**Ny lov om digital sikkerhet – får du eller noen av dine kunder nye plikter?**

Rett før helgen, 5. mai, foreslo Justis- og beredskapsdepartementet en ny lov om digital sikkerhet. Loven skal først og fremst stille sikkerhetskrav til nettverks- og informasjonssystemer og digitale tjenester som er nødvendige for å opprettholde leveransen av samfunnsviktige tjenester.

Les under om du eller dine kunder er pålagt å utarbeide nye risikovurderinger og benytte nye sikkerhetstiltak.

**Hva gjelder loven?**

Norge har mange lovreguleringer som vil ha betydning for digital sikkerhet, men ingen tverrsektoriell lov om digital sikkerhet. Den foreslåtte lov om digital sikkerhet (digitalsikkerhetsloven) med forskrift vil medføre en regulering av digital sikkerhet som ikke er tilstrekkelig ivaretatt i allerede eksisterende regler. «Digital sikkerhet» sikter til beskyttelse av «alt» som er sårbart fordi det er koblet til eller på annen måte avhengig av informasjons- og kommunikasjonsteknologi. I tillegg til å være rettet mot ulike sektorer og bransjer, skal loven også legge til rette for sikkerhet i IKT-produkter, IKT-tjenester og IKT-prosesser.

Loven pålegger forebyggende sikkerhetstiltak som gjør en virksomhet i stand til å stå imot angrep mot nettverks- og informasjonssystemer de er avhengige av. Videre skal loven sikre planer for håndtering av uønskede hendelser.

Digitalsikkerhetsloven med forskrifter følger opp Norges plikter etter EØS-avtalen, og skal sørge for å gjennomføre NIS-direktivet, cybersikkerhetsforordningen og gjennomføringsforordningen i norsk rett. Dermed er det begrenset hvor store endringer det blir i den før den vedtas.

Loven legger også opp til at det kan gis forskrift om sikkerhetssertifisering av IKT-produkter, IKT-tjenester og IKT-prosesser for å gjennomføre forpliktelser etter EØS-avtalen.

**Hvem er omfattet av loven?**

Loven skal forplikte virksomheter som har en særlig viktig rolle for å opprettholde kritisk samfunnsmessig og økonomisk aktivitet, til å overholde digitale sikkerhetskrav og varsle om alvorlige digitale hendelser.

Loven gjelder for det første tilbydere av nærmere spesifiserte samfunnsviktige tjenester. Mer konkret får loven betydning for en rekke store virksomheter innenfor energi, transport, helse, vannforsyning, bank, finansmarkedsinfrastruktur og digital infrastruktur. Forslag til § 6 i digitalsikkerhetsloven nevner at «tilbyder av en samfunnsviktig tjeneste» er virksomheter som

* leverer en tjeneste som er viktig for å opprettholde kritiske samfunnsmessige eller økonomiske aktiviteter,
* er avhengig av nettverks- og informasjonssystemer for å levere tjenesten, og
* kan få tjenesteleveransen betydelig forstyrret av en hendelse

Loven vil også omfatte tilbydere av digitale tjenester. Paragraf 9 i forslaget nevner at tilbydere av en digital tjeneste er virksomheter som tilbyr tjenester som definert i ehandelsloven § 1 andre ledd bokstav a og b i form av nettbaserte markedsplasser, nettbaserte søkemotorer eller skytjenester. Tjenestene nevnt i ehandelsloven, er informasjonssamfunnstjenester.

Det er ventet at det kommer nærmere avgrensning av hvilke aktører som er underlagt loven.

**Hvilke plikter pålegger loven?**

Loven stiller overordnede krav til sikkerhet og varsling, og loven angir hvilke sektorer den gjelder i. Også andre regelverk med tydeligere avgrensinger og konkretiseringer vil fremdeles ha betydning her.

* Risikovurderinger

Både tilbyder av en samfunnsviktig tjeneste og tilbyder av en digital tjeneste må gjennomføre en risikovurdering av nettverks- og informasjonssystemer som benyttes for å levere tjenesten.

* Hensiktsmessige og proporsjonale tekniske og organisatoriske sikkerhetstiltak

Begge typer tilbydere skal iverksette passende sikkerhetstiltak som samlet skal sørge for et sikkerhetsnivå som er tilpasset risikoen. Tilbydere skal dessuten iverksette tiltak for å forebygge, avdekke og redusere konsekvensene av hendelser, slik at tjenesteleveransen kan opprettholdes. Loven angir noen forhold som de ulike tilbyderne skal vektlegge ved vurderingen av hva som er et forsvarlig sikkerhetsnivå.

* Varslingsplikt

Både tilbyder av en samfunnsviktig tjeneste og tilbyder av en digital tjeneste skal uten unødig opphold og uten hinder av taushetsplikt varsle relevant organet om hendelser som virker betydelig inn på tjenesteleveransen

* Plikt til å utpeke en representant i Norge

En tilbyder av digitale tjenester som ikke har sitt hovedkontor i Norge eller en annen EØS-stat, og som tilbyr digitale tjenester i Norge, skal normalt utpeke en representant i Norge. Det er unntak for denne plikten hvis tilbyderen har utpekt en representant i en annen EØS-stat hvor tjenestene tilbys.

Loven vil mest sannsynlig fastsette nærmere bestemmelser i forskrift.

**Hvilken myndighet skal følge opp loven?**

Loven etablerer rammeverk for tilsyn med virksomhetene og åpner for å gi pålegg og eventuelt overtredelsesgebyr ved manglende oppfyllelse av pliktene. Myndighetene skal også ta imot varsler om alvorlige digitale hendelser.

Departementet legger opp til at eksisterende myndighetsstruktur brukes i størst mulig grad for å begrense behovet for nye kontaktpunkter for virksomhetene som blir underlagt regelverket. Myndigheter som allerede utfører oppgaver som ligner oppgaver digitalsikkerhetsloven pålegger dem, skal kunne samkjøre disse så langt det er mulig.

Departementet mener videre at eksisterende myndigheter også bør føre tilsyn med virksomheter som per i dag ikke er underlagt tilsyn.

**\*\*\***

Advokat og assosiert partner Ove A. Vanebo ved CMS Kluge Advokatfirma har skrevet denne teksten. Han tar gjerne en prat med andre partnere som er interesserte i å arbeide mer med den nye loven faglig eller kommersielt.