Forslag til merknader til ny forskrift om elektronisk kommunikasjonsnett og -tjenester (ekomforskriften)

Til kapittel 1. Krav til eier og tilbyder av elektroniske kommunikasjonsnett og -tjenester

Til § 1-1 Krav til bygging og dokumentasjon av elektronisk kommunikasjonsnett

Bestemmelsen viderefører gjeldende forskrift § 1-3 om krav til bygging av nett.
Første ledd viderefører og utvider virkeområdet til gjeldende § 9-5 første ledd som i dag gjelder for private nett, til å gjelde alle ekomnett, både private og offentlige.
Annet ledd er en videreføring av § 1-3 første ledd i sin helhet.
Forskriften § 1-3 gjeldende tredje ledd videreføres indirekte i første og annet ledd, og departementet foreslår at gjeldende tredje ledd utgår. Kravet i (nytt) annet ledd setter generelle og teknologinøytrale krav om at elektronisk kommunikasjonsnett skal bygges slik at ikke sluttbruker kan påvirke andre sluttbrukeres elektroniske kommunikasjon med den følge at det forårsakes fare for redusert tjenestekvalitet eller mulighet for avlytting. Dette kan oppnås på flere måter og ikke kun ved bruk av stjernestruktur som er spesifikt for koaksialkabelbaserte nett. Det viktigste er at kommunikasjonen beskyttes, og så lenge nettet bygges slik at det ivaretas ønsker ikke myndigheten å sette spesifikke krav som kun gjelder én type nett/kabel. For spesifikke krav kan legge en demper på teknologisk utvikling og utvikling av bransjestandarder.
I *tredje ledd* foreslås noen justeringer i forhold til gjeldende rett. For det første foreslås å knytte kravet til «eier», jf. ekomloven § 2-7. I tillegg tydeliggjøres at kravet til dokumentasjonsplikten skal gjelde alle nett, med unntak av nett som bare omfatter en husstand.

Til § 1-2 Krav til offentliggjøring av grensesnittspesifikasjon

Bestemmelsen viderefører § 1-5 med unntak av at annet ledd, siste punktums henvisning til § 13-1 om omsetning av utstyr (gjeldende § 8-1), fordi kravene som stilles etter § 13-1 ikke gjelder grensesnittspesifikasjoner.

Til § 1-3 Krav til opplysninger ved nødanrop

Bestemmelsen viderefører ekomforskriften § 6-2a, og utdyper forslag til ny ekomlov § 2-10
Første ledd utdyper hvilke abonnementsinformasjon som skal gjøres tilgjengelig for nødetatene. Dette inkluderer hemmelig nummer som også skal tilgjengeliggjøres ved nødanrop. *Annet ledd* regulerer den nettverkbaserte posisjonen som skal overføres for nødanrop fra mobilterminal.
Forslaget viderefører at tilbyderne skal sørge for at det også overføres opplysninger som angir terminalens lokalisering ved nødanropet med så høy grad av nøyaktighet som mulig. Nøyaktigheten skal etter nummer 1 fortsatt minst tilsvare den som oppnås ved å kombinere basestasjonens beregnede dekningsområde, sektorangivelse og beregning av terminalens avstand fra basestasjonen, dvs. såkalt timing advance. Videre skal opplysninger om basestasjonens faktiske dekning på bakgrunn av målinger eller beregninger fortsatt oversendes til nødetatene. Dette viderefører gjeldende rett.

Det foreslås i *tredje ledd* å videreføre en plikt til å overføre informasjon om mobilterminalens lokalisering innenfor en feilmargin på maksimalt 50 meter for minimum 80 prosent av nødanropene. Grunnen til at det ikke foreslås høyere krav enn 80 prosent av nødanropene, er at en viss andel av nødanrop vil være foretatt fra eldre mobiltelefoner uten GNSS- og/eller WiFi funksjonalitet. Anrop kan også ha blitt foretatt fra lokasjoner hvor det er begrenset med posisjonsinformasjon tilgjengelig fra satellitt eller andre kilder. Det er derfor per i dag behov for et visst slingringsmonn.
For å oppfylle bestemmelsen kan tilbyderne lage løsninger selv eller inngå samarbeid om posisjoneringstjenester med operativsystemleverandører eller andre. Google eller Apples AML-tjeneste vil være tjenester som kan benyttes. Det kan også finnes andre. For å sikre at det 80 prosent-kravet ikke blir stående over tid, presiserer bestemmelsen at nødanropet skal lokaliseres med så høy grad av nøyaktighet som mulig. For å oppfylle plikten kan tilbyderne selv utvikle de nødvendige tekniske løsningene, eller inngå samarbeid om posisjoneringstjenester med andre, for eksempel mobiltelefonprodusenter, operativsystemleverandører eller andre.
Videre foreslås det i *fjerde ledd* videreført at nødanrop skal kunne foretas ved bruk av mobilterminalens ordinære samtaleoppsett. Løsningen tilbyderne velger må derfor være utformet slik at innringer fortsatt skal kunne ringe nødnummer på ordinært vis, noe som innebærer at anropet skal kunne gjøres fra mobilens ordinære samtaleoppsett, og uten at det eksempelvis er nødvendig å laste ned en applikasjon eller annet for å kunne foreta samtalen. I utgangspunktet foreslås at posisjonsdata skal overføres selv om sluttbruker har reservert seg mot aktivering av stedstjenester, med mindre det følger av operativsystemet. Hensynet til sluttbrukers personvern må her vike for hensynet til nødetatenes behov og mulighetene for å utføre nødvendig assistanse for nødstilte personer. Forslaget til forskriftsbestemmelse operasjonaliserer dette kravet. For å hindre at informasjon misbrukes gjelder overføring av posisjonsinformasjon etter denne bestemmelsen bare så lenge nødanropet varer. Dette betyr at posisjoneringen aktiveres når nødanropet foretas og slås av når anropet er avsluttet. Når det gjelder aktører som tilbyr løsninger for utregning og/eller overføring av posisjonsdata ved nødanrop, foreslås det en plikt for dem til å legge til rette for at håndsettbaserte lokasjonsdata overføres til nødetatene. De som omfattes av forslaget kan være leverandører av operativsystem eller andre som tilbyr løsninger for utregningen og/eller overføring av posisjonsdata ved nødanrop.
I *femte ledd* foreslås videreført gjeldende rett om at det for anrop fra IP-telefon, hvor det i tillegg til overføring av opplysninger om telefonnummer, sluttbrukers navn og adresse, jf. første ledd, skal opplyses at overført adresse, jf. første ledd nummer 3, kan avvike fra faktisk lokasjon. Et slikt krav vil bidra til å lette nødetatenes arbeid med å lokalisere den nødstilte så raskt som mulig. Både nettverksinitierte- og håndsettbaserte løsninger kan benyttes for å oppfylle bestemmelsens krav. Bestemmelsen setter også setter krav til nøyaktighet. Bestemmelsen vil bidra at nødetatene får tilgang til mer nøyaktige lokaliseringsdata ved nødanrop – uavhengig av hvordan tilbyderne sørger for at dette målet nås.
Siste ledd gjennomfører ekomdirektivet artikkel 109 nummer 1 annet avsnitt, hvor der det fremgår at medlemsland skal fremme tilgang til nødtjenester gjennom nødnummer, fra elektroniske kommunikasjonsnett som ikke er offentlig tilgjengelig, men som muliggjør anrop til offentlige nett. Overføring av opprinnelsesmarkering fra private nett til nødetatene krever samarbeid mellom de involverte parter. Samarbeidet skal bestå av konkret assistanse for å gjennomføre forsvarlige nødanrop.

Til § 1-4 SMS og MMS til nødnummer

I *første ledd* er brukergruppen for SMS og MMS til nødnummer utvidet i henhold til ekomdirektivet direktivet artikkel 95 nummer 5 til å gjelde brukere med nedsatt funksjonsevne som ikke kan benytte talekommunikasjonstjeneste.
I *annet ledd* fremkommer det at det per i dag kun er forhåndsregistrerte sluttbrukere med funksjonsnedsettelser som kan benytte SMS og MMS ordningen. Andre sluttbrukere vil få en automatisk generert tilbakemelding om at SMS og MMS til nødetatenes nødmeldingstjeneste ikke er kommet frem, slik at de kan henvende seg til nødetaten på annet vis.
Tredje ledd regulerer kommunikasjon med nødetatene i form av video. Det er ikke avgjørende hvordan videostrømmen ble etablert. Anropet kan for eksempel initiert av innringer initiert ved videoanrop, eller det kan være i form av at innringer mottar en tekstmelding fra nødetat som ber ham trykke på en link som etablerer en videolink. Denne trafikken skal nulltakseres i tråd med de generelle prinsippene for nødkommunikasjon og slik at nødstilte ikke risikerer at videolinken avbrytes på grunn av tomt kontaktkort eller overskridelse av datamengde.
Tilbyder har kun plikt til vederlagsfri overføring, dersom etaten/-e kan og ønsker å motta video. Overføringen skal skje til nærmeste relevante nødmeldingssentral, etter avklaring mellom tilbyder og nødetat. Dersom en etat har løsninger for mottak, men ikke en annen, skal video formidles til den etat som har løsninger.
Det foreslås videre i *fjerde ledd* å videreføre at mobiltelefonen som brukes ved sending av SMS og MMS eller tilsvarende til nødnumrene skal posisjoneres som ved taleanrop. Det innebærer at forslaget i § 1-3 om at faktisk posisjon skal overføres dersom det er mulig, også skal gjelde for nødanrop via SMS og MMS.
Nasjonal kommunikasjonsmyndighet kan etter *femte ledd* fastsette grensesnitt for utveksling av informasjon mellom mødetater og tilbydere. Dette kan for eksempel gjelde tekniske rutiner og ansvarsfordeling.

Til § 1-5 Kostnadsfordeling ved eCall

Kostnader ved håndtering av eCall skal ikke belastes brukerne. Dette er i tråd med prinsippene for formidling av andre nødanrop. Etter *første ledd* er det tilbyder av offentlig elektronisk kommunikasjonstjeneste som for egen regning skal rute eCall til mottakssentral. Etter *annet ledd* er ekomtilbyderne med eget nett som skal bekoste oppgradering og tilrettelegging av sine systemer slik at informasjonen kan overføres fra kjøretøyet via eCall til valgt mottakssentral.
Tilbydernes plikt til å overføre data for egen regning til mottakssentralen omfatter imidlertid ikke foredling av dataene. Det er rådata i henhold til et avtalt format mellom tilbyderen og mottakssentral som skal leveres gratis til mottakssentralene. Mottakssentralene må etter *tredje ledd* selv dekke kostnadene til dataprogrammer og lignende som kreves for mottak av informasjonen.

Til § 1-6 Krav til skriftlig fullmakt

Bestemmelsen setter krav om skriftlig samtykke ved flytting av telefontjenester, internettjenester og andre elektroniske kommunikasjonstjenester. Bestemmelsen viderefører gjeldende forskrift § 1-10. Bestemmelsen er ment å sikre at avtalen om å bytte tilbyder er riktig forstått av begge parter, både sluttbruker og tilbyder, og at hva som avtales kan etterprøves og innehar en viss grad av notoritet.

Avtaleinngåelse på bakgrunn av oppsøkende telefonsalg er ikke alene nok for å bytte tilbyder. Sluttbruker må skriftlig akseptere innholdet i avtalen, for eksempel ved å besvare en SMS eller e-post. Likestilt med dette er signering av avtaledokumenter med elektroniske tillitstjenester, som for eksempel BankID.

Til § 1-7 Entydig identifisering av fysiske personer

Forslag til bestemmelse ble sendt på høring 3. september 2019, og høres igjen etter endringer og justert basert på innkommende høringsinnspill.

Departementet foreslår en presisering av hvordan entydig identifisering av sluttbruker som er fysisk person skal gjennomføres. *Første ledd* nummer 1 gjelder ved personlig oppmøte og stiller krav fremleggelse av originalt identitetsbevis. Bestemmelsen inneholder videre en uttømmende liste over hva et originalt identitetsbevis skal inneholde, jf. *bokstav a-c.*

Når det gjelder krav om fødselsnummer, bemerker departementet at dette er "nødvendig" for å oppnå entydig identifisering og kravet til "saklig behov" i personopplysningsloven § 12 er således oppfylt. Ved å innhente fødselsnummer muliggjøres en sikrere sammenligning av gitt informasjon med informasjon fra for eksempel Folkeregisteret. En slik sammenligning er nødvendig for å identifisere sluttbruker på en sikker måte. Uten tilgang til fødselsnummer bortfaller et sentralt element av identifiseringsprosessen, ved at man mister muligheten for presist sammenligningsgrunnlag, basert på numeriske verdier.

