POLITIET
POLITIDIREKTORATET

Forsvarsdepartementet
Postboks 8126 Dep
0032 OSLO

NATIONAL POLICE DIRECTORATE

Deres referanse:	Vår referanse:	Sted, Dato
2015/3139	201803108-15 008	Oslo, 04.10.2018

HØRINGSSVAR - FORSKRIFTER TIL NY SIKKERHETSLOV

1. Bakgrunn

Vi viser til Forsvarsdepartementets høringsbrev 2. juli 2018. Frist for høringen er satt til 1. oktober 2018.

Politidirektoratet har forelagt høringen for underliggende enheter. Vedlagt følger høringsuttalelser fra Kripos, Politiets utlendingsenhet (PU), Politihøgskolen (PHS), Politiets Fellestjenester (PFT), Oslo- og Innlandet politidistrikt, og Politiets IKT-tjenester (PIT). Innspill fra underliggende enheter er også delvis innarbeidet i direktoratets høringssvar.

Ny lov om nasjonal sikkerhet (sikkerhetsloven) ble vedtatt 1. juni 2018.[1] Forsvarsdepartementet foreslår i den forbindelse tre forskrifter til lov om nasjonal sikkerhet (sikkerhetsloven). Ny sikkerhetslov ble andre gangs behandlet og vedtatt av Stortinget 6. mars 2018, og i det vesentlige slik det ble fremmet av regjeringen i Prop. 153 L (2016-2017) *Lov om nasjonal* sikkerhet. Regjeringens forslag til lovvedtak baserte seg på anbefalingen fra det regjeringsoppnevnte sikkerhetsutvalgets utredning som forelå høsten 2016, NOU 2016:19 *Samhandling for sikkerhet.* Ifølge høringsnotatet er loven med tilhørende forskrifter som nå er på høring, planlagt å tre i kraft 1. januar 2019.

Virkeområdet når det gjelder hvilke virksomheter som faller inn under loven utvides, men det er ennå ikke avklart hvordan dette vil slå ut i politiet. For politiet vil det være avgjørende for utvidelsen av lovens nedslagsfelt hva som vil omfattes av "grunnleggende nasjonale funksjoner", og dermed hva som vil utpekes som skjermingsverdige objekter og infrastruktur Innholdsmessig innebærer forslaget en dreining fra å være et detaljert regelverk til å stille mer funksjonelle krav. Direktoratet vil derfor i høringssvaret synliggjøre usikkerheten som er knyttet til mulige økonomiske og administrative konsekvenser for politietaten, se punkt 6 nedenfor.

[1] Lovvedtak 27 (2017–2018).

Politidirektoratet

Post: Postboks 8051 Dep., 0031 Oslo
Besøk: Fridtjof Nansens vei 14/16
Tlf: 23 36 41 00
Faks: 23 36 42 96
E-post: politidirektoratet@politiet.no
Org. nr.: 982 531 950
Giro: 7694.05.18020
www.politi.no

Politidirektoratet disponerer høringssvaret med utgangspunkt i Forsvarsdepartementets skisserte forslag til tre forskrifter og knytter direktoratets merknader til aktuelle paragrafer og/eller kapitler, som foreslått i departementets høringsnotat.

2. Politidirektoratets generelle merknader

Inndeling i ulike forskrifter og korttitler
Forsvarsdepartementet ber om innspill til hvor mange forskrifter som er hensiktsmessig, men foreslår i høringsnotatet en reduksjon av antall forskrifter til følgende tre forskrifter:

- forskrift om myndighetenes roller og ansvar for nasjonal sikkerhet (myndighetsforskriften)
- forskrift om klarering av leverandører og personell (klareringsforskriften)
- forskrift om virksomhetens arbeid med forebyggende sikkerhet (virksomhetsforskriften)

Forsvarsdepartementet ber videre om innspill på offisielle korttitler på de tre forskriftene.

Politidirektoratet støtter departementets forslag til inndeling i tre nye forskrifter og foreslåtte korttitler. Den skisserte inndelingen fremstår som ryddig og brukervennlig da de har ulike brukergrupper.

Politiets utlendingsenhet tar til orde for at det fastsettes én forskrift. Oslo politidistrikt støtter den skisserte inndelingen i tre forskrifter, men har innvendinger til disposisjonen av virksomhetsforskriften, og peker blant annet på mangler ved definisjoner av sentrale begreper og formålsangivelser mv. i alle tre forskrifter.

Overgang til funksjonelle krav
Oslo politidistrikt er positiv til at lovens virkeområde utvides, men fremhever at Forsvarsdepartementets forslag i forskriftene i stor grad oppfattes som en forenkling av dagens detaljerte regelverk, og er på denne bakgrunn bekymret for at forenklingen har gått for langt.

Kripos støtter overgangen til mer funksjonelle krav, men peker samtidig på konsekvenser overgangen vil kunne medføre knyttet til økt ressursbruk hos virksomhetene, behov for at forebyggende sikkerhetsarbeid i større grad integreres i den øvrige virksomheten, samt behovet for tilstrekkelig kapasitet hos myndigheter med tilsyns- og rådgivningsansvar.

Politidirektoratet støtter merknadene til Oslo politidistrikt og Kripos.

Utveksling av trusselvurderinger og annen sikkerhetsinformasjon
I høringsnotatet punkt 4.3 drøfter departementet om det er behov for ytterligere presiseringer i forskriften om hvordan NSMs plikt til å tilrettelegge for informasjonsutveksling skal løses, og kommer til at det ikke er behov for ytterligere presiseringer enn det som allerede følger av ny sikkerhetslov § 2-3.

Som departementet viser til vil ny sikkerhetslov innebære at den enkelte virksomhet må ta et større ansvar for egen forebyggende sikkerhet. Den nevner også at en reell evne til å ta dette ansvaret vil avhenge av tilgang på trusselvurderinger og annen relevant informasjon for å styrke egen evne til forebygging og beskyttelse. NSM er gjennom loven gitt et særlig ansvar for å legge til rette for tilgang til slik informasjon.

Politidirektoratet deler ikke departementets syn på at det ikke er behov for nærmere presiseringer eller avklaringer av roller og tilretteleggingsansvaret. Politidirektoratet mener at verken forarbeid, lov eller forskrift i tilstrekkelig grad peker på konkrete og forpliktende tiltak og instrumenter for at NSM skal løse dette oppdraget, og hvordan dette praktisk skal løses i kombinasjon med rollen og utgangspunktet de har som sikkerhetsmyndighet i EOS-samarbeidet.

For det første besitter politiet (og PST) kunnskap om kriminaliteten (trusler) som er relevant kunnskap for virksomheter som skal etablere egenevne til å beskytte seg. For det andre er det grunn til å peke på at rollen som forplikter NSM til å tilrettelegge for informasjonsutveksling, er vanskelig i kombinasjon med NSMs rolle som EOS-tjeneste.

Det er på denne bakgrunn uheldig at NSM alene skal ha tilretteleggingsansvaret, uten en nærmere presisering og/eller avklaring av to konkret forhold. For det første hva som er politiets rolle hva gjelder utveksling av trusselvurderinger og annen sikkerhetsinformasjon, og for det andre, hvordan NSM skal sikre en reell og riktig informasjonsutveksling i kombinasjon med NSMs rolle som EOS-tjeneste. Sistnevnte er begrunnet i at det privat-offentlig samarbeid og informasjonsutveksling hovedsakelig og primært skal skje med utgangspunkt i EOS-samarbeidet med de begrensninger som alltid vil gjelde for dette samarbeidet.

