

Oslo, 30. september 2018

Høringssvar fra Abelia

Forskrifter til ny sikkerhetslov

Abelia er NHOs landsforening for kunnskaps- og teknologibedrifter, vi har vel 2 100 medlemsbedrifter med omtrent 48 000 årsverk over hele landet. Abelia har medlemmer innenfor blant annet IKT, undervisning, forskning, konsulenttjenester, kreative virksomheter og interesseorganisasjoner.

Bakgrunn

Abelia ønsker å takke for muligheten til å komme med høringssvar til forskrifter til ny sikkerhetslov. Vi har tidligere gitt innspill i flere fora og høringer knyttet til arbeidet med ny sikkerhetslov og forskriftene. Abelia er positive til regjeringens pågående arbeid med sikkerhet, og er generelt av den mening at det er høyst nødvendig med oppdatering av regelverket.

Norge er blant verdens mest digitaliserte land. Abelias [Omstillingsbarometer](#)¹ viser at Norges befolkning er de mest digitale i verden, målt i grunnkompetanse og bruk av teknologi. Norsk næringsliv rangeres til 4. plass i verden på teknologi og digitalisering, og på digitalisering av offentlige tjenester ligger vi på 9. plass i verden. Det er svært gledelig at Norge gjør det bra i internasjonal målestokk på disse målingene. Likefult betyr dette også at Norge er med på å trække opp den digitale stien, noe som også betyr at vi må være særlig oppmerksomme på risikobildet for digital kriminalitet, internasjonal etterretningsvirksomhet og på informasjonssikkerhet generelt.

Abelia representerer en stor bredde av næringslivet i Norge. En fellesnevner er at tillitt, trygghet, forutsigbarhet og sikkerhet er vesentlig for deres virksomheter. Med dette som utgangspunkt vil vi nedenfor fremme hensyn som vi mener bør tas i arbeidet med forskriftene spesielt og sikkerhetsområdet generelt.

Kostnader for næringslivet

I vårt [høringsinnspill til ny sikkerhetslov](#)² tok vi opp vår bekymring knyttet til høye, og uforutsigbare kostnader ny sikkerhetslov vil medføre for næringslivet. Etter at forskriftene er sendt på høring står fortsatt denne bekymringen seg. Eksempelvis er det uklart hva "grunnleggende nasjonale funksjoner" er, og hvordan det skal konkretiseres i praksis. I høringsnotatet beskrives det som:

«Grunnleggende nasjonale funksjoner» er tjenester, produksjon og andre former for virksomhet som er av en slik betydning at et helt eller delvis bortfall av funksjonen vil få konsekvenser for statens evne til å ivareta nasjonale sikkerhetsinteresser, jf. sikkerhetsloven § 1-5 nr. 2.

En funksjonsorientert definisjon som dette er som utgangspunkt bra, men uten følge av ytterligere presiseringer etterlater det like fullt usikkerhet om hva som vil omfattes. Det kan være uklart, i ny sikkerhetslov og tilhørende forskrifter, å vite om hvor det skjermingsverdige objektet slutter. Eksempelvis innbefatter elektronisk infrastruktur mye, og en krevende vurdering kan være om infrastrukturen er skjermingsverdig fra kjernenettet og helt ut til forbrukerens husvegg, eller hvor det evt. stopper.

Abelia mener at virksomheter aktivt bør involveres i vurderingene av hva som skal omfattes, og ved uenighet, gis adgang til å klage på avgjørelsen og hvor det er en hurtig behandling av slike klager. Vi ber videre om at definering av hva som er "grunnleggende nasjonale funksjoner" gis prioritet og at dette arbeidet igangsettes umiddelbart. Det bør på ingen måte være tvil om en virksomhet eier et skjermingsverdig objekt når et nytt regelverk trer i kraft.