Et D-nummer er et midlertidig ID-nummer som du får hvis en person har søkt om beskyttelse (asyl) i Norge, eller har en oppholdstillatelse og skal være her i mindre enn seks måneder. Et DUF-nummer er registreringsnummeret til en person i Utlendingsdirektoratets datasystem. Alle som søker om beskyttelse eller opphold i Norge får et DUF-nummer.

Første ledd nummer 2 gjelder entydig identifisering ved bruk av elektronisk identifikasjon. eID er blitt en viktig og vanlig måte å identifisere seg på som både er tilgjengelig og enkel. Bestemmelsen stiller krav til at den elektroniske identifikasjonen har et visst sikkerhetsnivå, jf. presiseringen om at eID må være på nivå betydelig eller høyt i henhold til selvdeklarasjonsforskriften.

Første ledd nummer 3 åpner opp for bruk av utenlandsk eID fra andre EØS-land. På samme måte som i nummer 2, må slik eID oppfylle kravene for sikkerhetsnivå "betydelig" eller "høyt" i henhold til eIDAS-forordningen artikkel 9 eller at det på annet vis verifiseres at dette nivået er oppfylt. eIDAs forordningen er innlemmet i EØS-avtalen og gjennomført i norsk rett i lov om elektroniske tillitstjenester.

I henhold til *første ledd nummer 4* aksepteres også avansert elektronisk signatur i henhold til eIDAS-forordningen artikkel 26.

Andre ledd gir enkelte unntak for kravene til identitetsbeviset i første ledd. For sluttbrukere som ikke har norsk fødselsnummer D-nummer eller DUF-nummer, oppstilles det ytterligere krav ved at fødselsdato, fødested og statsborgerskap skal fremgå av identitetsbeviset.

Tredje ledd inneholder et krav om at tilbyder skal dokumentere identitetskontrollen foretatt etter første ledd, ved at tilbyder registrerer at identitetsbevis er fremlagt og hvilken type bevis dette var. Registrering kan eksempelvis skje ved at tilbyder eller underleverandør i bestillingsdokumentet markerer hvilken type identitetsbevis og referansenummer/kontrollnummer mv. som er benyttet ved bestillingen.

Hensynene bak skjerpet entydig identifisering er redegjort for i høringen 3. september 2019.

Til § 1-8 Entydig identifisering når sluttbruker er et foretak mv.

Forslag til bestemmelse ble sendt på høring 3. september 2019, og høres igjen etter endringer og justert basert på innkommende høringsinnspill.

Bestemmelsen gjelder for hvordan entydig identifisering av sluttbruker som er en juridisk person, men ikke en fysisk person, skal gjennomføres. *Første ledd* oppstiller hvilke opplysninger som skal innhentes om sluttbrukeren.

Andre ledd gjelder i de tilfeller der en fysisk person handler på vegne av en juridisk person. I slike tilfeller skal reglene i § 1-7 komme til anvendelse. Definisjonen av foretak følger i utgangspunktet lov om foretakregister, men entydig identifisering går lengre enn det og omfatter i realiteten alle sluttkunder som ikke er fysiske personer, blant annet norske enkeltpersonforetak som ikke omfattes av registreringsplikten i foretaksregisterloven, stiftelser om ikke er inkludert, et juridisk arrangement eller en annen sammenslutning.

Tredje ledd oppstiller en plikt på tilbyder til å bekrefte opplysningene innhentet etter første ledd. Retten til å handle på vegne av en juridisk person, jf. annet ledd skal også bekreftes.

Fjerde ledd likestiller elektroniske segl som gyldig identifikasjon av juridiske personer med metodene beskrevet i første til tredje ledd. Det er videre henvist til de aktuelle regelverk som oppstiller krav til elektroniske segl.

Til kapittel 2 Sluttbrukerrettigheter

Til § 2-1 Nettnøytralitet

Viderefører gjeldende § 1-12 som gjennomfører europaparlamentets- og rådsforordning (EU) 2015/2120 innenfor rammen av EØS-avtalen.

Bakgrunnen for reglene om nettnøytralitet er målsetningen om å sikre at internett forblir en velfungerende, åpen og ikke-diskriminerende plattform for alle typer kommunikasjon og distribusjon av lovlig innhold. Prinsippet om nettnøytralitet medfører blant annet at sluttkunder kan velge innhold og utstyr uavhengig av hvilket ekomnett de er tilknyttet. Det nærmere innholdet i dette vil fremgå av forordningen som med bestemmelsen fortsatt vil være en del av norsk rett.

Til § 2-2 Leveringsvilkår

Forlag til bestemmelse viderefører delvis gjeldende § 1-7 og gjennomfører ekomdirektivet artikkel 103 og vedlegg IX. Formålet med bestemmelsen er å sikre at sluttbrukere får nødvendig informasjon fra tjenestetilbyderne. Bestemmelsen er ment å legge forholdene til rette for at sluttbruker skal kunne sammenlikne leveringsvilkår fra flere ulike tjenestetilbydere. Krav om offentliggjøring av vilkårene vil gjøre det enklere for sluttbruker å velge den løsning som er best for vedkommende, og dermed bidra med å fremme bærekraftig konkurranse.

Etter *første ledd* plikter tilbyder av internettilgangstjeneste og offentlig tilgjengelig person-til-person kommunikasjonstjeneste som tilbyr disse tjenestene til sluttbrukere å utarbeide og offentliggjøre leveringsvilkårene. Opplysningene skal ajourføres regelmessig og skal offentliggjøres på en klar, fyllestgjørende og maskinleselig måte.

Annet ledd spesifiserer nærmere hva leveringsvilkårene minst må inneholde i nummer 1 til 9. Opplistingen er en delvis videreføring av gjeldende krav til leveringsvilkår i gjeldende forskrift § 1-7. Oppramsingen er ikke uttømmende, men representerer et sett av minimumskrav.

Etter *nummer 1* skal leveringsvilkårene inneholde kontaktinformasjonen til tilbyderen, herunder navn og adresse.

Etter *nummer 2* skal leveringsvilkårene inneholde beskrivelse av tjenestenes og eventuelle tilleggstjenesters innhold og omfang. Dette inkluderer også eventuelle minstenivåer for tjenestekvalitet, og eventuelle begrensninger, blant annet begrensninger som pålegges av tilbyderen for bruk av terminalutstyr som er levert. Innhold og omfang omfatter også blant annet informasjon om hastighet og kapasitet for ulike typer tjenester og abonnementer.
Etter *nummer 3* skal leveringsvilkårene inneholde informasjon om standard avtalevilkår og særlige regler om bindingstid, bruddgebyrer, heving av pakketilbud eller elementer i pakketilbud, eventuelle fremgangsmåter ved portering.
Etter *nummer 4* skal leveringsvilkårene inneholde omfattende informasjon om takster for de tjenester som tilbys, herunder volum for databruk, tale og meldinger, for særlige takstplaner og tjenester som er underlagt særlige prisvilkår, gebyrer for tilgang og vedlikehold.
Etter *nummer 5* skal leveringsvilkårene inneholde informasjon om vedlikeholdstjenester som er tilgjengelig for sluttbrukeren.
Etter *nummer 6* skal leveringsvilkårene inneholde informasjon om kompensasjons- og refusjonsordninger hos tilbyderen. I tillegg skal leveringsvilkårene inneholde kontaktinformasjon til kundeservice, samt informasjon om klageordninger og tvisteløsning.
Etter *nummer 7* skal leveringsvilkårene inneholde detaljerte opplysninger om produkter og tjenester særlig utformet for sluttbrukere med nedsatt funksjonsevne. Dette gjelder eventuelle funksjoner, praksis, retningslinjer og fremgangsmåter og endringer i driften av tjenesten, som er særlig tilpasset sluttbrukere med nedsatt funksjonsevne. Informasjon om vilkårene skal være tilgjengeliggjort på en maskinleselig måte og i et format som gjør opplysningene tilgjengelige for sluttbrukerne med nedsatt funksjonsevne.
Etter *nummer 8* skal leveringsvilkårene til tilbyder av nummerbaserte person-til-person kommunikasjonstjenester inneholde informasjon om tilgang til nødmeldingstjenester og lokalisering av anrop, og enhver begrensning på sistnevnte.
Etter *nummer 9* skal leveringsvilkårene til tilbyder av nummeruavhengige person-til-person kommunikasjonstjenester inneholde informasjon om i hvilken grad tilgang til nødmeldingstjenester støttes eller ikke.
Merk at pliktene etter nummer 8 og nummer 9 er begrenset til kun å gjelde nummerbaserte person-til-person kommunikasjonstjenester.
Tredje ledd viderefører kravet om at tilbyder som tilbyr leveringspliktige tjenester skal inkludere informasjon om disse tjenestene spesielt i sine leveringsvilkår.

Til § 2-3 Opplysningskrav før avtaletilbud

Forslag til bestemmelse er ny, og gjennomfører ekomdirektivet artikkel 102 nummer 1. Bestemmelsen fastsetter hva tilbyder skal opplyse om før en forbruker blir bundet av avtale. Kravene er i tråd med artikkel 5 og 6 i direktiv 2011/83/EU om forbrukerrettigheter opplysningene som er oppført i vedlegg VIII i ekomdirektivet.
Første ledd gjelder informasjonsplikt for tilbyder av offentlig tilgjengelige elektroniske kommunikasjonstjenester med unntak av overføringstjenester som brukes til levering av maskin-til-maskin-tjenester. De konkrete kravene til informasjon før eventuell avtale inngås fremgår av forskriftsteksten.
Annet ledd gjelder tilbyder av internettilgangstjenester og offentlig tilgjengelige person-til-person kommunikasjonstjenester. Annet ledd hjemler kravene for hvilke opplysninger tilbyder av disse tilbyderne må gi før avtale inngås.

Tredje ledd regulerer hvilke opplysninger tilbydere av offentlig tilgjengelige nummerbaserte person-til-person kommunikasjonstjenester skal gi før avtale inngås.
Fjerde ledd hjemler at tilbydere av internettilgangstjenester i tillegg til opplysningene i første og annet ledd skal gi opplysninger som kreves i henhold til (EU) 2015/2120) (TSM-forordningen) artikkel 4 nummer 1 jf. ekomforskriften §1-12. Det vises direkte til TSM-forordningen i bestemmelsen fordi den er tatt inn i ekomloven som sådan.
I *femte ledd* fremgår det krav om at opplysningene skal gis på en klar og forståelig måte på et dokument som gjøres tilgjengelig av tilbyderen og som enkelt kan lastes ned. Kravene stilles for å gjøre opplysningene enkelt tilgjengelig for forbrukeren. Videre presiseres det i forskriften at tilbyderen uttrykkelig skal gjøre forbrukeren oppmerksom på tilgjengeligheten av dokumentet samt betydningen av å laste det ned av hensyn til fremtidig dokumentasjon og referanse. Det skal også sikres at forbrukeren skal få en uendret gjengivelse av tilbudt avtale.

Til § 2-4 Innhold i avtalesammendrag

Bestemmelsen gjennomfører ekomdirektivet artikkel 102 nummer 3 og 4.
I bestemmelsens *første ledd* hjemles det at avtalesammendraget skal vise de viktigste elementene i opplysningskravene som fremgår av ekomforskriften § 2-3. Med «de viktigste elementene» menes de elementene som utgjør hovedgrunnlaget for beslutningen om at avtalen inngås.
I *annet ledd* er det listet opp en detaljert beskrivelse av hva avtalesammendraget minst skal omfatte. I avtalesammendraget skal det også gis et sammendrag av de opplysningene som fremgår av (EU) 2015/2120 (TSM-forordningen) artikkel 4 nummer 1 bokstav d og e. Forordningen er gjennomført i norsk rett i ekomloven § 4-2 jf. forskriften § 2-1 og regulerer krav til nettnøytralitet.
Av artikkel 4 nummer 1 bokstav d følger det at tilbydere av internettilgangstjenester plikter å gi en klar og forståelig forklaring på hvilken nedlastings- og opplastningshastighet sluttbrukeren som minimum vil få, hva som er normalt tilgjengelig, hva som er maksimum og hva som er annonsert. Dette gjelder for fastnett. For mobilnett skal den estimerte maksimale og annonserte nedlastings- og opplastningshastigheten til internettilgangstjenestene oppgis. Tilbyderne plikter også å opplyse om hvordan betydelige avvik fra annonserte nedlastings- og opplastningshastigheter kan påvirke utøvelsen av sluttbrukernes rettigheter kva gjelder sluttbukernes rett til tilgang og distribusjon av innhold mv.
Tilbyderne plikter også å gi en klar og forståelig forklaring på hvilke rettsmidler som er tilgjengelige for forbrukeren i samsvar med nasjonal lovgivning i tilfelle kontinuerlig eller regelmessig gjentatt avvik mellom den faktiske ytelsen til internettilgangstjenesten, med hensyn til hastighet eller annen kvalitet på tjeneste-parametrene og ytelsen som er angitt.
Det følger av *tredje ledd* at tilbyder skal benytte malen for avtalesammendrag som offentliggjøres på Nasjonal kommunikasjonsmyndighets hjemmeside. Malen er utformet av Kommisjonen i samråd med BEREC for å oppfylle forpliktelsene som følger av annet ledd. Kommisjonen har utformet avtalesammendraget i «Commission Implementing Regulation (EU) 2019/2243 of 17 December 2019». Rettsakten er relevant for innlemming i EØS-avtalen.

