Forsvarsdepartementet
Postboks 8126 Dep
0030 OSLO

Deres ref.:

Vår ref.: 18/2722
Saksbehandler: Trond Simensen //
Sikkerhetsseksjonen

Vår dato: 13.09.2018

Høringssvar på forslaget til forskrifter til ny sikkerhetslov

Vi viser til Forsvarsdepartementet sin oversendelse av høringsbrev av 2. juli 2018 «Høring om nye forskrifter til sikkerhetsloven». Nedenfor følger våre merknader til forslagene. Del I inneholder svar på de punktene hvor departementet ba om kommentarer fra høringsinstansene. Del II er kommentarer til enkelte av forskriftsbestemmelsene.

DEL I: Merknader til høringsnotatet:

Behovet for å forskriftsfeste hvilke momenter om hvilke virksomheter som skal omfattes
Forskriftene inneholder ikke bestemmelser som inneholder hvilke momenter som skal legges til grunn for hvilke virksomheter som skal omfattes. NAV er enige med departementet i at det nå ikke er behov for å gi forskrift om hvilke virksomheter som skal omfattes av loven.

Inndelingen av forskriftene.
Forskriftene er delt opp i tre selvstendige forskrifter. NAV er i hovedsak enig i denne tredelingen og struktureringen i de enkelte forskrifter virker oversiktlig. Det kan være en utfordring knyttet til at det skjermingsverdige omfatter det sikkerhetsgraderte. Det kan være en utfordring i å holde tråden ved fortolkning av gyldighetsområder. Det kan kanskje være formålstjenlig å ta en gjennomgang av noen av kapitlene for å undersøke om det kan være behov for å bedre tydelighet, for å lette fortolkningen av bestemmelsene.

Klarering av utenlandske statsborgere
Nav mener at det er behov for en bestemmelse som konkretiserer vurderingstemaene for klarering av utenlandske statsborgere i forskriftene. Det er viktig å forhindre at vi klarerer feil personer. Hvis vi ikke klarer det vil det kunne få store negative konsekvenser. Det er samtidig viktig at vi får tilgang på utenlandsk kompetanse, som vi ikke har i Norge. I forslaget viderefører man tidligere forskrift, samtidig som man erkjenner at praktiseringen har vært for

NAV // ARBEIDS- OG VELFERDSDIREKTORATET // ØKONOMI- OG STYRINGSAVDELINGEN
Postadresse: Postboks 5 St. Olavs plass // 0130 Oslo
E-post: arbeids.og.velferdsdirektoratet@nav.no

www.nav.no //

snever. Kombinasjonen av ny lov, ønske om oppmykning av regelverket og virksomhetenes behov for utenlandsk arbeidskraft tilsier at vi må har regler med god presisjon. Det oppnås best gjennom forskriftsregulering.

Unntak fra krav om sikkerhetsklarering i særskilte tilfeller

NAV er noe usikker på det reelle behovet for unntaket fra sikkerhetsklarering, men har ingen innvendinger på selve det å ha en slik bestemmelse. Hva som skal være vurderingstemaet er rimelig klart og er en interesseavveingsbestemmelse som vi kjenner fra annet lovverk. Bestemmelsen er således hensiktsmessig utformet.

Varslingsplikten

Hovedvilkåret for varslingsplikten i lovens § 9-4 er formulert på følgende måte: «vurdere om anskaffelsen kan innebære en ikke ubetydelig risiko for at informasjonssystemet, objektet eller infrastrukturen kan bli rammet av eller brukt til sikkerhetstruende virksomhet.» Begrepet ikke ubetydelig risiko er et upresist begrep. Lovteksten gir ikke noen utfyllende momenter til denne vurderingen. Virksomhetene må foreta en risikovurdering, som normalt vil peke på noen risikoer. Det som er vanskelig er å vurdere når de aktuelle risikoene blir en «*ikke ubetydelig risiko».* Det legges opp til at sektormyndighetene skal kunne gi veiledere på dette spørsmålet. NAV mener det er nødvendig at det gis en forskrift i forhold til hva som ligger i varslingsplikten. Norske offentlige virksomheter blir ved økt digitalisering stadig mer sammenvevd med hverandre. Det å ha sektorvise veiledere vil da kunne føre til ulik praksis. En angriper vil da kunne velge å bruke den svakeste virksomheten for ramme sitt primære mål. Her det viktig med felles standarder. Det gjøres best ved forskrift eller ved en veileder fra en sikkerhetsmyndighet.