Deteksjon, analyse og informasjonsdelen står sentralt i enhver forebyggingsstrategi, og er særlig relevant for forebygging av IKT-kriminalitet. Vi mener politiet har de beste forutsetninger gjennom sitt oppdrag og mandat, til å være drivkraft og fasilitator for et informasjonsdelingsregime der alle sensorer for deteksjon av IKT-kriminalitet kan bidra og "høste" – innenfor et åpent og ugradert samarbeid. Det er i denne sammenheng naturlig å vise til mindretallet i Lysneutvalget, i spørsmålet om "forbedret nasjonal operativ evne gjennom samlokalisering"[2], side 273-275 i utvalgets rapport. Mindretallets standpunkt er godt begrunnet, og Politidirektoratet støtter de synspunkter og konklusjoner mindretallet fremmer.[3] Det vises i den forbindelse til Justis- og beredskapsdepartementets høringsbrev av 9. desember 2015 og vedlagt høringssvar fra Politidirektoratet 18. mars 2016 til utredningen "Digital Sårbarhet – Sikkert samfunn" (NOU 2015: 13).[4]

3. Merknader til forslag til forskrift om myndighetenes roller og ansvar for nasjonal sikkerhet (myndighetsforskriften)

Kapittel 3 – nasjonal responsfunksjon for alvorlige digitale angrep og nasjonalt varslingssystem for digital infrastruktur

§ 12 Utøvelse av nasjonal responsfunksjon for alvorlige digitale angrep og nasjonalt varslingssystem for digital infrastruktur

Av forslag til myndighetsforskriften § 12 følger det at NSM skal drive en nasjonal *responsfunksjon* for alvorlige digitale angrep og et nasjonalt varslingssystem for digital infrastruktur (VDI). Denne oppgaven ligger til NSM i dag, og sikkerhetsloven § 2-4, som stadfester NSMs plikt til å tilrettelegge for informasjonsutveksling, er ikke ment å innebære en realitetsendring fra gjeldende sikkerhetslov. Departementet ber om høringsinstansenes syn på om NSM skal gis mulighet til å pålegge VDI-tilknytning for de virksomheter som blir underlagt

[2] 21.11.2 side 2.
[3] NOU 2015:13 Digital sårbarhet – sikkert samfunn.
[4] Justis- og beredskapsdepartementets referanse 15/8216 og Politidirektoratets referanse 201504848-16.

loven, og eventuelt hvilke rammer en slik påleggskompetanse bør ha.[5] Dette bør ses i sammenheng med direktoratets merknader til virksomhetsforskriften § 56 om tilknytning til varslingssystemet for digital infrastruktur omtalt her i punkt 4.

Politidirektoratet gjør oppmerksom på at dette punktet også har nær sammenheng med merknadene i punkt 2 fjerde avsnitt om *utveksling av trusselvurderinger og annen sikkerhetsinformasjon*. Ved revisjonen av eksisterende sikkerhetslov (da funksjonen først ble lovfestet) ble det fastsatt at funksjonen skulle legges til NSM – mens den i ny sikkerhetslov overlater til forskrifter og departement å peke på hvilken myndighet som skal ha funksjonen. Politidirektoratet vil påpeke at funksjonen mangler avgrensning og et tydelig mandat.

Såkalte digitale angrep er per definisjon kriminelle handlinger. Det er en primæroppgave for politiet å bekjempe kriminalitet. Dette kan omtales som kriminalitetsbekjempelsesfunksjonen. Etterforsking og straffeforfølgning er – i tillegg til forebygging – sentrale komponenter i kriminalitetsbekjempelsesfunksjonen. Politiet og påtalemyndigheten er alene gitt ansvaret for etterforskning og straffeforfølgning. Dette er det såkalte politimonopolet, fastsatt gjennom politiloven.

Forskriften tillegger ikke denne responsfunksjonen mer enn at den skal "innhente, analysere og dele informasjon om digitale angrep" (jf. § 12) og ha et særlig ansvar for å "informere nasjonale og internasjonale aktører om trusler, sårbarheter og mulige tiltak" (jf. § 13). Etter Politidirektoratets oppfatning har NSM gjennom sin NorCERT-funksjon, utviklet en praksis og en forståelse hos både overordnet myndighet, sektormyndigheter og andre, der funksjonen gjør langt mer enn dette. Det er flere momenter som bidrar til dette:

Det er for det først naturlig å forstå begrepet "responsfunksjon" som noe mer enn å "innhente, analysere og dele informasjon". Respons må nødvendigvis handle om å respondere – underforstått på den informasjonen man innhenter og de analysene man gjør. En nasjonal responsfunksjon må følgelig handle om at man også agerer og handler. Politidirektoratet etterlyser i den forbindelse en klargjøring av hva slags respons NSM har mandat til, hvilke faktiske handlingsalternativer de har, hvordan disse er avstemt med øvrige myndigheters lovpålagte responsansvar osv.

Politiets fullmakter, myndighet og definerte funksjoner er utfordrende i kombinasjon med NSMs koordineringsrolle og responsfunksjonen i NSM NorCERT. Det er derfor et behov for å klargjøre roller og ansvar mellom politiet og NorCERT. Det må komme klarere frem hvilke begrensninger som faktisk ligger i NSMs mandat og myndighet, og hvilke deler av "digital hendelseshåndtering" NSM og NorCERT verken har ansvar for eller utfører. Dette vil typisk være etterforskningsoppgaver og håndhevingsoppgaver som følger av fullmakter og ansvar gitt i blant annet politiloven.

Videre må det skilles tydeligere på det som handler om informasjonsflyt og koordineringstiltak på teknisk nivå for å håndtere digitale hendelser, og det som handler om nasjonal koordinering av den totale innsatsen ved krisehåndtering. Ved ulike former for krisehåndtering er det politiet som leder og koordinerer innsatsen for å "håndtere hendelser". Gjennom en uklart definert NorCERT-funksjon oppstår uklarheter rundt om kriser som oppstår som følge IKT-hendelser skal håndteres etter andre prinsipper. NorCERT skal koordinere innsats på teknisk nivå for å gjenopprette normalt drift på systemer. Resten av krisehåndteringen skal politiet

[5] Se departementets høringsnotat s. 26 punkt 6.3.1. siste avsnitt.

koordinere. Politiet skal også koordinere på tvers av sektorer og ta nødvendig ledelse når eventuelle motstridende hensyn oppstår, herunder konkret hensynet til å gjenopprette normal drift. Dette er det behov for å klargjøre.

Et annet sentralt moment som underbygger behovet for å klargjøre roller og ansvar mellom politiet og NSM, er forståelsen av "Nasjonalt rammeverk for digital hendelseshåndtering". Rammeverket drøftes i St. Meld. 38 (2016–2017) *IKT-sikkerhet – Et felles ansvar*[6], som gir en statusoppdatering på oppfølgingen av Lysneutvalgets anbefalinger i NOU 2015:13.

I stortingsmeldingen pekes det blant annet på at regjeringen ønsker å styrke samarbeidet mellom private og offentlige myndigheter, mellom sivile og militære virksomheter og på tvers av landegrenser, for å styrke IKT-sikkerheten. Det fastslås at et helhetlig nasjonalt rammeverk for digital hendelseshåndtering skal bidra til å «tydeliggjøre ansvar og roller for myndighetsaktører og andre sentrale aktører innenfor digital hendelseshåndtering», og «tydeliggjøre og styrke rammene for samarbeid mellom virksomheter, responsmiljøet i sektoren, NSM, Etterretningstjenesten, PST og politiet for øvrig».[7] Politidirektoratet mener at rammeverket ikke bidrar til å klargjøre roller og ansvar mellom de nevnte aktørene, slik stortingsmeldingen forutsetter. Rammeverket er, slik det fremstår nå, først og fremst egnet til å tydeliggjøre kommunikasjonslinjer og varslingslinjer. Hovedsakelig gjelder dette NSM sin rolle vis-av-vis sektorvise responsmiljøer og virksomheter. Ansvar, roller og faktisk håndtering mellom myndighetsorganer er mer omfattende enn dette.

