POLITIET
OSLO POLITIDISTRIKT

Politidirektoratet

OSLO POLICE DISTRICT

Deres referanse:	Vår referanse:	Sted, dato
201604064	201609139	Oslo, 31. desember 2016

HØRINGSSVAR NOU 2016:19 SAMHANDLING FOR SIKKERHET - NY SIKKERHETSLOV

Innledning

Det vises til oversendelse av overnevnte med frist for uttalelse til Politidirektoratet 23. desember. En kortere fristoversittelse beklages.

Arbeidsgruppen har vært gitt i oppdrag å vurdere hva som bør reguleres i lov for å sikre nasjonal sikkerhet, for å beskytte kritisk infrastruktur, kritiske samfunnsfunksjoner og sensitiv informasjon mot tilsiktede, uønskede hendelser, både for den militære og sivile sektoren, på en kostnadseffektiv og balansert måte.

Det nevnes områder som helse, vann, mat, energi, finansielle tjenester og kommunikasjon, og at det er et økende trusselnivå mot norske IKT- baserte informasjonssystemer, og sårbarhet øker. Det er krav om tidsriktige og dynamiske verktøy for beskyttelse mot IKT-trusler. Det vises til at mens sikkerhetsloven gir bestemmelser for håndtering av informasjon som er sikkerhetsgradert, og som skal beskyttes av hensyn til rikets sikkerhet og andre vitale nasjonale sikkerhetsinteresser, finnes det også i våre ugraderte systemer svært mye informasjon som kan være sensitiv og samfunnsviktig.

Videre er det vist til EU-kommisjonens forslag av 7. februar 2013 til direktiv om tiltak for å sikre et høyt felles nivå for nettverk- og informasjonssikkerhet i EU. Gjennom direktivet etableres sektorovergripende minimumsstandarder for nettverks- og informasjonssikkerhet. Direktivet omfatter offentlig forvaltning, tilbydere av informasjonssamfunnstjenester, samt eiere og driftere av samfunnskritisk IKT-infrastruktur. Implementering av direktivet vil kreve lovhjemmel.

I tillegg til sikkerhetsloven foreligger det i dag mange ulike lover og forskrifter som stiller krav til informasjonssikkerhet og som bør harmoniseres, og håndhevingsspørsmål må vurderes, herunder om det er hensiktsmessig å skille mellom tilsynsoppgaver og oppgaver som knytter seg til rolle som forvaltningsorgan. Videre skal det vurderes regulering av selskaper som håndterer informasjon, teknologi og/eller fysiske aktiva av betydning for samfunnets sikkerhet mv.

ENHET/AVDELING

Telefon: (+47)
Telefaks: (+47)
E-post: politi@politiet.no

Org. nr: 982 531 950 mva
Bankgiro: 7964.05.02388
www.politi.no

Det er pekt på at det foreligger internasjonal lovgivning, herunder nordiske lands lovgivning, gjeldende EU-direktiver, NATOs standarder, samt Norges folkerettslige forpliktelser på handels- og investeringsområdet.

Utredningen gjelder for en stor del andre samfunnsområder og oppgaver enn det som vedrører politiet. Vi har likevel enkelte merknader.

Merknader til kapittel 7 – Ansvar for og utøvelse av forebyggende sikkerhet, samt tilsynsfunksjon

Pkt 7.7.9 – Generelle krav til forebyggende sikkerhet
Utredningen signaliserer en overgang til mer funksjonelle krav. Dette vil fremtvinge diskusjoner av hva som er "godt nok". Med varierende risikoforståelse og kunnskap vil funksjonelle krav uten en minimumsstandard gjøre arbeidet både for den enkelte sikkerhetsleder og for tilsynsmyndighetene langt vanskeligere. Det vil også trolig gi et unødig høyt antall tvistesaker.

