Til Forsvarsdepartementet

28. september 2018

Teknas innspill til forskrifter til ny sikkerhetslov

Tekna er Akademikerforeningens største fagorganisasjon med over 75 000 medlemmer. Våre medlemmer består av naturvitere og teknologer, høyt utdannede med master eller mer.

Tekna ønsker kommentere forskriftene med vekt på lovens utvidede virkeområde knyttet til den IKT-avhengighet som understøtter grunnleggende nasjonale funksjoner. Tekna mener det var helt avgjørende at ny sikkerhetslov ble utvidet for å ivareta digital infrastruktur i tillegg til fysisk infrastruktur. Viktige kritiske samfunnsfunksjoner, grunnleggende nasjonale funksjoner, er helt avhengig av sikre digitale løsninger og systemer. Disse er i økende grad utsatt for cyberangrep og utgjør en stadig større del av nasjonens sårbarhet. Tekna mener derfor IKT-sikkerhet generelt må prioriteres langt høyere enn det vi ser i dag. Tekna legger derfor mest vekt på sikring av kritisk digital infrastruktur og ikke på objektsikring i denne høringsuttalelsen.

Tekna mente det var viktig å etablere en mer dynamisk lov, hvor man innenfor lovens rammer kan utpeke objekter og tilpasse virkemidler og føringer i tråd med et trusselbilde i rask endring.

Tekna mener sikkerhetsloven, og tilhørende forskrifter, også må ivareta et næringsperspektiv. Næringsaktører som skal levere digitale tjenester og teknologisk løsninger til virksomheter underlagt sikkerhetsloven, må kunne utvikle og levere tjenester til alle sektorer. Til det kreves et felles rammeverk på tvers av sektorer som sikrer at det ikke utvikler seg ulik forståelse av lovverket og ulike krav til produktene og tjenestene. Det blir krevende for næringslivet å utvikle gode tjenester for sektorer som ikke har sektorovergripende felles rammeverk. Dette svekker god næringsutvikling innen IT-sikkerhet.

Tekna kommenterer på om forskriftene gir et tilstrekkelig rammeverk. Og om forskriftene klargjør lovens krav og om de setter gode rammer for skjønnsutøvelsen av rettslige standarder som ligger i loven. Tekna vil også påpeke andre forhold som vil være av betydning for om forskriftene vil gi oss redusert sårbarhet i grunnleggende nasjonale funksjoner.

Felles retningslinjer for vurderingene av sikkerhetsnivå og utfordringer med sektorprinsippet

Ny sikkerhetslov gir rom for skjønnsutøvelse av rettslige standarder. Dette gjelder både ved utpeking av objekt og infrastruktur, og ved etablering av sikringstiltak etter at objekter og infrastruktur er vurdert til å falle inn under lovens virkeområde. Skjønnet utøves av det enkelte sektordepartement. Tekna ber departementet vurdere ulike tiltak for å sikre at de ulike sektorene utøver skjønn på en omforent måte.

Avklaring av virkeområde og utpeking av skjermingsverdige verdier

I arbeidet med utpeking av objekter og infrastruktur, må departementet identifisere grunnleggende nasjonale funksjoner. Deretter identifisere

> *«hvilke virksomheter som er av vesentlig og avgjørende betydning for grunnleggende nasjonale funksjoner. Dette vil være virksomheter som råder over informasjon, informasjonssystemer, infrastruktur og objekt som er av vesentlig eller avgjørende betydning for grunnleggende nasjonale funksjoner. Det vil være særlig viktig å kartlegge hvilke informasjonssystemer, infrastrukturer og objekter som har betydning for virksomheter i flere sektorer. For å bestemme hvilke deler av objektene og infrastrukturene som skal klassifiseres og til hvilket nivå, må det vurderes hvilket tap man kan akseptere, som hvor mye av funksjonen det gjelder (kapasitet), for hvor lenge (varighet), og i hvilken grad innholdet i funksjonens leveranser forringes (kvalitet), før det får konsekvenser av avgjørende betydning for grunnleggende nasjonale funksjoner. Departementene skal ikke klassifisere større deler av infrastrukturene eller objektene, eller for en høyere klassifiseringsgrad, enn nødvendig*». (…)

Tekna mener det må utarbeides sektorovergripende felles retningslinjer for slike kartlegginger og vurderinger knyttet til utpeking. Det ligger en fare i at skjønnsvurderingen vil gi ulik oppfatning av risiko i de ulike sektordepartementene. Særlig vil dette gjelde vurderinger knyttet til sivil sektor. Det mener Tekna er svært uheldig.

