Høringsnotat – tilleggshøring om datasenterregulering til forslag til ny lov om elektronisk kommunikasjon (ekomloven) og ny forskrift om elektroniske kommunikasjonsnett og -tjenester (ekomforskriften)

1. Innledning

Datasenternæring i Norge er forholdsvis ny, og det stilles få særskilte krav til datasentre under gjeldende regelverk. Myndighetene har behov for å få en oversikt over datasentrene, inkludert datasenter som utvinner krypto, og foreslår med dette en registreringsplikt. Ekomtilbyderne har allerede en slik registreringsplikt, og departementet foreslår ingen endringer i denne i dette høringsbrevet.

En rekke virksomheter er avhengige av datasentre. Bortfall eller forringelse av tjenester vil kunne skape store utfordringer for en rekke aktører, herunder for grunnleggende nasjonale funksjoner og virksomheter som understøtter dette. Det foreslås derfor i tillegg i dette høringsbrevet å stille krav til sikkerhet og beredskap for datasentre, på lik linje med annen ekominfrastruktur. I høringen av ny lov om elektronisk kommunikasjon (ekomloven) som ble sendt på høring 2. juli 2021, ble det foreslått en hjemmel for å regulere datasenternæringen som tilhørende fasilitet til ekomnett- og tjenester. Etter høringen har Kommunal- og distriktsdepartementet vurdert at reguleringsforslaget ikke går langt nok i å stille krav til sikkerhet, og at kravene bør tydeliggjøres. Denne vurderingen er blant annet gjort på bakgrunn av Hurdalsplattformen der det fremgår det at det er et mål å styrke den digitale beredskapen. Datasentre i Norge er viktige for å sikre en robust nasjonal infrastruktur med raske, trygge og fleksible digitale tjenester over hele landet. Datasenter er en infrastruktur som lagrer og bærer digitale tjenester og data, og inngår som en viktig del av den digitale grunnmuren, på linje med infrastruktur for elektronisk kommunikasjon (ekom). St. meld. 28 (2020-21) om vår felles digitale grunnmur omtaler den økende sammensmeltingen av tradisjonell elektronisk kommunikasjon og IT-, sky- og datasentertjenester, hvor tredjepartsleverandører blir tettere integrert i ekomtilbydernes løsninger.

Mange kritiske tjenester leveres i dag fra datasentre og avhengigheten til datasentrene kan utgjøre en stor samfunnsmessig sårbarhet. Dersom det oppstår nedetid i digital infrastruktur, kan det ramme kritiske digitale tjenester. Siden samfunnets avhengighet til digitale tjenester blir stadig større, og stadig flere kritiske tjenester bæres av den digitale infrastrukturen, er det viktig med et bevisst forhold til sikkerhet og robuste løsninger. Datasentre legger også til rette for innovasjon og effektivisering både i næringslivet og det offentlige. Mange viktige funksjoner i samfunnet, hviler på tjenester som blir levert av datasentre. Noen eksempler på tjenester som datasentre bærer er mobiltjenester, som tale og data, betalingstjenester, helse- og velferdstjenester, kritiske kommunikasjonstjenester, TV- og radiodistribusjon (DAB), Forsvarets kommunikasjonstjenester og fremtidens nød- og beredskapskommunikasjon. Det er derfor behov for å stille tydeligere krav til sikkerhet og beredskap for datasenter. På noe sikt vil det også vurderes om enkelte datasenter har så

stor betydning for nasjonale sikkerhetsinteresser, at sikkerhetsloven bør gjøres gjeldende for disse. Dette er imidlertid ikke en del av kravene som foreslås innført nå.

Vi foreslår også endringer i forskrift om elektronisk kommunikasjon (ekomforskriften) som ytterligere operasjonaliserer kravene til sikkerhet. Ved å stille sikkerhetskrav, følges den nasjonale datasenterstrategien hvor det fremkommer at «*datasenter blir vurderte for relevant og formålstenleg regulering i ekomregelverket, for å følge opp den samla risikoen og sårbarheita hos ein datasenteraktør, som samlar og driftar aktivitet frå fleire ulike verksemder*».

Høringsbrevet inneholder også forslag om justeringer i enkelte lov – og forskrifts bestemmelser i forslag til ny ekomlov fra 2. juli 2021 som følger av forslaget om plikt til registrering og kravene til sikkerhet og beredskap som stilles til datasenter. Dette er blant annet forslag som gir datasentrene verktøy til å oppfylle pliktene, slik som mulighet til å innhente politiattest i visse tilfeller, og myndighetene kompetanse til å føre tilsyn med de nye bestemmelsene.

Det gjøres oppmerksom på temarapporten «Norske datasenter og digital autonomi» utgitt av Nasjonal sikkerhetsmyndighet 17. januar 2022, som gir sikkerhetsfaglige anbefalinger av relevans også for forslagene i dette høringsbrevet, herunder om krav til sikkerhet.

For å gjøre lov- og forskriftsforslagene lettere tilgjengelig, er endringene fra høringen av 2. juli 2021 kursivert, og forslagene er lagt opp med utgangspunkt i denne høringen.

2. Nærmere om forslag til nye sikkerhetskrav i høringen om ny ekomlov og ekomforskrift av 2. juli 2021

Forslag til ny ekomlov og ny ekomforskrift ble sendt på høring 2. juli 2021, med høringsfrist 15. oktober 2021. Basert på forslaget til ny lovtekst og innkomne høringsinnspill, forbereder Kommunal- og distriktsdepartementet en lovproposisjon som skal fremmes for Stortinget i løpet av høsten 2022.

I ovennevnte lovforslag fremgår det at samfunnet er helt avhengig av elektronisk kommunikasjon. Avhengigheten er økende og stadig mer kritisk. Teknologiutviklingen vil føre til en økende digitalisering innenfor alle samfunnskritiske funksjoner de nærmeste årene. Utviklingen forsterker koblingen mellom den digitale grunnmuren og samfunnsverdier som liv og helse, natur og miljø, økonomi, samfunnsstabilitet og demokratiske verdier og styringsevne. Infrastrukturens motstandsdyktighet mot naturhendelser og ekstreme påkjenninger blir stadig viktigere. Trusselaktørenes muligheter for å ramme virksomheter, infrastrukturer og tjenester innen elektronisk kommunikasjon er også mange. Digitaliseringen i de ulike samfunnssektorene forutsetter tilgjengelige ekomnett og –tjenester, herunder datasentre, som ivaretar kommunikasjonens konfidensialitet, autentisitet og integritet. Samfunnsutviklingen fordrer økt sikkerhet i nett og tjenester. Utviklingen medfører at det er mer omfattende og komplekst å skulle holde oversikt over og vurdere beskyttelsesbehovet for enkeltkomponentene i infrastruktur og informasjonssystemer. Bruk av funksjonelle krav og rettslige standarder er grunnleggende for at forebyggende sikkerhet skal utvikle seg i takt

med samfunnsutviklingen og endringer i risiko- og trusselbildet. Et funksjonelt regelverk stiller store krav til virksomhetens arbeid med forebyggende sikkerhet og til myndighetenes veilednings- og tilsynsarbeid for å oppnå et forsvarlig sikkerhetsnivå. I henhold til sikkerhetskravene i gjeldende ekomregelverk har tilbyder et ansvar for å tilby elektronisk kommunikasjonsnett og -tjeneste med forsvarlig sikkerhet for brukerne i fred, krise og krig, jf. § 2-10 første ledd.

På denne bakgrunn ble det foreslått endringer i ekomloven for å legge til rette for en ytterligere styrking av sikkerheten i elektroniske kommunikasjonsnett- og tjenester samt en ytterligere operasjonalisering av kravene i forskrift. Det vises særlig til forslag til ny ekomlov § 3-8, samt forslag til bestemmelser i lovens kap. 3 og ekomforskriften kap. 9. Høringen av ny ekomlov inneholdt enkelte forslag som stiller krav til datasenteroperatører, men det har i etterkant blitt klart at det foreligger et større behov for å regulere datasenternæringen enn det som er foreslått i den opprinnelige høringen. I denne tilleggshøringen fremmes det derfor forslag om en ytterligere regulering av datasentre for å sikre robuste og stabile datasentre i Norge med god sikkerhet. Forslagene til endringer i ekomloven og ekomforskriften tar utgangspunkt i forslaget slik det ble sendt på høring i 2021.

