Regelrådets uttalelse

Om: Utkast til lov som gjennomfører NIS-direktivet i norsk rett
Ansvarlig: Justis- og beredskapsdepartementet

Regelrådets konklusjon: **Forslaget er tilstrekkelig utredet**

Regelrådet

Regelrådet

Justis- og beredskapsdepartementet

Deres ref.:	Vår ref.:	Dato:	Vår saksbehandler:
18/6579	18/00291	22.03.2019	Kristin Johnsrud

Uttalelse

Om: Utkast til lov som gjennomfører NIS-direktivet i norsk rett

Konklusjon: Forslaget er tilstrekkelig utredet

Regelrådets samlede vurdering av forsalget

Regelrådet gjør oppmerksom på at denne uttalelsen bare gjelder utkast til lov som gjennomfører NIS-direktivet i norsk rett. Regelrådet uttaler seg ikke til NOU 2018:14 som ble sendt på høring samtidig, da utredningen ikke inneholder regelverksforslag og dermed faller derfor utenfor Regelrådets mandat.

Regelrådet mener at forslaget er tilstrekkelig utredet, jf. utredningsinstruksen pkt. 2-1 og 2-2.

Regelrådet vil gi Justis- og beredskapsdepartementet ros for en grundig utredning. Virkningene for næringslivet er kvalitativt godt beskrevet og begrunnet. Virkningene er ikke tallfestet, men departementet har gjengitt aktuelle tall fra EU-kommisjonens konsekvensutredning, noe som gir et godt bilde på kostnadenes størrelsesorden og bidrar til et godt beslutningsgrunnlag.

Etter Regelrådets vurdering er utredningen godt strukturert og gir berørte virksomheter et godt grunnlag for å forstå forslagene og vurdere virkningene. Regelrådet registrerer også at flere sektorer helt eller delvis allerede oppfyller direktivets krav, og at personopplysningsloven på enkelte områder også dekker kravene i NIS-direktivet.

Forutsatt at små og mellomstore virksomheter ikke omfattes av reglene mener Regelrådet at det er grunn til å tro at målene kan oppnås til en relativt sett lav kostnad for næringslivet.

Regelrådet ga i januar 2018 ga bistand til Justis- og beredskapsdepartementet med å granske konsekvensutredningen som fulgte med forslaget til NIS-direktiv.

Ta gjerne kontakt ved spørsmål.

Med vennlig hilsen
Sandra Riise
leder av Regelrådet

Dokumentet er elektronisk signert og har derfor ikke håndskrevne signaturer.

REGELRÅDET,
Kartverksveien 21, 3511 Hønefoss
ORG.NR.: 916195613

TELEFON: 32 11 84 00
E-POST: post@regelradet.no
www.regelradet.no

1. Om forslaget som er sendt på høring

Justis- og beredskapsdepartementet (heretter departementet) sendte den 21. desember 2018 på høring NOU 2018: 14 IKT-sikkerhet i alle ledd og utkast til lov som gjennomfører NIS-direktivet i norsk rett.

NOU 2018:14 IKT-sikkerhet i alle ledd – organisering og regulering av nasjonal IKT-sikkerhet inneholder ikke regelverksforslag og faller derfor utenfor Regelrådets mandat. Regelrådets uttalelse omhandler derfor bare høring om utkast til lov som gjennomfører NIS-direktivet i norsk rett.

NIS-direktivet har som formål å styrke IKT-sikkerheten i EU. Dette skal oppnås ved at medlemsstatene gjennomfører ulike tiltak for å styrke nasjonale kapasiteter og internasjonalt samarbeid. Medlemsstatene skal blant annet sørge for at tilbydere av samfunnsviktige tjenester og tilbydere av enkelte digitale tjenester, basert på en risikovurdering, gjennomfører hensiktsmessige og forholdsmessige sikkerhetstiltak. Tjenestetilbyderne skal også varsle om alvorlige hendelser. Det skal føres tilsyn med etterlevelsen. Mangelfull etterlevelse kan sanksjoneres. Direktivet stiller strengere krav til tilbydere av samfunnsviktige tjenester enn tilbydere av digitale tjenester. Det er disse forholdene forslaget til lov regulerer.

I juli 2016 sendte departementet på høring EU-kommisjonens forslag til EU-direktiv om sikkerhet i nettverk og informasjonssystemer. Formålet med høringen var å få belyst konsekvensene av å gjennomføre forslaget i norsk rett.

