Utkast

til lov om sikkerhet i nettverk og informasjonssystemer

Kapittel 1. Innledende bestemmelser

§ 1 *Formål*

Loven skal bidra til å opprettholde kritisk samfunnsmessig og økonomisk aktivitet ved å forebygge, avdekke, motvirke og varsle tilsiktede og utilsiktede uønskede hendelser i nettverk og informasjonssystemer som brukes for å levere samfunnsviktige tjenester.

§ 2 *Virkeområde*

Loven gjelder for tilbydere av samfunnsviktige tjenester innen samfunnssektorene energi, transport, helse, vannforsyning, bank, finansmarkedsinfrastruktur og digital infrastruktur.

Loven gjelder for tilbydere av digitale tjenester, som har sitt hovedforetak i Norge. Tilbyderen anses å ha sitt hovedforetak der den har hovedkontor. Loven gjelder ikke for tilbydere av digitale tjenester som er mikrovirksomheter eller små virksomheter.

Tilbydere av digitale tjenester som ikke er etablert innenfor EØS, kan ikke levere digitale tjenester i Norge uten å ha oppnevnt en representant som er etablert i ett av landene i EØS den leverer digitale tjenester til. Loven gjelder for slike tilbydere dersom den oppnevnte representanten er etablert i Norge.

Loven gjelder ikke for virksomheter som er underlagt EU-basert regelverk som stiller tilsvarende eller mer omfattende krav til sikkerhet og varsling enn de kravene som følger av denne loven.

Loven gjelder ikke for virksomheter som er omfattet av lov 15. juni 2018 nr. 44 om gjennomføring av EUs forordning om elektronisk identifikasjon og tillitstjenester for elektroniske transaksjoner i det indre marked.

Kongen kan gi forskrift med nærmere bestemmelser om lovens virkeområde.

§ 3 *Geografisk virkeområde*

Kongen kan i forskrift bestemme at loven helt eller delvis skal gjelde for Svalbard og Jan Mayen.

§ 4 *Definisjoner*

I denne loven menes med

1. tilbyder av samfunnsviktig tjeneste: virksomhet som leverer en tjeneste som er viktig for opprettholdelsen av kritiske samfunnsmessige- eller økonomiske aktiviteter, som er avhengig av nettverk og informasjonssystemer for å kunne levere tjenesten, og der en hendelse vil kunne få betydelig forstyrrende effekt på tjenesteleveransen, forutsatt at tjenesten omfattes av vedlegg II til NIS-direktivet, slik dette er tatt inn i EØS-avtalen.
2. tilbyder av digitale tjenester: tilbyder av skytjenester, digitale markedsplasser og digitale søkemotorer.
3. nettverk og informasjonssystemer:
    a. elektronisk kommunikasjonsnett, jf. lov 4. juli 2003 nr. 83 om elektronisk kommunikasjon (ekomloven) § 1-5 nr. 2
    b. en enhet eller en gruppe av sammenkoblede eller beslektede enheter, der en eller flere enheter behandler digitale data automatisk ved hjelp av et program
    c. digitale data som lagres, behandles, innhentes eller overføres ved hjelp av elementer som nevnt i bokstav a) eller b) for at dataene skal kunne driftes, vernes, beskyttes eller vedlikeholdes
4. hendelse: ethvert tilfelle av reell negativ virkning på sikkerheten i nettverk og informasjonssystemer

5. sikkerheten i nettverk og informasjonssystemer: den evnen nett eller informasjonssystemer har til å tåle, på et gitt tillitsnivå, enhver handling som går ut over tilgjengeligheten, autentisiteten, integriteten eller tilliten til lagrede, overførte eller behandlede data eller tilknyttede tjenester som tilbys eller er tilgjengelige via slike nett- og informasjonssystemer
6. betydelig forstyrrende effekt: en vurdering av hvilken virkning en hendelse har, som tar utgangspunkt i følgende momenter:
    a. antall brukere som er avhengig av tjenesten som tilbys av den berørte virksomheten
    b. i hvilken grad andre samfunnssektorer som er nevnt i § 2 er avhengig av tjenesten som tilbys av den berørte virksomheten
    c. hvilken virkning en hendelse kan ha i form av alvorlighet og varighet, for økonomiske og samfunnsmessige aktiviteter eller samfunnets sikkerhet
    d. den berørte virksomhetens markedsandel
    e. den geografiske spredning med tanke på området som kan bli påvirket av en hendelse
    f. den berørte virksomhetens betydning for at det er tilstrekkelig tilgang på tjenesten, tatt i betraktning hvilke alternativer som finnes
    g. særlige sektorspesifikke forhold
7. nettbasert markedsplass: en digital tjeneste som gjør det mulig for forbrukere og næringsdrivende å inngå nettbaserte salgs- eller tjenesteavtaler med næringsdrivende, enten på nettstedet til den nettbaserte markedsplassen eller på nettstedet til en næringsdrivende som bruker datatjenester som leveres av den nettbaserte markedsplassen
8. nettbasert søkemotor: digital tjeneste som gjør det mulig for brukere å foreta søk på i prinsippet alle nettsteder eller nettsteder på et bestemt språk, på grunnlag av en forespørsel om et hvilket som helst emne i form av et nøkkelord, en setning eller andre inndata, og som viser lenker hvor det er mulig å finne informasjon om det forespurte innholdet
9. skytjeneste: en digital tjeneste som gir tilgang til en skalerbar og fleksibel samling av delbare databehandlingsressurser