Til § 2-5 Spesifisert faktura

Bestemmelsen viderefører delvis gjeldende § 1-9 og gjennomfører ekomdirektivet artikkel 115 nummer 1 og vedlegg VI del A.
Etter *første ledd* følger utgangspunktet om at tilbyder av elektroniske kommunikasjonstjenester har anledning til å sende uspesifisert faktura, jf. ekomloven § 1-5 nummer 4.
Etter *annet ledd* skal tilbyder av internettilgangstjenester og tilbyder av offentlig tilgjengelig nummerbasert person-til-person kommunikasjonstjeneste kostnadsfritt tilby spesifisert faktura dersom sluttbruker ber om det. Spesifikasjonen i fakturaen må være slik at det er mulig for sluttbruker å kontrollere at fakturaen stemmer med faktisk forbruk.
Tredje ledd gjelder samtykke til spesifisert faktura for den som faktisk bruker abonnementet. Sluttbruker vil typisk være den som inngår avtale med tilbyder og som mottar fakturaen. Den kan i flere tilfeller være andre enn sluttbruker som bruker tjenesten som tilbys, for eksempel ved arbeidsforhold. Ved spesifisert faktura gis detaljert informasjon om bruken. Kravet til samtykke er satt for å vareta personvernhensyn og må sees i sammenheng med kravene til samtykke i personvernregelverket. Bestemmelsen kan sees i sammenheng med tilbydes taushetsplikt. Samtykkekravet gjelder ikke hvis bruker under 15 år. Dette samsvarer med at før fylte 15 år er den mindreårige for eksempel gitt samtykkekompetanse til blant annet å melde seg inn eller ut av foreninger eller selv ta avgjørelser som gjelder utdanning. For personer fra 18 år og eldre, som er under vergemål, vil vergemålsvedtaket kunne gi ytterligere regulering av samtykkekompetansen.
Fjerde ledd om at anrop som er kostnadsfrie for anropende sluttbruker, ikke skal angis i anropende sluttbrukers faktura, er ny. Ettersom formålet med spesifisert faktura er at sluttbruker skal kunne foreta kontroll av kostnadene, er det ikke nødvendig å spesifisere slike anrop.
I *femte ledd* videreføres Nasjonal kommunikasjonsmyndighets mulighet til å fastsette nærmere retningslinjer for spesifisering av faktura. Bestemmelsen åpner for at en ved en utvidelse av spesifiseringsplikten, kan tilbyder gis adgang til å ta kostnadsorientert pris for tjenesten.

Til § 2-6 Sperring av utgående anrop og meldinger

Bestemmelsen er i all hovedsak en videreføring av gjeldende ekomforskrift § 5-6. Pliktsubjekt er utvidet og gjelder ikke lenger bare leveringspliktig tilbyder, men alle tilbydere av nummerbaserte person-til-person kommunikasjonstjenester.
Etter bestemmelsens *første ledd* skal tilbyder av nummerbaserte person-til-person kommunikasjonstjenester kostnadsfritt og på anmodning fra sluttbruker

- sperre adgangen til anrop og meldinger til alle andre nummer enn de sluttbruker positivt har angitt at det skal være mulig å anrope eller sende melding til,
- sperre for anrop og meldinger til nummer angitt av sluttbruker, eller
- sperre for adgangen til å gjøre bestemte typer anrop og sende bestemte typer meldinger.

Sperring av bestemte typer anrop og meldinger, kan for eksempel være anrop og meldinger til nummer i internasjonal nummerplan eller MMS-meldinger.
Annet ledd gir sluttbruker en mulighet til å sette en øvre grense for variable kostnader som kan påløpe i hver faktureringsperiode. Når grensen nås, skal tilbyder sperre for videre mulighet til å gjøre anrop eller sende meldinger når slik bruk medfører økte kostnader. Når

øvre grense er nådd, kan sluttbruker likevel samtykke i videre bruk. Det understrekes at i tilfeller der bruker en annen enn sluttbruker som har inngått avtale med tilbyder, er det sluttbruker selv som må samtykke i videre bruk. Bruker kan ikke gi samtykke til videre bruk. I slike tilfeller kan samtykke til videre bruk ikke gis ved at tilbyder for eksempel sender en SMS som eventuelt bekreftes.

Til § 2-7 Fellesfakturert tjeneste

Bestemmelsen viderefører bestemmelsene i ekomforskriften kapittel 5a om fellesfakturerte tjenester, men reglene foreslås utvidet til også å gjelde alle varer og tjenester som faktureres sammen med elektroniske kommunikasjonstjenester. Dette vil gjelde kjøp av varer og tjenester som for eksempel gjøres via mobiltelefonregningen. Slik tredjepartsfakturering er gjerne betaling hvor kjøp i applikasjoner eller på internett betales ved at beløpet legges til mobiltelefonregningen. Dette kan være tjenester som for eksempel busstransport, parkering og kinoforestilling, men også fysiske varer som brus og snack fra automat eller andre varer fra nettbutikk.

Innkreving over telefonregningen for en vare eller tjeneste er en særskilt form for innkreving og forbundet med risiko. Det er brukeren av utstyret, typisk mobiltelefonen, som aktiverer kjøpet og slik inngår avtalen, men det er abonnenten som faktureres. Det gis kreditt for kjøpet, som innkreves ved neste faktura. Det er således et potensiale for overforbruk og etablering av vesentlig kreditt inngått av andre enn den som får faktura. Det foreslås derfor videreført at det kan settes en øvrebeløpsgrense per måned. Nederste beløpsgrense per abonnement er foreslått endret til 500 kr fra 250 kr. Beløpsgrensen har ikke vært oppjustert siden den ble vedtatt i 2008, og en terskel på kr 500 antas å være mer i tråd med tilsvarende beløpsgrenser ellers i samfunnet.

Pliktsubjektet etter bestemmelsen i ekomforskrift vil være tilbyder av offentlig tilgjengelig nummerbasert person-til-person kommunikasjonstjenester. Dette er en videreføring av dagens rettstilstand.

Merk at § 4-9 i ekomloven som pålegger å tilby en mulighet for å stenge for fellesfakturerte tjenester vil gjelde både for tilbydere av internettilgangstjenester og offentlig tilgjengelig nummerbasert person-til-person kommunikasjonstjeneste. De særlige reglene for fellesfakturerte tjenester på forskriftsnivå vil derimot kun gjelde tilbyder av offentlig tilgjengelig nummerbasert person-til-person kommunikasjonstjeneste.

Dette er i tråd med ekomdirektivet artikkel 115 og vedlegg VI del A som kun krever at det skal være mulig å stenge for såkalt tredjepartsfakturering, både for tilbydere av internettilgangstjenester og offentlig tilgjengelig nummerbasert person-til-person kommunikasjonstjeneste. Det oppstilles derfor to nivåer, der hovedregelen om mulighet for stenging gjelder både tilbydere av internettilgangstjenester og offentlig tilgjengelig nummerbasert person-til-person kommunikasjonstjeneste, og videre regulering i forskrift av fellesfakturerte tjenester som kun retter seg mot tilbyder av offentlig tilgjengelig nummerbasert person-til-person kommunikasjonstjeneste.

At særreguleringen av fellesfakturerte tjenester kun gjelder tilbyder av offentlig tilgjengelig nummerbasert person-til-person kommunikasjonstjeneste er også i overensstemmelse med gjeldende rett og i tråd med hvem som er pliktsubjekt etter betalingsdirektivet.

Etter gjeldende § 5a-1 kan tjenesten kun tilbys over særskilte nummerserier fastsatt av myndigheten. Dette foreslås endret til at fellesfakturert tjeneste levert ved utgående anrop fra bruker til nummer fastsatt for talekommunikasjonstjeneste, bare kan tilbys over særskilte

nummerserier fastsatt av myndigheten. Dette gjenspeiler bedre ordningen med bruk av nummer i seriene 820 og 829 for fellesfakturerte tjenester. Videre foreslås at der tilbyder ikke kan tilby sperring for bruk av fellesfakturerte tjenester over en gitt beløpsgrense, skal sluttbruker gjøres oppmerksom på det ved avtaleinngåelsen.
Gjeldende unntak for ikke å gi prisinformasjon om nummeropplysningstjenester før tjenesten leveres foreslås opphevet fordi disse kostnadene er høye, og det bør informeres om dette før tjenesten leveres.
Det foreslås videre presisert at det er tilbyder som skal sikre at tilbyder skal sikre at innholdet som leveres er lovlig.
Departementet foreslår å videreføre gjeldende klageordning for innholdstjeneste som leveres over elektronisk kommunikasjonsnett slik at Brukerklagenemnda fremdeles avgjør slike klager. For andre fellesfakturerte tjenester, foreslår departementet at klageordningen bare skal gjelde selve faktureringen.

Til § 2-8 Plikt til tilbyderportabilitet

Departementet foreslår å avvikle reglene om fast forvalg i ekomforskiften §§3-1 til 3-4. Fast forvalg som løsning er i praksis er foreldet og erstattet med nummerportabilitet. Eventuelle løsninger som fremdeles eksisterer foreslår departementet kan videreføres på privatrettslig grunnlag.
Første ledd, første punktum er en videreføring av ekomforskriften § 3-5 uten at det innebære materielle endringer. Bestemmelsen formuleres som en ren rettighetsbestemmelse og ikke som en definisjonsbestemmelse med rettighetsvirkning.
Første ledd, andre punktum er en gjennomføring av ekomdirektivet artikkel 106 nummer 3. Bestemmelsen medfører at kunder som sier opp en avtale ikke automatisk mister nummeret sitt, og at de fortsatt kan portere til en annen tilbyder i minst en måned etter oppsigelsen. Sluttbruker skal med andre ord ha rett til å utportere et nummer til en annen tilbyder i minst en måned etter den dagen da avtalen opphørte. Ved dette styrkes sluttbrukers rett til å kunne beholde et nummer sammenlignet med gjeldende ordning, der rett til utportering forutsetter at det foreligger et aktivt abonnement hos avgivende tilbyder. Retten til slik utportering gjelder både ved oppsigelse fra sluttbruker og fra tilbyder. Tilbyder kan ikke nekte utportering med henvisning til et påstått betalingsmislighold fra sluttbruker. Sluttbruker si fra seg denne retten. For at sluttbruker skal miste retten etter første ledd kan et slikt avkall tidligst gis i tilknytning til opphøret av avtalen.
Annet ledd fastsetter at avgivende tilbyder har plikt til å gi slipp på nummeret. Avgivende tilbyder kan ikke holde nummeret i «pant» for ubetalte regninger. Eventuelle tvister mellom sluttbruker og avgivende må løses innen privatrettslige rammer uavhengig av porteringsprosessen, men nummeret må porteres over.
Tredje ledd gir unntak for enkelte nummerserier hvor enkeltnummer ikke skal kunne flyttes ut av serien til annen tilbyder. Tilbyderbytte for disse seriene, vil eventuelt skje ved flytting av hele nummerserier.

Til § 2-9 Gjennomføring av tilbyderportabilitet

Forslag til bestemmelse viderefører og skjerper hovedinnholdet i gjeldende forskrift § 3-6, og gjennomfører ekomdirektivet artikkel 106 nummer 5.
Første ledd viderefører tilbyders plikt etter gjeldende rett til å innhente skriftlig fullmakt fra sluttbruker før portering, jf. § 1-5.