Den 12. desember 2017 anmodet departementet Regelrådet om bistand til å granske konsekvensutredningen som fulgte med forslaget til direktiv. Regelrådet bisto og ga veiledning gjennom møter og brev datert 19. januar 2018. Regelrådet vil bemerke at selv om Regelrådet ga departementet generell veiledning og bistand i vurderingen av EU-kommisjonens konsekvensutredning av NIS-direktivet, er det Regelrådets oppfatning at rådet er hildet til å vurdere utredningskvaliteten i denne saken. Etter Regelrådets vurdering bør det ikke være slik at en henvendelse om bistand og veiledning automatisk medfører at Regelrådet ikke kan avgi uttalelse til saken.

2. Regelrådets prioritering

Regelrådet skal bidra til at næringslivet ikke påføres unødvendige byrder gjennom nytt eller endret regelverk, jf. vedtekter for Regelrådet § 1.

Regelrådet skal vurdere utformingen av forslag til nytt eller endret regelverk, både lover og forskrifter, som påvirker næringslivets arbeidsbetingelser og øvrige relevante forhold, jf. vedtektene § 2 første ledd. Rådet står fritt til å prioritere hvilke saker man gir uttalelser i. På denne bakgrunn prioriterer Regelrådet å uttale seg om et utvalg av saker.

IKT-sikkerhet er viktig for norsk næringsliv i en tid hvor stadig flere tjenester digitaliseres. God IKT-sikkerhet kan etter Regelrådets vurdering være en konkurransefordel for de berørte virksomhetene. Et grunnleggende sikkerhetsnivå hos tilbydere av samfunnsviktige tjenester og tilbydere av digitale tjenester er også viktig for andre næringsdrivende som bruker disse tjenestene i sin næringsvirksomhet. Regelrådet mener derfor at forslaget til lov som gjennomfører NIS-direktivet i norsk rett er viktig for næringslivet som helhet.

3. Regelrådets vurdering av utredningen av konsekvenser for næringslivet

Det følger av Regelrådets vedtekter § 2 første ledd at Regelrådet skal ta stilling til om det er gjennomført konsekvensvurderinger etter de krav som utredningsinstruksen stiller, og om virkningene for næringslivet er tilstrekkelig kartlagt. Rådet kan vurdere hvorvidt nytt eller endret regelverk er utformet slik at målene oppnås til en relativt sett lav kostnad for næringslivet.

Som grunnlag for vurderingen nedenfor har Regelrådet særlig tatt utgangspunkt i kravene til innhold i beslutningsgrunnlaget i utredningsinstruksen kapittel 2. Det vil si pkt. 2-1 Minimumskravene til utredning og pkt. 2-2 Omfang og grundighet. Regelrådet har også sett hen til reglene om tidlig involvering av berørte i utredningsinstruksen pkt. 3-1.

3.1. Kostnadsvirkninger og nyttevirkninger for næringslivet

Etter Regelrådets vurdering gir høringsnotatet en grundig beskrivelse av kravene i direktivet, gjeldende rett i de berørte sektorene og virkningene av direktivet for de berørte. De berørte næringssektorene er beskrevet og virkningene for hver enkelt av dem er kvalitativt godt utredet. Virkningene for næringslivet er ikke tallfestet, men de kvalitative beskrivelsene er såpass grundige at Regelrådet ikke vil kritisere departementet for manglende tallfesting. Regelrådet registrerer imidlertid at departementet i høringsnotatet har gjort rede for aktuelle tall fra EU-kommisjonens konsekvensutredning. Etter Regelrådets vurdering kan dette gi et godt grunnlag for å vurdere kostnadsnivået for de berørte virksomhetene og i Norge. Departementet burde imidlertid kommentert overføringsverdien til norske forhold noe nærmere.

Regelrådet finner det positivt at departementet har gjort rede for blant annet Mørketallsundersøkelsen for 2016 som sier noe om IT-tilstanden i privat og offentlig næringsliv. Etter Regelrådets vurdering bidrar dette til å sette direktivet inn i en norsk kontekst, noe som styrker utredningen og gir økt forståelse for reglene.

Regelrådet vil også gi ros for vurderinger og henvisninger til sikkerhetsloven og personopplysningslovens krav og der disse overlapper og utfyller NIS-direktivets krav.