Dagen regelverk er detaljert, med plikt til å etablere risiko- og sårbarhetsbaserte tiltak utfra angitte minimumskrav. Ved å fjerne eksplisitte minimumskrav, antas det at avviket kan øke siden det vil skape grunnlag for økt usikkerhet. Sikkerhetsledere strever med å få forståelse for etablering av sikkerhetstiltak, og ved å gjøre kravene mindre presise vil dette ikke bli enklere. Forholdet er spesielt aktuelt for lavere nivåer i forvaltningen, hvor kunnskaps- og erfaringsgrunnlaget ofte er langt lavere enn i sentralforvaltningen. Dette samsvarer med FFI-rapport om sikkerhetstilstanden, der det påpekes at "modenhetsnivået" i norske virksomheter vedr sikkerhet er relativt lavt. I mange virksomheter er sikkerhetsoppgaver noe som enkeltansatte får tildelt ved siden av andre arbeidsoppgaver. Sett i sammenheng med manglende konkrete kompetansekrav, interne prioriteringer og tidspress, vil konkrete krav gjøre arbeidet for disse personene langt enklere.

Erfaringsmessig har arbeidet med etablering av sikkerhetstiltak etter krav i objektsikkerhetsforskriften vist seg mer krevende fordi den er mindre detaljert, og stiller derved større krav til kompetanse og erfaring hos sikkerhetspersonellet og andre involverte. Etter vår vurdering vil det vil ikke være mer kostnadseffektivt å redusere detaljgraden, da det vil bli mer kostbart og tidskrevende å vurdere sikkerhetstiltak samt følge opp at tiltakene faktisk fungerer. Det vil også kunne medføre store forskjeller i praktisk løsning mellom relativt like virksomheter. Videre vil en ved kun å stille funksjonelle krav overlate vurderingen i for stor grad til den enkelte virksomhet, skape grunnlag for unødige diskusjoner mellom virksomheter og kontrollmyndigheter, og komplisere kontrollmyndighetenes arbeid.

Som en sikkerhetsventil der virksomheten har vurdert og etablert for svake/dårlige sikkerhetstiltak, foreslår arbeidsgruppen at tilsynsmyndigheten vil kunne korrigere dette. Antall tilsyn sett i forhold til antall virksomheter samsvarer ikke med at en slik prosess har reell effekt.

Utvalget har diskutert om det er en fare for eventuell dobbeltregulering. Det vises i den sammenheng til dagens forskrift om sikkerhetsadministrasjon § 1-1, som stiller krav om samordning av tiltak. Manglende etterlevelse av denne bestemmelsen må sees i sammenheng med manglende konkrete krav til sikkerhetsutdanning, breddekompetanse og forvaltningserfaring hos sikkerhetspersonellet.

Ved revisjon av forskrifter til loven bør krav som er av teknologisk art vurderes beskrevet som *funksjonelle,* slik at en unngår stadige forskriftsendringer, men med krav om at minimumsstandard skal følge de av sikkerhetsmyndighetens krav til enhver tid. Kravene vil da kunne reguleres slik at de følger den teknologiske utviklingen bedre.

Merknader til kapittel 8 - informasjonssikkerhet

Pkt. 8.6.1 Beskyttelse av sikkerhetsgradert informasjon og tilhørende informasjonssystemer
Selv om det i lovforslaget anbefales å se begrepene *skjermingsverdig* og *sikkerhetsgradert* under ett, brukes begrepet skjermingsverdig flere steder i forarbeidene, som etter vår mening er et nyttig begrep som bør fastholdes.

Vi mener at enhetlig begrepsbruk er viktig. "Skjermingsverdig" er et kjent og innarbeidet begrep. Enhetlig begrepsbruk tilrettelegger for enhetlig behandling, ikke minst mellom ulike instanser.

Begrepet er også nyttig for å gi en grunnleggende forståelse for at det er informasjonens skjermingsverdighet og derav skadefølger som er grunnlaget for å sette en riktig gradering. Graderingsmerkingen er resultatet av en beslutning om behandling ut fra den skadevurderingen utsteder har foretatt. Likeledes vil det å fjerne minimumskrav til sikkerhetstiltak og kun basere seg på den enkelte virksomhets risikovurdering medføre at avsender ikke har kontroll på at de forutsetningene som er satt for behandling følges opp av mottakerne.