4. Merknader til forslag til forskrift om virksomhetens arbeid med forebyggende sikkerhet (virksomhetsforskriften)

Kapittel 1. Sikkerhetsstyring

§ 2 Styringssystem for sikkerhet

Ny lov om nasjonal sikkerhet § 4-1 bruker begrepet "virksomhetens styringssystem" og forskriften § 2 bruker begrepet "styringssystem for sikkerhet". Bestemmelsene er i stor grad basert på strukturen og de viktigste prinsippene i standarden ISO/IEC 27001. Denne standarden bruker begrepet *ledelsessystem*.

Oslo politidistrikt mener at begrepet "ledelsessystem" bør benyttes, og begrunner dette blant annet med at "ledelsessystem" er bredere og mer dekkende uttrykk. Oslo politidistrikt mener videre at § 3 bør ses i sammenheng med og følge opp § 2 ved å stille krav til hva et ledelsessystem som et minimum skal inneholde av styrende dokumentasjon. Politidirektoratet støtter Oslo politidistrikts merknader, og mener det er uheldig at det benyttes forskjellige betegnelser.

§ 4 Sikkerhetsmål

Politidirektoratet har tidligere påpekt gjennom skriftlige innspill til forskriftsarbeidet at "sikkerhetsmål" kan sammenblandes med "sikringsmål" i Norsk standard 5832. "Sikringsmål" defineres der som ønsket eller akseptabel tilstand for en entitets verdier under eller etter en uønsket hendelse.
Videre er det uheldig at det i overskriften benyttes "Sikkerhetsmål", mens det i teksten kun benyttes begrepet "sikkerhetsnivå". Dette skaper unødvendig begrepsforvirring.

[7] St. Meld. 38 (2016–2017) punkt 7.2 på side 30 om *Rammeverk for digital hendelseshåndtering.*

I merknadene til bestemmelsen fremgår det at sikkerhetsmål kan være delmål. Sikringsmål etter NS 5832 kan også være et delmål for eksempelvis en avgrenset del av virksomhet som risikoanalysen omhandler. Dette bidrar til å innføre unødvendig nye begrep, når vi har etablerte begrep som dekker formålet og benyttes i dag.

§ 5 Roller og ansvar i det forebyggende sikkerhetsarbeidet
Eksisterende forskrift om sikkerhetsadministrasjon definerer et antall roller i sikkerhetsorganisasjonen. I forslaget til ny forskrift er det opp til virksomhetens leder å definere *antallet roller som er nødvendig*. Politidirektoratet gjør oppmerksom på at det kan være fare for at virksomhetsledere ikke har kompetanse til å vurdere ressursbehovet/omfanget av sikkerhetslovarbeidet i egen virksomhet.

Oslo politidistrikt mener bestemmelsen annet ledd bør endres og kommer med forslag til ny forskriftstekst, samt fremholder at bestemmelsens tredje ledd bør presiseres for å klargjøre at bestemmelsen forplikter (jf. formuleringen "skal om mulig"). Politidirektoratet støtter Oslo politidistrikts merknader.

§ 6 Ressurser og kompetanse
Politidirektoratet mener at kravet om å *bekrefte identiteten sin med legitimasjon* ikke synes å ha sammenheng med overskriften *Ressurser og kompetanse*.

§ 7 Tiltak ved sikkerhetstruende virksomhet, avvik og kompromittering av sikkerhetsgradert informasjon
I § 7 fastsettes tiltak virksomheten skal gjennomføre dersom den utsettes for blant annet "sikkerhetstruende virksomhet". Etter Politidirektoratets vurdering kan sikkerhetstruende virksomhet omfatte alle tilfeller av tilsiktede hendelser fra en ondsinnet aktør. Det inkluderer både de tilfellene der det er en statlig aktør med intensjoner som truer statssikkerheten – og alle andre tilsiktede hendelser der en aktør bedriver aktivitet som kan true "nasjonale sikkerhetsinteresser". Dette er straffbar aktivitet der enten PST eller politiet har et åpenbart mandat, og vil kunne falle inn under plikten til å anmelde forholdet til politiet, jf. straffeloven § 196. Denne plikten må stå like sterkt som varslingsplikten til NSM etter sikkerhetsloven § 4-5, og følgelig burde også en slik plikt etter Politidirektoratets syn komme klart frem i § 7.

Kapittel 2. Generelle krav til beskyttelse av skjermingsverdige verdier

§ 11 Plikt til å vurdere risiko
Departementet skriver i høringsnotatet punkt 7.3.1 at bestemmelsen til en viss grad tilsvarer gjeldende forskrift om sikkerhetsadministrasjon § 4-2 om risikovurdering, men fremholder at bestemmelsens materielle innhold og språk er endret en del.

Oslo politidistrikt er av den oppfatning at § 11 bør endres, og knytter sine merknader til bestemmelsens siste ledd. Kripos peker på § 11 første ledd bokstav a, viser til en oppfatning i enkelte fagmiljøer om enkelte trusselaktører, og fremholder at det bør legges bedre til rette for en reell trusselvurdering og valg av relevante scenarioer i dette sikringsarbeidet.

Politidirektoratet forstår bestemmelsens første ledd slik at den såkalte "tre-faktor tilnærming" for identifisering av risiko legges til grunn; gjennom identifisering av verdi, trussel og sårbarhet. Politidirektoratet støtter en slik tilnærming, som vil være i tråd med Norsk Standard 5830-serien og veilederen mot terrorhandlinger utarbeidet av NSM-PST-POD.

Politidirektoratet vil i den forbindelse kommentere følgende forhold nærmere: For det første vil vi advare mot en sammenblanding av to ulike type risikovurderinger i samme bestemmelse. Bestemmelsen regulerer både risikostyring av en virksomhets måloppnåelse i forhold til fastsatt sikkerhetsnivå, samtidig som den omhandler en plikt til å vurdere risiko for at uønskede hendelser (sikkerhetstruende virksomhet) skal ramme en virksomhets verdier.

Vi anbefaler at bestemmelsen kun omhandler plikt til å vurdere risiko for uønskede hendelser som rammer verdiene, og ikke risikoen for *hvorvidt sikkerhetsnivået ikke oppnås*. Evaluering av kravet til forsvarlig sikkerhetsnivå og evaluering av om styringssystemet er egnet til å sørge for at kravet til sikkerhetsnivå oppfylles, blir behandlet i § 8. Alt om dette bør samles der, da risiko knyttet til virksomhetens oppnåelse av fastsatt sikkerhetsnivå tilhører virksomhetsstyring. Politidirektoratet understreker viktigheten av at disse to risikoområdene ikke sammenblandes. Tre-faktormodellen er heller ikke nødvendigvis egnet verktøy for å måle risiko for måloppnåelse. Det kan være helt andre type trusler som kan true måloppnåelse, eksempelvis personalhåndtering som medfører at kritisk personell slutter. Risiko for måloppnåelse måles gjerne gjennom to-faktor tilnærming, hvor det vurderes sannsynlighet og konsekvens for at ulike type scenarioer kan inntreffe og true fremdriften. Politidirektoratet anbefaler at risiko for oppnåelse av sikkerhetsnivå flyttes til bestemmelsen i § 4 om sikkerhetsmål eller i § 9 om virksomhetens leders gjennomgang.

For det andre bør § 11 første ledd bokstav c om avhengigheter til andre virksomheter endres til en plikt til å kartlegge alle kritiske avhengigheter, både interne og eksterne. Politidirektoratet viser til bestemmelsens første ledd, som gir virksomheten en plikt til å ta hensyn til tre forhold i forbindelse med vurdering av risiko:

a) hvilken sikkerhetstruende virksomhet de skjermingsverdige verdiene kan bli utsatt for (trusler)
b) sårbarheter knyttet til de skjermingsverdige verdiene
c) i hvilken grad virksomheten er avhengig av andre virksomheter for å fungere som den skal

Både bokstav a) og b) legger indirekte til grunn at virksomheten vet hva som er sine skjermingsverdige verdier. Dette vet ikke en større virksomhet uten en systematisk kartlegging. Årsaken er at skjermingsverdige verdier ofte har en avhengighetskjede til svært mange innsatsfaktorer som må omfattes av sikringen. Ved uønskede hendelser medfører dette negative overraskelser, som man ikke forutså, men som kan ramme hardt.