¹ <https://www.abelia.no/politikk/omstillingsbarometer-2018/>

² <https://www.abelia.no/contentassets/60b1642b7c884ade862aa109b38be15c/horingsinnspill-om-lov-om-nasjonal-sikkerhet.pdf>

Effekten av ny sikkerhetslov, og tilhørende forskrifter, er krevende for næringslivet å forutse, blant annet fordi pliktene virksomhetene vil omfattes av er utydelige. Departementet beskriver i høringsbrevet at kostnadene for etterlevelse av krav kan forventes å være moderat for selskap som allerede er omfattet, mens det for de som først blir omfattet av sikkerhetsloven etter ny ordning kan bli en større belastning. Begrensningene som trekkes frem i lovens §4-3 om at kostnadene ved sikkerhetstiltak skal stå i et rimelig forhold til det som kan oppnås med tiltaket er nødvendig. Praxis for hva som er et *rimelig forhold* kan bli avgjørende for bedriftenes konkurranseevne. Det bør, også i effektueringen av nytt regelverk, legges til grunn at sikkerhetstiltak ikke bør forringe bedriftenes konkurranseevne ved å påføre unødvendige kostnader. Abelia ønsker videre å påpeke at det vil være svært uheldig dersom praktiseringen av lovverket skulle få utilsiktede, uheldige og unødvendig fordyrende konsekvenser for næringslivet. Abelia forutsetter at konsekvenser for næringslivet, næringslivets kostnader og innovasjonsevne blir førende for det videre arbeidet med forskriftene, og effektueringen av disse.

Vi vil advare om at en tilbakevirkende kraft av regelverket kan få store følger for næringslivet. En rekke aktører som for eksempel tilbyr elektronisk infrastruktur i dag, har et betydelig antall objekter som i helhet utgjør dagens fungerende infrastruktur. Dersom mer omfattende sikringstiltak må gjennomføres på objekter som allerede er etablert og i drift, vil kostnaden være betydelig og muligens uoverkommelig.

Det er viktig at arbeidet med kritisk infrastruktur og kritiske samfunnsfunksjoner (KIKS) samordnes, siden det i dag er mange aktører som har forskjellige tolkninger og definisjoner. Det har ført til at aktørene har et uklart bilde på hva som ligger i KIKS og hvem som omfattes.

Den betydelige uforutsigbarheten ved konsekvensene av ny sikkerhetslov og tilhørende forskrifter gjør at Abelia mener det bør gjennomføres en evaluering innen minst ett, maksimalt tre, år etter ikrafttredelsen.

Begrensninger i leverandørmarkedet

Abelia har både norske og utenlandske bedrifter med virksomhet i Norge som medlemmer. Alle bidrar til verdiskaping og sysselsetting, og for Abelia er det et viktig overordnet prinsipp at alle bedrifter bør kunne konkurrere i det norske markedet, og at disse gis lik innsikt i vilkårene for virksomhet og konkurranse.

I den offentlige debatten blir det diskutert og spekulert i intensjonene til enkeltaktører. Abelia tar ikke stilling til hvilke enkeltaktører som bør, eller ikke bør, få mulighet til å levere kritisk infrastruktur eller håndtere ulike former for sensitiv informasjon. Vi tar ikke stilling til hvilke land Norge bør ha et sikkerhetspolitisk samarbeid med. Vi vil derimot advare mot et regelverk som fører til at beslutninger tas ensidig på grunnlag av den nasjonale opprinnelsen til virksomheter.

I en digital verden med et vesentlig tempo i teknologisk utvikling blir teknologien i seg selv et vesentlig sikkerhetsaspekt. Teknologi brukes med både "gode og onde" hensikter, og er i dag i stor grad et kappløp om den mest avanserte teknologien. Ny teknologi kan tidvis overkjøre gammel, og gjøre den usikker og utsatt for angrep. Når det tas beslutninger om hvem som kan, og ikke kan, velges som leverandører bør den teknologiske sikkerheten vektas tungt. Beslutninger bør ikke tas utelukkende på grunnlag av nasjonalitet. Dette vil kunne føre til manglende muligheter til å kjøpe den mest avanserte og sikreste teknologien.

Vi er bekymret for at slike føringer vil medføre svekket konkurranse i leverandørmarkedet for infrastruktur som omfattes av sikkerhetsloven. Slik svekkelse vil medføre både manglende mulighet til å fritt velge beste og sikreste produkter, samt det vil kunne heve prisnivået og med dermed utelukke de sikreste alternativene.