Lenker til aktuelle dokumenter i ovennevnte høring av 2. juli 2021 vedlegges her:
Høringsnotat om ny ekomlov
Forslag til ny ekomlov
Forslag til merknader til ny ekomlov
Forslag til ny ekomforskrift
Forslag til merknader til ny ekomforskrift

3. Nærmere om forslagene

I et digitalisert samfunn som vårt, er ekomnett og datasentre grunnmuren i vår nasjonale digitale infrastruktur. Nettene er som digitale transportveier, og datasentre er viktig for lagring av data og drift av digitale tjenester, både for privat og offentlig sektor. Det fremkommer av punkt 4.1 i Norske datasenter - berekraftige, digitale kraftsenter fra august 2021 https://www.regjeringen.no/no/dokumenter/norske-datasenter/id2867155/ *at «Norske datasenter står heilt sentralt i digitaliseringa av Noreg. Norske datasenter understøttar digitale tenester som er stadig viktigare for samfunnet. Forsvarleg tryggleik i komplekse digitale verdikjeder er derfor ei prioritert oppgåve, så vel i Noreg som i EU og verda elles. Norske datasenter må derfor lykkast med å dokumentere forsvarleg tryggleik – over tid – for å lykkast i både den norske og den internasjonale marknaden. Tryggleik i norske datasenter er ein sentral konkurranseparameter.*
Digitale infrastrukturar og system blir stadig meir komplekse, omfattande og integrerte. Det blir skapt avhengnader og sårbarheiter på tvers av ansvarsområde, sektorar og nasjonar. Det blir forventa at digitale tenester skal vere tilgjengelege til ei kvar tid. Ei vellykka digitalisering handlar òg om at løysingane oppfyller krav til tryggleik og personvern for den enkelte på ein god måte, og at vi kan ha tillit til at digitale løysingar fungerer slik dei skal.»

Det er i all hovedsak private aktører som bygger ekomnett og datasentre. Dette gjøres ut ifra kommersielle strategier og mange datasenter har allerede god sikkerhet fordi kundene

krever det. Driften bygger imidlertid på resultatkrav som ikke nødvendigvis tar hensyn til samfunnets sikkerhetsbehov i tilstrekkelig grad. Det er viktig å sikre den digitale grunnmuren. For ekominfrastruktur og -tjenester er det allerede stilt krav gjennom ekomloven og sikkerhetsloven. Det bør også stilles tilsvarende krav til datasentre i Norge, i første omgang ved å gjøre ekomlovens sikkerhetsbestemmelser gjeldende også for datasentre slik at det stilles krav om «forsvarlig sikkerhet». Dette innebærer at det stille krav om systematisk oppfølgning av sikkerhet og beredskap og at dette skal dokumenteres. I likhet med ekomtilbydere, foreslås det at datasenteraktørene gis mulighet til å kunne stille krav om politiattest ved ansettelse av personell som skal ha tilgang til datasenter. Det foreslås også at enkelte andre regler skal gjelde for datasenteraktørene som f.eks. at brudd på bestemmelsene vil kunne medføre sanksjoner. Endringer i ekomforskriften vil ytterligere operasjonalisere kravet til forsvarlig sikkerhet. Det foreslås blant annet nærmere krav om sikkerhetsstyring, risiko- og sårbarhetsanalyser, beredskapsplanlegging og øvelser, samt nasjonal autonomi. For å sikre bedre oversikt over aktørene i markedet, foreslås det også å innføre en registreringsplikt for datasenteraktører. Dette vil sikre oversikt over hvem som tilbyr datasentertjenester, herunder kontaktinformasjon til personer som er ansvarlig for datasenteroperatøren og datasenteroperatørens virksomhet. Registreringsplikten medfører at myndighetene får bedre oversikt over datasenternæringen i Norge. Dette er nødvendig for å sikre at rammebetingelsene tilpasses næringen og kundene. Det vil også gi mulighet til å føre tilsyn med at de nye sikkerhetskravene etterleves. I tillegg vil ansvarlig person for datasentrene kunne kontaktes av andre myndigheter, for eksempel av politiet, når dette er nødvendig. Krav om registrering gjelder også for ekomtilbydere i dag.

Forslaget dreier seg om å stille krav til sikkerhet for datasentre som digital infrastruktur, og vil ikke gripe inn i sikkerhet for innhold som er foreslått regulert av annet regelverk. Nasjonal kommunikasjonsmyndighet (Nkom) vil føre tilsyn med datasenternæringen.

I enkelte bestemmelser er det ikke nødvendig å foreta endringer for å inkludere datasenter og datasenteroperatører fordi dette følger av at lovens virkeområde forslås utvidet eller fordi bestemmelsene gjelder «enhver». Dette vil f.eks. være tilfelle i forslag til ny ekomlov §15-1 om myndighetens tilsyn, § 15-2 om opplysningsplikt til myndigheten og enkelte andre bestemmelser i forslag til ny ekomlov.

Departementet foreslår i utgangspunktet at sikkerhetsreguleringen skal gjelde alle datasenter som faller inn under definisjonen i § 1-5. Sikkerhetskrav vil således også gjelde for datasenter som utvinner krypto, fordi disse forvalter verdier attraktive for kriminelle aktører, både i form av servere og annen infrastruktur, samt tilgang til kraftressurser. Norge er folkerettslig forpliktet til å hindre at digital infrastruktur i Norge blir benyttet i digitale angrep mot andre land. Om et annet land har grunn til å tro at et datasenter i Norge benyttes på folkerettsstridig måte, har landet folkerettslig adgang til å beskytte seg. Dette kan i siste instans bety at landet vil mene at det har rett og anledning til å stanse angrepene i Norge. Dette vil kunne få stor betydning for datasenteret og senterets kunder.

Det er etter departementets vurdering, derfor hensiktsmessig at alle datasenter, også de som kun utvinner krypto, utarbeider, iverksetter og vedlikeholder planer for sikring av informasjon, informasjonssystemer og styringssystemer for å ivareta sin egen sikkerhet.

Departementet viser for øvrig til at det er mer hensiktsmessig å sette like sikkerhetskrav for alle datasenter enn å sette sikkerhetskrav som kun skal gjelde for noen datasenter, fordi skillet mellom de ulike aktivitetene datasenter driver med (co-location og kryptoutvinning) kan være glidende. Dette gjelder særlig fordi også enkelte co-location senter har kunder som utvinner kryptovaluta. Dersom det skulle stilles ulike sikkerhetskrav vil dette dessuten kunne føre til ulike konkurransevilkår.

Dette er bakgrunnen for departementets forslag om at sikkerhetsreguleringen skal gjelde alle datasentre. Departementet ber likevel om høringsinstansenes syn på om reguleringen bør differensieres, og i tilfelle hvordan.

4. Nytt i tilleggshøringen

Denne tilleggshøringen er lagt opp med utgangspunkt i høringen om ny ekomlov av 2. juli 2021, som dermed utgjør referansedokumentet.

4.1 Endringer i ekomloven § 1-2 – saklig virkeområde

Forslag til ny § 1-2 regulerer ekomlovens saklige virkeområde. Loven vil omfatte alle typer virksomhet i tilknytning til elektronisk kommunikasjon, og myndighetsutøvelse i forbindelse med bruk og utvikling av slik kommunikasjon. For å inkludere datasenter i lovens saklige virkeområde, foreslås det inntatt ordet «datasenter» i slutten av bestemmelsens første ledd første punktum.

For nærmere omtale av § 1-2 vises til Forslag til merknader til ny ekomlov på s. 3.