Bestemmelsens bokstav c) om avhengigheter til andre virksomheter bør endres til en plikt til å kartlegge alle kritiske avhengigheter, både interne og eksterne, gjennom en systematisk verdivurdering. Videre bør denne bestemmelsen listes opp før hensynet til truslene og sårbarheter som er knyttet til disse avhengighetene/verdiene. Dette skyldes at man ikke finner trusler og sårbarheter knyttet til aktuelle verdier før disse verdiene er kartlagt.

Politidirektoratet foreslår derfor at § 11 første ledd endres til følgende:

Virksomheten skal identifisere, analysere og evaluere risikoen for sikkerhetstruende virksomhet rettet mot virksomhetens skjermingsverdige verdier. Det skal tas utgangspunkt i virksomhetens fastsatte sikkerhetsmål i § 4 som skal gi et forsvarlig sikkerhetsnivå. Når virksomheten vurderer risikoen skal den ta hensyn til

a) *systematisk kartlagte skjermingsverdige verdier og tilhørende avhengigheter, både interne og eksterne*
b) *hvilke trusler som kan true de skjermingsverdige verdiene og avhengighetene*
c) *sårbarheter knyttet til de skjermingsverdige verdiene*

Vi viser til politidirektoratets merknader til § 53 som også understøtter behovet for at § 11 endres.

§ 14 Prinsipper ved valg og utforming av sikkerhetstiltak og § 15 Krav om bruk av evaluerte produkter og tjenester

Til § 14 fremholder departementet at bestemmelsen som angir prinsippene ved valg og utforming av sikkerhetstiltak, hovedsakelig innebærer en videreføring av gjeldende forskrift om informasjonssikkerhet kapittel 5. Departementet foreslår at prinsippene skal gjelde for sikring av *alle* skjermingsverdige verdier, ikke bare for sikring av informasjonssystemer.

Oslo politidistrikt foreslår en formulering som innebærer at virksomheten "*så langt det er mulig [skal]følge prinsippene om…*".

På bakgrunn av kravet om at enkelte typer tekniske produkter eller tjenester må evalueres før de tas i bruk, foreslår departementet i § 15 en bestemmelse som fastsetter at virksomheten skal bruke evaluerte produkter og tjenester når virksomheten skal velge sikkerhetstiltak. Oslo politidistrikt mener at bestemmelsens formulering ikke gir noe informasjon om hva slags produkter og tjenester bestemmelsen viser til, og peker på hva bestemmelsen som et minimum bør inneholde med videre henvisning til anerkjente standarder. Distriktet viser i den forbindelse til bestemmelsene om dokumentsikkerhet i dagens regelverk som gir klare og enhetlige bestemmelser om dokumentbehandling, blant annet informasjonssikkerhetsforskriften kapittel 2-4.

Politidirektoratet støtter Oslo politidistrikts merknader til §§ 14 og 15 i sin helhet.

Kap. 3 Beskyttelse av skjermingsverdig informasjon

§ 20 Forsvarlig sikkerhetsnivå for skjermingsverdig informasjon

Politidirektoratet oppfatter utkastet til forskrift som at det er opp til virksomheten å iverksette tilfredsstillende tiltak for skjermingsverdig informasjon og informasjon gradert BEGRENSET. Dette kan medføre at informasjon gradert BEGRENSET vil kunne sikres ulikt, ut fra hvilken risikovillighet den enkelte virksomhetsleder måtte ha og hva virksomheten anser som *enkle midler*. Etter eksisterende lovgivning vil virksomheten ved utlevering av informasjon gradert BEGRENSET, ha en forståelse av hvordan mottakende virksomhet håndterer informasjonen. Vi mener på denne bakgrunn at forslaget i § 20 tilfører en usikkerhet rundt hvordan gradert informasjon håndteres ved informasjonsutveksling.

Kap. 4 Sikkerhetsgradering og merking

§ 26 Merking av dokumenter og lagringsmedier

Politidirektoratet har tidligere spilt inn viktigheten av at regelverket knyttet til merking etter sikkerhetsloven videreføres. For å unngå sammenblanding med annen merking, er det viktig at forskriftsteksten fortsatt angir at den skal være rød på dokumenter gradert etter sikkerhetsloven, med angivelse av merkingens innhold. Politidirektoratet anbefaler at tidligere forskriftstekst på dette inntas, noe som også støttes av Oslo politidistrikt.

Kap. 5 Beskyttelse av informasjon gradert KONFIDENSIELT eller høyere

Oslo politidistrikt har i sin uttalelse flere merknader til blant annet §§ 33 til 43. Distriktet foreslår blant annet endringer i forslag til § 33 om sending av informasjon gradert KONFIDENSIELT eller høyere, og forslag til presisering i § 37 med at et kontrollert område skal etableres og fungere som en buffersone rundt beskyttet og ev. sperret område. Distriktet er enig i at det etableres en oversikt over hvem som har adgang til beskyttet sone, men mener denne oversikten ikke skal være synlig utenfor området. Videre oppfordrer distriktet om å se § 35 om krav til oversikt over informasjon gradert KONFIDENSIELT eller høyere i sammenheng § 41 som regulerer krav for informasjon gradert HEMMELIG eller høyere, samt forslag til at gjeldende regler om registrering og bevaring av tilintetgjøringsbevis videreføres i tillegg til forslaget i § 41 om krav om destruering. Distriktet peker endelig på flere mangler ved bestemmelsen om krav til forsendelse med kurer (§ 43). Politidirektoratet støtter Oslo politidistrikts merknader, og viser til distriktets uttalelse når det gjelder de nevnte bestemmelsene.

§ 44 Beskyttelse av rom og lokaler gradert for KONFIDENSIELT eller høyere

Politidirektoratet oppfatter forskriftsforslaget slik at dagens bestemmelse om midlertidig sikring av rom for gradert tale når rommet er innenfor beskyttet område, foreslås fjernet (forskrift om informasjonssikkerhet §§ 9-2 og 9-11). For politiet er muligheten til å kunne skalere gjennom midlertidig godkjenning av møterom, svært viktig i beredskapssammenheng. Oslo politidistrikt peker på at bestemmelsen ikke angir konkrete krav til hva som er minimumstiltak og vurderer dette opp mot risiko for at det vil påløpe kostbare ekstratiltak i etterkant.

Kap. 7 Beskyttelse av skjermingsverdig objekter og infrastruktur

§§ 52, 53 og 55

Etter Politidirektorats oppfatning innebærer nye forskrifter en kraftig forenkling av gjeldende krav til sikring av skjermingsverdige objekter i forskrift om objektsikkerhet. Forenklingen fra mer rigide regler til kun én bestemmelse med funksjonsbaserte krav, medfører høyere krav til kompetanse innen risikovurdering, hos den enkelte virksomhet. Vi viser her til våre innspill til høringsnotatets punkt 5 om økonomiske og administrative konsekvenser i punkt 6 i høringssvaret. Videre vises det til Politidirektoratets endringsforslag til virksomhetsforskriften § 11 "*Plikt til å vurdere risiko*". Funksjonskrav i § 53 som regulerer forsvarlig sikkerhetsnivå for klassifiserte objekter og infrastruktur, forsterker også behovet for at § 11 endres i tråd med vår anbefaling.

Oslo politidistrikt mener at det som er essensielt og vesentlig for å forstå kravene til beskyttelse av skjermingsverdige objekter og infrastruktur, ikke fremkommer tydelig av forskriften kapittel 7, og viser til at dette er godt beskrevet i høringsnotatet generelt og i departementets merknader spesielt. Politidirektoratet er enig i dette, og viser til våre kommentarer til § 11.

