Nye regler om digital sikkerhet i 2025 – implementering av EU-regelverk i Norge – er din virksomhet forberedt?

Kjetil Haare Johansen
Partner

Ketil Sellæg Ramberg
Partner

Hugo-A. B. Munthe-Kaas
Partner, Head of Compliance

Lars Albert Jøstensen
Senioradvokat

I desember 2023 ble den nye loven om digital sikkerhet (digitalsikkehetsloven) vedtatt. Loven er basert på EUs nye krav til digitalsikkerhet, og vil, sammen med en forskrift, implementere EUs direktiv om sikkerhet i nettverk- og informasjonssystemer, i første omgang gjennom det såkalte NIS1-direktivet.

Digitalsikkerhetsloven har enda ikke trådt i kraft, men vil tre i kraft i 2025, når forskrift om digital sikkerhet, som nå er på høring fra Justis- og beredskapsdepartementet, er vedtatt. Forskriften er på høring med frist 11. desember 2024.

Samtidig skrider EUs lovgivningsarbeid fort frem, og hvor EU allerede i 2022 vedtok et nytt direktiv om nettverk- og informasjonssystemer – NIS2-direktivet – som i sin helhet vil erstatte NIS1. NIS2-direktivet må også implementeres i Norge, og er nå i prosess med å bli innlemmet i EØS-avtalen som må skje først. Departementet har allikevel, i forslag til ny forskrift til digitalsikkerhetsloven søkt å ta høyde for enkelte av de utvidede kravene og pliktene etter NIS2-direktivet.

Det nye regelverket, som forventes å tre i kraft i løpet av 2025, vil stille nye og strengere krav til tilbydere av samfunnsviktige tjenester. Det vil også få implikasjoner for kunder av slike tilbydere, og for selskaper som ikke direkte er underlagt digitalsikkerhetsloven. Driftere av datasentre er ett eksempel på slike virksomheter. NSM – Nasjonal sikkerhetsmyndighet - vil samtidig få nye og utvidede hjemler til håndhevelse, og vil potensielt kunne illegge administrative bøter til selskaper på opptil 4% av den samlede årsomsetningen i foregående regnskapsår.

Er du forberedt på disse nye kravene og forpliktelsene?

Det nye regelverket vil medføre at cybersikkerhetsagendaen vil måtte seile til topps på prioritetslisten for mange selskaper.

NIS2 skulle i EU vært gjennomført i medlemsstatene senest 24. oktober i år, men så langt ligger implementeringen etter skjema, hvor kun et fåtall av EUs medlemsstater så langt har oppfylt kravene. Når NIS2 blir del av EØS-avtalen og implementeringen av denne kommer på plass i EU, vil kravene og forpliktelsene bli mye mer omfattende, og mange virksomheter stiller allerede, som kunder, krav til leverandørers etterlevelse av NIS2-forpliktelser, uavhengig av status på implementering i enkelt land i EU-/EØS.

Kravene som stilles er omfattende, og vil ha betydelig innvirkning på kravene til virksomheters styringssystemer, dets risikovurderinger, for sikkerhetstiltak samt hendelsesrapportering for leverandører (og kunder) av digitale tjenester og for virksomheter med samfunnsviktige funksjoner.

Formålet med digitalsikkerhetsloven er å bidra til å sikre grunnleggende krav til digital sikkerhet i virksomheter med særlig betydning for samfunnet ved å forebygge, avdekke og motvirke uønskede hendelser i nettverk og informasjonssystemer som brukes for å levere samfunnsviktige tjenester og digitale tjenester. Loven stiller krav til digital sikkerhet og varsling ved hendelser som virker betydelig inn på tjenesteleveransen, og angir virkeområdet i form av hvilke sektorer den gjelder for. Om du ikke vet om du er omfattet eller ei, eller om du indirekte påvirker, nå er tiden moden for å undersøke dette.

Hvem blir omfattet av kravene i forskriften?

Forskriftsforslaget presiserer hvem som vil være omfattet av digitalsikkerhetsloven og -forskriften. De som omfattes vil være tilbydere av eksempelvis:

- nettbaserte søkemotorer,
- skytjenesteleverandører,
- nettbaserte markedsplasser, samt
- tilbydere av samfunnsviktige tjenester innen:
  - Energi,
  - Transport,
  - Helse,
  - Vannforsyning,
  - Bank og finansmarkedsinfrastruktur, og
  - Digital infrastruktur.

I utgangspunktet dekkes ikke virksomhet på kontinentsokkelen, den økonomiske sonen og den tilstøtende sonen, og reglene gjelder ikke i utgangspunktet norsk oppstrøms petroleumsvirksomhet, herunder er landanlegg antatt å falle utenfor, men hovedtankanlegg for petroleumsbasert drivstoff vil eksempelvis være omfattet. Norsk oppstrøms petroleumsvirksomhet vil allikevel omfattes og underlegges reglene – på sikt.

NIS2-direktivet vil også utøke bransjer og sektorer som vil bli underlagt kravene i digitalsikkerhetsloven med forskrifter.