Annet ledd synliggjør at porteringen skal bygge på en avtale mellom tilbyder og sluttbruker, og at avtalen skal inneholde en dato og tidspunkt for portering. Porteringsprosessen skal være mottaker-drevet og en en-stegs prosess. Det vil si at sluttbruker kun avtaler med mottakende tilbyder, og denne tar seg av hele kontakten med avgivende tilbyder.
Kravet til «kortest mulig tid» *i tredje ledd* må tolkes i lys av den teknologisk utviklingen. Særlig vil muligheter for å fjernstyre bytte av tilbydertilhørighet kunne medføre at portering kan skje på svært kort tid, det vil si i løpet av minutter fremfor dager. Tredje ledd fastslår i likhet med direktivet at portering med aktivering skal skje på kortest mulig tid på den dato som er uttrykkelig avtalt med sluttbruker. Det er altså avtalen mellom mottakende tilbyder og sluttbruker som er utgangspunktet. Departementet foreslår å legge den norske gjennomføringen tett opp til direktivet, og at gjeldende rett med krav om fem virkedagers ramme for prosessen og en-dags responstid for avgivende utgår. Bestemmelsene innebærer således en dreining til fordel for mottakende tilbyder, og hvor fort denne klarer å gjennomføre en sikker portering.
Fjerde ledd er en videreføring av § 3-6, annet ledd, tredje setning. Det er mottakende tilbyder og sluttbruker som inngår avtalen. Ved å legge vekt på avtalen mellom sluttbruker og mottakende, reduseres muligheten for at avgivende tilbyder kan trekke ut prosessen. Bestemmelsen kan ses i sammenheng med det såkalte winback-forbudet i sjette ledd, som også er ment å effektivisere porteringsprosessen og hindre at avgivende bruker porteringsinformasjon til å vinne tilbake kunder.
Dersom fjernstyring av porteringsporsesser blir mer aktuelt, vil mottakende tilbyder kunne bestille portering med raskere effektuering. De administrative rutingen for portering må da endres for å kunne gi minimale tidsintervaller for bestilling, aksept og aktivering.
Femte ledd gjennomfører artikkel 106, nummer 5 om at avgivende tilbyder skal opprettholde tjenester frem til den nye tjenesten er aktivert. Dette er for å hindre tjenestebortfall.
Sjette ledd er en videreføring av «winback-forbudet» i gjeldende forskrift § 3-6. Forbudet innebærer at en tilbyder som mottar porteringsbestilling ikke kan foreta rettet markedsføring av sine tjenester overfor den aktuelle sluttbrukeren som porteringsbestillingen gjelder i en nærmere bestemt periode (forbudsperioden). De overordnede formålet med forbudet mot winback er å styrke konkurransen i markedet og rendyrke porteringsprosessene ved å redusere antallet avbrutte porteringer. Begrepet «markedsføring» er ikke definert i forskriften, men må forstås ut ifra hvordan begrepet er benyttet på andre rettsområder, herunder i markedsføringsloven. Alle former for kommunikasjon som er egnet til å fremme salget av avgivende tilbyders tjenester er å anse som «markedsføring».
Som eksempel på informasjon som ikke er nøytral i sjette ledd er kommunikasjon som innebærer positiv omtale av egen virksomhet eller produkter og tjenester eller negativ omtale av mottakende tilbyder, dennes produkter og tjenester. Kommunikasjon som innebærer omtale av potensielle og faktiske negative virkninger av tilbyderbyttet, herunder kommunikasjon som kan gi inntrykk av at tilbyderbyttet er komplisert og/eller byrdefullt, er heller ikke nøytral informasjon.
Det foreslås en mindre endring ved at i formuleringen «Avgivende tilbyder skal ikke bruke porteringsinformasjon i egen markedsføring rettet mot sluttbruker som porteres». Her foreslås «som porteres» opphevet fordi det er nummeret og ikke sluttbruker som porteres.

Til § 2-10 Ansvar for kostnader ved tilbyderportabilitet

Forslag til bestemmelse viderefører delvis gjeldende forskrift § 3-7. I tillegg foreslås å forskriftsfeste etablert praksis ved bruken av bestemmelsen slik at det fremkommer at avgivende tilbyder ikke kan kreve mottakende tilbyder for kostnader knyttet til porteringen. Portering er ofte et nullsumspill hvor tilbyder både mottar og avgir kunder. I henhold til forslaget skal det ikke være noen avregning mellom tilbyderne i forbindelse med portering. Forslaget går noe lenger enn ekomdirektivet artikkel 106 nummer 4 som fastsetter at avregningen mellom tilbydere skal være kostnadsbasert.
Endringen vil dessuten være til fordel for nyetablerte tilbydere fordi en avgift til avgivende kan medføre en etableringsbarriere siden en ny aktør i oppstartsperioden ofte vil ha flere inn-porteringer enn ut-porteringer.

Til § 2-11 Kompensasjon til sluttbruker

Forslag til bestemmelse gjennomfører ekomdirektivet artikkel 106 nummer 8. Overføringen av kompensasjonen skal skje på en enkel måte og innen rimelig tid.
Plikten til kompensasjon inntrer ved forsinkelse for aktivering av tjeneste, portering eller nedetid som overstiger én virkedag, eller dersom tilbyder ikke oppfyller service- eller installasjonsavtaler.
Dersom avgivende tilbyder må fortsette å tilby en tjeneste på grunn av forhold på mottakende tilbyder side, kan kompensasjonen også bestå i automatisk redusert vederlag fra sluttbruker til ny/mottakende tilbyder.
Størrelsen på kompensasjonen må vurderes konkret.
Sluttbruker skal få informasjon om kompensasjonsordningen, i det minste ved avtaleinngåelse.

Til § 2-12 Internasjonal gjesting i mobilnett

Bestemmelsen viderefører gjeldende ekomforskrift § 2-7 og gjennomfører EUs regelverk om internasjonal gjesting. Regelverket består av flere forordninger som regulerer ulike forhold knyttet til internasjonal gjesting. Regelverket innfører begrepet "roame like at home" som innebærer at norske mobilbrukere ikke skal betale mer for samtaler, SMS eller datatrafikk på reise i andre EØS-land enn hjemme. Dette gjelder innenfor et normalt forbruk. For å hindre unormalt høyt forbruk eller misbruk av et abonnement, kan tilbyder stille ett eller flere krav overfor sine kunder og eventuelt kreve prispåslag dersom kravene ikke oppfylles. Tilbyder skal informere kundene dersom slike krav tas i bruk og skal også informere Nasjonal kommunikasjonsmyndighet om dette.
Regelverket fastsetter maksimale grossistpriser for tale, SMS og data. Prisene gjelder både mellom netteiere i ulike land og for tilgang til gjestingstjenester for tjenesteleverandører som kjøper tilgang til mobilnett.
I annet ledd foreslås foreløpig inntatt et nytt ledd som er ment å regulere internasjonal gjesting mellom Storbritannia og Norge. I handelsavtalen med Storbritannia tas det sikte på å få i stand en regulering av priser for internasjonal gjesting i mobilnett på grossistnivå. Ved reise i Storbritannia er det ønskelig at norske sluttbrukere skal nyte godt av samme priser som i Norge forutsatt et normalt forbruk. Grossistprisreguleringen i avtalen vil eventuelt gjelde for norske tilbydere, også dersom disse tilbyderne videreselger tilgang til internasjonal gjesting. Handelsavtalen er ikke vedtatt, og forslaget kan eventuelt falle bort.

Til § 2-13 Prissammenlikningstjeneste

Bestemmelsen er ny og gjennomfører ekomdirektivet artikkel 103 nummer 2 og 3.
Etter *første ledd* skal myndigheten etter anmodning fra aktør godkjenne prissammenlikningstjeneste for internettilgangstjenester og offentlig tilgjengelige nummerbaserte person-til-person kommunikasjonstjenester så lenge nærmere bestemte krav i nummer 1 til 10 er oppfylt.
Nummer 1 krever at prissammenlikningstjenesten er gratis å bruke for sluttbrukere.
Nummer 2 viser til at tjenesten skal gi sluttbruker en effektiv mulighet til å sammenlikne ulike leverandørers priser. I tråd med ekomdirektivet artikkel 103 nummer 3 bokstav h) er dette begrenset til tilbud som er tilgjengelig for forbrukere.
Nummer 3 viser til at tjenesten skal gi sluttbruker en effektiv mulighet til å sammenlikne tjenestekvaliteten tilgjengelig hos de ulike leverandørene. I tråd med ekomdirektivet artikkel 103 nummer 3 bokstav h) er dette begrenset til tilbud som er tilgjengelig for forbrukere.
Nummer 4 krever at tjenesten er uavhengig fra tilbyder som tilbyr tjenester som omfattes av sammenlikningstjenesten. Dette innebærer at en tilbyder av internettilgangstjeneste ikke kan drive eller ha tilknytning til prissammenlikningstjeneste for internettilgangstjenester og tilsvarende for offentlig tilgjengelig nummerbasert person-til-person kommunikasjonstjenester. Dette skal bidra til å sikre at tilbydere behandles likt i søkeresultatene.
Nummer 5 krever videre at det skal være åpent og tydelig for sluttbrukeren hvem som eier og driver prissammenlikningstjenesten.
Nummer 6 viser til at tjenesten skal fremvise opplysninger av god kvalitet. Opplysningene skal være nøyaktige og oppdateres ofte. Det skal også være klart for sluttbruker hvilke kriterier og metoder tilbyderen bruker ved fremvisning av informasjonen. Det skal også fremgå når opplysningene sist ble oppdatert.
Nummer 7 krever at tjenesten bruker et forståelig språk for sluttbrukere.
Nummer 8 krever at tjenesten skal være tilgjengelig for og kunne inkludere alle tilbydere av enten internettilgangstjenester eller offentlig tilgjengelige person-til-person kommunikasjonstjenester.
Nummer 9 krever videre at tjenesten skal fremvise et rikt omfang av tilbud, som dekker en betydelig del av markedet. Dersom tjenesten ikke inkluderer alle aktører og tjenester på markedet skal dette fremkomme tydelig for sluttbruker før resultatene vises.
Nummer 10 krever at tjenesten skal kunne gi sluttbruker mulighet til å filtrere geografisk for tilbud av internettilgangstjenester i fastnett. Dette er i tråd med gjeldende krav til prissammenlikningstjenestene og skal sikre at sluttbruker får relevant informasjon i form av oversikt over tilgjengelige produkter der de bor.
Nummer 11 krever at tjenesten skal informere om og ha en effektiv rutine for rapportering av uriktige opplysninger i tjenesten.
Annet ledd gir prissammenlikningstjenester som er godkjent av myndigheten rett til å bruke et godkjentmerke utstedt av myndigheten. Et slikt godkjentmerke kan hjelpe sluttbrukere å finne gode sammenlikningsverktøy og vil gi tilbyderen legitimitet. Dette innebærer at myndigheten kan kontrollere, foreta nye vurderinger og eventuelt trekke tilbake godkjentmerke på et senere tidspunkt dersom dette blir nødvendig.
Tredje ledd gir tredjeparter som har planer om å tilby prissammenlikningstjeneste rett til å få tilgang til offentliggjort opplysninger fra tilbyder av internettilgangstjeneste eller offentlig tilgjengelig nummerbasert person-til-person kommunikasjonstjeneste i åpne dataformater.

Slik informasjonsinnhenting skal være kostnadsfritt for tilbyder av prissammenlikningstjeneste.

Til § 2-14 Hemmelig nummer

Forslag til bestemmelse viderefører gjeldende § 6-6 i sin helhet, med unntak at det presiseres at det er tilbydere av nummerbasert person-til-person kommunikasjonstjenester som har plikter etter bestemmelsen, jf. forslag til ny definisjon av elektronisk kommunikasjonstjeneste i § 1-5 nummer 4.

Tjenesten var i opprinnelig ment å være et tilbud til personer med et behov for anonymitet, for eksempel personer som har en utsatt offentlig posisjon eller som av andre grunner hadde en utsatt posisjon. Retten til å benytte hemmelig nummer er imidlertid ikke begrenset til dette, og det settes ingen krav til begrunnelse for å få tilgang til hemmelig telefonnummer.

Innholdet i tjenesten hemmelig nummer fremgår av *først ledd*. Tjenesten består av visse obligatoriske elementer. Dette er full reservasjon mot utlevering til allmenheten, skult nummervisning, informasjon om nummerets status som hemmelig til mottakende tilbyder ved tilbyderportering, og særskilte krav til informasjon og entydig identifisering.

Av annet ledd fremgår det at tjenesten også kan inneholde andre elementer, som for eksempel skjult nummer i den grad det ellers ville blitt vist på faktura, avgrensing av tilgang til abonnementsinformasjon i tilbyders organisasjon og annet.

Tjenesten skult nummervisning inngår som nevnt ovenfor og innebærer at anropende nummer ikke vises hos mottaker ved anrop. Dersom en sluttbruker har anmodet tilbyder om skjult nummervisning skal funksjonen aktiveres av tilbyder. Tjenesten skal ikke være avhengig av at sluttbruker selv må velge slike innstillinger. Dersom sluttbruker velger skjult nummervisning, så vil dette gjelde alle anrop, men unntak av anrop til nødetater.