Forskriften § 55 fastslår at en søknad om adgangsklarering må redegjøre for hvorfor virksomheten ikke kan iverksette andre egnede sikkerhetstiltak. Oslo Politidistrikt mener at forskriften mangler beskrivelse av formål med, definisjoner av og behovet for adgangsklarering og utvidet adgangsklarering, beskrivelse av anvendelsesområdene og vilkår for å anmode om iverksettelse, og fremholder dette bør tas inn i forskriften. Politidirektoratet er enig i dette, og mener at en slik presisering vil være klargjørende for den som anvender bestemmelsen i det daglige.

Kapittel 8. Nasjonalt varslingssystem for digital infrastruktur

§ 56 *Tilknytning til varslingssystemet for digital infrastruktur*
Etter gjeldende rett kan NSM og virksomheter som ønsker det, på frivillig grunnlag inngå avtale om tilknytning til varslingssystemet for digital infrastruktur (VDI), såkalt VDI-tilknytning. Forslag til ny virksomhetsforskrift § 56 er en videreføring av dagens system med *frivillig* VDI-tilknytning. Departementet vurderer muligheten for NSM til å kunne *pålegge* VDI-tilknytning. Departementet gjentar i høringsnotatet punkt 7.9.2 at alle virksomheter som underlegges loven bør være tilknyttet VDI, og ber også her om høringsinstansenes syn på en slik påleggskompetanse, og eventuelt hvilke rammer en slik påleggskompetanse bør ha. Departementet drøfter og utdyper videre hva som må reguleres i avtalen mellom partene for at tilknytningen til VDI skal få mest mulig effekt. Punktet må ses i sammenheng direktoratets merknader til myndighetsforskriften § 12 omtalt i punkt 3.

Politidirektoratet anerkjenner behovet for et robust og godt utbygget varslingssystem for digital infrastruktur. Vi støtter også at NSM gis påleggsmyndighet som innebærer å kunne pålegge virksomheter som faller inn under loven å være en del av slik varslingsinfrastruktur. Et godt utbygget sensornettverk er viktig for at NSM skal kunne bidra tilstrekkelig til kunnskap om trusselbildet og de sårbarheter som er under angrep.

Forskriften § 56 oppstiller et krav om at tilknytning til VDI skal skje gjennom en avtale mellom virksomheten og NSM, og at denne avtalen som et minimum skal regulere hvordan alvorlige angrep skal håndteres. I tilknytning til dette mener Politidirektoratet at det er sentralt at disse avtalene er innrettet slik at de ikke skaper tvil om de varslingsplikter og –adganger som foreligger (jf. f.eks. direktoratets merknad i punkt 4 til § 7 over, om strl. § 196). Det er også nødvendig at det i avtalen presiseres hvilke plikter og roller som følger av avtalen mellom virksomheten og NSM, og gjerne også ytterligere senker terskelen for å involvere politiet og ev. PST i de angrep VDI detekterer.

Kap. 9 Personellsikkerhet – § 58 og 59

Politidirektoratet mener at formuleringen "ikke er gitt sikkerhetsklarering" i § 58, som regulerer vilkår for å gi autorisasjon, ikke forenkler, men heller bidrar til mer uklarhet med hensyn til om manglende sikkerhetsklarering skyldes at det er søkt om klarering tidligere eller ikke. Også Oslo politidistrikt påpeker at forslag til formulering kan misforstås. Politidirektoratet foreslår at formuleringen endres tilbake til "person som etter avgjørelse ikke er gitt sikkerhetsklarering".

Vi peker også på at § 59 annet ledd er uklar og kan gi rom for misforståelser. Det vises til at ansvar/rolle som autorisasjonsansvarlig er klargjort i ny sikkerhetslov § 8-9 første ledd – *virksomhetens leder* [i bestemt entallsform]. Det kan neppe være tilsiktet direkte personlig fag- og saksansvar som må utøves av virksomhetens leder. Loven § 8-9 første ledd, sammenholdt med *tidligere autorisasjonsansvarlig* i forskriften § 59 annet ledd, gjør at § 59 blir noe uklar. Det er uheldig, siden § 59 annet ledd er utformet som en pliktregel. Det er også uklart om "*tidligere autorisasjonsansvarlig*" omfatter autorisasjonsansvarlig i annen virksomhet der omspurte subjekt har vært autorisert før, eller om det kun omfatter en tidligere leder som har autorisert samme person før i samme virksomhet, og som skal autoriser på ny. Politidirektoratet mener på denne bakgrunn at det er behov for presiseringer i § 59 annet ledd.
§ 62 Nødautorisasjon og § 63 om oversikt over personell med autorisasjon
Departementets forslag til endring i § 62 innebærer at det ikke lenger oppstilles et krav om at autorisasjon for høyeste nivå i nødrettstilfeller kun kan gis til personer som er klarert for et

lavere nivå. Oslo politidistriktet er uenig i forslaget, og fremholder at dagens krav om nødautorisasjon for STRENGT HEMMELIG bør videreføres. Oslo politidistrikt har også forslag til endring av formuleringen i § 63 siste ledd. Politidirektoratet tiltrer Oslo politidistrikts innspill til begge bestemmelser.

Kapittel 10 Sikkerhetsgraderte anskaffelser

Politiets fellestjenester mener blant annet at kapittelet generelt mangler definisjoner av begreper som benyttes i lov og forskriftene, og peker på enkelte begreper de mener bør endres og/eller presiseres.

§ 71 Krav til sikkerhetsavtalen etter sikkerhetsloven § 9-2 når leverandøren skal ha sikkerhetsgradert informasjon eller tilgang til skjermingsverdig objekt eller infrastruktur i eller fra sine egne lokaler
Politiets fellestjenester har merknader til § 71 første ledd bokstav a og bokstav c til d. Videre peker Politiets fellestjenester blant annet på hva som i tillegg bør fremgå av sikkerhetsavtalen.

§ 76 Forespørsel om leverandørklarering
Oslo politidistrikt foreslår at begrepet i setningen "klareringsmyndigheten" erstattes med "sikkerhetsmyndigheten" slik at setningen lyder som følger: "Oppdragsgiver skal be sikkerhetsmyndigheten om leverandørklarering".

Politidirektoratet støtter forslaget fra Oslo politidistrikt, da vi forstår regelverket som at også forespørsler om klarering av utenlandske leverandører skal gå gjennom den norske klareringsmyndigheten for leverandørklarering. Vi forstår det som at det er sikkerhetsmyndigheten som skal inneha denne rollen.

Politiets fellestjenester har i etterfølgende dialog med Politidirektoratet også påpekt at bestemmelsen bør regulere noe om hvordan man kan beskytte informasjon på nivå BEGRENSET hos utenlandske leverandører/underleverandører, og at dette kan utdypes i veiledningen. Det vises her til Politiets fellestjenesters utfyllende merknad til høringsuttalelsen 27. september 2018. Politidirektoratet er enig i at det er viktig med et klart og tilstrekkelig utfyllende regelverk for alle oppdragsgivere/anskaffende myndigheter som bruker utenlandske leverandører/underleverandører i forbindelse med sikkerhetsgraderte anskaffelser. Et forenklet regelverk med mindre regulering kan som ytterste konsekvens resultere i dårligere sikkerhet.

§ 77 Oversikt over sikkerhetsgraderte anskaffelser
Oslo politidistrikt mener at det i § 77 siste punktum bør kreves fortløpende innmelding av oversikt over sikkerhetsgraderte anskaffelser, ikke krav om at oversikten "årlig" skal innsendes klareringsmyndigheten som forslaget nå går ut på.

Politidirektoratet er enig i innspillet fra Oslo politidistrikt, og viser til at det ved autorisering av leverandører til nivå BEGRENSET kan oppstå en utfordring. Ettersom det ikke kreves leverandørklarering på dette nivået vil man ikke ha en mulighet til å bli varslet før avtaleinngåelsen dersom man er i ferd med å inngå avtale med en leverandør som tidligere har blitt nektet leverandørklarering.