I tillegg til utarbeidelse av felles retningslinjer, mener Tekna det bør vurderes å etablere et eget midlertidig objektutpekingsutvalg. Dette vil bidra til at alle sektorene har samme nivå for risikoaksept, men hvor sektoren selv bidrar inn for å ivareta sektorens egenart. Slik vil man kunne sikre at en vurderingspraksis kommer riktig ut fra starten av, og at vi ikke kommer i en situasjon hvor det utvikles forskjellige praksiser og standarder som over tid har potensiale til å sprike i alle retninger. Utvalget kan være midlertidig, og avvikles når man har fått på plass tilstrekkelig kompetanse, omforent praksis og klare retningslinjer med likt nivå for risikoaksept i hver sektor.

Kost-nytte-vurderinger

Tekna mener at selve vurderingen av om virksomheten helt eller delvis skal falle innenfor sikkerhetslovens virkeområde, skal gjøres på grunnlag av ROS-vurderinger og ikke ut fra en kost-nytte-vurdering. Tekna kan ikke akseptere at det er økonomi som avgjør risikoaksepten hvis det

ellers viser seg at objektet eller infrastrukturen er av en slik art at den vil falle inn under sikkerhetslovens virkeområde. Tekna støtter at man må gjøre kost-nytte-vurderinger knyttet til krav til tiltak etter utpeking. Hvis pålegg om sikringstiltak viser seg å være av en slik art at man ikke kan opprettholde virksomheten på grunn av en økonomisk merbelastning når man underlegges lovens krav, vil dette måtte kompenseres med friske midler i de årlige budsjetter. Tekna forventer at regjeringen redegjør for Stortinget i statsbudsjettet for 2019 om hvordan de tenker innrette slike kompensatoriske ordninger. Tekna viser til omtalen av kompensatoriske ordninger i Prop. 153 L (2016-2017), pkt. 17.4.

Skjønnsutøvelse av «forsvarlig sikkerhetsnivå»

Tekna har ovenfor omtalt faren for ulik skjønnsutøvelse i de ulike sektordepartementene. Dette vil også gjelde vurderinger av tiltak knyttet til forebyggende sikkerhet etter utpeking. Hvert departement fatter vedtak innenfor sitt ansvarsområde på grunnlag av egen skjønnsutøvelse. Tekna mener det er helt nødvendig at det også her formuleres forpliktende sektoruavhengige og overgripende kriterier for risikoaksept. Det er viktig å erkjenne sektorens egenart, spesielt ved utforming av sikringstiltak, men foreligger ikke et overordnet nasjonalt regelverk som formulerer kravene til forsvarlighetsvurderinger, vil det kunne bidra til at sektorene selv setter nivåene for risikoaksept og vi utvikler et svært varierende sikkerhetsnivå i de ulike sektorer.

Tekna er usikker på om det enkelte sektordepartement har tilstrekkelig kompetanse til å ha nødvendig forståelse av det totale nasjonale trusselbildet og til å se egen sektors virksomheter i en større nasjonal sammenheng. Uten en myndighet som aktivt veileder ut fra forpliktende sektoruavhengige krav, er det stor fare for at det utvikles sektorspesifikke skjønnsvurderinger som ikke er forenlig med det overordnede trusselbildet. Tekna mener det må tydelig presiseres i forskriften at det enkelte sektordepartement skal se vedtakene i et større nasjonalt sikkerhetsperspektiv og søke veiledning om dette før vedtak fattes.

Kompetanseutfordringer

Det kreves betydelig kompetanse til å gjøre gode vurderinger av sårbarheter i sektorer som i dag ikke er trent til det. Herunder i stor grad sivil sektor. Eksempelvis er helsesektoren en bransje som er midt i en stor digital omstilling uten at man har bygget kapasitet innen digital sikkerhetskompetanse hverken i departement eller nedover i kjeden av underliggende virksomheter og i leverandørkjeden. Tekna mener det må til en betydelig satsning på kompetansehevende tiltak innen teknologi og sikkerhet i flere departementer for å kunne utøve et godt skjønn knyttet til risikovurderinger og vurdering av sikkerhetsnivå. Kompetanse og god skjønnsutøvelse henger sammen.