Kongen kan gi forskrift med nærmere bestemmelser om definisjoner.

§ 5 *Forholdet til andre lover*

Dersom annen lov stiller krav om sikkerhet og varsling som minst tilsvarer denne loven, skal annen lov benyttes.

§ 6 *Behandling av personopplysninger*

Når det er nødvendig for å utføre pliktene som følger av loven, kan personopplysninger behandles. Dette gjelder også særlige kategorier personopplysninger.

Kapittel 2. Krav om sikkerhet og varsling for tilbydere av samfunnsviktige tjenester

§ 7 *Krav om sikkerhet for tilbydere av samfunnsviktige tjenester*

Tilbyderen av en samfunnsviktig tjeneste skal gjennomføre en risikovurdering av de nettverk og informasjonssystemer som benyttes for å levere tjenesten.

For å redusere risikoen skal tilbyderen iverksette hensiktsmessige og proporsjonale tekniske og organisatoriske sikkerhetstiltak. Tiltakene skal samlet sørge for et sikkerhetsnivå som er tilpasset risikoen. Ved vurderingen av hva som er et passende sikkerhetsnivå skal det blant annet ses hen til den teknologiske utviklingen.

For å opprettholde tjenesteleveransen skal tilbyderen iverksette proporsjonale tiltak for å forebygge, avdekke og redusere konsekvensene av hendelser.

Kongen kan gi forskrift med nærmere bestemmelser om sikkerhetskrav.

§ 8 *Krav om varsling for tilbydere av samfunnsviktige tjenester*

Tilbyderen av en samfunnsviktig tjeneste skal varsle det organ Kongen utpeker om hendelser som har betydelig innvirkning på opprettholdelsen av tjenesteleveransen. Ved vurderingen av om innvirkningen er betydelig skal det legges vekt på antall brukere som påvirkes, hendelsens varighet og størrelsen på det geografiske området som berøres av hendelsen.

Varselet skal inneholde nok opplysninger til at det kan fastslås om hendelsen har virkninger utover Norges grenser.

Kongen kan gi forskrift med nærmere bestemmelser om varslingskrav.

Kapittel 3. Krav om sikkerhet og varsling for tilbydere av digitale tjenester

§ 9 *Krav om sikkerhet for tilbydere av digitale tjenester*

Tilbyderen av en digital tjeneste skal gjennomføre en risikovurdering av nettverk og informasjonssystemer som benyttes for å levere tjenesten.

For å redusere risikoen skal tilbyderen iverksette hensiktsmessige og proporsjonale tekniske og organisatoriske sikkerhetstiltak. Tiltakene skal samlet sørge for et sikkerhetsnivå som er tilpasset risikoen. Ved vurderingen av hva som er et passende sikkerhetsnivå skal virksomheten se hen til den teknologiske utviklingen og ta hensyn til følgende elementer

a. sikkerheten i systemer og utstyr/anlegg
b. hendelseshåndtering
c. styring av opprettholdelse av tjenesteleveransen
d. overvåking, revisjon og testing
e. anerkjente internasjonale standarder

For å opprettholde tjenesteleveransen skal tilbyderen iverksette tiltak for å forebygge, avdekke og redusere konsekvensene av hendelser.

Kongen kan gi forskrift med nærmere bestemmelser om sikkerhetskrav.

§ 10 *Krav om varsling for tilbydere av digitale tjenester*

Tilbyderen av en samfunnsviktig tjeneste skal varsle det organ Kongen utpeker om hendelser som har betydelig innvirkning på tjenesteleveransen. Ved vurderingen av om innvirkningen er betydelig skal det legges vekt på antall brukere som påvirkes av hendelsen, dens varighet, størrelsen på det geografiske området som berøres, omfanget av funksjonalitetssvikten i tjenesten og omfanget av innvirkningen på økonomisk og samfunnsmessig aktivitet.