5. Merknader til forslag til forskrift om klarering av leverandører og personell (klareringsforskriften)

Skillet mellom adgangsklarering og sikkerhetsklarering og §§ 3, 6, 7 og 8
Departementets forslag innebærer at det er tilstrekkelig med sikkerhetsklarering for KONFIDENSIELT eller høyere for å få tilgang de høyeste klassifiserte skjermingsverdige objektene (KRITISK OG MEGET KRITISK), jf. forslaget § 3. Dette uten hensyn til objektets klassifisering etter sikkerhetsloven § 7-2 første ledd.
Etter gjeldende rett kreves sikkerhetsklarering for HEMMELIG eller høyere for tilgang til objekter klassifisert MEGET KRITISK.[8]

Politidirektoratet har ikke innvendinger til at sikkerhetsklarering gjør det unødvendig med egen adgangsklarering. Dette er også forutsatt i ny sikkerhetslov § 8-3. Politidirektoratet kan imidlertid *ikke* slutte seg til forslaget om at sikkerhetsklaring for sikkerhetsnivået KONFIDENSIELT er tilstrekkelig for å få adgang til objekter med klassifiseringsgradene MEGET KRITISK OG KRITISK.

Vi viser til Forsvarsdepartementets høringsbrev av 17. oktober 2017 om høring om ny sikkerhetslov[9] og Politidirektoratets høringssvar 27. januar 2017, der vi fremholdt at skillet mellom adgangsklarering og sikkerhetsklarering er lite hensiktsmessig. Vi pekte også på at skillet mellom adgangsklarering og sikkerhetsklarering, herunder grunnlaget for en forenklet prosess for adgangsklarering, ikke syntes tilstrekkelig begrunnet og problematisert. På denne bakgrunn støttet ikke Politidirektoratet forslaget om å legge opp til flere typer klarering. Dersom skillet opprettholdes, mente vi følgende:

> *Dersom skillet mellom adgangsklarering og sikkerhetsklarering opprettholdes, må det etter vårt syn kreves sikkerhetsklarering for logisk adgang til et objekt som kan gi tilgang til sikkerhetsgradert eller sensitiv informasjon. Vi er av den oppfatning at det er risikofylt å videreføre bestemmelsen om at det er opp til den enkelte objekteier å be departementet om tillatelse til å sikkerhetsklarere personell med mulighet for å utrette omfattende skade på grunnleggende samfunnsfunksjoner.*

Nærstående m.fl. inngår i personkontrollen når en person anmoder om sikkerhetsklarering for nivå HEMMELIG og STRENGT HEMMELIG. Det følger av forslaget i § 3 at opplysninger om nærstående ikke vil være en del av vurderingsgrunnlaget og klareringsavgjørelsen som er avgjørende for om personen får adgang til skjermingsverdig objekt eller infrastruktur. Departementets vurdering i siste avsnitt i høringsnotatet kapittel 4.4.4 (s. 19) fremstår som mangelfull, særlig vurderingen av nærstående m.fl. og deres mulige betydning for objektsikkerheten.

Det er tungtveiende sikkerhetsmessige hensyn som tilsier at det for adgang til objekter klassifisert som KRITISK må kreves sikkerhetsgrad HEMMELIG, og at det for objekter klassifisert MEGET KRITISK kreves sikkerhetsgradering STRENGT HEMMELIG. Det vil sikre at opplysninger om personer som det er krav om for sikkerhetsklarering HEMMELIG - STRENGT HEMMELIG, fremkommer og blir del av vurderingsgrunnlaget for klareringsavgjørelsen som gir personen tilgang til objektet.

[8] Forskrift om objektsikkerhet § 3-6 annet ledd.
[9] NOU 2016:19 *Samhandling for sikkerhet – Beskyttelse av grunnleggende samfunnsfunksjoner i en omskiftelig tid med forslag til ny sikkerhetslov*.

Forskriftsforslaget § 3 står også i strid med forslaget i samme forskrift § 6 fjerde ledd om adgangsklarering for objekter klassifisert som MEGET KRITISK, jf. § 8. Dette fordi adgang til objektet i medhold av ordningen § 3 ikke vil fange opp det som § 6 fjerde ledd er ment å sikre.

Synspunktet over bør ses i sammenheng med forslag til § 8, som regulerer hva den som skal gis adgangsklarering skal opplyse om etter § 7. Slik Politidirektoratet forstår, vil adgangsklarering primært være aktuelt der det *ikke* er behov for sikkerhetsklaring for å beskytte skjermingsverdig informasjon. I § 8 er kravet til hvilke egenopplysninger vedkommende skal opplyse om forskjellig avhengig av om det kreves enkel eller utvidet adgangsklarering.

Politidirektoratet foreslår at følgende endringer foretas i § 8 for å harmonisere regelverket i tråd med sikkerhensyn:

- bestemmelsene i forskriften § 6 første ledd, bokstav a) og § 7 første ledd gjelder for adgangsklarering for objekter/infrastruktur med klassifiseringsgrad VIKTIG. Dette har tilfølge at tredje ledd i § 6 blir overflødig og kan utgå.

- bestemmelsene i forskriften § 6 første ledd, bokstav b) samt § 7 første og annet ledd gjelder for adgangsklarering for objekter/infrastruktur med klassifiseringsgrad KRITISK. Dette har tilfølge at fjerde ledd i § 6 blir overflødig og kan utgå.

- bestemmelsene i forskriften § 6 første ledd, bokstav c) samt § 7 første og tredje ledd gjelder for adgangsklarering for objekter/infrastruktur med klassifiseringsgrad MEGET KRITISK.

Politidirektoratets forslag til endring av § 8 innebærer at sondringen mellom enkel og utvidet adgangsklarering kan utgå, herunder i § 10 med hensyn til hvilke registre som er kildegrunnlag ved adgangsklarering. Ut fra sikkerhetsmessige, reelle og rettstekniske hensyn, bør adgangsklarering og sikkerhetsklarering etter Politidirektoratets syn være mest mulig sammenfallende med bakgrunn i sammenhengen mellom forskriften § 3, ny sikkerhetslov § 7-2 første ledd og § 8-3. Når sikkerhetsklarering alene skal være tilstrekkelig til å få adgang til skjermingsverdig objekt, og sikkerhetsklareringen bygger på opplysninger innhentet fra registrer angitt i forskriften § 9, er det vanskelig ut fra sikkerhetsmessige hensyn å se hvorfor adgangsklarering skal ha et annet regime slik det legges opp til i § 10.

§ 9 Registre for personkontroll ved sikkerhetsklarering og tilgang til informasjon fra samtlige av politiets arbeidsregistre

Gjeldende forskrift om personellsikkerhet[10] § 3-4 i inneholder en liste over relevante registre NSM kan kreve å få registeropplysninger fra som ledd i den innledende personkontrollen. Tre av de ti registrene nevnt i loven forvaltes av politiet: reaksjonsregisteret, straffesaksregisteret, og registre ved Politiets sikkerhetstjeneste. Forslag til endring i § 9 innebærer lovteknisk at NSM kan innhente og videreformidle opplysninger fra a) "politiets registre".

Endringen til "politiets registre" vil bl.a. omfatte det som i gjeldende forskrift § 3-4 nr. 1 og 2 er benevnt som reaksjonsregisteret og straffesaksregisteret. Det vil også omfatte politiets arbeids- og etterretningsregistre, slik praksis er i dag, og andre registre eller saksarkiv.[11] Det

[10] FOR-2001-06-29-722.
[11] Se høringsnotatet punkt 8.2.5 første og annet avsnitt.

følger av omtalen i lovproposisjonen til sikkerhetsloven § 8-5 sjette ledd, som det vises til i høringsnotatet side 78, at «relevante registre» også omfatter opplysninger som virksomheten har lagret på annen måte, eksempelvis i elektroniske saksarkiv. Det er således ikke av avgjørende betydning hvordan opplysningene er lagret i virksomheten.