4.2 Endringer i ekomloven § 1-5 – definisjoner

I forslag til § 1-5 om definisjoner foreslås inntatt forslag til definisjoner av datasenter, datasentertjeneste og datasenteroperatør. Definisjonen av datasenter er en vid og generell definisjon av et datasenter, som kan spenne fra et enkelt datarom til en «hyperscale» datasenterinstallasjon på flere hundre megawatt effekt (MW). Hvilke datasenter som omfattes av denne reguleringen blir avgrenset gjennom de øvrige definisjonene.

Definisjonen av datasentertjenester sikter til tjenester som tilbys med utgangspunkt i et fysisk datasenter, som oftest omtalt som et «colocation datasenter». Dette omfatter tjenester slik som fysisk innplassering av kunders IT-utstyr, ev. at kunder tilbys IT-infrastrukturtjenester (infrastructure-as-a-service), og tilhørende tjenester knyttet til det fysiske datasenteret, blant annet strømforsyning, kjøling, fysisk sikkerhet og tilgangskontroll og tilgang til nettverk og nettverksleverandører. Opplistingen er ikke uttømmende.

Pliktsubjektet for bestemmelsene om datasenter vil være den fysiske eller juridiske personen som tilbyr/opererer datasenter og datasentertjenester i Norge, foreslått definert som datasenteroperatøren. Definisjonen av datasenteroperatør er todelt. Først siktes det til aktører som tilbyr andre tilgang til en datasentertjeneste (jf. definisjonen over) mot vederlag. Dette er såkalte «colocation»-aktører. Deretter siktes det til større aktører som etablerer og

opererer egne dedikerte datasenter for å produsere egne digitale tjenester, for eksempel skybaserte plattformtjenester (platform-as-a-service), og programvaretjenester (software-as-a-service). Dette er såkalte «hyperscale» datasenter og ev. andre større datasenter som brukes til å produsere viktige digitale tjenester. Definsjonen vil også omfatte dedikerte datasentre for kryptovalutautvinning. Definisjonen av de større datasenteroperatør har en avgrensing knyttet til allokert elektrisk effekt på datasenter. Formålet med denne avgrensingen er å sikre at reguleringen treffer de viktigste aktørene som opererer datasenter og datasentertjenester av en slik størrelse og omfang at de antas å ha en betydelig samfunnskritisk betydning, mens mindre aktører og rene virksomhetsinterne datasenter mv. ikke omfattes. Eventuelle datasenteroperatører som administrerer og opererer mindre distribuerte («edge») datasentre, og som i sum overstiger terskelverdien for installert effekt, vil også omfattes.

Definisjonen av datasenteroperatør er ikke ment å omfatte tilbydere av elektronisk kommunikasjon som realiserer tjenesteproduksjon av egne elektroniske kommunikasjonstjenester i egne datasenter (f.eks. 5G-tjenester). Dette er å betrakte som virksomhetsinterne datasenter, og reguleringen av sikkerheten til disse tjenestene dekkes allerede av kravene i ekomloven.

Datasenter som opereres av forsvarssektoren og politiet, inklusive Politiets sikkerhetstjeneste er unntatt.

Departementet ber spesielt om høringsinstansenes innspill på definisjon, i lys av formålet med reguleringen. Det bes også særlig om innspill på terskelverdien som fastsettes i forskrift, se under. Det er også ønskelig med høringsinstansenes syn på eventuelle muligheter til å omgå regelverket ved for eksempel etablering av flere små datasentre under den definerte terskelverdien.

4.3 Ny bestemmelse i ekomloven kap. 3 – registreringsplikt og sikkerhet i datasenter

Bestemmelsens første ledd inneholder en registreringsplikt for datasenteroperatør. Formålet med kravet til registrering, er å sikre myndighetene en oversikt over datasenternæringen, på lik linje med ekombransjen. Det understrekes at registreringsplikten ikke innebærer en tillatelses eller godkjennelsesordning fra myndighetenes side. Det dreier seg om en ren registreringsplikt og datasenteroperatør kan starte opp virksomhet så snart registeringen er gjennomført. Registeringen skjer elektronisk hos Nasjonal kommunikasjonsmyndighet (Nkom). En registeringsplikt er blant annet nødvendig for at Nkom skal kunne følge opp datasenteraktørene, f.eks. gjennom tilsyn. En registreringsplikt vil også gi kontaktinformasjon som vil komme til nytte i politiets arbeid med kriminalitetsbekjempelse knyttet til datasenternæringen. Innholdet i registreringsplikten foreslås nærmere regulert i forskrift, se under. Forskriftsreguleringen tar høyde for at registreringsplikten for datasenter er ny, og gjør det enklere å foreta justeringer i plikten ved eventuelle behov.

Annet ledd foreslår å stille krav til sikkerhet i datasenter og er utformet med utgangspunkt i de samme forpliktelsene som stilles til sikkerhet i ekomnett og -tjenester, jf. forslag til ny ekomlov § 3-8 se høringsbrev s. 14-22 og forslag til merknader s. 42-44. Annet ledd første punktum stiller krav om forsvarlig sikkerhet. Med begrepet «forsvarlig» menes at datasenter og tjenester skal være tilgjengelige, og at integriteten, autentisiteten og konfidensialiteten

skal beskyttes. Det er datasenteroperatørs ansvar at tjenestene som tilbys holder et forsvarlighetsnivå. Annet ledd annet punktum stiller krav til at datasenteroperatør skal opprettholde forsvarlig beredskap i datasenter og tjenester. I dette ligger også blant annet at datasenteroperatør skal treffe alle nødvendige tiltak for å sikre størst mulig tilgjengelighet for datasentertjenester også i tilfelle av force majeure hendelser. Dette reflekteres også i myndighetens kompetanse til å fatte enkeltvedtak for å sikre at datasenteroperatør iverksetter nødvendige tiltak for å sikre forsvarlig sikkerhet, jf. tredje punktum. Kravet til at viktige samfunnsaktører skal prioriteres ved behov er det samme som stilles til ekomtilbyderne. Det stilles krav om at eventuelle kostnader ved vedtak etter annet ledd dekkes av datasenteroperatør.

Tredje ledd, første punktum inneholder et krav om systematisk oppfølging av sikkerhet og beredskap i datasentertjenester, samt stiller krav til dokumentasjon av sikkerhetsmessige vurderinger av betydning. Ekomforskriften utdyper kravene til dokumentasjon og stiller minimumskrav til hvilke vurderinger som bør foreligge. Annet punktum presiserer hvilke momenter som skal vektlegges i vurderingen av om sikkerhetsnivået for forsvarlig sikkerhet er oppfylt, men er ikke uttømmende. Best tilgjengelig løsning vil variere over tid, og utviklingen vil føre til at det jevnlig må foretas forsvarlighetsvurderinger og påfølgende oppgraderinger. Datasenteroperatør skal vurdere kompenserende tiltak dersom den valgte tekniske løsningen som systemet bygger på inneholder kjente svakheter. Kravet skjerpes jo viktigere tjenester datasenteret bærer. Det fremgår ikke eksplisitt av ordlyden at sikkerhetstiltakene skal være forholdsmessige, men dette kravet følger av forvaltningsretten som også vil gjelde på dette området. Forholdsmessigheten må vurderes konkret i det enkelte tilfelle. Med forholdsmessig menes at kostnadene et tiltak påfører virksomheten må ses i sammenheng med tjenestenes betydning og tiltakets nytteverdi. Kostnader som langt overstiger tiltakets nytteverdi eller tjenestens betydning må anses som uforholdsmessige. Tiltakene skal også være egnede for å oppnå formålet.

