



JUSTIS- OG
BEREDSKAPSDEPARTEMENTET

Postboks 8005 Dep.
0030 OSLO

Svar på invitasjon om høring av digitaliseringssikkerhetsforskriften

Tolletaten viser til høring av forslag til forskrift til lov 20. desember 2023 nr. 108 om digital sikkerhet (digitalsikkerhetsloven) med frist 11. desember 2024. Digitalsikkerhetsloven settes i kraft når forskriften blir vedtatt. Tolletaten har fått innvilget en utsatt frist til 20. desember 2024, til å komme med våre innspill.

Tolletaten vil først generelt bemerke at vi støtter at loven suppleres og utdypes med en forskrift. Vi har imidlertid noen innspill:

Virkeområdet er en sentral del av NIS og NIS2. Tilbydere av samfunnsviktige tjenester er definert i digitalsikkerhetsloven § 6 og må etter første ledd bokstav a til e oppfylle tre kumulative vilkår: virksomheten må levere en tjeneste som er viktig for å opprettholde kritiske samfunnsmessige eller økonomiske aktiviteter, den må være avhengig av nettverk og informasjonssystemer for å levere tjenesten, og kan få tjenesteleveransen betydelig forstyrret av en hendelse. Forskriftsutkastet § 1 regulerer hvilke virksomheter som er å anse som tilbydere av samfunnsviktige tjenester. Tolletaten er per i dag ikke klassifisert som en samfunnsviktig tjeneste i henhold til forslaget § 1.

I § 2 første ledd bokstav a fremgår det at loven gjelder for tilbydere av samfunnsviktige tjenester innenfor samfunnssektorene energi, transport, helse, vannforsyning, bank, finansmarkedsinfrastruktur og digital infrastruktur. Opplistingen følger av NIS- direktivets vedlegg II.

Tolletaten utfører samfunnsviktige tjenester ved at vi ivaretar 19 sektormyndigheters krav til varer som krysser grensen. Dette gjelder for eksempel matsikkerhet, medisinsk sikkerhet, miljøsikkerhet med mer. Tolletaten fungerer som det første kontaktpunktet for all import og eksport av varer til Norge, og har en nøkkelrolle i å sikre at samfunnet til enhver tid har tilgang på godkjente varer i den lovlige vareførselen.

Loven definerer ikke uttømmende hvilke tilbydere som omfattes av loven, jf. forskriftens § 4 som gjelder for andre tilbydere av samfunnsviktige tjenester enn de som er nevnt i § 1, hvor ansvarlig departementet i særlige tilfeller kan fatte vedtak om at loven helt eller delvis skal gjelde. Unntaket er imidlertid begrenset til områdene nevnt i digitaliseringssikkerhetslovens § 2, noe som tilsier at Tolletatens virke faller utenfor loven og forskriftens ramme. Ettersom Norge ikke er medlem av EU står Tolletaten likevel i en særstilling sammenlignet med EU medlemslandenes

tollmyndigheter. Norges forsyningssikkerhet er sårbar for forstyrrende hendelser på grensen dersom det oppstår en forstyrrende hendelse, som rammer våre nettverk.

Hvordan andre tilbydere av samfunnsviktige ytelser enn Tolletaten reguleres vil være relevant for Tolletaten, selv om vi direkte ikke omfattes av datasikkerhetsloven. Vi ønsker derfor å gi noen innspill til forslaget som er på høring.

Slik vi forstår forskriftens § 5 om innmelding av tilbyder av samfunnsviktig tjeneste, så vil den bare dekke virksomheter som inngår i lovens virkeområde på de utpekte sektorområdene. Dette er imidlertid uklart og bør presiseres.

I punkt 4.2.4 foreslås det at tilbydere av samfunnsviktige tjenester skal rapportere til både Nasjonal sikkerhetsmyndighet og relevante tilsynsmyndigheter. Departementet skriver at «*Virksomheter som opererer innen flere sektorer, må melde inn til samtlige tilsynsvirksomheter i sektorene de opererer i, samt Nasjonal sikkerhetsmyndighet.*» Dette kan innebære at virksomheter må rapportere til flere kanaler, noe som kan gjøre prosessen mer komplisert med større sjanse for at det oppstår feil underveis i prosessen.

For å forenkle og klargjøre rapporteringen, anbefaler Tolletaten at det defineres én enkelt kanal for innmelding og kommunikasjon, inkludert ved opphør av tjenester. Denne kanalen bør være ansvarlig for å videreformidle rapporteringen til relevante aktører.

I punkt 4.2.5 og forskriftens § 2 foreslås det at mikrovirksomheter, dvs. virksomheter med færre enn 50 ansatte og en årlig omsetning under 10 millioner euro, unntas fra § 13 og § 15 i loven. Vi har forståelse for at bestemmelsen følger av EU-regelverk, men savner en begrunnelse for hvorfor disse unntakene også skal gjøres gjeldende i Norge.

Vi tror det vil være problematisk å etablere en presedens der underleverandører til samfunnsviktige tjenester ikke er underlagt de samme kravene som hovedtilbyderne. Å unnta disse virksomhetene vil kunne undergrave de eksisterende sikkerhetskravene, svekke beskyttelsen av samfunnskritiske tjenester og bryte sikkerheten i leverandørkjedene.

