HELSETILSYNET
tilsyn med barnevern, sosial- og helsetjenestene

05 APR 2019

Justis- og beredskapsdepartementet
Postboks 8005 Dep

0030 OSLO

DERES REF: / YOUR REF:	VÅR REF: / OUR REF:	DATO: / DATE:
	2019/909 3 PBØ	1. april 2019

Høringssvar - NOU 2018:14 IKT-sikkerhet i alle ledd og utkast til lov om sikkerhet i nettverk og informasjonssystemer(NIS-direktivet)

Statens helsetilsyn viser til høringsbrev 21. desember 2018 fra Justis- og beredskapsdepartementet med to saker på felles høring:

1.Utredning fra IKT-sikkerhetsutvalget (Holte-utvalget) NOU 2018: 14 IKT-sikkerhet i alle ledd – Organisering og regulering av nasjonal IKT-sikkerhet.

2.Regjeringens utkast til lov som gjennomfører EUs direktiv om sikkerhet i nettverk og informasjonssystemer (NIS-direktivet) i norsk rett.

Videre viser vi til e-post av den 13. mars fra Justis- og beredskapsdepartementet ved seniorrådgiver Roger Kolbotn, hvor det ble gitt utsatt høringsfrist til 29. mars. Etter henvendelse til seniorrådgiver Roger Kolbotn ble det gitt ytterligere utsatt frist til den 3. april.

Det opplyses i høringsbrevet at departementet «..sender de to sakene på felles høring fordi det er nær sammenheng mellom dem. Det gjelder særlig Holte-utvalgets anbefaling nr. 1 om en ny IKT-sikkerhetslov, der de i stor grad viser til lovutkastet om NIS-direktivet». Det fremgår at departementet ikke har tatt stilling til Holte-utvalgets anbefalinger, og at: «Lovutkastet og tilhørende høringsnotat viser hvilke minimumsforpliktelser som følger av NIS-direktivet».

Departementet ønsker «..at høringsinstansene vurderer utkastet til lov om NIS-direktivet for seg. Vi må være forberedt på å skulle oppfylle direktivets minimumsforpliktelser uavhengig av anbefalingene fra Holte-utvalget. Konkret når det gjelder utkast til lov om NIS-direktivet ber vi høringsinstansene særlig gi innspill på følgende spørsmål:

Statens helsetilsyn
Norwegian Board of Health Supervision
Org. nr.: 974 761 394

Postadresse / *Postal address:*
Pb. 231 Skøyen,
0213 Oslo, Norway
Besøksadresse / *Street address:*
Møllergata 24

Fakturaadresse / *Invoice address:*
Statens helsetilsyn
Fakturamottak DFØ
Pb. 4746, 7468 Trondheim
EHF-format - adresse 974761394

Tlf. / *Tel.*: (+47) 21 52 99 00
E-post / *E-mail*:
postmottak@helsetilsynet.no
Internett: www.helsetilsynet.no

- I hvilken grad arbeides det per i dag systematisk med IKT-sikkerhet i din virksomhet? Følges for eksempel visse standarder for sikkerhetsstyring eller internkontroll?
- Beskriv hvilke positive konsekvenser forslaget til gjennomføring av NIS-direktivet vil få for din virksomhet.
- Beskriv hvilke negative konsekvenser forslaget til gjennomføring av NIS-direktivet vil få for din virksomhet.
- Er din virksomhet per i dag underlagt krav til IKT-sikkerhet og varsling? Hvilket regelverk – lover, forskrifter eller annet – er det som stiller slike krav?
- Bør en slik lov som foreslås i denne høringen vedtas selv om vi ikke er forpliktet til det i henhold til EØS-avtalen?»

Statens helsetilsyn vil innledningsvis på denne bakgrunn kort omtale forholdet til gjennomføring av NIS-direktivet for egen virksomhet når det gjelder «sikkerhet i nettverk og informasjonssystemer».

Videre har vi slått sammen våre kommentarer og spørsmål knyttet til foreliggende utkast til lov som gjennomfører NIS-direktivet i norsk rett og til NOU 2018: 14 IKT-sikkerhet i alle ledd.

Sammendrag

Statens helsetilsyn er enig i at digital sikkerhet for samfunnsviktige tjenester vil kunne styrkes gjennom lovregulering og at innføring av NIS-direktivet vil kunne utgjøre en hensiktsmessig start i en lengre prosess, jf. Holte-utvalgets anbefaling om å nedsette et eget lovutvalg som skal utrede en lov som stiller krav om IKT-sikkerhet til alle norske virksomheter.