Tjenesten reservasjon mot helt eller delvis utlevering av nummer, navn eller adresse til allmennheten inngår som nevnt ovenfor også som i hemmelig nummer. Hemmelige nummer skal ikke opplyses på forespørsel, eller finnes tilgjengelig i offentlig opplysningstjenester. Politiet, påtalemyndighet og andre myndigheter med særskilt hjemmel i lov, kan få utlevert hemmelig nummer.

Det foreslås i *tredje ledd* å videreføre kravet om at sluttbruker med hemmelig telefonnummer skal identifisere seg på lik linje som ved etablering av nytt abonnement, dersom sluttbruker ønsker å gjøre endringer i egne abonnementsopplysninger hos tilbyder. Formålet med dette er å hindre at uvedkommende initierer en endring av tjenesten og dermed urettmessig får tilgang til informasjonen.

I *fjerde ledd* foreslår departementet å videreføre krav til at avgivende tilbyder ved portering av hemmelig telefonnummer skal informere mottakende tilbyder om nummerets status som hemmelig. Denne informasjonen er ment å begrense risikoen for at mottakende tilbyder feilaktig offentliggjør informasjon om nummer, navn og adresse etter portering. Avgivende tilbyder som ikke oppfyller informasjonsplikten, og mottakende tilbyder som feilaktig gir ut slik informasjon på tross av at avgivende tilbyder har informert om nummerets status som hemmelig, kan bli ilagt overtredelsesgebyr. Dersom tilbyder ikke overholder pliktene som gjelder tjenesten hemmelig nummer ved portering, kan dette utgjøre misbruk av portering, kan det også føre til pålegg om å yte kompensasjon til sluttbruker.

I henhold til tilbydernes praksis kan ikke sluttbruker avbestille hemmelig telefonnummer i forbindelse med en pågående porteringsprosess. Avbestilling må gjøres enten før eller etter

at portering er gjennomført. Endring, herunder oppsigelse av hemmelig telefonnummer krever identifisering tilsvarende etablering av nytt abonnement.
I *femte ledd* foreslås det videreført at tilbyder ved etablering, endring, oppsigelse og portering skal informere om tjenestens innhold, pris for tjenesten, samt annen relevant informasjon. Tilbyders plikt til å gi slik informasjon skal bidra til at sluttbruker til enhver tid har oversikt over hav som omfattes av tjenestens innhold.

Til § 2-15 Reservasjonsrett knyttet til nummer, navn og adresse

Forslag til bestemmelse gjelder sluttbruker rett til å reservere seg helt eller delvis mot at informasjon om sluttbruker fremgår av nummeropplysningstjenester eller på annet vis utleveres til allmennheten. Bestemmelsen viderefører gjeldende forskrift § 6-2 tredje ledd, og gjennomfører kommunikasjonsverndirektivet (2002/58/EC) artikkel 12 nummer 2.
I *annet ledd* presiseres at det er tilbydere av nummerbasert person-til-person kommunikasjonstjenester som har plikter etter bestemmelsen, jf. forslag til § 1-5.
Rett til å reservere seg etter denne bestemmelsen ikke er det samme som hemmelig nummer etter § 2-15. Hemmelig nummer har et høyere beskyttelsesnivå.

Til § 2-16 Likeverdig tilgang for sluttbrukere med nedsatt funksjonsevne

Bestemmelsen er ny og presiserer omfanget av pliktene som tilbydere av offentlig elektronisk kommunikasjonstjeneste er pålagt i ekomloven § 4-16. Formålet med bestemmelsen er å definere hvilke tilbydere, tjenester, utstyr og informasjon som omfattes av plikten.
I *første ledd* presiseres det at pliktene til å sikre likeverdig tilbud av ekomtjenester til sluttbrukere med nedsatt funksjonsevne, gjelder internettilgangstjenester og talekommunikasjonstjenester. Disse tjenestene er nærmere definert i ekomloven § 1-5. Talekommunikasjonstjenester omfatter i denne sammenheng også kommunikasjonsmidler som er særlig beregnet på sluttbrukere med nedsatt funksjonsevne som bruker tekstformidlingstjenester. Tilbydere skal sikre at sluttbrukere som er døve eller har nedsatt hørsel eller taleforstyrrelser har kontinuerlig tilgang til en teksttolkformidlingstjeneste. Bestemmelsen presiserer videre at det er tilbyderne selv som plikter å finansiere tilbudet av tjenestene på en måte som sikrer likeverdig tilgang for sluttbrukere med nedsatt funksjonsevne. Tilbydere kan velge å utvikle tjenesten selv eller gjennom et samarbeid med en leverandør. Tilbydere kan også velge å samarbeide seg imellom om hvordan utforme tjenesten.
Første ledd fastsetter at talekommunikasjonstjenester skal kunne leveres sammen med sanntidstekst. Dette innebærer i praksis at alle, inkludert sluttbrukere med nedsatt funksjonsevne, vil kunne benytte seg av kommunikasjonstjenester. Tjenesten må kunne utføre tolkning fra tekst til tale og omvendt i sanntid slik at døve, hørselshemmede og personer med taleforstyrrelser får likeverdig tilgang til talekommunikasjonstjenester. Tilbydere kan velge å utvikle tjenesten selv eller gjennom et samarbeid med en leverandør. Tilbydere kan også velge å samarbeide seg imellom om hvordan tjenesten utformes.
Etter *annet ledd* følger det at når video tilbys sammen med en talekommunikasjonsløsning, skal tjenesten være en totalkonversasjonsløsning. Definisjonen av totalkonversasjon er hentet fra ekomdirektivet artikkel 2 nummer 35.
Tredje ledd presiserer at tilbyder selv skal finansiere tjenesten. I gjeldende rett er tjenester til brukere med særlige behov en del av de leveringspliktige tjenestene, og inkludert finansieringsmuligheten for leveringspliktige tjenester. Det er de ikke lengre.

Det følger av fjerde ledd at tilbydere må sikre at informasjon om tjenester, avtalevilkår og utstyr må formidles på en universell utformet måte som gjør den tilgjengelig for sluttbrukere med nedsatt funksjonsevne.

Til § 2-17 Unntak for mikroforetak som tilbyder

På tilsvarende måte som i forslag til ny ekomlov § 4-19 presiseres at kravene i §§ 2-2 til 2-15 ikke gjelder for mikroforetak som kun tilbyr nummeruavhengige person-til-person kommunikasjonstjenester.

Til kapittel 3 Tilgang

Til § 3-1 Funksjonelt skille

Forslag til bestemmelse viderefører gjeldende ekomforskrift § 2-6a i sin helhet, og gjennomfører ekomdirektivet artikkel 77 nummer 3. Vilkårene for å pålegge en tilbyder med sterk markedsstilling funksjonelt skille fremgår av forslag til ny ekomlov § 7-13.
Forslag til § 3-1 angir hvilke krav et pålegg om funksjonelt skille etter ekomloven § 7-13 som et minimum skal inneholde.
Etter nummer 1 er det krav om at det skal gis en nøyaktig beskrivelse av skillets art og grad og at det gis en særlig angivelse av den rettslige statusen for den separate forretningsenheten.
Etter nummer 2 er det krav om at myndigheten skal identifisere eiendelene til den atskilte forretningsenheten samt produktene eller tjenestene som denne enheten skal tilby.
Etter nummer 3 er det krav om at pålegg om funksjonelt skille skal inneholde organisatoriske tiltak som skal sikre uavhengigheten mellom de atskilte forretningsenhetene, herunder personalet som er ansatt i den adskilte enheten, og den korresponderende insentivstrukturen. Etter nummer 4 stilles det krav til at det gis regler som sikrer at forpliktelsene oppfylles og overholdes.
Etter nummer 5 er det videre krav til at det skal gis regler som sikrer åpenhet og transparens om prosedyrer knyttet til driften, særlig overfor andre berørte interessenter og parter.
Etter nummer 6 stilles det krav til et system for tilsyn for å sikre overholdelse av forpliktelsene, herunder offentliggjøring av en årlig rapport.
Bestemmelsen angir hvilke krav et pålegg om funksjonelt skille som et minimum skal inneholde, og gir således ingen uttømmende angivelse av plikter som kan pålegges i tilknytning til funksjonelt skille.
Pålegg av funksjonelt skille skal følge prosedyrene i ekomloven §§ 14-2 og 14-3.

Til § 3-2 Vurdering av tilgang til infrastruktur for mobile tjenester

Forslag til bestemmelse er ny og gjennomfører ekomdirektivet artikkel 61 nummer 4 annet ledd. Forslaget til bestemmelse gir en liste over momenter som myndigheten skal ta i betraktning før forpliktelser om felles utnyttelse av passiv infrastruktur eller tilgang til lokale nettgjestingstjenester pålegges.
Myndigheten skal blant annet vurdere om slike pålegg vil være nødvendig for å tette hull i dekningen, for eksempel langs hovedferdselsårer (vei og jernbane) og i bestemte geografiske områder. Myndigheten skal videre ta hensyn til at felles bruk og andre forhold i tilknytning til at deling av infrastruktur skal være teknisk mulig å gjennomføre, til konkurransen i markedet og til teknologisk innovasjon. Myndigheten skal også vurdere både

investeringsincentiv fremover i tid og investeringsrisiko for tilbyder som blir pålagt tilgangsplikt. Det innebærer at myndigheten må vurdere hvilken virkning pålegg etter bestemmelsen vil kunne ha for investeringer som allerede er gjort og villigheten til å gjøre nye investeringer.
Et pålegg om å gi tilgang til infrastruktur for mobile tjenester skal i størst mulig grad innrettes mot å fremme bærekraftig konkurranse, effektive investeringer og innovasjon samt å maksimere nytten for sluttbrukerne.

Til § 3-3 Gjennomføring av forordning om BEREC

Forslag til bestemmelse er ny og gjennomfører europaparlaments- og rådsforordning (EU) 2018/1971 om opprettelsen av Sammenslutningen av europeiske reguleringsmyndigheter for elektronisk kommunikasjon (BEREC) og Byrået for støtte til BEREC (BEREC-kontoret). BEREC-forordningen inneholder videre en maksimalprisregulering av internasjonale nummerbaserte kommunikasjonstjenester og er ment å beskytte brukerne mot urimelig høye priser for internasjonale anrop og SMS. Reguleringen omfatter priser for internasjonale nummerbaserte kommunikasjonstjenester som starter i Norge og avsluttes i utlandet. Maksimalprisreguleringen er gjennomført i gjeldende ekomlov og forskrift, henholdsvis i § 4-15 og § 2-8, og trådte kraft 1. juli 2019. Ved den foreslåtte gjennomføringen av BEREC-forordningen i forskrift er det ikke lenger behov for gjeldende § 2-8 i ekomforskriften og bestemmelsen foreslås dermed opphevet.
Bestemmelsen forutsetter at BEREC-forordningen tas inn i EØS-avtalen.

Til kapittel 4 tilgang til radio og fjernsyn

Til § 4-1 Krav til tilbyder av adgangskontrolltjenester

Bestemmelsen viderefører gjeldende ekomforskrift § 4-1 med unntak av at henvisningene til lovbestemmelsene i ekomloven er oppdatert.
Innholdsleverandører skal tilbys tilgangstjenester uavhengig av om tilbyder av adgangskontrolltjeneste har sterk markedsstilling. Slik tilgang skal tilbys på objektive, rimelige og ikke-diskriminerende vilkår, jf. ekomloven § 8-1, første ledd. Kravet om regnskapsmessig skille skal synliggjøre eventuell kryss-subsidiering slik at myndighetene bl.a. blir i stand til å undersøke om tilbyder av adgangskontrolltjeneste etterkommer krav til ikke-diskriminering.
Adgangskontroll er en funksjon der åpen tilgang til en beskyttet radio- eller fjernsynstjeneste er betinget av abonnement eller annen form for individuell forhåndsavtale. Adgangskontrollsystem ivaretar adgangskontroll for digital radio og fjernsyn i et elektronisk kommunikasjonsnett. Brukerutstyr for digital radio og fjernsyn er utstyr som tilkobles eller integreres i radio- eller fjernsynsapparater for å få tilgang til digitale radio- og fjernsynstjenester.
Annet ledd setter krav til tilbydere av andre tilgangsbegrensende funksjoner. Dersom andre funksjoner enn adgangskontroll reduserer sluttbrukers tilgang til digitale radio- og fjernsynstjenester, kan det gis pålegg om at tilbud som omfatter slike funksjoner skal gis på objektive, rimelige og ikke-diskriminerende vilkår. API (Application Programming Interface) er et programvaregrensesnitt, et kommunikasjonsprogram mellom nytteprogram og operativsystem som benyttes av innholds- og tjenestetilbydere for å kunne levere digitale radio- og fjernsynstjenester.