Regelrådet finner det videre positivt at departementet har gjennomgått de berørte sektorene og vurdert om gjeldende rett oppfyller direktivets krav når det gjelder både sikkerhetstiltak og varsling. Regelrådet registrerer at flere sektorer og virksomheter allerede oppfyller direktivets krav. For eksempel fremgår det av høringsnotatet at elektrisitetssektoren, jernbanesektoren og drikkevannssektoren oppfyller direktivets krav til IKT-sikkerhet. For de øvrige sektorene er det noe større usikkerhet. Videre fremgår det at elektrisitetssektoren, bank og finansmarkedsstrukturene, og tilbydere av DNS-tjenester er underlagt varslingskrav som tilsvarer direktivets krav. Regelrådet vi gi departementet ros for en grundig gjennomgang på dette området. Disse vurderingene vil etter Regelrådets vurdering være av stor betydning for høringsinstansenes mulighet til å vurdere virkningene av forslaget.

3.2. Konkurransevirkninger for næringslivet

Regelrådet registrerer at departementet i det alt vesentligste har foreslått en minimumsimplementering av direktivet. Etter Regelrådets vurdering synes departementet å ha et bevisst forhold til dette valget som blant annet er begrunnet i et ønske om like regler i EU og hensynet til konkurransen. Det er også grunn til å anta at norske virksomheter kan være et enklere mål for angripere dersom vi ikke har samme nivå på IKT-sikkerheten her som i resten av EU.

Etter Regelrådets vurdering kunne departementet imidlertid også kommentert konkurranseforholdene innad i næringer hvor noen blir og noen ikke blir omfattet av reglene, og hvilke konsekvenser dette kan få for konkurransen innad i næringen.

3.3. Forenkling for næringslivet

Etter Regelrådets vurdering inneholder forslaget ikke konkrete forenklingstiltak.

Regelrådet viser til at både NIS-direktivet, sikkerhetsloven og personopplysningsloven stiller krav om varsling. Regelrådet vil i denne forbindelse anmode myndighetene om å utrede og vurdere om det er mulig og fornuftig å samordne varslingene. Blant annet kan det med fordel utredes om virksomhetene kan varsle ett sted og at myndighetene deretter kan dele informasjonen seg imellom.

3.4. Digitalisering

Regelrådet viser til at å styrke IKT-sikkerhet er det grunnleggende formålet med forslaget til lov som gjennomfører NIS-direktivet i norsk rett.

Regelrådet registrerer at departementet foreløpig ikke har tatt endelig stilling til hvilke myndigheter som i alle tilfeller skal ta imot varsler, men at det legges opp til at eksisterende myndighetsstruktur bør benyttes i størst mulig grad. Regelrådet vil anmode departementet i det videre arbeidet om å vurdere om eksisterende løsninger kan brukes, og om eksisterende løsninger kan digitaliseres og forenkles. Videre bør departementet i det videre arbeidet legge til rette for kostnadseffektive og brukervennlige løsninger for rapportering fra virksomhetene til myndighetene.

3.5. Særskilt vurdering av hensynet til små virksomheter

Gjennomgangen i høringsnotatet av de berørte sektorene, herunder vurderingen av hvilke og hvor mange virksomheter som vil bli berørt, gir grunn til å tro at forslaget primært vil gjelde for store virksomheter. Blant annet fremgår det av høringsnotatet at kraftprodusenter må eie produksjonsanlegg på minst 50 MVA og at virksomheter som driver forsyning og distribusjon av drikkevann må nå 10 000 personer.

Regelrådet registrerer at når det gjelder tilbydere av digitale tjenester fremgår det av direktivet at mikrovirksomheter og små virksomheter ikke omfattes. Med mikrovirksomheter og små virksomheter menes virksomheter som har færre enn 50 ansatte og som har en årlig omsetning eller årlig samlet balanse som ikke overstiger 10 millioner euro. Departementet skriver i høringsnotatet at de tar sikte på å definere mikrovirksomheter og små virksomheter nærmere i forskrift.

3.6. Alternative tiltak

Departementet skriver i høringsnotatet at der det er påkrevet av hensyn til legalitetsprinsippet eller informasjonsformål foreslår departementet lovregler. Dette gjelder først og fremst der det pålegges plikter med hensyn til gjennomføringen av sikkerhetstiltak, varsling av hendelser, tilsyn og sanksjoner. Regelrådet deler departementets syn om at lovregulering er nødvendig i denne saken og at det på denne bakgrunn ikke er grunnlag for å utrede andre overordnede tiltak.