Videre kan det være høyst uklart for det enkelte sektordepartement å identifisere hvilke virksomheter som er av vesentlig og avgjørende betydning for grunnleggende nasjonale funksjoner. Dette vil være virksomheter som **råder over** informasjon, informasjonssystemer, infrastruktur og objekt som er av vesentlig eller avgjørende betydning for grunnleggende nasjonale funksjoner. Tekna viser til høringsbrevet hvor det fremgår at

*«det vil være **særlig viktig å kartlegge hvilke informasjonssystemer, infrastrukturer og objekter som har betydning for virksomheter i flere sektorer**».*

Dette fordrer både intern sektorkompetanse i hvert departement, men også sektorovergripende kompetanse. Det må avansert sikkerhetskompetanse inn i den enkelte virksomhet, i ledelsen og i styrerommet, til å gjøre gode ROS-analyser som skal legges til grunn for departementets vedtak. Man kan stille seg spørsmålet om det er mulig for hvert departement, innen forsvarlige tidsrammer, å bygge opp nødvendig kompetanse internt i sektoren. Her gjenstår et betydelig løft for å komme opp på et akseptabelt nivå i flere sektorer.

Tekna mener det må investeres i avansert IT-sikkerhetskompetanse internt i nasjonale virksomheter. Sterk satsing på spesialistkompetanse, gjennom å øke antallet offentlige PhD og nærings-PhD, hvor man bruker sikkerhetsklarerbare kandidater, må prioriteres. Tekna etterlyser en klar strategi for å sikre utvikling av avansert IT-sikkerhetskompetanse i virksomheter underlagt sikkerhetslovens virkeområder.

Tekna mener:

- *at det må utarbeides sektorovergripende felles retningslinjer for kartlegginger og vurderinger knyttet til utpeking av objekter og infrastruktur*
- *at det må formuleres forpliktende sektoruavhengige og overgripende kriterier for risikoaksept*
- *at det etableres et midlertidig objektutpekingsutvalg til man har fått på plass tilstrekkelig kompetanse og omforent praksis med likt nivå for risikoaksept i hver sektor*
- *at kost-nytte-vurderinger ikke skal legges til grunn ved utpeking av objekter og infrastruktur*
- *at regjeringen i statsbudsjettet for 2019 må redegjøre for hvordan de tenker innrette kompensatoriske ordninger for inndekning av uforholdsmessig stor økonomisk merbelastning av implementering av sikringstiltak i tråd med sikkerhetsloven*
- *at det må tydelig presiseres i forskriften at det enkelte sektordepartement skal se vedtakene i et større nasjonalt sikkerhetsperspektiv og søke veiledning om dette før vedtak fattes*
- *at det bør pålegges departementene, før vedtak fattes, å ha et forpliktende samarbeid med sikkerhetsmyndigheten eller de sektorovergripende departementer for å få en vurdering av eget vedtak i et større nasjonalt sikkerhetsperspektiv, fortrinnsvis i sivil sektor*
- *det må legges frem en klar strategi for å sikre utvikling av avansert IT-sikkerhetskompetanse i virksomheter underlagt sikkerhetslovens virkeområder.*

Virksomheter som faller utenfor sikkerhetslovens virkeområde

Tekna mener det er svært viktig at sektordepartementene, i tillegg til utpeking av hele eller deler av virksomheter som skal underlegges sikkerhetsloven, også samtidig skal identifisere og holde oversikt over øvrige virksomheter som er av vesentlig betydning for grunnleggende nasjonale funksjoner, og melde disse oversiktene inn til sikkerhetsmyndigheten. På den måten vil man kunne sørge for at de virksomheter, eller deler av virksomheter som faller utenfor lovens virkeområde, men som har betydning for grunnleggende nasjonale funksjoner, ligger i departementets oversikter til løpende vurdering.

