

Justis- og beredskapsdepartementet
Postboks 8005 Dep
0030 OSLO

Deres ref:

Vår ref: 18/05085-4

Dato: 21.03.19

Utlendingsdirektoratets svar på felles høring av NOU 2018:14 IKT-sikkerhet i alle ledd og utkast til lov som gjennomfører NIS-direktivet

Utlendingsdirektoratet (UDI) viser til Justis- og beredskapsdepartementets høringsbrev av 21. desember 2018. Departementet har bedt om innspill innen 22. mars 2019.

Departementet har sendt to saker på felles høring;

- Utredning fra IKT-sikkerhetsutvalget (Holte-utvalget) NOU 2018:14: IKT-sikkerhet i alle ledd. Heretter referert til som Holte-utvalget.
- Utkast til lov om gjennomføring av EUs direktiv i norsk rett om sikkerhet i nettverk og informasjonssystemer. Heretter referert til som lovutkastet.

Innledende kommentar til høringsbrevet;

Departementet har ikke tatt stilling til Holte-utvalgets anbefalinger, men sender sakene på felles høring da det er nær sammenheng mellom dem. Det er ikke indikert hvilke anbefalinger eller vurderinger i Holte-utvalgets utredning departementet særlig ønsker innspill på.

De konkrete spørsmål departementet ønsker vurdert i forhold lovutkastet, med unntak av spørsmålet om en slik lov bør vedtas selv om Norge ikke er forpliktet til det, er direkte knyttet til høringsinstansenes virksomhet. Lovutkastet oppfyller bare minimumsforpliktelsene etter NIS-direktivet, det vil si at offentlig forvaltning som helhet ikke er omfattet av lovutkastets virkeområde.

Som offentlig forvaltningsorgan er UDIs kommentarer til lovutkastet gitt med henblikk på Holte-utvalgets anbefaling om å utrede en ny lov om IKT-sikkerhet for samfunnskritiske virksomheter og offentlig forvaltning.

Svar på høringsbrevets spørsmål knyttet til lovutkastet

I hvilken grad arbeides det per i dag systematisk med IKT-sikkerhet i din virksomhet? Følges for eksempel visse standarder for sikkerhetsstyring og internkontroll?

UDI arbeider med å få på plass et helhetlig styringssystem for informasjonssikkerhet. Som en del av dette arbeidet skal UDI fastsette sikkerhetsmål, samt utarbeide og ferdigstille en informasjonsstrategi. Policydokumentene for personvern og sikkerhet er også under revisjon.

Vi arbeider kontinuerlig med risiko og risikoreduserende tiltak, herunder bedre rutiner for oppfølging av risikoreduserende tiltak. UDI ønsker å følge ISO 27001 som førende standard for arbeid med informasjonssikkerhet. Vi benytter veiledere fra Direktoratet for forvaltning og ikt (Difi) og Nasjonal sikkerhetsmyndighet (NSM) som er basert på ISO 27001.

Internrevisjonen i UDI gjennomførte i 2018 en revisjon knyttet til informasjons-sikkerhet i UDI. Kopi av Revisjonsrapport 4/2018 – «Informasjonssikkerhet; baseline, målbildet og sikkerhetsstrategi» er sendt Justis- og beredskaps-departementet. Rapporten er unntatt offentlighet jf. offentleglova § 15 første ledd.

Beskriv hvilke positive konsekvenser forslaget til gjennomføring av NIS-direktivet vil få for din virksomhet.

Holte-utvalget peker på at det i dag er et stort antall lover og forskrifter som har som formål å ivareta informasjonssikkerheten på tvers av sektorene. Det er i tillegg stor variasjon i forhold til hvor klare kravene til informasjonssikkerhet er, og det varierer i hvilken grad informasjonssystemer er omfattet av regelverket. Økende digitalisering i både offentlig og privat virksomhet, og den gjensidige avhengigheten som all samhandling medfører, tilsier at ulike krav til informasjonssikkerhet øker sårbarheten betydelig.

Generelt er det UDIs vurdering at et felles nasjonalt regelverk, som er i overensstemmelse med EUs regelverk, vil være positivt nasjonalt og i norske virksomheters samhandling med land i EU.