Fjerde ledd første punktum gir også myndigheten vedtakskompetanse og mulighet for å inngå avtaler med datasenteraktør for å gjennomføre tiltak som sikrer nasjonale behov for sikkerhet, beredskap og funksjonalitet, ut over det som dekkes av forsvarlig sikkerhet i annet ledd. Annet punktum gjør det klart at merkostnader knyttet til slike tiltak skal kompenseres av staten basert på fyllestgjørende dokumentasjon fra datasenteroperatør. I tredje punktum foreslås at myndigheten skal ha en mulighet til å kreve refundert unødvendige kostnader fra virksomhet som nevnt i tredje ledd dersom anskaffelsen som virksomhet har foretatt for å sikre oppfyllelse av nasjonale behov for sikkerhet, beredskap og funksjonalitet i datasentertjeneste, medfører kostnader som er høyere enn de med rimelighet burde være. Hensikten med regelen er å gi virksomheten et sterkere insitament til å fremforhandle anskaffelser som er kostnadseffektive også når staten kompenserer alle kostnadene. Vurderingen av kostnadene når det er aktuelt å benytte regelen vil bli gjort på bakgrunn av dokumentasjonen som fremlegges, erfaringer med sammenlignbare kostnader, standardpris og priser som andre aktører melder inn.

Femte ledd tillegger myndigheten forskriftskompetanse. Det er presisert at forskriftskompetanse også omfatter registreringsplikten og nasjonal autonomi. I tillegg foreslås det presisert at myndigheten kan gi forskrift om sikkerhetsrevisjon slik at

myndigheten blant annet kan pålegge tilbyder å underlegges en sikkerhetsrevisjon av et eksternt revisjonsfirma. Videre foreslås det at myndigheten kan gi forskrift om finansiering. Myndigheten kan blant annet i forskrift pålegge tilbyder å dekke kostnadene med uavhengig sikkerhetsrevisjon. I femte ledd annet punktum gis myndigheten hjemmel i forskrift eller ved enkeltvedtak til å gjøre unntak fra registreringsplikten. Dette er først og fremst ment som en sikkerhetsventil for å unngå urimelige resultater, og eventuelt også klargjøre grensene for registreringsplikten dersom det skulle bli behov for dette. Bestemmelsen gir også en hjemmel for myndigheten gjennom forskrift eller i enkeltvedtak å pålegge datasentre under terskeverdien om å registrere seg. Dette kan for eksempel være aktuelt dersom en datasenteroperatør etablerer flere små datasentre for å unngå registreringskravet.

4.4 Endring i ekomloven § 3-9 – Krav om politiattest

Åpne trusselvurderinger og rapporter fra offentlige myndigheter har i en årrekke pekt på innsidetrusler som en utfordring for både offentlige og private virksomheter. Gode sikkerhetsrutiner for personkontroll ved, under og etter ansettelse er derfor vurdert som nødvendig for å redusere denne risikoen. Datasenter, på lik linje med ekomnett og -tjenester, blir stadig viktigere for dagens digitaliserte samfunn, og det er derfor viktig å sikre disse.

Politiattest vil være et hjelpemiddel for å unngå at kriminelle miljøer får tilgang til sensitiv informasjon og informasjon om infrastruktur. I energisektoren har man i energiloven § 9-5 inntatt en bestemmelse som gir hjemmel for beredskapsmyndigheten til å gi forskrift om at enheter som inngår i Kraftforsyningens beredskapsorganisasjon (KBO) kan kreve fremlagt politiattest fra personer som skal ha tilgang til klassifiserte anlegg. Hjemmelen ble tatt inn fordi man anså anlegg klassifisert etter forskrift 7. desember 2012 nummer 1157 om sikkerhet og beredskap i energiforsyningen (kraftberedskapsforskriften kapittel 5) for å være av vesentlig betydning for energiforsyningen, og at misbruk av informasjon om slike anlegg i sin ytterste konsekvens kan føre til at samfunnskritiske funksjoner blir satt ut av spill.

Departementet foreslår en utvidelse av forslag til ny ekomlov § 3-9 første ledd som vil gi datasenteroperatør, på lik linje som ekomtilbydere, rett til å kreve fremleggelse av ordinær politiattest av personer som skal ha tilgang til datasenter med vesentlig betydning for sikkerheten i nett eller tjenester. Formålet med å innføre et krav om politiattest er å bedre datasenteroperatørs mulighet til å sikre informasjon, utstyr eller systemer i datasenter med vesentlig betydning for sikkerheten i nett eller tjenester mot personer som av ulike grunner ikke er egnet til å ha tilgang til informasjonen og anleggene. En politiattest inneholder opplysninger om eventuelle straffedommer og lovovertredelser, og skal behandles i henhold til lov 15. juni 2018 nummer 38 om behandling av personopplysninger (personopplysningsloven) § 11. Politiregisterloven § 37 angir hvilke formål som berettiger krav om politiattest. Bestemmelsen kan blant annet brukes for å utelukke fysiske og juridiske personer fra stilling, virksomhet, aktivitet eller annen funksjon dersom et lovbrudd gjør en person uegnet og manglende utelukkelse vil kunne medføre betydelige skadevirkninger. Det følger av forskrift 20. september 2013 nummer 1097 om behandling av opplysninger i politiet og påtalemyndigheten (politiregisterforskriften) § 36-1 at politiattest kan utstedes til person som har fått tilbud om eller er innstilt til en konkret stilling, virksomhet, aktivitet eller annen funksjon. Nye krav om innhenting og fremlegges av politiattest vil som følge av dette bare

gjelde ved nyansettelser. Dersom vedkommende er sikkerhetsklarert eller innehar adgangsklarering fra Sivil klareringsmyndighet, vil det ikke stilles krav om politiattest, jf. forslag til ny ekomlov § 3-9 annet ledd. Det foreslås i tillegg at myndigheten kan gi nærmere bestemmelser om bruk av politiattest, jf. forslag til ny ekomlov § 3-9 tredje ledd.

4.5 Endring i ekomloven § 3-12 - Tillate bruksbegrensninger

Gjeldende ekomlov § 2-5 regulerer ekomtilbyders adgang til å gjennomføre bruksbegrensninger i elektroniske kommunikasjonsnett og -tjenester, og gir myndigheten kompetanse til å pålegge tilbyder å gjennomføre nødvendige bruksbegrensninger. Formålet med bestemmelsen er å sikre kontinuitet i brukerens elektroniske kommunikasjon og at bruksbegrensningene som foretas er nødvendige og forholdsmessige. Også for datasenteroperatør kan det oppstå et behov for å tillate bruksbegrensning, og det foreslås derfor å inkludere datasenteroperatør i forslag til ny ekomlov § 3-12.

Første ledd gir myndigheten kompetanse til å gi datasenteroperatør pålegg om å gjennomføre bruksbegrensninger. Slike pålegg kan gis av hensyn til nasjonal sikkerhet og andre viktige samfunnsinteresser, og skal være godt begrunnet. Myndigheten må ta hensyn til at kunder ved bruksbegrensninger vil kunne bli stående uten datasentertjenester i en mellomperiode. Det er med andre ord en høy terskel for å pålegge bruksbegrensninger. Første ledd legger opp til at myndigheten skal forta en konkret vurdering i det enkelte tilfellet. Pålegg etter første ledd skal begrunnes.

Annet ledd pålegger datasenteroperatør å gjennomføre nødvendige bruksbegrensninger i nødsituasjoner. Når det gjelder de opplistede nødsituasjonene som gir datasenteroperatør plikt til å innføre bruksbegrensninger, forutsettes det at datasenteroperatør selv tar stilling til om det foreligger fare for sabotasje mot datasenteret. Når det gjelder alvorlige trusler mot liv eller helse kan datasenteroperatør selv ta stilling til dette, eller det kan skje i samarbeid med myndigheter. Datasenteroperatør kan også ta selvstendig stilling til åpenbare tilfeller av trusler mot offentlig sikkerhet eller offentlig orden, men det vil i de fleste tilfeller være mest aktuelt for datasenteroperatør å foreta bruksbegrensninger som skyldes slike forhold i samråd med myndigheten.

4.6 Endring i ekomloven § 15-12 – Overtredelsesgebyr

Gjeldende ekomlov gir hjemmel til å ilegge overtredelsesgebyr i § 10-13 ved overtredelse av lov og forskriftsbestemmelser. Bestemmelsen er foreslått videreført i ny ekomlov § 15-12, med enkelte endringer, se forslag til merknader til ekomloven lenke til merknader se s. 149-150.