Presiseringen knyttet til § 8-5 tilsier at NSM ved personellkontroll også skal ha tilgang til informasjon fra straffesaksløsninger og etterretningsregistre (En vesentlig del av informasjonen som finnes i disse registrene er gradert som følge av prinsippet om kildebeskyttelse og skjerming (Etterretningsdoktrine for politiet s. 20). Mye av det som er lagt inn i enkelte av disse registrene er også "råinformasjon" som ikke er satt i kontekst. Det er først når data og informasjon bearbeides og settes i sammenheng, at dette vil kunne gi full verdi i en personkontroll. Ett eksempel på dette er som følger: ved uttrekk fra etterretningsregisteret fremgår det at NN er oppført i en beslaglagt telefonbok til en kjent gjengkriminell. I en etterforsking av den kjente gjengkriminelle fremkommer at han har hatt telefonisk kontakt med NN 6 ganger. For at denne type informasjon skal gi noen "mening" må den settes inn i kontekst. Er kontakten av kriminell karakter eller er det snakk om avtale om kjøring av barn til fotballtrening?

Kripos mener den foreslåtte utvidelsen av adgangen til å utlevere opplysninger fra "politiets registre" favner for bredt. De peker på at bestemmelsen etter ordlyden omfatter alle politiets sentrale registre, herunder kriminaletterretningsregisteret, politioperative registre og informantregisteret. Det pekes på at det i merknadene til bestemmelsen er forutsatt at "politiets registre" også omfatter "politiets arbeids- og etterretningsregistre" mv. Videre vil det omfatte opplysninger innhentet med hjemmel i straffeprosessloven 16a, 16b og 16d og opplysninger fra spaning og etterforskning som ikke er inntatt i et register. Kripos mener at henvisningen til "politiets arbeids- og etterretningsregistre" i merknadene til bestemmelsen, er uklar. Det presiseres at politiet har ett sentralt kriminaletterretningsregister, og "arbeidsregistre" er ikke et uttrykk som brukes i politiet. Det er etter Kripos' syn uklart hvilke registre departementet mener å henvise til ved bruk av dette uttrykket.

Kripos trekker særlig frem analyse og bruk av opplysninger fra blant annet politioperative registre og kriminaletterretningsregistre, og fremholder at riktig bruk av opplysningene forutsetter kjennskap til politiets arbeidsmetoder, registerets funksjon, og ikke minst god kjennskap til etterretningsfaget, for å kunne avgjøre hvilken vekt opplysningene skal tillegges. Kripos mener NSMs adgang til å innhente opplysninger bør begrenses, og kommer med forslag til hvordan dette kan gjøres for enkelte registre. Kripos mener videre at NSM bør få bistand fra politiet til å analysere informasjon dersom informasjon skal utleveres fra politioperative registre og kriminaletterretningsregisteret.

Politidirektoratet minner om at en klareringsmyndighet skal forholde seg til faktaopplysninger ved avgjørelsen og ikke uverifisert informasjon. Politidirektoratet vil påpeke viktigheten av at all etterretningsproduksjon som foregår følger prinsippene for etterretning. I dette ligger blant annet at etterretningsproduksjonen må være underlagt sentralisert kontroll. Dette blir etter vår vurdering best ivaretatt dersom politiet gis et ansvar for å sammenstille informasjonen og samlet gi en vurdering av opplysninger før de oversendes til NSM. Politidirektoratet viser til Kripos' uttalelse.

§ 12 Behandlingsansvarliges plikter ved utlevering av opplysninger

I høringsnotatet punkt 8.2.8 fremgår det at bestemmelsen tilsvarer gjeldende bestemmelse i forskrift om personellsikkerhet § 3-4 fjerde ledd. Bestemmelsen må sees i sammenheng med

ny sikkerhetslov § 8-4 niende ledd om at behandlingsansvarlig skal legge til rette for digital overføring av opplysningene.

Det er i dag ikke mulig å foreta et enkelt søk som dekker alle de forskjellige registre og arkiv politiet benytter. Dette medfører at man må utføre manuelle søk. En del av arbeidsregistrene er heller ikke knyttet opp mot sentral server, men ligger knyttet til system og register lokalt hos politiet. Etter Politidirektoratets oppfatning understreker dette betydningen av at det opprettes en funksjon som har til oppgave å bearbeide informasjonen før de oversendes NSM.

Akkreditering av lufthavnansatte og adgangsklarering ved norske lufthavner

Fra 1. september 2016 ble det som en midlertidig ordning innført krav om at ansatte ved norske lufthavner som skal ha tilgang til sikkerhetsbegrenset område ved lufthavnene, skal akkrediteres av politiet før tilgang blir gitt, jf. forskrift om forebyggelse av anslag mot sikkerheten i luftfarten mv. (forskrift om sikkerheten i luftfarten)[12] § 35a jf. politiregisterforskriften § 38-5. Justis- og beredskapsdepartementet understreket at ordningen skulle være midlertidig, og at man tok sikte på å innta regler om adgangsklarering av lufthavnansatte i ny sikkerhetslov.

Akkreditering etter politiregisterforskriften § 38-5 innebærer at politiet foretar en vurdering av personer som skal gis adgang til bestemte områder hvor det av sikkerhetsmessige eller tungtveiende ordensmessige grunner er nødvendig med en kontroll av personen. Etter bestemmelsens tredje ledd skal politiet gi tilbakemelding til den sikkerhetsansvarlige kun om personen akkrediteres eller ikke. Det er så opp til sikkerhetsansvarlig å vurdere konsekvensen av manglende akkreditering. For luftfarten er dette regulert i forskrift om sikkerhet i luftfarten mv. § 35a. Kripos er av Politidirektoratet gitt oppgaven med akkrediteringer som er hjemlet i denne bestemmelsen.

Kripos framholder i sin uttalelse at akkrediteringsordningen ikke egner seg som en permanent løsning. Politidirektoratet ser også betenkeligheter med å benytte akkrediteringsordningen på denne måten og er enig i at ordningen ikke bør videreføres. For det første gir politiregisterforskriften ingen klagerett på politiets beslutning om ikke å akkreditere. Det er heller ingen begrunnelsesplikt, etter politiregisterforskriften § 38-5 skal den som akkrediterer bare gi tilbakemelding om vedkommende akkrediteres eller ikke (svare ja eller nei). For det andre vil den som nektes akkreditering i praksis heller ikke få innsyn i grunnlaget for beslutningen.

Retten til innsyn i opplysninger som er registrert i forbindelse med akkreditering reguleres av politiregisterloven § 49. Hensynet til nasjonal og offentlig sikkerhet i bestemmelsens fjerde ledd nr. 2 tilsier at det er nødvendig å unnta opplysninger om grunnlaget for beslutningen i alle saker om akkreditering. Bakgrunnen for at man ønsket å benytte akkrediteringsordningen var behovet for å kunne innhente en vurdering fra PST, og ikke at det var ment at det skulle opplyses om det var registrert opplysninger om personen eller ikke. Akkrediteringsordningen er opprinnelig beregnet på tids- og stedsavgrensede arrangementer. Det å bli nektet akkreditering til et konkret arrangement vil ikke utgjøre et stort inngrep for den enkelte. Politidirektoratet mener at det er større betenkeligheter knyttet til å benytte akkrediteringsordningen til å utelukke noen fra et område når det innebærer at de mister jobben. Kripos mener at et vedtak som kan få så store konsekvenser for enkeltmennesker bør kunne påklages og at dagens ordning bør erstattes av adgangsklareringsinstituttet i ny sikkerhetslov. Politidirektoratet er enig i det.

[12] FOR-2011-03-01-214.

I redegjørelsen for tematikken *adgangsklarering ved norske lufthavner* viser Kripos til sikkerhetsloven § 7-1 og støtter departementets betraktning i høringsnotatet punkt 4.4.1 om kompleksiteten ved sikring av infrastrukturer. Kripos vurderer videre sikkerhetsloven § 8-3, myndighetsforskriften § 2, samt viser til NOU 2016: 19[13] og Prop. 153 L (2016–2017)[14], og finner det uklart om innføring av adgangsklarering ved alle norske lufthavner vil avhenge av at luftfartsinfrastrukturen som helhet blir klassifisert som skjermingsverdig, eller om det er tilstrekkelig at deler av infrastrukturen, for eksempel knutepunktene, klassifiseres som skjermingsverdige.