Teknologiprodukter er ofte sammensatt av deler fra en rekke ulike underleverandører i en verdikjede. Ofte vil flere av disse underleverandørene være fra land Norge ikke har et sikkerhetspolitisk samarbeid med. Det kan være svært krevende å spore og kvalifisere opphavet til alle deler av slike verdikjeder. Fokuset bør derfor dreies mot å sette leverandører som er omfattet av sikkerhetsloven i stand til å vurdere risiko, sette sikkerhetskrav og bygge operasjonsmodeller som ivaretar sikkerhetsaspektet på en god måte. En viktig faktor her vil være et økt krav om tredjepartstesting av utstyr for å sikre at produkter og tjenester tilfredsstiller sikkerhetskravene. Videre mener

Abelia at det bør tillegges betydelig vekt på at de leverandører som er underlagt sikkerhetslovens bestemmelser, gis reell mulighet for selvstendige risikoanalyser og basert på dette stiller krav til sine underleverandører.

Sikkerhetsklarering

Med utvidelse av ny sikkerhetslovs nedslagsfelt vil det også være økt behov for sikkerhetsklarering. Klarering er et avgjørende element for næringsliv som på den ene siden er omfattet av særlige sikkerhetskrav, og på den andre siden også leverandører de benytter for blant annet å ivareta sikkerheten.

Dessverre opplever næringslivet i dag at sikkerhetsklareringer tar svært lang tid, er uforutsigbare og lite transparente med hensyn til hvem som kan og ikke kan få sikkerhetsklarering. Dette medfører økt risiko, redusert sikkerhet, tapt verdiskaping og personlig og yrkesmessig usikkerhet for enkeltindividene det gjelder.

I EOS-utvalgets årsmelding for 2017 viser utvalget til at de i de seks foregående årsmeldinger har påpekt at saksbehandlingstiden i klareringssaker er alt for lang. Dette gjelder både anmodning om klarering, anmodning om innsyn, klage 1. instans og klage 2. instans. Det er kritikkverdig at kontrollorganet skal måtte påpeke dette over så lang tid, uten at det gjøres nødvendige grep. Dette bør utbedres umiddelbart.

Abelia mener det bør være sammenheng mellom de krav som stilles til næringslivet, og tilgangen på de ressurser næringslivet er avhengig av for å møte kravene som stilles av myndighetene.

Vi ber derfor om at departementet, gjennom sitt arbeid med høringen og omkringliggende aktivitet, sikrer forutsigbarhet gjennom økt transparens i vurderingskriterier og betydelig kortere saksbehandlingstider. Ventetiden på overføring av sikkerhetsklarering fra land Norge samarbeider med bør være så kort som mulig.

Leverandørklarering vil også kunne bli mer aktuelt med utvidelsen av lovens virkeområde. Her bør det tillegges stor vekt på behovet for god grunnsikring, risikovurderinger, revisjoner, tester og operasjonsmodeller hos virksomheter som har leverandører som skal klareres.

Kompetanse

Abelia har i flere år påpekt behovet for økt IT-kompetanse generelt i Norge, og økt IT-sikkerhetskompetanse spesielt. Flere rapporter deriblant Lysne-utvalgets rapport belyser kompetansebehov på sikkerhetsområdet. Abelia benytter igjen anledningen til å understreke hvor avgjørende det er at vi i Norge evner å heve IT-kompetansen generelt og sikkerhetskompetanse spesielt i samfunnet. Med et relativt lavt antall personer med IKT-sikkerhetskompetanse blir vi sårbare som nasjon. Når også Traavik-utvalget påpeker at økt og tilstrekkelig kompetanse er en forutsetning for at en ny sikkerhetslov vil fungere i praksis, bør dette være en ytterligere vekker. Ny sikkerhetslov og tilhørende forskrifter skaper ytterligere press på IKT-sikkerhetskompetanse, og tiltak for å avlaste dette presset bør prioriteres.

Samarbeid mellom offentlig og privat sektor

Koordinerte ondsinnede angrep, gjerne med internasjonalt opphav blir stadig mer vanlig. Skillet mellom hva som er et angrep mot det norske samfunnet og hva som er et angrep mot enkeltvirksomheter kan være uklart. Angrep kan utføres på tvers av sektorer og konsekvensene kan ramme bredt.