Det forslås inntatt i første ledd nr. 1 en referanse til forslaget til ny bestemmelse om datasenter § 3-13, slik at brudd på denne kan sanksjoneres med overtredelsesgebyr.

4.7 Endring i ekomloven § 15-13 – Straff

Nytt forslag til ekomlov § 15-13 om straff videreføres fra gjeldende ekomlov § 12-4 i en noe forenklet form. Bestemmelsen skal brukes ved brudd på regler som verner viktige samfunnsinteresser. Nærmere omtale av bestemmelsen er gitt i merknader til ekomloven, se lenke til merknader s. 150.

Det forslås inntatt i første ledd nr. 1 en referanse til forslaget til ny bestemmelse om datasenter § 3-13, slik at brudd på denne kan sanksjoneres med straff.

4.8 Endring i ekomloven § 17-1 – Sektoravgift og gebyr

Forslag til ny ekomlov § 17-1 viderefører gjeldende ekomlov § 12-1. Kostnader knyttet til utførelsen av Nasjonal kommunikasjonsmyndighets forvaltningsoppgaver finansieres av de som reguleres av Nasjonal kommunikasjonsmyndighet og bruker tilsynets tjenester i henhold til de årlige budsjettvedtakene fra Stortinget gjennom pålegg om sektoravgifter og gebyr. Blant forvaltningsoppgavene som kan finansieres på denne måten er kostnader knyttet til sektorspesifikt tilsyn med aktører i markeder for utstyr for elektroniske kommunikasjonsnett og -tjenester, aktørene i markeder for radio- og terminalutstyr og oppgaver knyttet til forvaltning av frekvens-, nummer-, navne- og adresseressurser. Denne listen er ikke uttømmende. Vi foreslår også å inkludere datasenteroperatør i opplistingen i første ledd annet punktum slik at det tydeliggjøres at sektoravgift og gebyr også vil pålegges disse virksomhetene. Se ytterligere omtale i merknader til ekomloven s. 156-157. Departementet understreker at ved finansieringen av Nasjonal kommunikasjonsmyndighet skal inntektene og utgiftene gå i null.

5. Endring i ekomforskriften

5.1 Ny bestemmelse om registringsplikt for datasenteroperatør

Ekomtilbydere har i dag plikt til å registrere seg hos Nasjonal kommunikasjonsmyndighet, jf. gjeldende ekomforskrift § 1-2. Formålet med bestemmelsen er å gi myndigheten en oversikt over hvilke aktører som er tilstede i markedet. Dette er nødvendig av flere grunner, blant annet av hensyn til Nasjonal kommunikasjonsmyndighets tilsynsvirksomhet. I tillegg vil det være viktig for politiet i arbeidet med kriminalitetsbekjempelse å kjenne datasenterets kontaktperson. Det er derfor nødvendig å sikre at datasenteroperatører registrerer seg hos Nasjonal kommunikasjonsmyndighet.

I første ledd foreslås det at datasenteroperatør har plikt til å registrere seg hos Nasjonal kommunikasjonsmyndighet. Registreringen foregår online. Det fremgår også av forslaget at virksomheten kan starte opp tilbud når registrering er sendt. Dette er ikke ment å være en tillatelsesordning som involverer skjønn og vedtak fra myndighetens side.

Forslag til annet ledd har regler om hva en registreringsmelding skal inneholde. Registreringsmeldingen skal omfatte en erklæring fra en fysisk eller juridisk person om at vedkommende har til hensikt å begynne å tilby datasentertjenester og de

minsteopplysningene som kreves for at det skal kunne føres et register eller en liste over datasenteroperatører. Registreringsplikten inneholder en del informasjon som er nødvendig for at myndigheten kan ha en oversikt over næringen, og føre tilsyn og gi rettigheter etter reglene som foreslås her.

Vi ber særlig om høringsinstansenes syn på forslaget i annet ledd nr. 8 som stiller krav til opplysning om norske statlige, fylkeskommunale og kommunale myndigheter, organer og virksomheter som er kunder hos datasenteret. Statsforetak og særlovselskap er egne rettssubjekter og vil som et utgangspunkt ikke anses som statlig eller kommunal myndighet. Dette er offentlige organer eller virksomheter som rettslig og økonomisk er utskilt fra stat og kommune. Departementet foreslår at plikten til å opplyse om kunder også bør omfatte egne rettssubjekter, som er utskilt fra stat eller kommune. Dette gjelder bl.a. statsforetak, særlovselskap og interkommunale selskaper.

Formålet med forslaget er å få en oversikt over hvilke datasentre som har samfunnskritiske kunder. Departementet ønsker en tilbakemelding på i hvilken grad disse myndighetene er kunder av datasentrene direkte eller om de kjøper tjenester av skytjenesteleverandører, som igjen kan være kunde hos en datasenteraktør. Videre vil slike kundelister kunne være svært dynamiske, noe som medfører at slike opplysninger må vedlikeholdes med jevne mellomrom.

Formålet med forslaget i annet ledd nr. 9 om at det skal opplyses et anslag på prosentvis andel av kraftforbruket som skal anvendes til utvinning av kryptovaluta, er for å kunne identifisere hvilke datasentre som driver kryptovalutautvinning og i hvilken grad. Departementet er klar over at kraftforbruket vil kunne være svært dynamisk og være avhengig av den til enhver tid gjeldende kundemasse, og at det kan være utfordrende å holde registreringen oppdatert. Dette er bakgrunnen for at vi ber om et anslag, og ikke en fullstendig oversikt til enhver tid. Vi ber særlig om høringsinstansenes tilbakemelding på dette forslaget.

Myndigheten, det vil i praksis si Nasjonal kommunikasjonsmyndighet, kan fastsette et standard meldingsskjema som skal brukes til registreringen, jf. tredje ledd. Det følger videre av forslaget at tilbyder skal melde fra om endringer i de registrerte opplysningene snarest mulig slik at registeret er så oppdatert som mulig, og senest innen to uker. Dette gjelder også opplysninger om at virksomheten legges ned.

5.2 Ny bestemmelse om terskelverdi for datasenteroperatør

Terskelverdien i ekomloven § 1-5 nr. 36 foreslås satt til 1 MW. Terskelverdien er absolutt og registreringsplikten inntrer når man operer datasenter over denne terskelverdien. Det bes særlig om høringsinstansenes tilbakemelding på terskelverdien. Departementet foreslår å legge terskelverdien i forskrift slik at den lettere kan justeres over tid.

5.3 Endring i ekomforskriften kap. 9 sikkerhet og beredskap

I høring av forslag til endringer i ekomforskriften er det foreslått et nytt kapittel 9 om sikkerhet og beredskap som er gitt med hjemmel i forslag til ny ekomlov § 3-8 sjette ledd. Forskriftsbestemmelsene i kapittel 9 utdyper kravet til systematisk oppfølgning av sikkerhet i nett og tjenester slik de fremgår av § 3-8. Det foreslås at bestemmelsene gis anvendelse også for datasenteraktører, med enkelte justeringer. De foreslåtte endringer i ekomforskriften vil gis med hjemmel i ny lovbestemmelse om datasenter.

De foreslås endringer i følgende forskriftsbestemmelser:

§ 9-1 Sikkerhetsstyring

§ 9-2 Risiko- og sårbarhetsvurdering

§ 9-3 Grunnsikring

§ 9-4 Særskilte krav til informasjon, informasjons- og styringssystemer

§ 9-5 Beredskapsplanlegging og øvelse

§ 9-6 Sikkerhetsrevisjon

§ 9-7 Oppfølgingsplikt

§ 9-8 Varsel

§ 9-9 Nasjonal autonomi

§ 9-10 Prioritering av tjenestetilbud

Se merknader til forslag til ny ekomforskrift hvor nærmere begrunnelse for forslagene fremgår på sidene 29-36. Vi ber særlig om høringsinstansenes tilbakemelding på om forslagene til endringer i ekomforskriftens kap. 9 er tilstrekkelig tilpasset ulike typer datasenter, herunder for «co-location-aktører» og «hyperscalere».