Dersom markedsundersøkelser viser at tilstrekkelig interoperabilitet og valgfrihet ikke oppnås, kan myndighetene innenfor rammene av EØS-avtalen pålegge bruk av åpent programvaregrensesnitt i samsvar med relevante standarder eller spesifikasjoner.

Til § 4-2 Krav til innehaver av immaterielle rettigheter til adgangskontrollprodukter og adgangskontrolltjenester

Bestemmelsen viderefører gjeldende ekomforskrift § 4-2, som hovedsak er en videreføring av krav fastsatt i lov 25. juni 1999 nr. 50 om standarder ved overføring av fjernsynssignaler

Til § 4-3 om krav til felles krypteringsalgoritme og mottak av ukrypterte signaler

Bestemmelsen setter krav til hvordan forbrukerutstyr som er beregnet på mottak av digitale fjernsynssignaler, via bakkenettet eller fra kabel eller satellitt, som selges eller leies eller på annen måte gjøres tilgjengelig, og som kan dekryptere digitale fjernsynssignaler skal kunne dekryptere og vise innholdet i slike signaler. Kravet skal sikre at utstyr, for eksempel fjernsynsapparater, dekodere og bilradiomottakere som tilbys til forbrukere er teknisk innrettet slik at det kan mottas digitale fjernsynssendinger og radiosendinger og dermed sikre at forbrukeren kan nyttiggjøre seg utstyret.

Til § 4-4 om krav til samvirkningsevne for digitale fjernsynsapparater og bilradiomottakere

Bestemmelsens *første ledd* setter krav til digitale fjernsynsapparater som markedsføres for salg eller utleie slik at det kan overføres digitale fjernsynssignaler.
Bestemmelsens *annet ledd* setter krav til at bilradiomottakere som er integrert i nye kjøretøy gruppe M skal ha mottaker som kan motta og gjengi minst radiotjenester som tilbys via digitalt bakkenett. Dette innebærer at bilradiomottakerne på det norske markedet skal kunne anvendes til å ta imot radiosendinger som sendes på DAB+. For hvilke kjøretøy som faller inn under gruppe M vises det til kjøretøyforskriften.
Bilradiomottakere som er i samsvar med harmoniserte standarder eller deler av slike som det er offentliggjort henvisninger til i EØS-tillegget til Den europeiske unions tidende, skal anses å oppfylle kravet som omfattes av disse standardene eller deler av dem.

Til kapittel 5 Leveringsplikt

Til § 5-1 Tilgang til offentlig telefontjeneste og bredbånd

Deler av bestemmelsen ble hørt 3.9.19, og er ikke gjenstand for høring i denne omgang. Det kan være aktuelt å videreføre annet ledd i gjeldende § 5-1 uten endringer i ny forskrift.

Til § 5-2 Beregning av kostnader ved leveringspliktige tjenester

Forskriftsbestemmelsen er en videreføring av gjeldende forskriftsbestemmelse § 5-7, og gjennomfører ekomdirektivet artikkel 89, jf. vedlegg VII del A.
Det følger av ekomloven § 5-2 at tilbyder etter § 5-1 som påføres en urimelig byrde ved å tilby leveringspliktig tjeneste kan ha krav på kostnadsdekning, på nærmere vilkår. Tilbyder må fremlegge en beregning som viser nettokostnadene knyttet til de leveringspliktige tjenestene. Tilbyder skal dokumentere at kostnadene utgjør en urimelig byrde. Det er ikke enhver byrde som skal kompenseres, kun urimelige byrder. Den finansielle byrden må i

tillegg være av en slik størrelse at ikke kostnadene ved å sette opp en finansieringsordning gjør finansieringsordningen uhensiktsmessig.
Det er videre kun nettokostnadene som kan dekkes av en eventuell finansieringsordning. Nettokostnadene beregnes som forskjellen mellom de nettokostnader et foretak har dersom det har plikt til å tilby leveringspliktige tjenester, og de nettokostnader foretaket ville ha hatt dersom det ikke hadde hatt denne plikten. Leveringspliktige tjenester skal tilbys på en kostnadseffektiv måte. Det skal vektlegges hvilke kostnader som et foretak ville ha valgt å unngå dersom det ikke hadde hatt plikt til å tilby leveringspliktige tjenester. Ved beregning av nettokostnaden skal det vurderes hvilke fordeler tilbyderen av leveringspliktige tjenester har. Dette gjelder både immaterielle og indirekte fordeler, for eksempel mulige markedsfordeler. Kostnadene skal beregnes særskilt for hver leveringspliktig tjeneste.
Det følger av *annet ledd* at Nasjonal kommunikasjonsmyndighet avgjør hva som skal regnes som nettokostnader ved levering, og om dette utgjør en urimelig byrde. Beregningen skal bygge på kostnader for
i) elementer av de aktuelle tjenestene som bare kan tilbys med tap eller på kostnadsvilkår som ikke er i samsvar med alminnelige forretningsstandarder.
Denne kategorien kan omfatte tjenester som tilgang til nødmeldingstjenester, visse offentlige betalingstelefoner, visse tjenester eller utstyr til sluttbrukere med nedsatt funksjonsevne osv.
ii) visse sluttbrukere eller grupper av sluttbrukere som bare kan betjenes med tap eller på kostnadsvilkår som ikke er i samsvar med alminnelige forretningsstandarder. Det skal i beregningen tas hensyn til kostnadene ved å tilby bestemte nett og tjenester, inntektene og medlemsstatens eventuelle pålagte geografisk bestemte gjennomsnittstakster.
Denne kategorien omfatter de sluttbrukerne eller gruppene av sluttbrukere som ikke ville ha blitt betjent av en tilbyder som driver forretningsmessig uten plikt til å tilby leveringspliktige tjenester.
Nettokostnaden for bestemte deler av plikten til å tilby leveringspliktige tjenester beregnes for seg for å unngå at eventuelle direkte eller indirekte fordeler eller kostnader beregnes to ganger. Den samlede nettokostnaden for et foretaks plikt til å tilby leveringspliktige tjenester beregnes som summen av nettokostnadene for hver enkelt del av plikten til å tilby leveringspliktige tjenester. Det skal også tas hensyn til eventuelle immaterielle fordeler.
Nasjonal kommunikasjonsmyndighet har ansvaret for å kontrollere beregningen av nettokostnadene, og skal godkjenne regnskapet. Alternativt kan Nasjonal kommunikasjonsmyndighet velge å fremlegge regnskapet til godkjenning av en uavhengig instans utpekt av Nasjonal kommunikasjonsmyndighet. Beregningen av kostnader skal være offentlig.

Til § 5-3 Finansiering av leveringspliktig tjenester

Forskriftsbestemmelsen er en videreføring av gjeldende ekomforskrift § 5-8, og gjennomfører ekomdirektivet artikkel 90, jf. vedlegg VII del B.
Det følger av ekomloven § 5-2 at når tilbyder etter § 5-1 påføres en urimelig byrde ved å tilby leveringspliktig tjeneste kan tilbyderen anmode om å få nettokostnadene ved leveringsplikten dekket.
Dekning eller finansiering som kompenserer for urimelige byrder ved levering av leveringspliktige tjenester innebærer finansielle overføringer, og skal foregår på en objektiv måte som sikrer innsyn, som ikke innebærer forskjellsbehandling og som er rimelig. Det

betyr at overføringene skal foretas på en måte som fører til minst mulig vridning av konkurransen og av brukernes etterspørsel.
Nasjonal kommunikasjonsmyndighet kan pålegge tilbyder å bidra til å finansiere leveringspliktige tjenester. Fordelingsordning som kan være et fond skal anvende en metode som er åpen og nøytral for å samle inn bidrag, slik at faren for dobbel innkreving av bidrag på foretakets innsats og resultat unngås. Nasjonal kommunikasjonsmyndighet kan bestemme at det ikke skal kreves bidrag fra tilbyder med liten markedsandel, tilbyder som har tilbudt tjenester i kort tid, eller som har nasjonal omsetning under en grense fastsatt av myndigheten.
Departementet avgjør hvem som skal forvalte finansieringsordningen.
Finansieringsordningen kan forvaltes av Nasjonal kommunikasjonsmyndighet, eller av en ekstern uavhengig forvalter. Organet skal være ansvarlig for å samle inn bidrag fra foretak som vurderes som pliktige til å bidra til nettokostnaden for plikten til å tilby leveringspliktige tjenester i medlemsstaten. Dette organet skal også overvåke overføringen av beløp eller administrative utbetalinger til foretak som har krav på å motta betaling fra finansieringsordningen.
Eventuelle utgifter i forbindelse med deling av kostnader ved leveringspliktige tjenester skal skilles ut fra de øvrige utgifter og anføres særskilt for den enkelte tilbyder. Slike utgifter kan bare pålegges tilbydere som tilbyr tjenester det er innført en finansieringsordning for.

Til § 5-4 Rapportering

Forskriftsbestemmelsen er en videreføring av gjeldende ekomforskrift § 5-9, og medfører at Nasjonal kommunikasjonsmyndighet kan kreve at leveringspliktig tilbyder skal gjennomføre rapporteringer og herunder fremskaffe nødvendige opplysninger og dokumentasjon om den leveringspliktige tjenesten. Formålet med rapporteringsplikten er å gjøre det mulig for myndigheten å vurdere eventuelt nærmere krav til innhold i og utforming av leveringspliktig tjeneste.

Til § 5-5 Begrensing av koblingssalg

Forskriftsbestemmelsen er en videreføring av gjeldende ekomforskrift § 5-10 og gjennomfører ekomdirektivet artikkel 88.

Til kapittel 6 Frekvenser

Til § 6-1 Utforming av småcellebasestasjoner

I bestemmelsen foreslås Kommisjonens gjennomføringsforordningen (EU) 2020/1070 fra 20. juli 2020, i tråd med ekomdirektivet artikkel 57 nummer 2, som angir nærmere karakteristikker og fysiske og tekniske egenskaper for såkalte småcellebasestasjoner, dvs. trådløse aksesspunkt med begrenset rekkevidde, tatt inn i ekomforskriften. Ekomdirektivet kapittel IV (artikkel 56 til 58) omhandler innføring og bruk av trådløst nettverksutstyr. Artikkel 57 omhandler etablering og drift trådløse aksesspunkt med kort eller begrenset rekkevidde. Artikkel 57 nummer 2 bestemmer at kommisjonen skal angi de fysiske og tekniske egenskapene, herunder størrelse og effekt, for slike aksesspunkter.
Bestemmelsen i foreslår at denne forordningen skal gjelde som norsk forskrift med eventuelle tilpasninger. Dette forutsetter at forordningen tas inn i EØS-avtalen.

I henhold til ekomdirektivet er det forventning om at slike aksesspunkter vil ha en positiv effekt på utnyttelsen av frekvensressurser og utviklingen av trådløse kommunikasjonsløsninger. I henhold til ekomdirektivet artikkel 57 bør slike aksesspunkt ha minimal visuell påvirkning på omgivelsene, noe som stiller krav til blant annet størrelse, herunder volum og vekt. Småcellebasestasjoner skal etter forordningen ikke overstige en størrelse på 30 liter.
Forordningens angivelser vil ved forskriftsendringen i ny § 6-1 gjelde for etableringen av slike aksesspunkt i Norge.