Næringslivet generelt, og IKT-sektoren spesielt, er helt avhengig av støtte fra norske myndigheter i form av løpende informasjonsutveksling for å kunne eliminere eller begrense skadevirkninger i samfunnet.

Utteksling av trusselvurderinger og annen sikkerhetsinformasjon må styrkes. Det er viktig at relevante aktører blir informert slik at alvorlige hendelser ikke får et større omfang enn nødvendig på grunn av manglende vilje eller evne fra myndighetene til å dele informasjon (kapittel 4.3). Denne informasjonen må være umiddelbar, og må tilflytte både offentlige og private virksomheter.

I forslaget til forskriftene står det at NSM *kan* dele informasjon, men i flere sammenhenger har relevante virksomheter påpekt at det er vanskelig å få relevant informasjon fra NSM. Bruken av "*kan dele*" er derfor ikke

tilstrekkelig hvis man skal klare å komme med raske mottiltak. Abelia anbefaler at NSM, og andre relevante instanser, forpliktes til å dele relevant informasjon.

De nye forskriftene må også stille tydelige krav til hvilke konkrete trusselvurderinger og annen sikkerhetsinformasjon som skal deles. Det bør også fremkomme av forskrift hvordan denne type informasjon skal formidles (muntlig, papir, elektronisk) til mottaker. Eventuell bruk av skjermingsverdige, graderte eller ugraderte systemer må fremkomme i forskriftene. Det er for eksempel ikke tilstrekkelig med halvårlige informasjonsmøter med PST eller NorCERT.

Videre bør mottak av slik informasjon ikke være betinget av betalingsevne, men heller av informasjonens relevans for virksomheten. Informasjonsflyten mellom offentlig og privat virksomhet vedrørende hendelser bør være kostnadsfri.

Innen sikkerhetsfeltet sitter myndighetene i dag med en lang rekke roller fordelt på få offentlige aktører. Eksempelvis vil det å inneha kontroll- eller reguleringsmyndighet på et område hvor den offentlige instansen også har inntekstgenererende arbeid kan bli problematisk. Vi vil særlig gjøre oppmerksom på en voksende bekymring om NSMs mange roller, som spenner fra å være tilsynsmyndighet, rådgiver, sikkerhetstester, kursholder, godkjenningssinstans mm.

Informasjonssikkerhet er et fagfelt som også representerer store verdiskapingsmuligheter, og potensielt mange nye arbeidsplasser og eksportmuligheter. I likhet med [Digital21](https://digital21.no/)³, mener Abelia det offentlige må ta verdiskaping i privat næringsliv på alvor. Ryddighet og rettferdighet i offentlig opptreden i markeder hvor det eksisterer private virksomheter er en vesentlig del av dette. For eksempel må konkurranse foregå på like vilkår der hvor både det offentlige og private tilbyr kurs, sikkerhetstester og lignende.

Annet

- **Kapittel 7.2.7.** I høringsnotatet bes det om å vurdere ordlyden «sikkerhetstruende virksomhet». Abelia mener bruken av begrepet er pedagogisk misvisende, og anbefaler i stedet bruk av begrepet "sikkerhetstruende aktivitet".
- **Kapittel 7.4.1.** Den nye sikkerhetsloven får et bredere nedslagsfelt enn tidligere og det vil bety at flere private bedrifter blir underlagt loven, og at mer informasjon blir gradert BEGRENSET. Siden flere av leverandørene til disse virksomhetene er internasjonale, og siden aktuell kompetanse er lite tilgjengelig, vil det være svært viktig å få gode og raske rutiner for klarering/autorisasjon for å kunne bidra til stabil og sikker drift. Det etterlyses derfor enklere/tydeligere rutiner for personell fra Nordiske land, NATO-land eller EU-land for å sikre operasjonell kapasitet og leveranseevne som også tilfredsstiller sikkerheten.

Abelia vil avslutte med å takke for muligheten til å komme med innspill.

På vegne av Abelia,



Kjetil Thorvik Brun
Leder teknologi og digitalisering

³ <https://digital21.no/>