Et nærmere svar på spørsmålet om positive konsekvenser er avhengig av hva som defineres som samfunnsviktige tjenester og tilbydere av digitale tjenester, samt om offentlig forvaltning skal omfattes av regelverket. Det fremgår av høringsnotatet at direktivet som lovutkastet skal implementere, har som formål å forbedre det indre markedets funksjon og bidra til økonomisk vekst i EU ved å sikre kontinuitet i leveransen av de aktuelle tjenestene. Det fremgår videre av kapittel 5.3 at departementet har gitt Nasjonal sikkerhetsmyndighet (NSM) i oppdrag å utarbeide mer konkrete vilkår for hvilke virksomheter som skal omfattes.

Som del av offentlig forvaltning vil lovutkastet slik det foreligger i dag, få begrenset virkning for UDI. Det er imidlertid en positiv konsekvens at vi kan ha større tillit til IKT-sikkerheten til private aktører som vi samhandler med og som regnes som tilbyder av samfunnsviktige tjenester, når det finnes felles krav til IKT-sikkerhet.

Dersom lovutkastet også omfatter offentlig forvaltning, slik Holte-utvalget anbefaler og slik EU-kommisjonen oppfordrer medlemslandene til, vil konsekvensene bli flere og tydeligere for UDI. Et felles regelverk vil først og fremst øke sikkerheten og tilliten til våre tjenester og oppgavene vi utfører. Økt sikkerhet betyr økt stabilitet i tjenestene, færre uønskede hendelser og mindre ressursbruk på gjenoppretting av feil eller skader som følge av dårlig sikkerhet. De økte kostnadene som forsterkede krav til IKT-sikkerhet vil medføre må veies opp mot de innsparinger vi på sikt kan få som følge av de positive konsekvensene som er beskrevet over.

Beskriv hvilke negative konsekvenser forslaget til gjennomføring av NIS-direktivet vil få for din virksomhet.

I høringsnotatet punkt 8.3 om varslingskrav, fremgår det at virksomheten må vurdere etter hvilket regelverk det skal varsles i tilfelle hendelse. I lovutkastet, sikkerhetsloven og personopplysningsloven, som er aktuelle for offentlig forvaltning, er varslingskravene ulikt utformet. Departementet legger til grunn at virksomhetene må vurdere om det skal varsles etter ett eller flere regelverk. UDI mener det blir uoversiktlig og en uhensiktsmessig bruk av ressurser å varsle etter flere regelverk. Det bør også vurderes om det kan medføre at en hendelse ikke blir varslet i det hele tatt fordi det antas at det er varslet etter andre regelverk. Etter UDIs vurdering vil det være mer hensiktsmessig med et felles varslingsystem for virksomhetene.

Er din virksomhet i dag underlagt krav til IKT-sikkerhet og varsling? Hvilket regelverk – lover, forskrifter eller annet – er det som stiller slike krav?

UDI som forvaltningsorgan er omfattet av ny sikkerhetslov som trådte i kraft 1. januar 2019. Sikkerhetslovens formål er å sikre grunnleggende nasjonale funksjoner. I det pågående arbeid for å definere hva som ligger i grunnleggende nasjonale funksjoner, har Justis- og beredskapsdepartementet identifisert grensekontroll under lov og orden. Som systemansvarlig for Utlendingsdatabasen (UDB) som leverer informasjon til bruk i grensekontrollen, vil deler av UDIs virksomhet ha virkning for grunnleggende nasjonale funksjoner. I høringsnotatet til lovutkastet punkt 7.1.1 legger departementet til grunn at sikkerhetskravene i sikkerhetsloven mer enn oppfyller direktivets krav.

I tillegg er UDI omfattet av personvernforordningen og personopplysningsloven, samt forvaltningsloven med tilhørende eforvaltningsforskrift.

Bør en slik lov som foreslås i denne høringen vedtas selv om vi ikke er forpliktet til det i henhold til EØS-avtalen?

UDI viser til Holte-utvalgets vurderinger av IKT-rikobildet som beskriver hvordan økende digitalisering utgjør en strukturell sårbarhet i samfunnet, og hvordan offentlig og privat virksomhet har en gjensidig avhengighet. Behovet for en felles lov på tvers av nasjonale sektorer og i samsvar med internasjonale standarder er ikke avhengig av om det er en formell forpliktelse til det. UDI mener det er hensiktsmessig å vurdere om en slik lov også bør omfatte offentlig forvaltning.

Med hilsen

Stephan Mo
avdelingsdirektør

Ina Knarvik Hørnes
seksjonssjef

Dokumentet er godkjent elektronisk i Utlendingsdirektoratet og har derfor ingen signatur.

Brevet sendes kun elektronisk.