Tekna mener det må etableres klare krav til forebyggende sikkerhet av de virksomheter som ikke faller inn under sikkerhetsloven, men som er i et grenseland. Dvs. de som vil ligge på listen over virksomheter som er av betydning for grunnleggende nasjonale funksjoner, men som ikke er utpekt til å falle inn under sikkerhetsloven. Her kan man legge DSBs listing av samfunnets kritiske funksjoner til grunn. Kravstilling kan gjerne gjøres gjennom det sektorspesifikke regelverket, men den overordnede rammen må være lik. Tekna mener dette i altfor liten grad har blitt problematisert. Hverken hva angår regulering og krav til disse virksomhetene og de ressursene som kreves for oppfølging og veiledning.

NSM får et betydelig større oppdrag i å veilede virksomhetene i de ulike sektorene, men deres ressurser er i hovedsak dimensjonert til å veilede og føre tilsyn med de virksomheter som faller inn under sikkerhetslovens virkeområde. Tekna mener det derfor må legges inn betydelig økte budsjettrammer for både departementer og NSM eller andre sektortilsyn og rådgivningsorganer ved forskriftenes ikrafttredelse.

Dette synliggjør og understreker behovet for økt kompetanse i departementet og underliggende virksomheter.

Tekna mener:

- *at det må etableres klare krav til forebyggende sikkerhet av de virksomheter som ikke faller inn under sikkerhetsloven, men som er i et grenseland*
- *at det må settes av tilstrekkelig med ressurser hos sikkerhetsmyndigheten og andre egnede organer og myndigheter til å gi veiledning til virksomheter som ligger utenfor sikkerhetslovens virkeområde, men i «gråsonen»*

Hvor langt ned i verdikjeden man skal sette krav til leverandørene av utstyr, systemer og support-tjenester.

Tekna mener eiere av kritisk infrastruktur/systemer må ansvarliggjøres gjennom klare krav til det de leverer av tjenester, utstyr og systemer, herunder hvordan disse produseres og hvem de produseres av. Sikkerhetsmyndigheten må veilede ut fra disse kravene. Tekna mener forskriften bør ha bestemmelser om hvordan leverandørene følges opp. Det er eier som har ansvaret for å følge opp at bestemmelsene blir fulgt. Dette må fremgå tydelig av forskriften.

Er kravet at leverandørkjeden skal være registrert i og driftes fra land vi har et sikkerhetssamarbeid med, må denne land-informasjonen gjøres tilgjengelig gjennom veiledning fra sikkerhetsmyndigheten.

I den grad en tjenesteleverandør eier kritisk infrastruktur/system, kan det stilles krav til hvordan systemer driftes og forvaltes. Myndighetene bør oppstille krav til driftskonsept, fjerntilgang, autorisasjon av personell mv.

Det er avgjørende at man kan stole på digital infrastruktur i en krisesituasjon. Siden stadig flere systemer og komponenter kan driftes og monitoreres uten fysisk tilgang til systemene, utgjør ikke bare angrep fra utenforstående, men også selve leverandøren av utstyret, en risiko. Det kan plasseres såkalte bakdører direkte i enkelte av de elektroniske komponentene som er svært vanskelige å oppdage ved normal bruk og drift. Systemene kan også i mange tilfeller manipuleres gjennom oppgradering eller endring av kode uten at brukeren har mulighet til å detektere dette. Systemer kan da fjern-manipuleres, endres eller tappes for data uten at eieren merker noen ting til dette. I verste fall kan man risikere at viktig digital infrastruktur settes ut av spill i en kritisk situasjon. Tekna mener dette er en sårbarhet som har vært underkommunisert i Norge over tid, og at dette har satt oss i en sårbar situasjon og et avhengighetsforhold til elektronikkleverandører som andre land av sikkerhetsmessige hensyn ikke ønsker å bruke. Det er derfor viktig at man gjør en faglig vurdering av risikoen for slike hendelser ved valg av leverandører av utstyr og systemer i kritisk infrastruktur.

Tekna mener elektronisk kommunikasjon er vår viktigste og mest kritiske infrastruktur. Sårbarheten er enorm hvis det blir utfall i mobil- eller bredbåndsnettene. Tekna mener derfor de mest sentrale kommunikasjonstjenestene, som å ringe og sende hverandre informasjon, i gitte situasjoner må kunne driftes innenfor Norges grenser og med norske ressurser alene, helt uavhengig av utlandet. Dette er ikke uten videre mulig i dag.

Tekna mener Norge, i kritiske situasjoner, bør ha full nasjonal kontroll på de viktigste kommunikasjonsveiene.