Til punkt 5.3.2 og i § 6 andre ledd, hvor det foreslås en bestemmelse om at styringssystemet skal baseres på «anerkjente standarder», bør det presiseres nærmere hva som ligger i dette. Manglende presisering kan føre til usikkerhet for virksomheter som benytter seg av internasjonale leverandører eller som opererer i flere jurisdiksjoner. Uklare regler kan skape utfordringer for både tilbydere av samfunnsviktige tjenester og tilsynsmyndigheter, da det vil være vanskelig å sikre at sikkerhetsnivåene er tilstrekkelige og harmoniserte på tvers av landegrenser. Tolletaten anbefaler derfor at Nasjonal sikkerhetsmyndighet får ansvaret for å definere hvilke anerkjente standarder som bør benyttes, og at dette gjøres gjennom veiledning for styringssystemer.

Til punkt 5.3.3. om risikovurdering vil Tolletaten bemerke at manglende tydelige og felles retningslinjer kan resultere i inkonsekvent praksis, noe som kan føre til kritiske sikkerhetsgap som går uoppdaget. For eksempel kan virksomheter i samme sektor tilnærme seg risikovurderinger på ulik måte, noe som kan skape usikkerhet både internt og for tilsynsmyndighetene.

For å sikre at risikovurderingene utføres med samme kvalitet på tvers av virksomheter, bør Nasjonal sikkerhetsmyndighet som minimum definere den overordnede prosessen for risikovurdering. Dette kan inkludere scenario- og tiltaksbanker som virksomhetene kan bruke, og som bør oppdateres regelmessig i samsvar med det gjeldende trusselbildet. Disse ressursene bør være sektorspesifikke for å ta hensyn til de ulike risikofaktorene i hver bransje.

Til punkt 5.3.5 savner Tolletaten tiltak som sikrer evnen til å håndtere og oppdage hendelser. I tillegg til kravene til styringssystemet, bør det defineres at et organisatorisk tiltak er å ha dedikert personell for operativ sikkerhet. Dette kan enten være egne ansatte eller ekstern kompetanse fra sikkerhetsleverandører, som kan ivareta den tekniske sikkerheten, samt sikkerhetsarkitektur for nettverket og informasjonssystemene.

Til punkt 5.3.5.2 savner Tolletaten at det nevnes at tilbydere av samfunnsviktige tjenester også kan pålegges å følge anbefalinger fra Nasjonal sikkerhetsmyndighet om teknologiske sikkerhetstiltak. Dette vil sikre at virksomhetene kontinuerlig kan tilpasse seg nye trusselbilder og teknologisk utvikling.

Til punkt 5.3.5.3 vil vi påpeke at de fysiske sikringstiltakene som beskrevet forutsetter at tilbydere av samfunnsviktige tjenester har egne datasentre med fysisk kontroll over lokasjonen. Virksomheter som skal flytte sine datasentre til skyleverandører i løpet av de kommende årene vil vanskelig kunne oppfylle kravene i § 11 i den foreslåtte forskriften. Forskriftsteksten bør ivareta dette bedre.

Når skyleverandører som Microsoft, Amazon eller Google benyttes, har tilbyderne ikke kontroll over hvilke fysiske datasentre som benyttes (kun geografiske lokasjoner), eller hvordan dataene er fordelt på tvers av flere fysiske lokasjoner globalt. I tillegg kan data være spredt på tvers av forskjellige land, noe som kan gjøre det vanskelig å sikre tilstrekkelig fysisk beskyttelse i henhold til lovens krav.

Videre kan dette bli enda mer utfordrende når underleverandører benyttes av skyleverandørene, som ofte kan ha sine egne datasentre som er utenfor virksomhetens direkte kontroll. Eksempler på dette kan være tjenester som tilbys gjennom en tredjeparts integrasjon eller når flere nivåer av underleverandører er involvert i drift og vedlikehold av datasentrene, noe som ikke er et uvanlig oppsett. I slike tilfeller blir det svært vanskelig å sikre at de fysiske sikkerhetstiltakene oppfyller kravene i loven, da ansvaret blir delt på flere aktører.

Til punkt 12 og forskriftens § 23 om overtredelsesgebyr foreslås det en øvre ramme på 25G (p.t. 3 millioner kroner) for offentlige virksomheter. I og med at dette overtredelsesgebyret er av samme type som personvernforordningens overtredelsesgebyr, er det viktig at disse etter en helhetsvurdering kan avkortes ved en overtredelse som gjelder begge regelverk. Et sikkerhetsbrudd vil også ofte være et brudd på personvernforordningen. Tolletaten har ingen innspill for øvrig til dette punktet.

Med hilsen

Marius Mølmen Moen

Avdelingsdirektør

Ellen Baardvik

Seniorrådgiver

Dokumentet er elektronisk godkjent

Mottaker(e):
JUSTIS- OG
BEREDSKAPSDEPARTEMENTET

Kopimottaker(e):
FINANSDEPARTEMENTET