Pkt. 8.6.3 Informasjonssystemer og infrastruktur
Utvalget foreslår bruken av begrepet "skjermingsverdig informasjonssystem" om både ugraderte og graderte informasjonssystemer som må beskyttes. Begrunnelsen for å sikre også de ugraderte systemene støttes. Begrepet skjermingsverdig brukes i dagens terminologi. Dersom det benyttes også i annen kontekst med avvikende betydning kan det gi grunnlag for misforståelser.

Argumentasjonen for endringen av begrepet er helhetlige sikkerhetstiltak rundt informasjonssystemet. Etter vår oppfatning skal ikke en virksomhet ha helhetlig sikkerhet rundt et informasjonssystem, men snarere sikre sine informasjonssystem som del av helhetlige sikkerhetstiltak, som vektlegger gode, praktiske og hensiktsmessige løsninger for brukerne. Tydeligheten i kravet må derfor legges på verdivurderingen av informasjonssystemene med krav om sikkerhetstiltak og godkjenningsprosesser for både ugraderte og graderte systemer. Videre bør det i forskrift angis krav om at godkjenningsmyndighet skal vurdere om de helhetlige sikkerhetstiltakene i virksomheten generelt og informasjonssystemet spesielt er tilstrekkelige før systemet eventuelt godkjennes og tillates tatt i bruk.

Pkt. 8.6.7 Beskyttelsesinstruksen
Utvalget anbefaler å ikke ta beskyttelsesinstruksen inn i ny sikkerhetslov. Med bakgrunn i erfaringer med hvordan beskyttelsesinstruksen er kjent, oppfattes og etterleves, samt for å forenkle sikkerhetstiltak vil det etter Oslo politidistrikt oppfatning være hensiktsmessig å ta inn beskyttelsesinstruksen som lov.

Sikkerhetstiltakene i beskyttelsesinstruksen bærer preg av papirbasert forvaltning. Det er uklarheter i virksomhetenes tolkning av beskyttelsesinstruksen § 12, noe som gjør at enkelte virksomheter ikke oppfatter om de har en klar plikt til å etterleve kravet i § 12, eller om det er valgfritt basert på en lokal risikovurdering og tilgang til sikkerhetsgodkjente informasjonssystemer. Oslo politidistrikt erfarer at det praktiseres - dels bevisst - feilgradering av informasjon. F.eks. blir informasjon som burde vært sikkerhetsgradert BEGRENSET, i stedet merket som FORTROLIG. Dette for å kunne behandle det på et ikke sikkerhetsgodkjent system, som er det som er stilt til rådighet. Tilsvarende gjør manglende kjennskap til instruksens eksistens at informasjon ikke blir sikret ut over det som eventuelt følger av personopplysningsloven eller andre særlover.

Med dagens regelverk vil en nyansatt person i statsforvaltningen kunne gis tilgang til informasjon STRENGT FORTROLIG samme dag som en har blitt ansatt, uten at det foreligger videre vurderingsgrunnlag av personens kjennskap til interne rutiner, regler og skikkethet. For sikkerhetsgradert informasjon er det krav om autorisasjon, og som oftest sikkerhetsklarering. I både politiregisterforskriften og personopplysningsforskriften er det krav om autorisasjon basert på opplæring, tjenstlig behov og dokumentasjon på tilgangen. Med bakgrunn i at det er potensielt større og alvorligere skadefølger om uvedkommende får tilgang til beskyttelsesgradert informasjon anbefales det at det også i beskyttelsesinstruksen stilles krav om autorisasjon for tilgang. Kravet må omfatte opplæring, vurdering av skikkethet og en tydeliggjøring av taushetsplikten i tillegg til notoritet omkring autorisasjonen. Det bør vurderes om en kan se nytten av å bruke tilsvarende rutiner som gjelder for autorisasjon til BEGRENSET. Arbeidet bør ikke medføre merarbeid for den enkelte virksomhet utover at tilfeldig praksis standardiseres og settes i system. Effektiv forvaltning vil innebære at en foretar en helhetlig vurdering av tilgangs- og opplæringsbehovet og gjennomfører autorisasjonsprosessen ut fra konkrete behov.