Til § 6-2 Søknad om særskilt tillatelse til bruk av frekvenser til øvingsformål

Forskriftsbestemmelsen er i all hovedsak en videreføring av nåværende forskriftsbestemmelse, og inneholder krav til søknader og vurderingsmomenter ved behandling av søknader fra Forsvaret, Etterretningstjenesten og politiet om tillatelser til bruk av frekvenser og utstyr etter ekomloven § 11-14. Bestemmelsen skal også gjelde for Etterretningstjenesten, i tråd med endringene i ekomloven som trådte i kraft 1. januar 2021.
Første ledd stiller krav til at søknader må være mottatt av Nasjonal kommunikasjonsmyndighet så lang tid i forveien av en øvelse at Nasjonal kommunikasjonsmyndighet kan varsle parter og rettighetshavere i god tid før øvelsen, i tråd med ekomloven § 9-14 tredje ledd. Hvor lang tid som er nødvendig avhenger blant annet av hvilke andre tjenester øvelsen kan få konsekvenser for. Dersom øvelsen innebærer bruk av frekvenser som vil kunne påvirke for eksempel fly-, tog- eller skipstrafikk, vil Nasjonal kommunikasjonsmyndighet måtte innhente uttalelser fra andre relevante myndigheter ved behandling av søknaden, og saksbehandlingstiden kan i slike saker være lang. Det vil også være aktuelt å stille krav om at den som får tillatelse må sørge for at det sendes ut NOTAM eller andre varsler i god tid før frekvensene skal tas i bruk. Dette innebærer at søknader i mange tilfeller må sendes inn i relativt god tid, det kan være flere uker eller måneder, før øvelsen skal finne sted. Søknader som ikke tillater tilstrekkelig saksbehandlingstid vil bli avslått av Nasjonal kommunikasjonsmyndighet.
I a*nnet ledd* stilles det krav til utforming av søknadene om tillatelse fra henholdsvis Forsvaret, Etterretningstjenesten og politiet. Søknadene skal angi frekvensområde, beskrivelse av det geografisk avgrensede området hvor øvelsen skal gjennomføres og i hvilke områder øvelsen kan få konsekvenser for andre brukere eller rettighetshavere, og tidsrom for øvelsen. Kravet til angivelse av i hvilke områder øvelsen kan få konsekvenser for andre brukere, er nytt i forskriften. Bakgrunnen for kravet er at Nasjonal kommunikasjonsmyndighet i en del tilfeller har behov for denne informasjonen for å vurdere hvilke konsekvenser øvelsen vil kunne få for andre brukere og rettighetshavere. Dette gjelder for eksempel der øvelsen skal innebære tilsiktet forstyrrelse av GNSS-frekvenser, hvor Nasjonal kommunikasjonsmyndighet også har behov for å få informasjon om utstyret som skal benyttes, utstrålt sendereffekt, teoretiske beregninger av hvor langt signalene vil rekke mv.
Dersom Forsvaret søker om å få gjennomføre øvelse på områder utenfor Forsvarets permanente øvingsområder etter ekomloven § 11-14 annet ledd, skal Forsvaret begrunne behovet for dette. Nasjonal kommunikasjonsmyndighet skal foreta en konkret vurdering av om det er forsvarlig å gjøre unntak fra hovedregelen om at Forsvarets øvelser skal gjennomføres på Forsvarets permanente øvingsområder etter ekomloven § 11-14.
Av *tredje ledd* fremgår momenter Nasjonal kommunikasjonsmyndighet skal legge vekt på ved vurderingen av søknader. Søkerens og samfunnets behov for at slik øvelse skal kunne

gjennomføres må vurderes opp mot de konsekvenser en gjennomføring av øvelsen kan påføre berørte parter og rettighetshavere. I vurderingen skal det tas hensyn til sikkerhet, stabilitet, dekningsgrad og eventuelle begrensninger for nødanrop og andre kritiske funksjoner.
I *fjerde ledd* stilles det krav om at bruken skal medføre minst mulig skadelig interferens og påføre brukere så få og kortvarige kommunikasjonsavbrudd som mulig.

Til § 6-3 Søknad om særskilt tillatelse til bruk av frekvenser for Kriminalomsorgen

Forskriftsbestemmelsen er i all hovedsak en videreføring av nåværende forskriftsbestemmelse § 9a-2, og angir krav til søknad og vurderingsmomenter ved behandling av søknader fra Kriminalomsorgen etter ekomloven § 11-15. I tillegg til å stille krav til søknaden i *første ledd*, følger det av *annet ledd* at det bare kan gis tillatelse som dekker området for fengsler med høyt sikkerhetsnivå.
Det følger av *tredje ledd* at valg av teknisk løsning skal gjøres i samråd med Nasjonal kommunikasjonsmyndighet, og at frekvensbruken skal innrettes slik at det i minst mulig grad fører til skadelig interferens i de offentlige mobilkommunikasjonsnettene. Dette er en videreføring av eksisterende rett, og er ment å bidra til at vanlige mobilbrukere utenfor fengslene forstyrres i minst mulig grad. Frekvensbruken kan få konsekvenser for dekningen i mobilnettene og for muligheten til å gjennomføre nødanrop. Dersom konsekvensene for vanlige brukere av mobilnettene anses å bli for store, kan Nasjonal kommunikasjonsmyndighet nekte å gi tillatelse.
Bestemmelsen stiller krav om at bruken skal medføre minst mulig skadelig interferens for andre brukere. Dette kan medføre at i den grad det er behov for å opprette mer eller mindre permanente sikkerhetssoner (mobilregulerte soner), så skal andre brukere av offentlig mobilkommunikasjonsnett ikke forstyrres, eller forstyrrelsene skal være minimale. Dette gjelder selv om konsekvensen blir at det stilles krav til lokaliseringen av i fengsler med høyt sikkerhetsnivå for at slike soner kan opprettes.

Til § 6-4 Søknad om til bruk av frekvenser for å ivareta særskilte allmennyttige formål

Forskriftsbestemmelsen er ny, og bygger i hovedsak på forskriftsbestemmelsene §§ 9a-1 og 9a-2. Bestemmelsen gjelder krav til søknad og gjennomføring etter forslag til ny § 11-16 i forslag til ny ekomlov.
I *første ledd* stilles det krav om at søknaden må være mottatt av Nasjonal kommunikasjonsmyndighet i rimelig tid før frekvensen skal tas i bruk. Bakgrunnen for dette er at Nasjonal kommunikasjonsmyndighet skal kunne foreta en forsvarlig behandling av søknaden, herunder innhente innspill fra berørte parter, og varsle rettighetshavere i god tid før øvelsen skal gjennomføres. Hvor lang tid som er nødvendig vil blant annet avhenge av hvilke andre tjenester øvelsen kan få konsekvenser for. For øvelser som potensielt vil kunne påvirke for eksempel fly-, tog- eller skipstrafikk kan saksbehandlingstiden være lang.
Annet ledd stiller krav til hva søknaden skal inneholde. Det stilles strengere krav til innhold i søknaden for søknader etter særbestemmelsen i § 11-16 enn etter § 11-13 og 11-14. Foruten å angi frekvensområder for øvelsen, geografiske avgrensning av området for øvelse og der øvelsen kan få konsekvenser for andre brukere, og tidsrom for øvelsen, skal søker gi en nærmere beskrivelse av behovet for å gjennomføre øvelsen eller beredskapsformålet og

det særskilte allmennyttige formålet det skal oppfylle. I søknaden må søker også gi en beskrivelse av hvem som skal gjennomføre øvelsen, og hvilket utstyr som skal benyttes.
Tredje ledd inneholder tilsvarende bestemmelse som er angitt i gjeldende ekomforskrift § 9a-1 annet ledd.
Etter fjerde ledd stilles krav om at bruken skal medføre minst mulig skadelig interferens og påføre brukere så få og kortvarige kommunikasjonsavbrudd som mulig. Ved behandling av søknader om tillatelse etter § 11-16 må det særlig tas stilling til om vilkåret om at øvelsen må ivareta særskilte allmennyttige formål er oppfylt.

Til kapittel 7 nummer, navn og adresser

Til § 7-1 Implementering av nummerserier

Bestemmelsen er en videreføring av gjeldende § 6-5.Det fremgår av forslag til *første ledd* at tilbydere av offentlig nummerbasert person-til-person kommunikasjonstjeneste gjensidig skal implementere hverandres nummerserier vederlagsfritt slik at alle-til-alle-kommunikasjon blir mulig.
Pliktsubjektet i forslaget er "tilbydere av offentlig nummerbasert person-til-person kommunikasjonstjeneste" i tråd med de nye definisjonene av begrepene i ny ekomlov § 1-5.
Bestemmelsen kan ses i sammenheng med nummerforskriften § 5 annet ledd, som stiller krav til at den som får tildelt nummerressurser ikke skal forskjellsbehandle andre tilbydere av elektroniske kommunikasjonstjenester med hensyn til nummerressurser som gir tilgang til deres tjenester.

Til § 7-2 Tilleggsfunksjoner knyttet til offentlig talekommunikasjonstjenester

Bestemmelsen er en videreføring av gjeldende § 6-4. Oppdateringene er av språklig karakter og medfører ikke realitetsendring. Tilleggsfunksjoner kan for eksempel være mulighet for sperring av utgående samtaler, beløpsgrenser for bruk, viderekobling og direkte innvalgs-funksjoner.
Tonesignalering, DTMF – «dual tone multi frequency», er normalt tilgjengelig i telefonsystemer og benyttes i dag særlig i kundeløsninger for bedriftsmarkedet. Eksempel på dette er tastevalg i sentralbordløsninger.

Til § 7-3 Nummeropplysningsinformasjon

Bestemmelsen er hovedsakelig en videreføring av gjeldende ekomforskrift § 6-3 om plikt til å utveksle nummeropplysningsinformasjon og gjeldende § 6-2 annet, fjerde, femte og sjette ledd, og gjennomfører ekomdirektivet artikkel 112.
Det presiseres i forslag til *første ledd* at det er tilbyder av nummerbasert person-til-person kommunikasjonstjeneste som har plikt til å gjøre tilgjengelig informasjon om sluttbruker til nummeropplysningstjenester.
Forslaget til *annet ledd* nummer 1 viderefører kravet i gjeldende ekomforskrift § 6-3 annet ledd nummer 2 om at tilbyder skal overføre informasjon om brukers etternavn, fornavn og mellomnavn for personlige brukere eller firmanavn til tilbydere av nummeropplysningstjeneste. Når juridisk eier av abonnement og bruker ikke er den samme, skal bare brukers navn overføres. I tillegg presiseres det at når sluttbruker er en juridisk person skal organisasjonsnummer overføres. Dette er nytt.

Det følger av forslag til *tredje ledd* at det er forbudt for tilbyder å utlevere nummeropplysningsinformasjon om barn som er registrert som bruker av et abonnement, dersom det ikke foreligger samtykke fra foresatte eller verge. Bestemmelsen åpner for at barnet etter fylte 15 år selv kan trekke tilbake dette samtykket. Etter fylte 18 år skal informasjonen overføres, men først etter at registrert bruker er blitt varslet om dette og gitt mulighet til å vurdere om den ønsker å reservere seg helt eller delvis mot at opplysningene overføres til nummeropplysningsvirksomheter. Det er ikke foreslått konkrete krav i forskriften til hvor lang varslingstid som kreves. En periode på en måned fra varsel sendes og til abonnementsinformasjon overføres, bør i utgangspunktet være tilstrekkelig tid for registrert bruker til å reservere seg mot at informasjon om nummer, navn og/eller adresse utleveres. Kravene i tredje ledd gjelder for alle abonnementsavtaler, også de som allerede er inngått.
I forslaget til *fjerde ledd første punktum* fastsettes det at tilbyder ikke skal utlevere nummeropplysningsinformasjon til nummeropplysningsvirksomhet om sluttbrukere som disponerer hemmelig nummer eller som har reservert seg mot at informasjonen om egne nummer, navn eller adresser utleveres til allmennheten. Dette er en videreføring av gjeldende § 6-3 tredje ledd.
Forslaget til fjerde ledd *annet punktum* er hovedsakelig en videreføring av gjeldende§ 6-2 fjerde ledd. Det presiseres i forslaget at nummeropplysningsvirksomheten plikter å umiddelbart slette opplysninger om sluttbrukere som disponerer hemmelig nummer, eller som har reservert seg mot offentliggjøring av opplysninger. Dette innebærer at nummeropplysningsvirksomheten uten opphold skal fjerne informasjon om sluttbruker som disponerer hemmelig nummer eller som har reservert seg mot utlevering av informasjon til nummeropplysningsvirksomheter.
Det fremgår av forslag til *niende ledd* at tilbyder av nummeropplysningstjeneste skal sikre at nummeropplysningssystemet er i overensstemmelse med personopplysningsloven og at det ikke gis opplysninger i strid med taushetsplikt. Dette er en videreføring av plikten i gjeldene § 6-2 sjette ledd. Det foreslås presisert i annet punktum at dette innebærer at plikten ikke innskrenker sluttbrukers rettigheter fastsatt i eller i medhold av personopplysningsloven.

Til § 7-4 Nummervisning

Innholdet i bestemmelsen viderefører i hovedsak gjeldende forskrift § 6-1 med den endring at det presiseres at det er tilbydere av nummerbasert person-til-person kommunikasjonstjenester som har plikter etter bestemmelsen.
Første ledd i bestemmelsen gjennomfører ekomdirektivet vedlegg VI del B bokstav a.
Med nummervisning menes at anroperens nummer vises for den anropte før samtalen opprettes. Denne ressursen skal tilbys i samsvar med relevant lovgivning om vern av personopplysninger og personvern, særlig kommunikasjonsvernbestemmelsene i ekomloven og i forskriften.
I den grad det er teknisk mulig, skal tilbyderne stille data og signaler til rådighet for å gjøre det lettere å tilby nummervisning og tonesignalering over medlemsstatenes grenser.
Annet ledd gjennomfører kommunikasjonsverndirektivet artikkel 8, og er også en videreføring av gjeldende rett.
Femte ledd gjør unntak fra reservasjonsretten i annet ledd for så vidt gjelder anrop til nødmeldingstjeneste. Ved anrop til nødmeldingstjenesten skal nummeret vises selv om sluttbruker har reservert seg mot nummervisning.