Varselet skal inneholde nok opplysninger til at tilsynsmyndigheten eller responsmiljøet kan fastslå om hendelsen har virkninger utover Norges grenser.

Plikten til å varsle en hendelse gjelder bare dersom tilbyderen har tilgang til informasjon som er nødvendig for å kunne vurdere om hendelsen har betydelig innvirkning på tjenesteleveransen.

Kongen kan gi forskrift med nærmere bestemmelser om varslingskrav.

Kapittel 4. Responsmiljøer, tilsynsmyndigheter, pålegg, tvangsmulkt og overtredelsesgebyr

§ 11 *Responsmiljøer*

Kongen kan utpeke ett eller flere responsmiljøer som skal kunne motta varsler etter loven.

Kongen kan i forskrift gi nærmere bestemmelser om responsmiljøer og hendelseshåndtering.

§ 12 *Tilsynsmyndigheter*

Kongen utpeker en eller flere tilsynsmyndigheter som skal føre tilsyn med tilbydere av samfunnsviktige og digitale tjenester.

Det skal bare føres tilsyn med digitale tjenester etter at tilsynsmyndigheten har mottatt opplysninger om overtredelser av bestemmelser gitt i eller i medhold av denne loven og når tilsynsmyndigheten finner det nødvendig.

Tilbydere av samfunnsviktige tjenester og tilbydere av digitale tjenester skal etter pålegg fra tilsynsmyndigheten gi de opplysninger den krever for å utføre sine oppgaver. Tilsynet skal til enhver tid ha uhindret adgang til ethvert sted som omfattes av loven.

Tilbydere av samfunnsviktige tjenester og tilbydere av digitale tjenester plikter å medvirke til gjennomføring av tilsynet.

Kongen kan gi forskrift om gjennomføring av tilsyn.

§ 13 *Pålegg*

Ved overtredelse av bestemmelser gitt i eller i medhold av loven kan tilsynsmyndigheten gi tilbydere av samfunnsviktige tjenester og tilbydere av digitale tjenester pålegg om at forholdet skal bringes i orden. Tilsynsmyndigheten kan sette en frist for oppfyllelse av pålegget.

§ 14 *Tvangsmulkt*

For å sikre at plikt etter vedtak som er fattet i medhold av § 13 blir oppfylt, kan tilsynsmyndigheten ilegge en tvangsmulkt som løper inntil forholdet er brakt i orden.

Vedtak om tvangsmulkt kan påklages til departementet.

Kongen kan gi forskrift om tvangsmulkt, herunder om mulktens størrelse og varighet og om gjennomføring av tvangsmulkten.

§ 15 *Overtredelsesgebyr*

Tilsynsmyndigheten kan pålegge en virksomhet overtredelsesgebyr dersom virksomheten eller noen som handler på dennes vegne har overtrådt bestemmelser gitt i eller i medhold av denne loven eller har gitt uriktige eller ufullstendige opplysninger til tilsynsmyndigheten. Dette gjelder selv om ansvaret for overtredelsen ikke kan rettes mot noen enkeltperson. Fysiske personer kan bare ilegges overtredelsesgebyr for forsettlige eller uaktsomme overtredelser.

Ved fastsettelse av overtredelsesgebyrets størrelse skal det særlig legges vekt på overtredelsens grovhet, overtredelsens varighet, utvist skyld og virksomhetens omsetning.

Dersom den ansvarlige for overtredelsesgebyret er en virksomhet som inngår i et konsern, hefter foretakets morselskap og morselskapet i det konsern selskapet er en del av, subsidiært for beløpet.

Adgangen til å pålegge overtredelsesgebyr foreldes etter fem år. Fristen avbrytes når tilsynsmyndigheten meddeler virksomheten at denne er mistenkt for overtredelse av loven eller vedtak fastsatt med hjemmel i loven.

Vedtak om overtredelsesgebyr kan påklages til departementet.

Kongen kan gi forskrift om overtredelsesgebyr, herunder om vilkår for å ilegge overtredelsesgebyr, om størrelsen på overtredelsesgebyret, om rente og tilleggsgebyr dersom overtredelsesgebyret ikke blir betalt ved forfall og om frafall av ilagt overtredelsesgebyr.

Kapittel 5. Ikrafttredelse

§ 16 *Ikrafttredelse*

Loven trer i kraft fra det tidspunktet Kongen bestemmer. Kongen kan sette i kraft forskjellige bestemmelser til ulik tid.