Dersom de nødvendige ressursene for å sikre kritiske kommunikasjonstjenester ikke kan underlegges nasjonal kontroll i en krise- eller krigssituasjon, kan dette få svært alvorlige følger for den nasjonale styringsevnen.

Tekna mener det er viktig at det gjøres gjeldende et krav til nasjonal autonomi for norske ekomnett, jfr. ekomforskriftens § 8-6, og anbefalingene fra Nkom i rapporten «Nasjonal autonomi i norske elektroniske kommunikasjonsnett»[1]. Det er viktig med slik beredskap når truslene i stadig større grad er nettbaserte.

Tekna mener myndigheten bør stille krav til hvem og på hvilken måte man kan akseptere en avhengighet av andre, eller aller helst stille krav om at vi skal være uavhengig av andre. Dette mener Tekna er realiserbart.

Et avbøtende middel når man vurdere at man ikke kan ha tillit til sine underleverandører er å sette krav til gjennomgående kryptering mv. Tekna mener det per i dag ikke foreligger noen fullgode tekniske svar på dette.

Tekna mener:

- *at forskriften bør ha bestemmelser om krav til leverandørene og hvordan disse følges opp*
- *at forskriften må presisere en ansvarliggjøring av eier av kritisk infrastruktur*
- *at myndighetene bør oppstille krav til driftskonsept, fjerntilgang, autorisasjon av personell mv.*
- *at Norge, i kritiske situasjoner, bør ha full nasjonal kontroll på de viktigste kommunikasjonsveiene.*

Hvordan skal man føre tilsyn etter sikkerhetsloven – veiledende og rådgivende tilsyn versus sanksjonerende tilsyn.

Sikkerhetsmyndigheten (NSM eller utpekt sektormyndighet) plikter iht. forvaltningsloven å veilede, samtidig som de har et tilsynsansvar. Myndigheten må imidlertid ikke ta eierskap til eller godkjenne en spesifikk løsning e.l. Dette ansvaret ligger udelt hos eier. Det er avgjørende viktig at myndighetsrollen skiller klart mellom rådgivnings- og tilsynsfunksjonene internt. Veiledende tilsyn bør utgå for å hindre rolleblanding.

[1] https://www.nkom.no/teknisk/sikkerhet-og-beredskap/ekomsikkerhet/nasjonal-autonomi-i-ekomnett/_attachment/28350?_ts=15b8b7aa1e5

Bestemmelsene om sikkerhetsklarering

Klarering av utenlandske borgere:

Ny sikkerhetslov § 8-7
Tekna er enig i at det er behov for en oppmykning av praksis, og at handlingsrommet benyttes i større grad.

Det er behov for ytterligere føringer for å sikre at oppfølgingen og praktiseringen i større grad vil gjennomføres i tråd med loven. Blant annet:

Forskriften § 14 Personhistorikk
Nytt fjerde ledd er relevant for aktuell problemstilling der en arbeidstaker (dette kan være så vel utenlandsk som norsk statsborger) har jobbet i Norge med sikkerhetsklarering i flere år, og der vedkommende har innledet forhold til en person fra et land som ikke har et sikkerhetssamarbeid med Norge. Klareringsmyndigheten har ikke nødvendig personhistorikk for partneren for de siste 10 årene. En klassisk situasjon der manglende personhistorikk hos partneren har medført tilbakekall/avslag på sikkerhetsklarering med en påfølgende oppsigelse.

I slike tilfeller har vedkommende hatt en sterk tilknytning til både Norge og arbeidsgiveren sin. Det fremstår rigid at personen uten videre skal miste klareringen på bakgrunn av at man ikke kan fremskaffe personhistorikken til partneren gjennom et sikkerhetssamarbeid med partnerens hjemland.

Nytt fjerde ledd gir tilstrekkelig fleksibilitet i slike tilfeller, men denne kan med fordel gjøres til en skal-regel. I forslaget til nytt punkt i forskriften står det blant annet at:

«Det kan vurderes om det finnes andre måter, f.eks. kontakt med arbeidsgivere, utdanningsinstitusjonen vedkommende hevder å ha vært student ved, eller andre for å verifisere at oppholdet har funnet sted for det angitte formålet, og med det kompensere for den manglende tilgangen på personopplysninger.(…)» Etter Teknas syn bør utgangspunktet være at *det skal vurderes om det finnes andre måter (…)*

Ved å ilegge klareringsmyndigheten en plikt til å vurdere om det finnes andre måter for å verifisere oppholdets formål, vil det formodentlig fremgå av avgjørelsen i hvilken grad dette er gjort og klareringsmyndighetens vurderinger blir med det mer transparente og etterprøvbare.