Ikrafttredelse

NAV er enig i at det bør gis en bestemmelse som angir hvilke momenter som skal legges til grunn for ikrafttredelsen av loven for det enkelte informasjonssystem, infrastruktur og objekt. Det er viktig at ikraftredelsestidspunkter også settes i forhold til økonomiske behov og budsjett tildelinger.

Klassifisering av skjermingsverdige objekter og infrastruktur

NAV mener forskriftene har en god oppbygning i forhold til klassifisering og har ikke forslag til endringer. Hvis vurderingene som virksomheten, departementet og NSM gjør er harmoniserte, vil jo resultatene kunne bli de samme. I en innkjøringsfase vil det vel kunne bli noe sprik i vurderingene. Veiledning og fortolkningshjelp vil jo kunne bidra til harmonisering. I §52 synes NAV at det at noe blir utsatt for manipulering burde vært listet som en separat trussel, da det ikke synes nærliggende å tolke dette inn verken under skadeverk, ødeleggelse eller rettsstridig overtakelse. Rettsstridig overtakelse bør enten defineres i forskriftene, evt. at det vises til definisjon i annet regelverk, slik at innhold og omfang av begrepet kommer klart fram.

Bruk av tredjepart til å gjøre sikkerhetsundersøkelser

NAV anser forskriftenes § 6 som hensiktsmessig og at relevante krav og kriterier er dekket. Vi ser derfor ikke at det er behov for ytterligere kriterier i den aktuelle bestemmelsen.

Pålegges kompetanse for NSM om tilknytning til VDI
NAV har ingen innvendinger mot at NSM gis kompetanse til å pålegge virksomheter å knytte seg til VDI.

Eierskapskontroll
NAV kan ikke se behov for ytterliggere bestemmelser om eierskapskontroll

Tilsyn
NAV synes at det er en fordel at bestemmelsene forskriftsfestes med den begrunnelse departementet nevner (forutberegnelighet) og harmonisering på tvers av departementsområdene.

Forsvarlig sikkerhetsnivå.
NAV synes ikke forsvarlighetskravet er sterkt nok og generelt nok. NAV mener det her er nødvendig å differensiere på eksterne og interne trusselaktører og med nyansering av krav mot de ulike trusselaktørene. Vi anser at kravene i første ledd er tilstrekkelige i forhold til interne trusselaktører, men ikke i mot eksterne trusselaktører.

Eksterne truselaktører har både stor evne og vilje til å utføre skadelige handlinger i forhold til skjermingsverdig informasjon. Fra NAV sitt ståsted fremstår trusselen fra de eksterne som større enn fra de interne trusselaktørene . Det er derfor nødvendig å ha et høyere krav til forsvarlig sikkerhetsnivå mot eksterne trusselaktører. Avveiningen mellom konfidensialitet, integritet og tilgjengelighet er annerledes i forhold til eksterne trusselaktører, da de ikke har behov for tilgjengelighet. Det gjør at det kan gjennomføres mer omfattende sikkerhetstiltak mot eksterne trusselaktører uten at det skader den interne tilgjengeligheten.

NAV foreslår derfor at det innarbeides et krav for forsvarlig sikkerhetsnivå i forhold til eksterne trusselaktører. Nytt første ledd i forskriftenes § 20 kan da være

§ 20 Forsvarlig sikkerhetsnivå for skjermingsverdig informasjon
Når virksomheten håndterer risikoen knyttet til skjermingsverdig informasjon, jf. § 12, er kravet til et forsvarlig sikkerhetsnivå oppfylt dersom informasjonen ikke med enkle midler kan endres, gå tapt eller gjøres utilgjengelig av interne trusselaktører. For eksterne trusselaktører er det et forsvarlig sikkerhetsnivå dersom informasjonen ikke med betydelige midler kan endres, tilintetgjøres eller gjøres utilgjengelig. For informasjon som er sikkerhetsgradert, gjelder i tillegg et krav om at den ikke med enkle midler kan bli kjent for uautoriserte personer.

Definisjoner
NAV mener at det det er riktig at definisjonene er fastsatt i forskriftene. NAV ber departementet vurdere om «rettsstridig overtakelse» også bør defineres, eller innta en henvisning til en legaldefinisjon. Dette for å oppnå tydelighet i fortolkning.

