til kritisk infrastruktur som virksomheten eier eller råår over kan innebære en ikke ubetydelig risiko for rikets selvstendighet og sikkerhet eller andre vitale nasjonale sikkerhetsinteresser". Videre kan Kongen i statsråd nekte å gjennomføre anskaffelsen, eller sette vilkår for denne.

Med forbehold av hva som kan følge av forskrift, gir ikke lovforslagets § 29 a virksomhetene eksplisitte forpliktelser utover selve varslingsplikten. Imidlertid vil etterlevelse forutsette at virksomheten har tilstrekkelig kompetanse til å kunne vurdere i hvilken grad vilkår for varsling er oppfylt. Selv om det forutsettes at nærmere vurderingskriterier vil følge av forskrift, er Oslo politidistrikt usikre på om det i alle sammenhenger er hensiktsmessig at slike vurderinger skal knyttes til den enkelte anskaffelse, fremfor at varslingsplikten er forhåndsdefinert med utgangspunkt i den aktuelle infrastrukturens angitte klassifisering el. tilsv. Riktignok kan veiledere og instruksjoner nærmere forklare hva varslingsplikten vil innebære og redusere variasjon i skjønnsmessig vurdering mellom den enkelte anskaffelse til et system, men likefremt vil enhetlig forvaltning fordre tilstrekkelig krav til kontinuitet mellom de ulike anskaffelsesprosessene og/eller undersystemer. Dette vurderes å være spesielt krevende i tilfeller der systemansvaret deles mellom flere virksomheter.

Selv om Oslo politidistrikt bifaller formålet med å styrke det rettslige grunnlaget til å stille sikkerhetsmessige krav til kritisk infrastruktur som ikke faller inn under definisjonen om sikkerhetsgraderte anskaffelser, bemerkes risikoen som kan følge av ulik forståelse av loven. Ulike enkeltvurderinger rundt gyldigheten av varslingsplikten ifm komponentanskaffelser, kan i verste fall reversere samtlige forutgående sikkerhetsinvesteringer gjort i systemet. Innføring av ny § 29 a bør således være kompliment til, og ikke erstatning for, øvrig eksisterende regelverk vedrørende identifisering og klassifisering av objekter og infrastruktur.

AVSLUTNING

Oslo politidistrikt oversender sine bemerkninger til høringsforslaget som anmodet, uten ytterligere kommentarer.

Med hilsen

Åge Sandvik
avdelingsdirektør

Terje Kristiansen
politiinspektør

Dokumentet er elektronisk godkjent uten signatur.

Saksbehandler:
Anders Høye Tøraasen
Rådgiver sikkerhet
Telefon: 22669722