Når det gjelder forslaget til nasjonal autonomi vises det til datasenterstrategien Norske datasenter - berekraftige, digitale kraftsenter hvor det i punkt. 4.1.1 fremgår at datasenter med tjenester lokalisert i Norge, i større grad kan nyttes til samfunnskritiske funksjoner og skjermingsverdige informasjonssystemer enn datasentre lokalisert i utlandet.

6. Økonomiske og administrative konsekvenser

Forslaget vil medføre administrative konsekvenser for myndighetene ved innføring av en registreringsplikt. Dette antas å være en relativt avgrenset oppgave. I tillegg vil Nasjonal kommunikasjonsmyndighet få et nytt ansvar med blant annet å føre tilsyn med datasentre. Det nye ansvaret vil inngå som en del av tilsynets ordinære oppgaver.

Departementet legger til grunn at kostnaden ved å utvide ordningen med politiattest til å gjelde datasentrene på de foreslåtte vilkårene vil føre til noe økte kostnader for staten. Disse kostnadene antas likevel å bli relativt små, fordi datasenteraktørene er relativt få og politiattest vil med stor sannsynlighet kun vil bli innhentet for et fåtall ansatte. Slike kostnader må dessuten sees i sammenheng med samfunnsnytten. Den ekstra sikkerheten dette verktøyet vil medføre må ansees å mer enn oppveie en liten merkostnad.

En rekke av datasentrene stiller allerede strenge sikkerhetskrav av kommersielle grunner. Departementet antar at kravene som foreslås stilt av myndigheten, allerede håndteres i en eller annen form av datasentrene i dag. For de datasenter der det er avvik mellom kravene som stilles og sikkerhetsnivået i dag vil det imidlertid kunne påløpe kostnader som følge av innføring av sikkerhetskrav. Departementet legger til grunn at den ekstra sikkerheten som kravene i så fall vil medføre, vil oppveie eventuelle kostnader. Innføring av sikkerhetskrav og myndighetens tilsyn med disse, vil også kunne gi datasenteraktørene tilgang til informasjon som kan gjøre det lettere å ivareta egen sikkerhet.

Registreringen vil foregå online, og selve registreringen vil neppe medføre kostnader av betydning for datasentrene. Registreringen må også holdes oppdatert noe som kan føre til at det totalt sett påløper noen kostnader. Hvor store disse kostnadene blir vil avhenge av virksomhetens art. Departementet mener at dette er kostnader som en næringsvirksomhet av noe størrelse, jf. definisjonene, må regne med i dagens samfunn.

7. Forslag til endringer i utkast til ny ekomlov

§ 1-2 Saklig virkeområde

Første ledd første punktum skal lyde:

Loven gjelder virksomhet knyttet til elektronisk kommunikasjon og tilhørende utstyr, og *datasentre*.

§ 1-5 Definisjoner:

Følgende nye definisjoner skal lyde:

34. Datasenter: Et datasenter er et anlegg sammensatt av servere og andre komponenter som blir brukt til å organisere, prosessere, behandle, lagre og transportere data.

35. Datasentertjeneste: en tjeneste som tilbys i, eller i tilknytning til datasenter, herunder innplassering (areal), fysisk sikkerhet, strøm, kjøling, overvåknings- og analysetjenester, nettverkstilgang og IT-infrastrukturtjenester.

36. Datasenteroperatør: enhver fysisk og juridisk person som tilbyr andre tilgang til datasentertjeneste mot vederlag, eller som eier eller driver datasenter med en allokert elektrisk effekt over en terskelverdi som fastsettes av myndigheten i forskrift. Forsvarssektoren og politiet, inkludert Politiets sikkerhetstjeneste, omfattes ikke.

§ 3-9 Krav om politiattest

Første ledd skal lyde:

Tilbyder av elektronisk kommunikasjonsnett og -tjeneste med unntak av nummeruavhengig person-til-person-kommunikasjonstjeneste*, og datasenteroperatør,* kan kreve fremleggelse av ordinær politiattest av personer som skal ha tilgang til informasjon, elektronisk kommunikasjonsnett, tilhørende fasiliteter, *datasenter,* utstyr eller systemer med vesentlig betydning for sikkerheten. Politiattesten skal ikke være eldre enn 90 dager.

Det kreves ikke politiattest for personer som innehar gyldig sikkerhetsklarering eller adgangsklarering i henhold til sikkerhetslovens bestemmelser.

Myndigheten kan gi forskrifter om fremleggelse av politiattest.

§ 3-12 Tillatte bruksbegrensninger

Første ledd og annet ledd skal lyde:

Myndigheten kan pålegge tilbyder *eller datasenteroperatør* å gjennomføre bruksbegrensning i elektronisk kommunikasjonsnett og -tjeneste*, eller i datasentertjeneste,* av hensyn til nasjonal sikkerhet eller andre viktige samfunnsinteresser.

Tilbyder *og datasenteroperatør* skal gjennomføre nødvendige bruksbegrensninger i nødssituasjoner som innebærer alvorlige trusler mot liv eller helse, nasjonal sikkerhet eller offentlig orden, eller fare for sabotasje mot *datasenter,* nett eller tjeneste.

Ny § 3-13 Datasenter

Datasenteroperatør har plikt til å registrere seg hos myndigheten før virksomheten starter opp. Virksomheten kan settes i gang når registrering er sendt.

Datasenteroperatør skal tilby og opprettholde datasentertjenester med forsvarlig sikkerhet for brukerne i fred, krise og krig. Datasenteroperatør skal opprettholde forsvarlig beredskap, og viktige samfunnsaktører skal prioriteres ved behov. Myndigheten kan treffe enkeltvedtak for å sikre at datasenteroperatør iverksetter tiltak som gir forsvarlig sikkerhet og beredskap. Datasenteroperatør skal dekke kostnadene ved oppfyllelsen av dette.

Datasenteroperatør skal sørge for systematisk oppfølging av sikkerhet og beredskap i datasentertjenesten, og skal dokumentere et forsvarlig sikkerhetsnivå. I vurderingen av hva som er forsvarlig skal det blant annet tas hensyn til beste tilgjengelige tekniske løsning, tiltakenes kostnad og nytteverdi, datasentertjenestens betydning og anerkjente standarder.

Myndigheten kan treffe enkeltvedtak eller inngå avtale om gjennomføring av tiltak for å sikre oppfyllelse av nasjonale behov for sikkerhet, beredskap og funksjonalitet i datasenter utover det som følger av første ledd. Merkostnader ved levering av slike tiltak skal kompenseres av staten med basis i fyllestgjørende dokumentasjon som fremlegges av virksomheten for myndigheten. Myndigheten kan fatte vedtak om at virksomheten skal refundere dokumenterte utgifter som ikke er relevante i gjennomføringen av de avtalte eller pålagte tiltakene.

Myndigheten kan gi forskrifter om pliktene i paragrafen her, herunder om finansiering, nasjonal autonomi, sikkerhetsrevisjon og registreringsplikt. Myndigheten kan i forskrift eller

enkeltvedtak gi unntak fra registreringsplikten eller pålegge datasenteroperatører som driver datasenter under terskelverdien å registrere seg.