Kapittel 5. Leverandørklarering
Ifølge departementet innebærer forslaget til § 31 (vurderingsgrunnlaget for leverandørklarering) kun enkelte språklige endringer. Politiets fellestjenester mener at det ikke finnes gode grunner til at styret skal klareres slik § 31 gir anvisning på og minner om at det må være et dokumentert behov.

Politiets fellestjenester opplyser at det er uklarhet knyttet til henvisningen i § 33 første ledd om kontroll av om leverandøren oppfyller sikkerhetskravene. Det bør presiseres at det er *denne forskriften* § 31 det vises til, da det kan forstås som at det gjelder virksomhetsforskriften § 31. I tillegg fremsetter PFT forslag til språklige endringer i § 34.

PFT peker særlig på at stort sett alle leverandører og underleverandører har behov for råd og veiledning slik at de forstår krav som følger av lov og forskrifter. På bakgrunn av PFTs erfaring på området ber politiet om å bli involvert i det fremtidige arbeidet med slike veiledninger som det er behov.

6. Særlig om økonomiske og administrative konsekvenser

Forsvarsdepartementet legger til grunn at nytt regelverk i utgangspunktet ikke vil medføre økte utgifter for virksomheter som er omfattet av gjeldende regelverk, og som oppfyller gjeldende krav til sikring av informasjon, informasjonssystem, objekt og infrastruktur. Politidirektoratet er ikke enig i Forsvarsdepartementets vurdering.

Politidirektoratet viser til tidligere uttalelser vedrørende økonomiske og administrative konsekvenser av ny sikkerhetslov med forskrifter, herunder i høringsuttalelsen til loven punkt 8.[15] I høringsuttalelsen understrekes viktigheten av at økonomiske og administrative konsekvenser av nye forskrifter blir godt kartlagt og at det samtidig lages en realistisk finansieringsplan. Det bemerkes at de økonomiske og administrative konsekvensene av nye forskrifter ikke er kartlagt, og at det på nåværende tidspunkt ikke er mulig å gi konkrete beskrivelser eller anslag av økonomiske og administrative konsekvenser av ny sikkerhetslov med forskrifter. Usikkerhet knyttet til hvilke deler av politiet som defineres som «grunnleggende nasjonale funksjoner" med understøttende skjermingsverdige objekter og infrastruktur trekkes i denne sammenheng frem som avgjørende for at det på nåværende tidspunkt ikke gis en mer konkret beskrivelse. I lovforarbeidene til ny sikkerhetslov vises det til arbeidet som er gjort i forbindelse med kartlegging av samfunnskritiske funksjoner for hva som omfattes av "grunnleggende nasjonale funksjoner". Dette kan medføre at deler av politiets virksomhet vil omfattes av "grunnleggende nasjonale funksjoner".

[13] Punkt 6.4.2.
[14] Punkt 6.7.2 på side 115.
[15] Politidirektoratets referanse 201604064-24 og Forsvarsdepartementets referanse 2015/3139.

Politidirektoratet vurderer at loven generelt stiller større krav til virksomhetens sikkerhetsarbeid, samt en endring fra detaljerte krav til sikkerhet, til mer funksjonelle krav. Dette innebærer ustrakt bruk av konkrete risikovurderinger for å finne frem til egnede sikringstiltak. Samlet stiller dette større krav til organisering, kapasitet, kompetanse og prosesser for sikkerhet i politiet.

Deler av politinettet vil være skjermingsverdig informasjonssystem som omfattes av ny sikkerhetslov og forskrift. Politidirektoratet oppfatter at forslaget kan medføre behov for betydelig investeringer i politiets IKT-systemer, samt investeringer for å sikre annen infrastruktur og personell. Investeringene vil videre kunne medføre økte drifts- og forvaltningskostnader[16]. I tillegg er det nødvendig med økt bemanning med sikkerhetsfaglig kompetanse for å etterleve ny lov med forskrifter. Summen av investeringene og driftskonsekvensene antas å bli betydelig.

Utarbeidelse av risikoanalyser med konkrete egnede sikringstiltak skal gjøres jevnlig. Dette er tidkrevende og kontinuerlig arbeid, og forutsetter personellressurser med sikkerhetsfaglig kompetanse. Denne type kompetanse er meget begrenset, samtidig som etterspørselen er høy. Det vil også være behov for kompetanseløft innen øvrige deler av virksomheten, da dette vil involvere organisasjonen utover dedikerte sikkerhetsressurser. Et tilstrekkelig kompetanseløft for dagens og et utvidet antall personellressurser, er avgjørende for å sikre etterlevelse av den nye loven.

Politiets erfaring fra bl.a. implementering av ny politiregisterlov, viser at denne type etablerings- og implementeringsaktiviteter er krevende og at det ofte er nødvendig med bruk av konsulentbistand for å ha tilstrekkelig antall kompetente ressurser tilgjengelig. Bruk av konsulentbistand bør reduseres mest mulig, da det, i tillegg til økte kostnader, kan gi uheldige konsekvenser med hensyn til eierskap og nærhet til sikkerhetsarbeidet i den enkelte virksomhet. Det utgjør i tillegg en sikkerhetsrisiko å la sikkerhetsgradert informasjon om etaten tilflyte eksterne som ikke selv har et sikkerhetsmessig behov for den. Derfor bør det sikres tilstrekkelig tid i forbindelse med implementeringen av regelverket til kompetanseheving hos egne ressurser, for å kunne benytte egne ansatte i størst mulig grad.

Politidirektoratet kan ikke se at det foreslås noen frist for implementering av sikringstiltak for nye, identifiserte objekter. Det vises til implementeringen av gjeldende objektsikkerhetsregelverk, der det ble det gitt en urealistisk frist for sikring av skjermingsverdige objekter. Det forutsettes at det gis realistiske frister for iverksetting av sikkerhetstiltak.

Politidirektoratet mener at konsekvensene av det samlede regelverket må kostnadsberegnes. For politiets del forutsettes det at etaten tilføres midler for å håndtere de økte kravene og det økte omfanget knyttet til implementering av nytt lovverk. Politiets driftsbudsjett er generelt stramme, samtidig som etaten står midt i en reform og der det er krav til at politiet frigjør budsjettmidler som følge av kostnadseffektivisering i et betydelig omfang. Dersom politiet ikke tilføres midler, må nødvendige sikringstiltak vurderes prioritert på bekostning av tjenesten i politidistrikt og særorgan for øvrig.

[16] Jf. Politidirektoratets høringssvar (201604064-24) til sikkerhetsloven *Samhandling for sikkerhet* (NOU 2016:19), og Forsvarsdepartementets referanse 2015/3139.

Politidirektoratet mener det må sikres tilstrekkelige overgangsordninger slik at implementeringen av forslag til nye forskrifter blir praktisk gjennomførbar.

Med hilsen

Håkon Skulstad
Assisterende politidirektør

Knut Smedsrud
avdelingsdirektør

Dokumentet er elektronisk godkjent uten signatur.

Vedlegg:
- Kripos' høringsuttalelse 14. september 2018
- Oslo politidistrikts høringsuttalelse 4. september 2018
- Politiets IKT-tjenester (PIT) høringsuttalelse 3. september 2018
- Politiets utlendingsenhets høringsuttalelse 4. september 2018
- Innlandet politidistrikts uttalelse 3. september 2018
- Politihøgskolen (PHS) høringsuttalelse 24. september 2018
- Politidirektoratets høringsinnspill 18. mars 2016 Høringsinnspill – Digital sårbarhet – Sikkert samfunn.
- Politiets Fellestjenester (PFT) høringsuttalelse 17. september 2018
- Politiets Fellestjenester (PFT) utdypende merknad til høringen 27. september 2018.