Det foreslås at beskyttelsesinstruksen gis som lov. For å redusere kompleksitet bør sikkerhetstiltakene omfatte både nformasjonssikkerhet og personellsikkerhet, og være lik det som gjelder for sikkerhetsgradert informasjon. Sikkerhetstiltakene må ha definerte minimumskrav i tillegg til at de skal baseres på en risikovurdering. Det bør utpekes et fagmiljø som skal forvalte loven, herunder både faglig oppfølging og være tilsynsmyndighet.

Merknader til kapittel 9 – Objekt og infrastruktursikkerhet
Utvalget har ikke drøftet nøkkelpersonell og beredskapsressurser som en faktor som må beskyttes. Personell som er innsatsfaktorer til grunnleggende nasjonale funksjoner på lik linje med eiendom definert som skjermingsverdig objekt, bør gis tilsvarende beskyttelse. For eksempel er det klare krav til sikring av et jagerfly, men uten pilot er flyet ubrukelig. Tilsvarende vil gjelde for annet nøkkelpersonell som drifter kritiske ressurser. Per i dag berører verken lov eller forskrift nøkkelpersonell som verdiobjekter. Det bør derfor stilles krav til at den enkelte virksomhet skal vurdere beskyttelsestiltak for eget personell, herunder informasjon om personellet i egne informasjonssystemer.

Merknader til de enkelte bestemmelsene
Lovforslaget inneholder ingen legaldefinisjoner, i motsetning til någjeldende lov. Dette er uheldig.

§ 2-1 Departementets ansvar og myndighet etter loven
Den styrkningen av departementets ansvar som er foreslått støttes. Gjeldende sikkerhetslov med forskrift om informasjonssikkerhet § 3-1 gir overordnet forvaltningsorgan myndighet til å

godkjenne underliggende organ for behandling av sikkerhetsgradert informasjon. Denne bestemmelsen bør videreføres som en bestemmelse i ny forskrift om sikkerhetsstyring. Bestemmelsen baseres på lovforslagets § 2-1, første ledd bokstav a, og må gi overordnet myndighet plikt til å holde egen oversikt og rapportere til sikkerhetsmyndigheten hvilke virksomheter i egen sektor som er godkjent for behandling av sikkerhetsgradert informasjon eller som loven for øvrig skal gjelde for. Bestemmelsen vil gi grunnlag for følgende forhold:

- Budsjett (basert på faktiske oppgaver)
- Godkjenning av informasjonssystemer (til aktuelt godkjenningsnivå for virksomheten)
- Høyest tillatte nivå å anmode om sikkerhetsklarering i virksomheten (rettsikkerhet og kapasitet hos klareringsmyndighet)
- Kontroll, tilsyn og inspeksjon
- Kompetansebehov
- Grunnlag for å vite hvem som kan motta og behandle sikkerhetsgradert informasjon

§ 2-2 pkt d (Sikkerhetsmyndigheten)
Grunnlaget for at sikkerhetsmyndigheten skal være i stand til å holde tverrsektoriell oversikt over virksomheter som er godkjent for behandling av gradert informasjon, er at det enkelte departement holder sikkerhetsmyndigheten orientert om godkjenninger gitt i egen sektor. Bestemmelsen er viktig også for at sikkerhetsmyndigheten skal være i stand til å støtte forvaltningen med tilstrekkelige ressurser ut fra konkrete behov, som f. eks. kurs/opplæring, bemanning mv for å sikre en god og hensiktsmessig tjeneste.

§ 2-3 Informasjon om trusselvurderinger og risikohåndtering
Bestemmelsen angir et ansvar for å formidle relevant informasjon til underliggende etater. Forslaget vil være et viktig element for å skape en omforent risikoforståelse og evne til å etablere og vedlikeholde dynamiske sikkerhetstiltak i fredstid, noe som igjen legger grunnlag for evne til å reagere bedre ved økt beredskap. Det vil i tillegg være ønskelig at fagmyndigheter følger opp trusselinformasjon med anbefalinger om tiltak.

§ 3-1 Tilsyn med virksomheter
Det legges opp til et skille mellom sektorer som har en sikkerhetsorganisering som gjør at de er i stand til å følge opp i egen sektor eller etat, og sektorer som ikke har etablert tilsvarende ordninger. Dagens regelverk gir overordnet ansvar og myndighet på eget og underlagt nivå – herunder ligger en plikt til å kontrollere egen virksomhet mv.