§ 15-12 Overtredelsesgebyr

Første ledd nr. 1, nr. 2 og nr. 3 skal lyde:

Myndigheten kan ilegge overtredelsesgebyr overfor fysiske personer og foretak dersom personen, foretaket eller noen som handler på vegne av foretaket forsettlig eller uaktsomt:

1. Overtrer § 2-1 første ledd, annet ledd eller tredje ledd, § 2-2 første ledd, § 2-3 første ledd, § 2-5, § 2-7 første ledd eller annet ledd, § 2-8, § 2-9 første ledd, § 2-10 første ledd, annet ledd, tredje ledd eller fjerde ledd, § 2-11 første ledd eller annet ledd, § 3-1 første ledd, annet ledd eller fjerde ledd, § 3-2 første ledd, annet ledd eller fjerde ledd, §3-3 første ledd, § 3-4 første ledd, annet ledd eller tredje ledd, § 3-5 første ledd eller fjerde ledd, § 3-6 første ledd, § 3-7 første ledd, § 3-8 første ledd eller annet ledd, §3-10 første ledd, § 3-12 annet ledd, tredje ledd, femte ledd, sjette ledd, sjuende ledd eller åttende ledd, *§ 3-13 første ledd, annet ledd eller tredje ledd,* § 4-1, §4-3 første ledd, § 4-4 første ledd, § 4-5 første ledd eller annet ledd, § 4-6 første ledd, fjerde ledd eller femte ledd, § 4-8 første ledd eller annet ledd, § 4-9 første ledd eller annet ledd, § 4-11, § 4-12 første ledd, annet ledd eller tredje ledd, § 4-13, § 4-14 første ledd, annet ledd, tredje ledd, fjerde ledd eller femte ledd, § 4-17 første ledd, annet ledd, tredje ledd eller fjerde ledd, § 4-18 første ledd, § 4-19, § 5-4 første ledd eller annet ledd, § 7-3 annet ledd, § 7-6 fjerde ledd, § 7-9 første ledd, § 7-10 tredje ledd, § 7-13 annet ledd, § 8-1 første ledd eller tredje ledd, § 9-2 første ledd eller tredje ledd, § 9-4 første ledd, § 11-10 første ledd, annet ledd, tredje ledd eller fjerde ledd, § 11-2 første ledd, § 11-10 første ledd, annet ledd, tredje ledd eller fjerde ledd, § 11-11 første ledd, § 12-2 første ledd, § 12-4 første ledd, § 12-5 første ledd eller annet ledd, § 13-1 første ledd, annet ledd eller fjerde ledd, § 13-2, § 15-3 første ledd eller annet ledd.

2. Overtrer forskrift gitt med hjemmel i § 2-1 fjerde ledd, § 2-2 annet ledd, § 2-4 annet ledd, § 2-6 fjerde ledd, § 2-7 tredje ledd, § 2-8 annet ledd, § 2-9 annet ledd, § 2-10 sjette ledd, § 2-11 tredje ledd, § 2-12 sjette ledd, § 3-1 femte ledd, § 3-2 femte ledd, § 3-3 annet ledd, § 3-4 fjerde ledd, § 3-5 femte ledd, § 3-6 tredje ledd, § 3-8 sjette ledd eller sjuende ledd, § 3-9 tredje ledd, § 3-10 annet ledd eller tredje ledd, § 3-11 tredje ledd, § 3-12 niende ledd, *§3-13 femte ledd,* § 4-2. § 4-3 tredje ledd, § 4-4 tredje ledd, § 4-5 tredje ledd, § 4-7, § 4-8 tredje ledd, § 4-9 tredje ledd, § 4-10 annet ledd, § 4-14 sjette ledd, § 4-15, § 4-16, § 4-17 femte ledd, § 4-18 annet ledd, § 5-1 tredje ledd, § 5-2 tredje ledd, § 5-3 tredje ledd, § 6-4 ellevte ledd, § 6-5 annet ledd, § 7-1 tredje ledd, § 7-2 sjette ledd, § 7-3 tredje ledd, § 7-4 femte ledd, §7-5 femte ledd, § 7-6 femte ledd, § 7-7 fjerde ledd, § 7-8 annet ledd, § 7-9 tredje ledd, § 7-12 sjette ledd, § 7-13 femte ledd, § 8-1 fjerde ledd, § 9-2 fjerde ledd, §10-1 femte ledd, § 10-2 femte ledd, § 10-3 sjuende ledd, § 10-4 femte ledd, § 10-5 femte ledd, § 10-6 sjette ledd, § 11-2 sjette ledd, § 11-6 sjette

ledd, § 11-10 åttende ledd, § 11-11 femte ledd, § 12-1 tredje ledd, § 12-2 fjerde ledd eller femte ledd, § 12-3 annet ledd, § 12-4 fjerde ledd, § 12-5 tredje ledd, § 12-6 tredje ledd, § 12- 7 sjette ledd, § 12-8, § 13-1 femte ledd, § 15-1 annet ledd, § 15-2 fjerde ledd eller § 15-4 annet ledd.

3. Overtrer enkeltvedtak fastsatt med hjemmel i § 2-3 annet ledd eller tredje ledd, § 44 2-4 annet ledd, § 2-6 første ledd, annet ledd eller tredje ledd, § 2-11 tredje ledd, § 2-12 fjerde ledd, § 3-8 første ledd, tredje ledd, fjerde ledd, femte ledd eller sjette ledd, § 3-10 annet ledd, § 3-11 første ledd, § 3-12 første ledd, *§ 3-13 fjerde ledd,* § 4-3 annet ledd, § 5-1 første ledd eller annet ledd, § 5- 2 annet ledd, § 5-3 første ledd, § 6-4 tredje ledd eller femte ledd, § 6-5 første ledd, § 7-1 første eller annet ledd, § 7-2 første ledd, annet ledd, tredje ledd, fjerde ledd eller femte ledd, § 7-4 første ledd, annet ledd, tredje ledd eller fjerde ledd, § 7-5 første ledd, tredje ledd eller fjerde ledd, § 7-6 første ledd, annet ledd eller tredje ledd, § 7-7 første ledd, annet ledd eller tredje ledd, § 7-10 første ledd eller annet ledd, § 7-11 første ledd, § 7-12 annet ledd, tredje ledd eller fjerde ledd, § 7-13 første ledd eller tredje ledd, § 8-1 første ledd, § 9-1 annet ledd, tredje ledd eller fjerde ledd, § 9-2 fjerde ledd, § 9-3 sjette ledd, § 9-4 fjerde ledd eller femte ledd, § 10-2 første ledd, § 10-3 første ledd, annet ledd, tredje ledd eller fjerne ledd, § 10-4 første ledd eller tredje ledd , § 10-5 første ledde eller tredje ledd, § 10-6 tredje ledd, § § 11- 10 femte ledd, § 11-11 annet ledd eller tredje ledd, § 12-2 femte ledd, § 12-3 første ledd, § 12-4 tredje ledd, § 12-6 første ledd eller annet ledd, , § 13-1 annet ledd eller tredje ledd, § 15- 3 første ledd eller annet ledd, § 15-4 første ledd, § 15-5 første ledd, annet ledd, tredje ledd eller fjerde ledd, § 15-8 første ledd eller annet ledd. 4. overtrer pålegg fastsatt med hjemmel i § 15-2.

§ 15-13 Straff

Første ledd nummer 1 skal lyde:

Med bøter eller fengsel inntil ett år straffes den som forsettlig eller uaktsomt:

1. overtrer § 2-10 første, annet, tredje eller fjerde ledd(anrop til nødmeldingstjeneste og geografisk lokalisering av nødanrop), § 2-11 første og annet ledd (eCall), § 3-1 første, annet og fjerde ledd (vern av kommunikasjon og data), § 3-2 første og annet ledd (taushetsplikt), 3- 3 første ledd (sletting av data), § 3-6 første ledd (tilrettelegging for lovbestemt tilgang til informasjon), § 3-8 første og annet ledd (sikkerhet i nett og tjenester), *§ 3-13 (datasenter) første ledd, annet ledd og tredje ledd,* § 3-10 første ledd (Formidling av viktig melding), § 11-2 første ledd (tillatelse til bruk av frekvenser), § 12-2 første ledd (tillatelse til bruk), § 13-1 første, annet ledd og tredje ledd (omsetning av utstyr), § 13-2 (utstyr som er beregnet på å forstyrre elektronisk kommunikasjon) og § 15-3 (medvirkning ved tilsyn)

17-1 Sektoravgift og gebyr

Andre ledd skal lyde:

Sektoravgift og gebyr kan pålegges tilbydere av elektroniske kommunikasjonsnett og -tjenester, og aktører som tilbyr utstyr for elektronisk kommunikasjon. Det samme gjelder den som får tilgang til frekvens-, nummer-, navn- og adresseressurser, *datasenteroperatør* og andre som reguleres i eller i medhold av denne loven.