I tillegg til ovennevnte tiltak som gjennomføres i forkant av en eventuell klarering/re-klarering, kan det også være relevant å gi klarering med forbehold for at det gjennomføres enkelte tiltak i klareringsperioden. For eksempel kan det avholdes jevnlige sikkerhetssamtaler med både vedkommende og partneren.

Nytt punkt i § 8-7 andre ledd om bruk av andre risikoreduserende tiltak som bruk av vilkår f.eks. stillingsklarering.

I utgangspunktet fremstår dette som et bra virkemiddel for å få flere personer inn i stillinger der det er behov for deres kompetanse og de ikke fyller vilkårene for klarering. Bekymringen ligger i hvilket grunnlag klareringsmyndigheten vil ha for å foreta denne vurderingen om stillingsklarering skal gis. Det vises til at klareringen ligger sentralt hos sikkerhetsmyndigheten, men vurderingen om blant annet stillingsklarering skal gis fordrer formodentlig god kunnskap om virksomheten, infrastrukturen

der og den konkrete stillingen. Det er et spørsmål om klareringsmyndigheten sentralt vil ha tilstrekkelig kunnskap om dette for å foreta denne vurderingen. Det er en risiko for at manglende kunnskap om de lokale forholdene, påvirker tilbøyeligheten til å benytte seg av muligheten.

Tekna ser at et utvidet virkeområde for lov og forskrift vil bety et økt behov for sikkerhetsklarerbart personell. Tekna mener det må sette av tilstrekkelig ressurser for arbeidet med sikkerhetsklarering for å få ned saksbehandlingstiden.

Tekna mener:

- *at regelverket bør gi sterkere føringer for å sikre at klareringsmyndigheten benytter handlingsrommet til å klarere utenlandske statsborgere i stor nok grad*
- *at forskriften § 14, 4. ledd (Personhistorikk) endres til: «Det skal vurderes om det finnes andre måter, f.eks. kontakt med arbeidsgivere etc.»*
- *at det bør åpnes for å gi klarering med forbehold for at det gjennomføres bestemte tiltak i klareringsperioden*
- *at det er en risiko for at manglende kunnskap om de lokale forholdene, påvirker klareringsmyndighetens tilbøyelighet til å benytte seg av muligheten til å gi stillingsklarering.*
- *at saksbehandlingstiden på søknader om sikkerhetsklarering må kortes ned.*

Ikrafttredelse og arbeidet med utpeking.

Tekna viser til at forskriftene er ment å tre i kraft 1. januar 2019. Nytt arbeid med utpeking skal ha som utgangspunkt at informasjon, objekter og infrastrukturer som er omfattet av gjeldende sikkerhetslov, i utgangspunktet vil være omfattet av ny sikkerhetslov. Departementet viser til at det

«*derfor vil være særlig fokus på å kartlegge hvilke informasjonssystemer, infrastruktur eller objekter som omfattes av utvidelsen av lovens virkeområde, og viser til at denne vil være begrenset. Deretter viser departementet til at det vil ta noe tid før virksomheten er utpekt og legger til grunn av offentlige myndigheters saksbehandlingskapasitet tilsier også at det vil måtte gjøres en gradvis vurdering av virksomheter og objekter. For disse virksomhetene vil det imidlertid uansett måtte gis en rimelig frist for implementering av sikringstiltak* (...).

Tekna mener:

- *at det må kunne stilles klare krav til når en full gjennomgang og utpeking skal være gjennomført*
- *at det på utpekingstidspunktet må kunne forelegges en tidsfrist for når sikringstiltak skal være på plass.*

Tekna ser frem til de endelige forskrifter foreligger, og de tiltak regjeringen vil sette i gang for å kunne sikre at forskriften får den effekt som er nødvendig og i tråd med intensjonen bak ny sikkerhetslov.

Med vennlig hilsen
Tekna – Teknisk-naturvitenskapelig forening

Lise Lyngsnes Randeberg
President

Line Henriette Holten
konst. generalsekretær