Nye bestemmelser må styrke og ikke svekke kravet til overordnet virksomhets plikt til kontroll. En svekkelse av sektormyndighetens plikter vil ikke bare stride mot ansvars og nærhets- og likhetsprinsippet men også gjøre at sikkerhetstiltak ikke får nødvendig prioritet eller blir tilstrekkelig implementert i etatsstyringen. Erfaringsmessig er det over år vist en klar sammenheng mellom manglende overordet kontroll, og sikkerhetstilstanden hos underliggende virksomheter. Antallet virksomheter som er underlagt loven gjør at verken sikkerhetsmyndigheten eller enkelte sektortilsyn vil være i stand til å ha tilstrekkelig kapasitet til å gjennomføre tilsyn som gir et tilstrekkelig klarhet i sikkerhetstilstanden, samt å etablere og opprettholde den hyppigheten som det erfaringsmessig er nødvendig å ha for å sikre en kvalitetsmessig tilstrekkelig god sikkerhetstjeneste. Forholdet må sees i sammenheng med merknadene gitt til § 2-1.

Det foreslås derfor at § 3-1 legger opp til en tilsynsmyndighet som i dag, men at det i § 2-1 tilføyes et nytt punkt d. Punktet må tydeliggjøre det enkelte departements (og andre

overordnede virksomheters) plikt til å føre kontroll med, og inspisere underlagte virksomheter. Det må forventes at det enkelte departement har evne til å gjennomføre slik kontroll på lavere nivå sett i sammenheng med det generelle ansvaret og myndighet departementet har for kontroll med sikkerhetstilstanden, godkjenninger og oppfølging av underlagte virksomheter eller vedtak om at andre virksomheter underlegges loven. Dette vil også føre til en klarere ansvarliggjøring, samt at sikkerhetsstyringen følger anerkjente prinsipper for kvalitetsledelse.

De sektorer som i dag har kapasitet og kompetanse til gjennomføring av kontroll i egen sektor eller etat, vil kunne gjøre dette videre. Sikkerhetsmyndigheten vil som nasjonal fagmyndighet også være den høyest rangerte tilsynsmyndigheten og være et komplement til sektorenes inspeksjoner, men også ha en svært viktig rolle med kontroll og oppfølging av sektorenes kontrollvirksomhet.

Ved tilsyn med departementer bør sikkerhetsmyndigheten sende rapport til SMK, ikke minst om det enkelte departement ikke følger opp sine plikter etter loven.
§ 3-2

Bestemmelsene om koordineringsplikt mellom tilsynsorganer er positivt. Hensikten må være at kapasiteten brukes fornuftig. Formålet som er beskrevet er for å hindre for stor belastning for tilsynsobjektet. Erfaringsmessig har belastningen for et tilsynsobjekt med sikkerhetstilstanden i virksomheten å gjøre. Samtidig vil en virksomhet med gode rutiner og effektiv sikkerhetstjeneste ikke oppleve et tilsyn som belastende, men som kompetansehevende og motiverende siden det anerkjenner og bekrefter nedlagt innsats. En virksomhet med dårlige rutiner og ineffektiv sikkerhetstjeneste vil kunne oppleve eller beskrive et tilsyn som "ødeleggende" eller "forstyrrende" for aktiviteten i lang tid fremover. Den reelle årsaken til denne opplevelsen skyldes det merarbeidet som oppstår på bakgrunn av tilsynet. Dette er oppgaver som skulle vært utført tidligere, men som virksomheten ikke har, eller har hatt evne og eller vilje til å utføre. Manglende kontroll, eller lang tid siden sist kontroll fra overordnet virksomhet eller sikkerhetsmyndighet er også ofte en medvirkende årsak til manglende fokus og prioriteringer. Koordineringsplikten må derfor ha som formål å sikre at flest mulige virksomheter blir kontrollert og at ressursene som brukes på kontroller blir best mulig utnyttet.