Fysisk sikkerhet i datasentre vil som et utgangspunkt ikke reguleres av digitalsikkerhetsloven, men av ny ekomlov, men virksomheter som omfattes av digitalsikkerhetsloven, og som eventuelt benytter seg av datasentere, må allikevel sørge for at de har tilstrekkelig sikkerhet i egen verdikjede, herunder for datasentre og eksterne leverandører som benyttes.

Tilbydere innen flysikringstjenesten, drift av flyplasser, flyselskaper med kommersiell transport, jernbane, t-bane og trikk, trafikkstyring og veiovervåkning, alarmsentraler for eCall, overvåkning av kysttrafikk, havner og havneanlegg, rederier, helse- og omsorgssektoren, systemer for rekvirering av legemidler og andre medisinske produkter, vannforsyning, toppnivådomener, samt samtrafikkpunkter for internett omfattes også.

Virksomheter som har færre enn 50 ansatte og som har en årlig omsetning eller årlig samlet balanse som ikke overstiger 100 millioner kroner, vil ikke være omfattet i utgangspunktet, med mindre det fattes vedtak om loven allikevel skal gjelde for disse.

Hvilke krav stilles?

Forslaget stiller krav om at virksomheter som omfattes, må etablere styringssystemer for digital sikkerhet, gjennomføre risikovurderinger, og sørge for hendelseshåndtering og varsling innen 24 timer etter en digital hendelse.

Styringssystemene skal være basert på "anerkjente standarder", uten at dette er nærmere angitt i forskriften. Styringssystemene må gjøres kjent for virksomhetens ansatte, underleverdører, og andre leverandører som utfører arbeid for eller på vegne av virksomheten. I så måte kan det være verdt å ta med i betraktning en lange og uoversiktlige leverandørkjeder i seg selv kan utgjøre en særlig eksponering og sårbarhet som kan benyttes.

Basert på risikovurderingene som skal gjøres, må man lage en risikohåndteringsplan, og treffe nødvendige organisatoriske, teknologiske, fysiske sikkerhetstiltak samt iverksette nødvendige sikkerhetstiltak for personell. Krav til tekniske sikkerhets tiltak, vil være å ha skriftlige instrukser for rutiner og prosedyrer, to- eller flerfaktorautentisering for adgang til nettverk og informasjonssystemer, tilgangskontroll til innholdet i nettverk og informasjonssystemer basert på tjenstlig behov og tiltak for segmentering av tjenester basert på et prinsipp om minste minimum av rettigheter, og tiltak for å opprettholde tjenesten i form av tilstrekkelig strømtilførsel, eventuelt nødtilførsel av strøm, samt å iverksette tiltak for robuste nettverks tilganger, sikkerhets tiltak for personell, samt benytte taushetsplikt eller konfidensialitetserklæringer, og gjøre oppfølgning og kontroll av underleverandører.

Ved hendelser må det varsles innen 24 timer, med krav til oppdatering av varselet innen 72 timer, og med avgivelse av en hendelsesrapport til NSM – Nasjonal sikkerhetsmyndighet inne én måned fra første varsel.

Videre inneholder forskriftsforslaget bestemmelser om deling av taushetsbelagt informasjon, uavhengig av det dreier seg om tekniske innretninger og fremgangsmåter og/eller om drifts- eller forretningsforhold som det vil være av konkurransemessig betydning å hemmeligholde. Forslaget til forskrift inneholder også enkelte bestemmelser om behandling av personopplysninger.

Nye hjemler for håndheving lagt til Nasjonal sikkerhetsmyndighet (NSM)

Overtredelse av reglene i digitalsikkerhetsloven med forskrift, kan medføre store økonomiske sanksjoner i form av bøter (overtredelsesgebyr) opp til 4 % av årsomsetningen. For offentlige virksomheter kan overtredelsesgebyret maksimalt settes til opptil 25 ganger grunnbeløpet, som gir en bot i størrelsesorden på om lag 3 millioner kroner.

NSM kan videre kreve opplysninger fra virksomheter og kreve tilgang til lokaler for å håndheve regelverket, samt at NSM kan fatte vedtak gi tilbydere pålegg om at eventuell regelverksbrudd skal bringes i orden, samt treffe vedtak om tvangsmulkt for å sikre at pålegg blir oppfylt.

Trenger du mer informasjon?

Trenger du mer informasjon om NIS2 særskilt, så kan du finne mer informasjon om dette her: NIS2 (Network and Information Systems Directive) | DLA Piper

DLA Piper kan også tilby en gjennomgang av regelverket og hvordan best sikre din virksomhet gjennom tilgang til våre fageksperter, både nasjonalt, i Norden og internasjonalt.

Ønsker du en slik gjennomgang, ta da kontakt med:

- **Ketil S. Ramberg** - IPT (inkl. GDPR)
- **Lars Albert Jøstensen** - Forsikring og cybersikkerhet
- **Hugo Munthe-Kaas** - Compliance
- **Kjetil Haare Johansen** - EU/EØS-regulatorisk