Lovutkastet som gjennomfører NIS-direktivet i norsk rett må imidlertid klargjøre lovens virkeområde, tydeliggjøre hvordan pliktsubjektene skal forholde seg til tverrsektorielt og sektorielt regelverk og konkretisere innholdet av kravene. Det må klargjøres hvordan de som er underlagt flere regelverk skal varsle flere responsmiljøer og tilsynsmyndigheter, og hvordan ansvars- og myndighetsfordelingen er mellom de ulike respons- og tilsynsmyndigheter.

Videre må det utredes hvilke økonomiske og administrative konsekvenser gjennomføring av NIS-direktivet i norsk rett vil ha. Etter hva Helsetilsynet kan se er ikke grunnleggende implementeringskostnader for helsesektoren nærmere utredet. Det fremgår at konsekvensene ved innføring av direktivet vurderes som relativt begrenset.

Etter Helsetilsynets vurdering må de administrative og økonomiske konsekvensene for sektortilsyn utredes på en tilstrekkelig måte både for Fylkesmannen og Statens helsetilsyn som tilsynsmyndighet med helse- og omsorgstjenesten.

Helsetilsynet mener videre det er behov for å avklare innholdet i NSM sin koordineringsrolle og forholdet til sektortilsynsmyndighetenes tilsynsansvar. Etter Helsetilsynets vurdering bør ikke NSM kunne utøve myndighet overfor sektortilsynene, men ha en veiledende og koordinerende rolle.

NIS-direktivets betydning for egen virksomhet når det gjelder sikkerhet i nettverk og informasjonssystemer

Norsk helsenett (NHN) drifter all IKT-struktur i Statens helsetilsyn.

NHN har i oppdrag å levere og videreutvikle hensiktsmessig, pålitelig og sikker nasjonal IKT-infrastruktur for effektiv samhandling mellom alle aktører i helse- og omsorgssektoren. Statens helsetilsyn har siden 1. januar 2017 fått levert IKT-driftstjenester fra NHN. En del av oppdraget til Norsk Helsenett er å drifte helse- og omsorgssektorens nasjonale kompetansesenter for informasjonssikkerhet (HelseCERT). Hovedoppgaven er å forebygge, oppdage, varsle og håndtere IKT-trusler i sektoren, og HelseCERT jobber systematisk og metodisk med tiltak som øker sikkerheten for alle som benytter Helsenettet.

Statens helsetilsyn jobber systematisk med IKT-sikkerhet og har fokus på å oppnå akseptabel sikkerhet i informasjonsbehandlingen, herunder tilgjengelighet, funksjonalitet og integritet. Når det gjelder spørsmålene (spesielt spørsmål 1 og 4) knyttet til egen virksomhet, så ønsker vi i første rekke til NHNs høringsuttalelse av den 22. mars 2019.

Lovutkastets saklige virkeområde for helse- og omsorgstjenesten

Virkeområde omtales på s. 7 følgende i høringsnotatet. Departementet foreslår at lovens virkeområde skal tilsvare NIS-direktivet for både tilbydere av samfunnsviktige tjenester og tilbydere av digitale tjenester, jf. punkt. 5.3.3 og 5.3.4 og lovutkastet § 2. Hva som er en samfunnsviktig tjeneste defineres i § 4 nr. 1 og tilbyder av digitale tjenester i nr. 2.

Etter Helsetilsynets vurdering er ikke kriteriet/vilkåret «tilbyder av samfunnsviktige tjenester» veldig klargjørende. Definisjonen i lovutkastet § 4 nr. 1 gir lite veiledning:

> «tilbyder av samfunnsviktig tjeneste: virksomhet som leverer en tjeneste som er viktig for opprettholdelsen av kritiske samfunnsmessige- eller økonomiske aktiviteter, som er avhengig av nettverk og informasjonssystemer for å kunne levere tjenesten, og der en hendelse vil kunne få betydelig forstyrrende effekt på tjenesteleveransen, forutsatt at tjenesten omfattes av vedlegg II til NIS-direktivet, slik dette er tatt inn i EØS-avtalen».

Departementet opplyser at virkeområdet kan være uklart og at Nasjonal sikkerhetsmyndighet(NSM) har fått i oppdrag å utarbeide mer konkrete vilkår for hvilke virksomheter som skal omfattes av loven, jf. høringsnotatet på s. 16 første og andre avsnitt. Videre henviser departementet inntil videre til tilsvarende arbeid i Sverige og Storbritannia og fra "Myndigheten för samhällsskydd och beredskap" (MSB) er følgende listet for helse- og omsorgssektoren:

> « Hälso- och sjukvårdssektorn
> 1. hälso- och sjukvårdsverksamhet som omfattas av hälso- och sjukvårdslagen (2017:30), tandvårdslagen (1985:125) eller detaljhandel med läkemedel enligt lagen (2009:366) om handel med läkemedel, och som:
> a) omfattar minst 20 000 patientbesök per år, eller
> b) minst 20 000 expedieringar per år, eller

c) har ett upptagningsområde där avståndet till likvärdig tjänst uppgår till minst 200 km.»