§ 3-4 Stedlig tilsyn
Som del av forskrift må det gis bestemmelser om hvilke krav som stilles til legitimering av tilsynsmyndighet. Hensikten er å unngå at noen kan skaffe seg adgang til områder eller opplysninger ved å opptre som falsk tilsynsmyndighet. Tiltaket vil også legge forholdene til rette for tillit mellom tilsynsmyndighet og kontrollert virksomhet.

§ 4-2 Sikkerhetsstyring
Dagens krav til kompetanse er definert som "tilstrekkelig i forhold til virksomhetens behov" uten at tilstrekkelighetsbegrepet er spesifisert ytterligere. Det kan stilles spørsmålstegn ved om dette er tilstrekkelig for å unngå for store variasjoner i forståelse og praksis. Etter Oslo politidistrikts oppfatning vil det være nødvendig med en definert minimumsstandard eksempelvis gitt i ny forskrift om sikkerhetsstyring. En slik bestemmelse kan også følges opp med at sikkerhetsmyndigheten plikter å ha en veiledningsnorm for kompetanse innen det enkelte fagområde, og plikt til å sikre et tilstrekkelig kompetansetilbud for å dekke behovet.

§ 4-3 Risiko og sårbarhetsanalyse
I kommentarene til denne bestemmelsen vises det til at rådgiving kan bidra til uheldige situasjoner bl.a. i forhold til regelverk og inhabilitet mv, og at sektormyndigheter må vurdere hvor langt man kan gå. Dette bør muligens også gjenspeiles i lovteksten.

§ 4-4 Krav til dokumentasjon
Det fremgår at hensikten med bestemmelsen er å legge til rette for tilsyn. Etter vår oppfatning må hensikten med dokumentasjon i en virksomhet må være å skriftliggjøre bestemmelser om organisering, herunder det som er angitt som krav i dagens forskrift om sikkerhetsadministrasjon kapittel 3. Dokumentasjonen brukes for å organisere egen virksomhets sikkerhetsarbeid.

Formålet med tilrettelegging for tilsyn i gjeldende lov var at sikkerhetsarbeidet skulle være basert på et klart definert regelsett slik det ble etablert med sikkerhetsloven m/forskrifter. Før denne trådte i kraft var bestemmelsene en samling med mer eller mindre kjente direktiver og instrukser som gjorde at kontroll med utførelsen ved flere anledninger førte til diskusjoner om hva som var gjeldende krav. Selve innføringen av sikkerhetsloven gjorde derved arbeidet med tilsyn og inspeksjon langt enklere og mer ensartet i forståelse av minimumskrav.

§ 4-5 Øvelser
Kravet om øvelser med en frekvens som sikrer at formålet med bestemmelsen ivaretas er meget positivt. Minimumskrav bør angis i forskriften vedr hyppighet mv.

§ 4-6 Varsling
Slik vi ser det, er det muligens bedre pedagogikk å benytte begrepet "rapportering" fremfor "varsling.

§ 5-4 Tekniske sikkerhetsundersøkelser
Selv om gjeldende lovs begrep "avtitting" er nokså ukjent ord, er det etter vår oppfatning nyttig å unngå ordet "innsyn" for en situasjon hvor noen "sniktitter". Innsyn benyttes i flere rettslige sammenhenger om det å skaffe seg lovlig adgang til informasjon.

§ 6-6 Inntrengningstesting av skjermingsverdige informasjonssystemer
Bestemmelsen gjelder kun når virksomheten ber om bistand. Etter vår oppfatning bør det også som del av et *tilsyn* vurderes om sikkerhetsmyndigheten skal ha mulighet til å gjennomføre de samme kontroller som utføres ved en penetrasjonstesting på sikkerhetsgodkjente systemer. Det bør stilles krav om at et slikt kontrolltiltak er basert på risikovurdering, eller ved klar mistanke om at etablerte sikkerhetstiltak ikke er tilstrekkelige.

§ 7-4 Testing av sikkerhetssystemer
Også dette gjelder når virksomheten anmoder om bistand. Etter vår oppfatning bør sikkerhetsmyndigheten ha mulighet for å teste sikkerhetssystemer i en virksomhet på selvstendig grunnlag.

Aktualitet for denne bestemmelsen samt forslaget til tilsvarende bestemmelse i § 6-6 vil særlig gjelde dersom sikkerhetstiltak ikke har konkrete minimumskrav som grunnlag, men kun baseres på den enkelte virksomhets vurdering.