8. Forslag til endringer i ekomforskriften

§ 1-9 Registreringsplikt for datasenter
Ny § 1-9 skal lyde:

Datasenteroperatør etter ekomloven § 3-13 har plikt til å registrere seg hos myndigheten før virksomheten starter opp. Tilbud kan settes i gang når registrering er sendt.

Datasenteroperatør som har registreringsplikt skal skriftlig opplyse om:

1. *datasenteroperatørs navn,*
2. *norsk organisasjonsnummer eller datasenteroperatørens rettslige status, form og registreringsnummer dersom datasenteroperatøren er registrert i et handelsregister eller et lignende offentlig register i EØS,*
3. *norsk adresse eller adressen til datasenteroperatørens eventuelle hovedforetak i EØS, og eventuelt en sekundær filial,*
4. *datasenteroperatørens nettadresse,*
5. *datasentrenes fysiske lokasjon*
6. *kontaktperson som er ansvarlig for datasenteroperatøren og dennes kontaktinformasjon,*
7. *beskrivelse av tjenestene som tilbys*
8. *norske statlige, fylkeskommunale og kommunale myndigheter, organer og virksomheter som er kunder hos datasenteret*
9. *anslag på prosentvis andel kraftforbruket som skal anvendes til utvinning av kryptovaluta*
10. *forventet oppstart av virksomheten*

Myndigheten kan fastsette standardskjema som skal nyttes ved registreringen. Endringer i registrerte opplysninger skal snarest mulig og senest innen to uker meldes til myndigheten.

§ 1-10 Terskelverdi for datasenteroperatør
Ny § 1-10 skal lyde:

Terskelverdien i ekomloven 1-5 nr. 36 er 1 MW eller mer.

§ 9-1 Sikkerhetsstyring
§ 9-1 første, tredje og fjerde ledd skal lyde:

Tilbyder *og datasenteroperatør* skal etablere og vedlikeholde et styringssystem for sikkerhet som beskriver virksomhetens sikkerhetsarbeid. Systemet skal sikre at virksomheten oppfyller krav gitt i eller med hjemmel i lov.

Dokumentasjon for tilbyders *og datasenteroperatørs* styringssystem for sikkerhet skal etableres.

Tilbyder *og datasenteroperatør* skal jevnlig kontrollere og revidere planverk og dokumentasjon knyttet til virksomhetens sikkerhetsstyring for å sikre at krav fastsatt i eller med hjemmel i lov er oppfylt.

§ 9-2 Risiko- og sårbarhetsvurdering

§ 9-2 skal lyde:

Tilbyder skal utarbeide og vedlikeholde risiko- og sårbarhetsvurderinger for å ivareta forsvarlig sikkerhet i elektronisk kommunikasjonsnett og elektronisk kommunikasjonstjeneste. *Datasenteroperatør skal utarbeide og vedlikeholde risiko- og sårbarhetsvurderinger for å ivareta forsvarlig sikkerhet i datasentertjenester.* Risiko- og sårbarhetsvurderingene skal være av et slikt omfang at tilbyder kan identifisere organisatoriske, fysiske, logiske og menneskelige sikkerhetstiltak.

Ved endringer som kan påvirke sikkerheten skal tilbyder *og datasenteroperatør* vurdere hvilken risiko endringene medfører.

Risiko- og sårbarhetsvurderinger *som nevnt i første og andre ledd* skal dokumenteres.

§ 9-3 Grunnsikring

§ 9-3 første, annet og tredje ledd skal lyde:

Tilbyder skal utarbeide, iverksette og vedlikeholde grunnsikringstiltak for å ivareta forsvarlig sikkerhet i elektronisk kommunikasjonsnett og elektronisk kommunikasjonstjeneste. *Datasenteroperatør skal utarbeide, iverksette og vedlikeholde grunnsikringstiltak for å ivareta forsvarlig sikkerhet i datasentertjenester.* Grunnsikringstiltak innebærer en kombinasjon av barrierer, deteksjons-, verifikasjons- og reaksjonstiltak.

Tilbyder og *datasenteroperatør* skal planlegge skadebegrensningstiltak som kan iverksettes i situasjoner som ikke kan håndteres fullt ut med grunnsikringstiltakene.

Tilbyder *og datasenteroperatør* skal ha en plan for å gjenopprette et forsvarlig sikkerhetsnivå.

§ 9-4 Særskilte krav til informasjon, informasjons- og styringssystemer

§ 9-4 skal lyde:

Tilbyder *og datasenteroperatør* skal utarbeide, iverksette og vedlikeholde planer for sikring av informasjon, informasjonssystemer og styringssystemer. Sikringsplaner innebærer som et minimum at tilbyder utarbeider og iverksetter prosedyrer for tildeling av

rettigheter, tilgangskontroll, endring, sletting, logging, redundans, sikkerhetskopiering, vedlikehold og testing for å ivareta tilgjengelighet, autentisitet, integritet og konfidensialitet.

Tilbyders *og datasenteroperatørs* sikringsplaner skal dokumenteres fortløpende.

§ 9-5 Beredskapsplanlegging og øvelser

§ 9-5 skal lyde:

Tilbyder skal utarbeide og vedlikeholde beredskapsplaner for å ivareta forsvarlig sikkerhet i elektronisk kommunikasjonsnett og elektronisk kommunikasjonstjeneste. *Datasenteroperatør skal utarbeide og vedlikeholde beredskapsplaner for å ivareta forsvarlig sikkerhet datasentertjenester.* Tilbyders og *datasenteroperatørs* beredskapsplaner skal dokumenteres.

Tilbyder *og datasenteroperatør* skal jevnlig gjennomføre beredskapsøvelser med det innhold og omfang som er nødvendig for å vedlikeholde og utvikle virksomhetens kompetanse og evne til å håndtere uønskede hendelser. Plan for gjennomføring av beredskapsøvelser skal dokumenteres.

Tilbyder *og datasenteroperatør* skal på forespørsel delta i beredskapsøvelser arrangert av myndigheten.

§ 9-6 Sikkerhetsrevisjon

§ 9-6 Sikkerhetsrevisjon skal lyde:

Nasjonal kommunikasjonsmyndighet kan i særlige tilfeller pålegge tilbyder av offentlig elektronisk *kommunikasjonsnett, tilbyder* av offentlig tilgjengelig elektronisk kommunikasjonstjeneste *eller datasenteroperatør* å foreta en sikkerhetsrevisjon av hele eller deler av virksomheten. Revisjonen skal foretas av en uavhengig, kvalifisert tredjepart, og resultatet av revisjonen skal sendes Nasjonal kommunikasjonsmyndighet. Tilbyderen *eller datasenteroperatør* skal dekke alle kostnader ved revisjonen. Pålegget skal regnes som en prosessledende avgjørelse.

§ 9-7 Oppfølgingsplikt

§ 9-7 skal lyde:

Tilbyder *og datasenteroperatør* skal følge opp at leverandører, entreprenører og andre kontraktører som utfører arbeid for eller på vegne av virksomheten etterlever sikkerhetskrav fastsatt i eller med hjemmel i lov.

§ 9-8 Varsel

§ 9-8 syvende ledd skal lyde:

Bestemmelsens første ledd, tredje ledd, fjerde ledd og femte ledd gjelder tilsvarende for datasenteroperatør.

§ 9-9 Nasjonal autonomi

§ 9-9 skal lyde:

Nasjonal kommunikasjonsmyndighet kan i krise- og beredskapssituasjon pålegge tilbyder *og datasenteroperatør* å utføre drift og vedlikehold av tjenestetilbudet med personell og tekniske løsninger som er lokalisert på norsk territorium.

§ 9-10 Prioritering av tjenestetilbud

§ 9-10 annet ledd skal lyde:

Myndigheten kan i særlige tilfeller så langt det er nødvendig for å sikre offentlige interesser, pålegge tilbyder *og datasenteroperatør* å gi prioritet til viktige samfunnsaktører ved gjenoppretting etter driftsstans.