Det er vanskelig å omsette disse kriteriene/momentene opp mot norske forhold og avgjøre hvilke virksomheter innenfor helse- og omsorgsektoren som skal eller forventes å identifisere seg omfattet av utkastet til lov om IKT-sikkerhet i nettverk og informasjonssystemer.

Departementet legger en opp til at den enkelte virksomhet selv må vurdere om den omfattes av lovutkastet, og ikke en identifiseringsprosess ved departementene som følger av sikkerhetsloven.

Prinsipielt er Statens helsetilsyn enig i en slik tilnærming. På den annen side illustrerer den pågående identifiserings- og utpekingsprosess etter sikkerhetsloven at det kan være svært vanskelig å ta stilling til hvilke virksomheter som faller inn under den nye lovenes virkeområde. Noen tilsvarende utfordringer vil det trolig være for foreliggende lovforslag.

Det er viktig at det blir klart hvilke virksomheter og tjenester som omfattes av lov om IKT-sikkerhet i nettverk og informasjonssystemer. Behovet for klarhet gjelder særlig siden loven innfører varslingsplikt og har hjemler for tilsynsmyndigheten til å kunne gi pålegg, ilegge tvangsmulkt og overtredelsesgebyr.

Helsetilsynet ser at det i en tverrsektoriell lov kan være vanskelig å gi en presis avgrensning i lovtekst og forarbeider som gir tilstrekkelig og konkret veiledning om virkeområde til virksomheter på ulike sektorer. Vi ber derfor om at departementet i etterkant av at loven vedtas vurderer om JD i samarbeid med sektordepartementene og –direktoratene (på helseområdet: HOD og Helsedirektoratet) bør utarbeide mer konkret veiledning i rundskriv.

Lovutkastets regulering av sikkerhetskrav for helsesektoren

I høringsnotatet kap. 7. omtales gjeldende rett tverrsektorielt og sektorvis, herunder under 7.1.11 spesifikt for sektor helsetjenester med omtale av de sentrale helselovene med elementer og berøringspunkter til IKT-sikkerhet for helsesektoren.

Det fremgår at utenom kravene som følger av personvernforordningen art. 32, jf. pasientjournalloven § 22 og helseregisterloven § 21 at det ikke er særlige krav til IKT-sikkerhet.

Det uttales på s. 34 i høringsnotatet at:

> *«Siden det stort sett er personopplysningsloven og helselovgivningens fokus på sikring av helseopplysninger som er grunnlaget for det meste av informasjonssikkerhetsarbeidet i sektoren i dag, kan det være behov for at virksomhetene utvider omfanget av risikostyring og sikkerhetstiltak til også å omfatte annen kritisk infrastruktur. Et eksempel kan være byggteknisk infrastruktur og en del medisinsk-teknisk utstyr»*

Under departementets vurdering i punkt 7.3 gis det uttrykk for at gjeldende rett i varierende grad og på ulikt vis stiller krav om sikring av informasjon, og at

virksomhetene som omfattes av regelverkene må foreta konkrete vurderinger av hvert enkelt regelverk for å vurdere hvilke informasjonssystemer som skal sikres og etter hvilket regelverk. Lignende uttrykkes om sikkerhetskravene etter den tverrsektorielle personopplysningsloven og lovutkastet, og at «Virksomheten må foreta en konkret vurdering av sikkerhetsbehovet for hvert enkelt system».

Reguleringen av kravene til sikkerhet gjennom ulike lover og forskrifter er krevende og komplisert å sette seg inn i. Delvis reguleres ulike forhold og delvis er det overlappende regulering i ulike regelverk. Helsetilsynet vil derfor be Justis- og beredskapsdepartementet ta initiativ overfor Helse- og omsorgsdepartementet og Helsedirektoratet med sikte på å utarbeide rundskriv som kan gi virksomhetene i nødvendig veiledning.

