Oslo universitetssykehus

Justis- og beredskapsdepartementet
Postboks 8005 Dep,
0300 Oslo

Vår ref.:	Deres ref.:	Saksbeh.:	Dato:
2016/10773	15/5866	HTh	12.9.2016
Oppgis ved all henvendelse			

Høringssvar om forslag til nytt EU-direktiv om sikkerhet i nettverk og informasjonssystemer

Det vises til invitasjon til høring på Forslag til EU-direktiv om sikkerhet i nettverk og informasjonssystemer (NIS-direktivet (5581/16)). Oslo universitetssykehus vurderer det som viktig at det etableres internasjonale felles føringer. Spesielt er dette et viktig tiltak for å sikre at internasjonale leverandører vet hva som er gjeldende standard og at dette er likt innen størst mulig dekningsområde.

I det følgende besvares om EU-direktivet vurderes til å berøre virksomheten og sektoren, samt enkeltkommentarer til direktivet.

Vurdering av direktivets relevans for virksomheten og sektoren
Oslo universitetssykehus forvalter store volum av sensitive personopplysninger og er også en av de aktuelle typer organisasjon som er nevnt i vedlegget på forslaget om direktiv. Det vurderes dermed at Oslo universitetssykehus vil bli regulert av dette direktivet dersom det blir gjort gjeldende.

Spesialisthelsetjenesten håndterer store volum av sensitive personopplysninger og interesseområdet er bredt regulert i gjeldende rett ved en rekke særlover og generelle lover for ivaretakelse av personvernet. I tillegg kommer ny personvernforordning i EU til å gjelde direkte for Norge (fra 2018).
De samme krav og regulering av internkontroll er også uttrykt som forutsetning ved tilkobling til Norsk Helsenett, og er samlet i bransjenormen «Norm for informasjonssikkerhet for helse», forvaltet av direktoratet for e-helse.

Videre er Oslo universitetssykehus regulert av Sikkerhetsloven (iht. beslutning gjort kjent av Helse- og omsorgsdepartementet 19. desember 2014).

Med nevnte gjeldende reguleringer og rammer vil forslaget i begrenset grad innebære mer noe nytt idet det ikke er noen nye krav/reguleringer som kommer med forslaget, bortsett fra at vi får en felles regulering i EU/EØS området. Det burde dermed i mindre grad innebære nye økonomiske eller administrative konsekvenser, forutsatt at de ulike føringer og kontroller som er tiltenkt sikres en god

harmonisering. I det følgende er det derfor noen punkter i det nye direktivet som er viktig å kommentere.

Enkeltvise kommentarer til direktivet

(27) og **(28)** benytter begrepet *significant disruptive effect*. Det anbefales at det ikke kun ses på volumvurderinger når det gjelder helsesektoren, men også på samhandling, effektivitet, kvalitet og selvsagt pasientsikkerhet. Dette blir mer hensiktsmessig belyst i **kapittel 1, artikkel 6, 1)**, og anbefaler derfor at **(28)** kun peker til denne artikkelen.

(34), **kapittel II, artikkel 8, 1)**, samt **kapittel IV, artikkel 14, 5)** m.fl. beskriver oppgavene og kompetansen til det nasjonale kompetanseorganet («*competent authorities*») og kontaktpunkt («*single point of contact*»). Det legges i departementets dokumenter føringer for at dette arbeidet i stor grad vil dekkes av eksisterende NSM NorCERT. Denne vurderingen støttes, og det er naturlig at NSM NorCERT bekler denne oppgaven, men det må da som en forutsetning gjøres en grundig evaluering av NSM NorCERTs organisering, rapportering og ledelse. En utvidelse av arbeidsoppgavene slikt direktivet legger til grunn, vil også kreve en kompetanse-, kultur- og kommunikasjonsendring fra dagens praksis. **Kapittel IV, artikkel 15, 2a)** legger også føringer for tilsyn og revisjon ved at «*competent authorities shall have the powers and means to require operators of essential services to provide the information necessary to assess the security of their network and information systems, including documented security policies.*» Dette vil være en ny type tilsynsfunksjon, hvor kontroll av både styring og etterlevelse vil inngå. En slik tilsynsfunksjon finnes ikke i dag, utover det som gjøres av Riksrevisjonen og Datatilsynet. Om NSM NorCERT skal utføre også dette, må det sikres at kompetansen, samhandling, kultur og forståelse harmoniseres med den sivile og offentlige del av samfunnet som vil omfattes av NIS-direktivet.

Samspillet mellom «*competent authority*» og f.eks. Datatilsynet må også ses nærmere på i det videre arbeidet, for å unngå unaturlig overlapp eller manglende ansvarsforhold i arbeidsoppgaver.

(40), **(59)**, **(61)** samt **kapittel IV, artikkel 14, 6)** beskriver en varslingsplikt ved hendelser. Det er i all hovedsak enighet i intensjonen om bedre informasjonsdeling i informasjonssikkerhetsmiljøene både i og på tvers av sektorene. Samtidig fremstår formuleringene i disse kravene på en slik måte at den ansvarlige virksomheten, som utfører rapporteringen, ikke har noen kontroll eller styring på hvordan *competent authority* eller *CSIRT* velger å dele denne informasjonen videre. En slik type varslingsplikt må hensynta integriteten og konfidensialiteten til den rapporterende part. Slik varsling må dermed underlegges følgende to hensyn:

i) varslingen må klassifiseres iht. TLP eller annen relevant standard
ii) varslingen kan ikke videredistribueres uten samtykke fra den rapporterende part.

(52) kan med fordel tydeliggjøres slik at ansvaret for informasjonssikkerhet i informasjonssystemer og nettverk som behandler personopplysninger og sensitive personopplysninger, alltid ligger hos databehandlingsansvarlig. Plikter og myndighet skal inngå i en databehandleravtale. Dette vil også regulere pliktene iht. NIS-direktivet.

Kapittel III, artikkel 11, 2) beskriver det overnasjonale «*cooperation group*». Vi vil anbefale at det vurderes om deltagelse i «*cooperation group*» ikke bør begrenses til kun representasjon fra nasjonal «*competent authority*» eller «*single point of contact*». Representasjonen bør – om mulig – være bredt sammensatt med involvering fra sektorene som er omfattet av **vedlegg 2**. Vi anser at dette er nødvendig for å gi gruppen nødvendig legitimitet og kompetanse.

Avsluttende vurdering og konklusjon
Direktivet har som primærformål å styrke det indre markedets evne til å motstå hendelser i cyberrommet, ved å sikre at alle medlemslandene etablerer et felles minimum av informasjonssikkerhet og et effektivt samarbeid på tvers av landegrensene. Oslo universitetssykehus HF ønsker et godt regulativt rammeverk, basert på anerkjente standarder, velkommen.

Samtidig oppfatter vi at direktivet fremstår byråkratisk tungt, med mange rapporterings- og styringsledd. Faren er at en slik struktur også bidrar til uoversiktlighet og uklarhet. Hvordan direktivets krav omsettes til praksis, må derfor vurderes nøye og kontinuerlig måles opp mot direktivets formål, for å sikre at utfallet faktisk forbedrer sikkerhetsnivået i EU-området.

Direktivets rolle er ikke å foreslå tiltak, men med liten endring i innholdet, kunne direktivet med fordel vært enda tydeligere på hvordan ENISA og medlemslandene kan benytte eksisterende standarder innenfor fagfeltet, for å oppnå direktivets mål.

Med vennlig hilsen
Oslo universitetssykehus

Bjørn Erikstein
administrerende direktør