Sikkerhetstruende virksomhet.
Begrepet er greit definert. Men det kan være en utfordring for forskriftene at fokuset på trusler som ikke er bevisste handlinger er noe lite. Når loven dekker integritet og

tilgjengelighet er det behov for å prioritere dette opp, sammenlignet med den tid hvor fokuset mer ensidig var på konfidensialitet. Hvis tilfeldige hendelser kan påvirke grunnleggende nasjonale funksjoner, så må også det handteres.

Plikt til å handtere risiko.
NAV kan ikke se at vi trenger vi denne bestemmelsen. Plikten fremgår av andre bestemmelser og er etter sitt innhold selvsagt. Slik den fremstår i dag binder den sammen andre bestemmelser gjennom paragraf henvisningene, men uten eget innhold. Bestemmelsen må fylles med noe mer innhold dersom den skal ha noen hensikt.

DEL II Merknader til paragrafene

Merknader til forskrift om virksomhetens arbeid med forebyggende sikkerhet:
§14. Her vil vi nevne at vi i NAV skiller mellom sikkerhetsprinsipper, som (b) er et eksempel på, til forskjell fra sikkerhetsarkitekturprinsipper (a, c-e). Forskriftene kunne gjort bruk av en slik karakterisering av prinsipper. Av sikkerhetsprinsipper anvender vi også prinsippet om tjenestedeling, sikkerhetsmessig lønnsomhet, ansvarsprinsippet og proporsjonalitetsprinsippet. Av arkitekturprinsipper også autoriserte aktiviteter, sikkerhet ved feil, tillitsprinsipper, sikkerhet ved design og strukturprinsipper. Framheving av prinsipper for sikkerhet og for sikkerhetsarkitektur er viktig for arbeidet med sikkerhet. Vi foreslår at prinsipp-karakterisering og utvalg av prinsipper som skal framheves gjennomgås i forbindelse med ferdigstillelse av forskriftene.

§19. NSM er gitt adgang til å kunne dispensere fra sikkerhetskrav. NAV mener at denne adgangen bør legges til ansvarlig departementer, med råd fra NSM. Vi mener at det er gunstig at myndigheten til å fastsette krav for sikkerhet og føre tilsyn iht. sikkerhetskravene holdes adskilt. Likedan mener vi at det normalt bør unngås å gi tilsyn kompetanse til å fastsette sikkerhetskrav.

§ 21. Forskriftene sier at det ved destruering av informasjon med sikkerhetsgrader under konfidensielt skal brukes en metode som ikke gjør det mulig å rekonstruere innholdet. NAV har forståelse for at man ikke forskriftsfester konkret hvilken metode som skal benyttes, men ser det som hensiktsmessig at NSM gir ut en veileder på dette hvor dette konkretiseres.

§70. Regelen for hvilken informasjon en tilbyder skal få tilgang til er godt formulert. Håndhevelsen av bestemmelsen kan bli utfordrende, der vi har informasjon, objekt eller infrastruktur som omfattes av skjermingsverdig-kriteriet å avgrense det som er underlagt reguleringen fra det som ikke er underlagt, samt selve reguleringen av det som er underlagt. Det blir viktig med generell og god veiledning her. NAV antar at det blir NSM som må utarbeide dette. Særlig blir det viktig å gi operativ hjelp til å avgrense hva tilbydere og leverandører skal kunne ha tilgang til.

§71. NAV savner også et punkt om krav til leverandørens medarbeideres sikkerhetsatferd, for eksempel ved at det til bokstav b føyes til 'og hvordan slik informasjon skal behandles og god sikkerhetspraksis ivaretas'.

§72. NAV mener vilkårene for dette unntaket ikke er tilstrekkelig. En dyktig ekstern fagperson vil kunne gjøre skadelige handlinger, og som ikke oppfattes av den som holder oppsyn. Det bør derfor være et skjerpet krav utover «under oppsyn». Et slik skjerpet krav kan for eksempel være 'under kvalifisert oppsyn'. NSM kan gis i oppgave og gi veiledende retningslinjer om hva som er et kvalifisert oppsyn og dermed kvalifiserer for unntak fra å inngå sikkerhetsavtale.

Med hilsen

Grete Øwre
Økonomi og styringsdirektør
Økonomi- og styringsavdelingen

Terje Andre Olsen
Seksjonsjef
Sikkerhetseksjonen

Dette dokumentet er godkjent elektronisk og har derfor ingen signatur

Kopi til
Arbeids- og sosialdepartementet