Varslingskrav

I punkt 8.1 beskrives gjeldene rett tverrsektorielt og sektorvis. Blant annet virksomhetens plikt til å varsle sikkerhetsmyndigheten og sektormyndigheten dersom den har blitt rammet av eller det er begrunnet mistanke om at sikkerhetstruende virksomhet har rammet eller vil kunne ramme virksomheten, og virksomhetens plikt til å varsle Datatilsynet etter personopplysningsloven ved «..brudd på sikkerheten som fører til utilsiktet eller ulovlig tilintetgjøring, tap, endring, ulovlig spredning av eller tilgang til personopplysninger som er overført, lagret eller på annen måte behandlet».

For helsesektoren omtales også enkelte andre varslingsordninger, herunder varsler ved uønskede hendelser knyttet til pasientbehandling.

Departementet foreslår likelydende krav om varsling av hendelser til myndighetene i tråd med direktivets krav i lovutkastet §§ 8 og 10. Videre legger departementet til grunn at varslingen av hendelser i størst mulig grad bør skje i tråd med Rammeverk for håndtering IKT-sikkerhetshendelser og i størst mulig grad ved bruk av eksisterende myndighetsstruktur.

Helsetilsynet støtter at varslingen av hendelser i størst mulig grad bør skje i tråd med Rammeverk for håndtering IKT-sikkerhetshendelser som beskriver håndtering av IKT-sikkerhetshendelser i og på tvers av virksomheten. Det kan også være grunn til at flere myndigheter og tilsynsmyndigheter i sektoren orienteres, men det sentrale bør være at varslene går til myndigheter med ressurser og kompetanse for å følge opp varselet og hendelsen.

Lovutkastets regulering av tilsyn med IKT-sikkerhet på helseområdet – økonomiske og administrative konsekvenser

Det fremgår på høringsnotatets s. 3 at «Myndighetene skal føre tilsyn med virksomhetene og kan gi pålegg og eventuelt gebyr ved manglende oppfyllelse av pliktene. Myndighetene skal også ta imot varsler om alvorlige IKT-sikkerhetshendelser.

Departementet mener at eksisterende myndighetsstruktur bør benyttes i størst mulig grad. Der det per i dag eksisterer sektormyndigheter, skal deres hjemler justeres slik at de er i samsvar med direktivet når det gjelder tilsyn og sanksjonering. Departementet tar videre utgangspunkt i at eksisterende myndigheter også bør føre tilsyn med virksomheter som per i dag ikke er underlagt tilsyn».

Statens helsetilsyn forstår det slik at vi er en av flere myndigheter som forutsettes eller er tiltenkt å føre tilsyn virksomheter innenfor helsesektoren og deres etterlevelse av lov om sikkerhet i nettverk og informasjonssystemer, jf. utkastet § 12 første ledd og tilsvarende forutsetninger om at departementet kan vedta at sektortilsyn skal føre tilsyn med ny sikkerhetslov.

På samme måte som tilsyn etter ny sikkerhetslov vil gjennomføring av direktivet - basert på at oppgavene skal bygge på eksisterende myndighetsstruktur- utfordre tilsynsmyndighetene med helsetjenestens samlede ressurser og medføre press på omprioritering fra tilsyn med helsetjenestens kjerneoppgaver til tilsyn med IKT-sikkerhet.

Etter hva Helsetilsynet kan se er ikke de økonomiske og administrative kostnadene for sektortilsyns tilsyn med loven konkret vurdert eller beskrevet. Det fremgår på s. 64 i høringsnotatet at «For myndighetene er det oppgavene med å føre tilsyn og å motta varsler som vil være kostnadsdrivende. Slike konsekvenser gjennomgås sektorvis under». For helsesektoren gjennomgås og konkretiseres imidlertid ikke de økonomiske og administrative konsekvensene av å legge ansvar og oppgaver til tilsynsmyndigheten med helsetjenesten i punkt 12.3.10.

Etter Helsetilsynets vurdering vil oppfølgning og tilsyn med loven som gjennomfører NIS-direktivet kreve IKT- sikkerhetskompetanse og -ressurser som vi per i dag ikke har.

Helsetjenesten er i økende grad avhengig av velfungerende og stabile digitale løsninger for å yte forsvarlige helsetjenester. Det inkluderer løsninger som sikrer at nødvendig pasientinformasjon er tilgjengelig, autentisk og at personvernhensyn blir ivaretatt. Statens helsetilsyn har i samarbeid med øvrige helsemyndigheter og Datatilsynet foretatt en gjennomgang for å avklare roller og ansvar. Det er enighet om at tilsynet med helsetjenestens teknologiske ressurser bør styrkes. Statens helsetilsyn har derfor igangsatt et utviklingsarbeid med sikte på å styrke tilsynet med helsetjenestens digitale løsninger, både faglig og kapasitetsmessig, med utgangspunkt i virksomhetenes plikt til å yte forsvarlig helsehjelp og kravene til helsetjenestens informasjonssystemer. Statens helsetilsyn har fått tildelt ressurser fra Helse- og omsorgsdepartementet for å utvide vår kapasitet på dette området.