§ 8-2 Sikkerhetsautorisasjon
Etter Oslo politidistrikts oppfatning er det ikke åpenbart hvorfor begrepet "sikkerhetsautorisasjon" innføres. "Autorisasjon" er kjent, og skulle uansett være tilstrekkelig.

Kravet om å holde sikkerhetsmyndigheten orientert om de som til enhver tid er autorisert synes som et ambisiøst krav. Autorisasjon er en aktivitet som medfører kontinuerlige endringer. Løpende innrapportering antas å medføre et betydelig merarbeid for sikkerhetsmyndigheten langt utover den effekten ordningen vil kunne ha. Det må forutsettes at sikkerhetsmyndigheten har tilgang til en effektiv søkefunksjon som også må omfatte at samtlige som autoriseres for BEGRENSET må registreres elektronisk av sikkerhetsmyndigheten. Slik oversikt finnes pr i dag kun hos autoriserende myndighet.

Som et tiltak for å sikre bedre etterlevelse av autorisasjonsregimet i den enkelte virksomhet anses det som mer formålstjenlig å pålegge den enkelte virksomhet å foreta rapportering av autoriserte til nærmeste overordnede virksomhet. Som tilsynsmyndighet har sikkerhetsmyndigheten hjemmel til å pålegge virksomheter å oversende gjeldende autorisasjonsliste for kontroll.

Manglende oppdateringer av autorisasjonsliste til overordnet myndighet vil gi grunnlag for at nærmeste overordnet virksomhet reagerer overfor underlagt virksomhet.
En utfordring i dag er manglende oversikt over hvor personellsikkerhetspapirer til en person som slutter er oppbevart. Her kan det knyttes krav til at om en sikkerhetsklarert person slutter i en virksomhet skal dette innrapporteres til klareringsmyndigheten. Tilsvarende innrapportering kan skje når personellsikkerhetspapirer overføres til ny arbeidsgiver. Dette vil gi grunnlag for den samme oversikten, basert på en viss risiko da den ikke uten videre omfatter alle personer autorisert for BEGRENSET. Den vil likevel kunne omfatte utenlandske statsborgere autorisert for BEGRENSET, siden godkjenning av om vedkommende skal kunne autoriseres avgjøres av vedkommende virksomhets klareringsmyndighet.
Ved autorisasjon for BEGRENSET er det ikke krav om sikkerhetsklarering, men slik autorisasjon skal ikke gis dersom vedkommende er nektet sikkerhetsklarering. Dersom en person blir nektet sikkerhetsklarering og senere skifter arbeidsgiver, er det mulig at ny arbeidsgiver ikke er kjent med forholdet og autoriserer vedkommende. Det bør derfor være krav om at forut for autorisasjon til BEGRENSET skal autoriserende myndighet kontakte klareringsmyndigheten og forsikre seg om at vedkommende kan autoriseres.

§ 9-1 Sikkerhetsgradert anskaffelse
Definisjonen omfatter ikke at en leverandør selv kan utarbeide sikkerhetsgradert informasjon. Dette er noe som leverandører gjør både i form av selve leveransen samt i form av intern sikkerhetstjeneste.

Det foreslås derfor at teksten gis et tillegg:
Med sikkerhetsgradert anskaffelse menes en anskaffelse som innebærer at leverandøren av varen eller tjenesten vil kunne få tilgang til <u>eller selv tilvirke</u> sikkerhetsgradert informasjon...

11-4 Straff
Det er etter vår oppfatning grunnlag for å stille spørsmålstegn ved om dagens straffenivå står i forhold til de samfunnsmessige konsekvensene som kan oppstå som følge av brudd på lovgivningen. Generelt ved sanksjoner på dette området vil gjelde at virksomheter kan

spekulere i å omgå krav og pålegg, dersom sanksjonsnivået ikke står i forhold til investerings- og driftskostnadene ved å etablere nødvendige tiltak.

Med vennlig hilsen

Sveinung Sponheim
visepolitimester

Saksbehandler:
Øyvind Steindal /RB
Telefon: 99208239