Direktivet er et minimumsdirektiv. Direktivet gir likevel medlemsstatene rom for nasjonale tilpasninger på flere områder. Når det gjelder tilbydere av digitale tjenester er handlingsrommet mindre, da dette er grenseoverskridende virksomhet. Tilbyderne må følgelig ha så like regelverk som mulig å forholde seg til i hele EU. Departementet skriver i høringsnotatet at de foreslår at lovens virkeområde, sikkerhetskrav og varslingskrav tilsvarer direktivet. Regelrådet oppfatter det dermed slik at departementet har gått for en minimumsgjennomføring av direktivet på disse områdene. Etter Regelrådets vurdering er dette valget gjennomgående godt begrunnet i høringsnotatet.

Slik Regelrådet forstår det gir direktivet en del handlingsrom når det gjelder tilsyn og sanksjoner. Etter Regelrådets vurdering kunne departementet på disse områdene utredet alternative løsninger. Når det gjelder valg av sanksjonsnivå redegjør departementet for løsningene som er valgt til Sverige, Storbritannia og Danmark. Regelrådet finner det positivt at departementet viser til hvordan sanksjonsbestemmelsene er utformet i andre land og bruker dette i vurderingen av hvordan bestemmelsene bør utformes i Norge.

3.7. Forutsetninger for en vellykket gjennomføring for næringslivet

Regelrådet finner det positivt at departementet i 2016 sendte EU-kommisjonens forslag til direktiv på høring, og at departementet har brukt høringsinstansenes innspill i den videre saksbehandlingen.

Departementet skriver i høringsnotatet at det fremdeles kan være uklart om en virksomhet er omfattet av lovens regler for tilbydere av samfunnsviktige tjenester. Departementet har derfor gitt Nasjonal sikkerhetsmyndighet (NSM) i oppdrag å utarbeide mer konkrete vilkår for hvilke virksomheter som omfattes. Departementet skriver også at det muligens skal utarbeides terskelverdier innenfor hver

sektor. Departementet ser for seg at en slik liste tas inn i en forskrift til den foreslåtte loven. Regelrådet deler departementets syn om at dette vil gjøre det enklere for virksomhetene å vurdere om de omfattes av direktivet. Selv om departementet skriver at dette arbeidet ikke er ferdigstilt, finner Regelrådet det positivt at departementet har henvist til tilsvarende arbeid i Sverige og Storbritannia. Listen som er utredet av svenske myndigheter er tatt inn i høringsnotatet og gir etter Regelrådets vurdering et godt bilde av mulige berørte virksomheter i Norge.

For øvrig viser departementet også til at «NSMs grunnprinsipper for IKT-sikkerhet» gir god veiledning i grunnleggende IKT-sikkerhet, og at disse prinsippene kan være et godt utgangspunkt for å ha tilstrekkelig god IKT-sikkerhet i virksomheten. Departementet opplyser også om «Rammeverk for håndtering av IKT-sikkerhetshendelser», og at denne kan gi gode råd som virksomhetene kan dra nytte av. Regelrådet finner det positivt at departementet i høringsnotatet gir veiledning og gir kravene i direktivet innhold. Dette gir høringsinstansene bedre forutsetninger for å forstå hva som må til for å oppfylle kravene i direktivet.

Departementet gir gjennomgående informasjon om tilstøtende regelverk slik som sikkerhetsloven og personopplysningsloven. Departementet gir også vurderinger av de tilfeller der regelverkene helt eller til dels overlapper. Blant annet skriver departementet i høringsnotatet at dersom reglene i personopplysningsloven følges, så vil kravene i direktivet også være oppfylt. Etter Regelrådets vurdering gir dette nyttig informasjon for de berørte virksomhetene. Mange virksomheter har brukt store ressurser på å oppfylle det nye personopplysningsregelverket (GDPR). Etter Regelrådets vurdering er det positivt at dette arbeidet også kan dekke flere formål.

4. Er forslaget utformet slik at målene oppnås til en relativt sett lav kostnad for næringslivet?

Det fremgår av høringsnotatet at kravene om sikkerhet og varsling vil kunne innebære økte kostnader for berørte virksomheter. Departementet skriver videre at inndekningen av økte kostnader ikke er mer tyngende enn det som naturlig følger med samfunnsutviklingen. Etter Regelrådets vurdering er det grunn til å tro at god IKT-sikkerhet også vil ha egenverdi for virksomheten. Regelrådet registrerer også at flere sektorer helt eller delvis oppfyller direktivets krav og at personopplysningslovens krav på enkelte områder også dekker NIS-direktivets krav.

Forutsatt at små og mellomstore virksomheter ikke omfattes av reglene mener Regelrådet at det er grunn til å tro at målene kan oppnås til en relativt sett lav kostnad for næringslivet.