Ut fra utvalgets utredning og foreliggende høringsnotat ser vi at en slik utvidelse av vår tilsynsvirksomhet i noen grad vil være overlappende med tilsyn med overholdelse av pliktene etter lov om sikkerhet i nettverk og informasjonssystemer. Hvor stor grad av overlapping det vil bli avhenger av hvilket innhold som legges i kravene etter denne nye loven og omfanget av tilsynsaktiviteter som forventes.

Forutsatt at sektortilsynsmyndighetene gis handlingsrom til å finne egnede løsninger for å ivareta tilsynsansvaret som beskrives i høringsnotatet, slik at dette tilsynet i omfang og innhold lar seg kombinere med sektortilsynsmyndighetenes øvrige tilsyn på IKT området, vil de økonomiske og administrative konsekvensene av forslaget være mer begrenset.

Statens helsetilsyn er positive til utvalgets anbefaling om at NSM skal ha en koordineringsrolle ved IKT-sikkerhetstilsyn, jf. arenaen for IKT-tilsyn som NSM har

etablert og som etter det opplyste i utredningen vil bli videreutviklet til å omfatte de sektortilsynene som blir utpekt etter den nye sikkerhetsloven. Samtidig er det viktig å avklare innholdet i denne rollen og forholdet til de enkelte sektortilsynsmyndighetenes ansvar.

I Holte-utvalgets utredning under punkt 19.2 fremgår at tilsyn må koordineres bedre og utvalget viser til at tilsyn med IKT-sikkerhet bør skje på lignende måte som samordningen av tilsyn etter HMS-regelverket, bruk av tilsynskalender og ved arenaen for IKT-tilsyn som NSM har etablert for tilsyn med sikkerhetsloven.

For tilsyn etter sikkerhetsloven peker utvalget på at NSMs rolle blir å sikre en helhetlig, samordnet og tverrsektoriell tilnærming. «De vil føre tilsyn med de utpekte sektortilsynene, men også med virksomheter i sektorer med utpekte sektortilsyn der det er «tvingende nødvendig». NSM har i den forbindelse allerede fått et sterkt samordningsmandat for tilsyn, og dette mener utvalget det bør bygges på i den utvidede samordning av IKT-sikkerhetstilsynene.»

Ved gjennomlesning av utkastet til gjennomføring av NIS-direktivet er det ikke like tydelige at det er sektortilsyn som skal være tilsynsmyndighet som etter Holte-utvalgets beskrivelse. NSM sin rolle og myndighet knyttet til samordning av IKT-sikkerhetstilsynene er heller ikke utførlig beskrevet i høringsnotatet.

Det fremgår imidlertid at det er eksisterende myndighetsstruktur som i størst mulig grad bør benyttes, og at Kongen utpeker en eller flere tilsynsmyndigheter som skal føre tilsyn i medhold av lovutkastet § 12. Videre inneholder lovutkastet flere forskriftshjemler, herunder hjemmel for å gi forskrift om gjennomføring av tilsyn.

Helsetilsynet antar derfor at NSM skal ha samme samordningsfunksjon som de er gitt sikkerhetsloven, slik at samordningen også vil kunne innebære at NSM gis myndighet til å styre sektortilsynenes prioriteringer og utøvelse av tilsyn.

Som redegjort for i arbeidet med å utforme tilsynsordningen for ny sikkerhetslov mener Statens helsetilsyn en slik beskrivelse av koordineringsrollen er problematisk. Det må være den enkelte tilsynsmyndighet som er ansvarlig for de prioriteringer som må foretas og for utførelsen av tilsyn. At NSM gis en form for styrings- eller tilsynsmyndighet over sektortilsynsmyndighetene mener vi ikke er en naturlig del av koordineringsrollen. Samarbeidet og koordineringen på IKT-sikkerhetsområdet bør heller utformes etter modell fra samarbeidet mellom HMS-tilsynsetatene, men slik at NSM med sin fagkompetanse vil innta en ledende rolle i veiledning og koordinering.

Med hilsen

Jan Fredrik Andresen
direktør

Pål Børresen
seniorrådgiver

Brevet er godkjent elektronisk og sendes derfor uten underskrift

Saksbehandler: Pål Børresen, tlf. 21 52 99 67

Kopi- Helse- og omsorgsdepartementet