Reservasjonsretten kan også innskrenkes midlertidig dersom det foreligger begrunnet mistanke om at den reserverte brukeren anvender det reserverte nummeret til telefonsjikane. I *sjette ledd* presiseres at tilbyder skal informere sluttbrukeren om rettigheten etter bestemmelsen.

Til § 7-5 Blokkering av anrop

Bestemmelsen viderefører og utvider gjeldende § 6-1 tredje ledd i ekomforskriften. *Første ledd* utvider tilbyders plikt til å blokkere anrop også til tilfeller der anropet er ledd i svindelvirksomhet. Bestemmelsen vil blant annet dekke spoofing, wangiri, urettmessig bruk av ikke-reelle nummer (visning av nummer som ikke kan ringes, bruk av andres nummer mv.).
Tilbyder som har utenlands-gateway vil være en sentrale aktører for blokkering av inngående anrop fra utlandet. Andre aktører som terminerer trafikk nasjonalt vil også kunne være i en posisjon for å vurdere ektheten på det inngående anropet.
Hvis tilbyder finner det rimelig å anta eller vurderer at anropet med tilstrekkelig grad av sannsynlighet tilhører en av kategoriene, vil det foreligger en plikt til å blokkere. Det er ikke nødvendig at tilbyder finner det bevist. Vurderingen vil bero på en samlet vurdering hvor flere momenter kan spille inn, slik som kunne ringemønster, kundeklager, nummerlokasjon, historikk, originerende destinasjon osv.
Etter *annet ledd* skal tilbyder føre statistikk over hvilke nummer som blokkert, antallet blokkeringer og på hvilket grunnlag blokkering er foretatt.

Til § 7-6 Gjennomføring av forordning om toppnivådomenet .eu

Bestemmelsen foreslår å videreføre gjeldende forskrift § 6-7 om gjennomføring av reglene om toppnivådomenet .eu. Forordningene om .eu er innlemmet i EØS-avtalen. Norske innbyggere og selskaper fikk ved innlemmingen av rettsaktene i EØS-avtalen og gjennomføringen i norsk rett, like rettigheter som EU borgere og selskaper til å registrere domenenavn under .eu.
Innføring av et toppdomene .eu for EU i 2005/2006 er ment blant annet å lette handelen i .eu ved at kun selskaper som er bundet av EUs regulering, blant annet på forbrukerområdet, får tilgang til toppdomenet.

Kapittel 8 Kommunikasjonsvern

Til § 8-1 Behandling av trafikkdata

Bestemmelsen viderefører gjeldende ekomforskrift § 7-1 som setter skranker for tilbyders behandling av trafikkdata. Tilbyderbegrepet er ved implementeringen av ekomdirektivet utvidet til også å omfatte nummeruavhengige tjenester, jf. kommunikasjonsverndirektivet artikkel 2 som henviser til rammedirektivets definisjoner, nå erstattet av ekomdirektivet som i artikkel 125 tredje avsnitt fastsetter at henvisninger til rammedirektivet skal forstås som henvisninger til ekomdirektivet.
Etter forslaget til § 8-1 *første ledd* skal tilbyder av elektronisk kommunikasjonsnett og tilbyder av offentlig elektronisk kommunikasjonstjeneste bevare taushet om trafikkdata og slette eller anonymisere trafikkdata. Nærmere om taushetsplikten og sletteplikten fremgår av merknadene til ekomloven § 3-2 og § 3-3 og departementet viser til omtalen under disse bestemmelsene.

Etter forslaget til *annet ledd* faller det innenfor tilbyders lovlige behandling av trafikkdata å benytte de lagrede opplysningene til fakturering, trafikkstyring, kundeforespørsler, markedsføring av elektronisk kommunikasjonstjeneste og avsløring av urettmessig bruk av elektronisk kommunikasjon. Slik behandling av trafikkdata hos tilbyder kan bare foretas av personer som har fullmakt for utførelsen av arbeidet fra tilbyderen, og skal begrenses til det som er nødvendig for utførelsen av de spesifikke arbeidsoppgavene. Ved at kun et begrenset utvalg personer får tilgang til trafikkdataene antas det at risikoen for personvernkrenkelser reduseres. Ordlyden behandling favner enhver bruk av trafikkdata, slik som innsamling, registrering, organisering, strukturering, lagring, tilpasning eller endring, gjenfinning, konsultering, bruk, utlevering ved overføring, spredning eller alle andre former for tilgjengeliggjøring, sammenstilling eller samkjøring, begrensning, sletting eller tilintetgjøring. Departementet viser til at definisjonen av behandling i Europaparlaments- og rådsforordning (EU) 2016/679 av 27. april 2016 om vern av fysiske personer i forbindelse med behandling av personopplysninger og om fri utveksling av slike opplysninger, gir føringer for hvordan ordlyden behandling i § 8-1 må forstås.
Gjeldende definisjon av trafikkdata er tatt inn blant definisjonene i forslaget til ekomloven § 1-5 . Både trafikkdata knyttet til fysiske og andre juridiske personer er omfattet. Eksempler er data som angir kommunikasjonens opphavssted, bestemmelsessted, rute, klokkeslett, dato, omfang, varighet og underliggende tjeneste.
Gjeldende § 7-1 annet ledd om forklaring av lokaliseringsdata er heller ikke tatt med i forslaget til § 8-1 da det allerede ivaretas av definisjoner i ekomloven § 1-5. Departementet gjør oppmerksom på at trafikkdata-begrepet også elementer av lokaliseringsdata som f.eks. hvilken basestasjon brukeren er tilknyttet når vedkommende gjennomfører en samtale, eller den lokalisering som skjer når brukeren eller applikasjoner på brukerens mobiltelefon laster ned data fra nettet. En anmodning fra politiet om utlevering av trafikkdata fra tilbyder vil derfor omfatte noe lokaliseringsdata.
Forslaget i tredje ledd viderefører gjeldende rett. Annen behandling av trafikkdata enn den som er nevnt i ekomloven § 3-3 første ledd, herunder behandling til markedsføringsformål, krever samtykke fra bruker, jf. ekomloven § 3-3 annet ledd. Regler om samtykke er gitt i forskriften § 8-3 og må forstås innenfor rammene av personvernforordningen artikkel 4 nummer 11.

Til § 8-2 Behandling av lokaliseringsdata

Bestemmelsen viderefører gjeldende ekomforskrift § 7-2 og gir skranker for tilbyders behandling av lokaliseringsdata inkludert signaleringsdata. Tilbyderbegrepet er ved implementeringen av ekomdirektivet utvidet til også å omfatte nummeruavhengige tjenester, jf. merknaden til § 8-1 over.
I forslaget *første ledd* vises til at tilbyder av elektronisk kommunikasjonsnett og tilbyder av offentlig elektronisk kommunikasjonstjeneste skal bevare taushet om lokaliseringsdata inkludert signaleringsdata, og slette eller anonymisere slike data. Nærmere om taushetsplikten og sletteplikten fremgår av merknadene til ekomloven § 3-2 og § 3-3 og departementet viser til omtalen under disse bestemmelsene.
Etter *annet ledd* skal behandlingen begrenses til det som er nødvendig for levering av den tjeneste som bruker har samtykket til. Regler om samtykke er gitt i forskriften § 8-3.
Behandling av lokaliseringsdata inkludert signaleringsdata hos tilbyder kan bare foretas av

personer med fullmakt fra tilbyderen. Ved at kun et begrenset utvalg personer får tilgang til lokaliseringsdata antas det at risikoen for personvernkrenkelser reduseres.
Ordlyden behandling favner enhver bruk av lokaliseringsdata og signaliseringsdata. Signaleringsdata omtales i § 1-5 nummer 24. Departementet ser ikke lenger behov for å ha en egen definisjon av signaleringsdata idet definisjonen av lokaliseringsdata må anses for å omfatte alle relevante signaleringsdata.
I de offentlig tilgjengelige mobilnettene omfatter lokaliseringsdata f.eks. data om hvilke basestasjoner terminalen har vært tilknyttet. I offentlig tilgjengelig fastnett vil lokaliseringsdata typisk være data om nettermineringspunktets fysiske adresse.

Lokaliseringsdata vil også være trafikkdata, jf. merknaden til § 8-1. Trafikkdata som også angir lokalisering, kan for eksempel være hvilken basestasjon som brukeren er tilknyttet når vedkommende gjennomfører en samtale, eller når brukeren eller applikasjoner på brukerens mobiltelefon laster ned data fra nettet. Hvorvidt lokaliseringsdata kommer fra en aktiv handling fra sluttbrukeren eller om terminalen oppdaterer seg automatisk uavhengig av aktiv bruk, vil variere.

Til § 8-3 Samtykke

Bestemmelsen viderefører gjeldende ekomforskrift § 7-4, og gjennomfører forpliktelser som følger av krav til samtykke i kommunikasjonsverndirektivet artiklene 6 og 9.
Det foreslås presisert at samtykke som eventuelt må innhentes for å behandle trafikk- eller lokaliseringsdata, skal forstås på samme måte som i personvernforordningen artikkel 4 nummer 11 (som gjennomført i personopplysningsloven). Dette innebærer bl.a. at samtykket må være klart, aktivt og informert. Når det gjelder kravet til informasjon fra tilbyder er dette av pedagogiske hensyn ytterligere presisert i bestemmelsens første ledd annet punktum. Det er videre forutsatt at samtykket enkelt og vederlagsfritt skal kunne trekkes tilbake av brukeren. Når det gjelder lokaliseringsdata som omfattes av § 8-2 skal det, i tillegg til adgang til et generelt tilbakekall, legges til rette for at brukeren midlertidig skal kunne trekke tilbake sitt samtykke. Dette kan være aktuelt for å unngå at andre kan få kjennskap til lokaliseringen av brukeren for hver enkelt oppkobling til nettet eller ved hver enkelt bruk av tjenesten.

Til § 8-4 Informasjon til abonnenten eller bruker om ruting av nasjonal trafikk

Bestemmelsen viderefører gjeldende regler om produksjon eller formidling av nasjonal elektronisk kommunikasjon ved ruting utenfor Norges grenser i gjeldende ekomforskrift § 7-5. For at slik ruting skal være tillatt må tilbyderen oppfylle visse vilkår.
Første ledd gjelder ruting innenfor EFTA/EØS-området, mens *annet ledd* gjelder ruting utenfor EFTA/EØS-området etter søknad. Med ruting menes i denne sammenheng transport av nettverkspakker (f.eks. internettprotokollpakker) over et elektronisk kommunikasjonsnett. Når nasjonal elektronisk kommunikasjon blir rutet i transitt gjennom et land, vil det kunne føre til at tilbyder bryter taushetsplikten etter ekomloven ettersom flere land har regler for overvåking av grenseoverskridende trafikk. Departementet viser til at Lysne I-utvalgets rapport om digital sårbarhet (NOU 2015:13) og Lysne II-utvalgets rapport av 26. august 2016 «Digitalt grenseforsvar (DGF)», peker på utfordringer ved internasjonalisering og faren for konfidensialitetsbrudd i forbindelse med overvåking av grenseoverskridende trafikk og lagring av data utenfor Norges grenser. Bestemmelsen i § 8-4 skal sikre tilbyders lovlige drift.

Etter § 8-4 *første ledd* er taushetsplikten etter ekomloven § 3-2, ikke til hinder for at tilbyder produserer eller formidler nasjonal elektronisk kommunikasjon ved å benytte elektronisk kommunikasjonsnett og -tjeneste eller tilhørende fasiliteter utenfor Norges grenser, men innenfor EFTA/EØS-området, dersom abonnent eller bruker informeres om dette. Informasjonen skal angi i hvilket land tilbyders produksjon eller formidling skal foregå, og må gis på en entydig måte og være lett tilgjengelig for abonnent eller bruker. Bruker skal gis en kortfattet forklaring om hele verdikjeden utenfor Norges grenser, og hva dette kan innebære for kommunikasjonens konfidensialitet. Plikten vil være oppfylt dersom informasjonen er inntatt i avtalen med abonnenten, med opplysning om at nærmere informasjon kan finnes på tilbyders nettsider. Et særlig spørsmål er om det er tilstrekkelig at endringer i ruting etter avtaleinngåelse opplyses om på tilbyders internettsider, sosiale medier eller andre informasjonskanaler. I lys av skjerpede krav i personvernforordningen mener departementet at opplysninger gitt kun på denne måte neppe på en tilfredsstillende måte ivaretar informasjonskravet i § 8-4, men at opplysninger også må formidles direkte til den berørte f.eks. via e-post, gjerne med en henvisning til hvor brukeren kan søke utdypende informasjon. Dette innebærer en skjerping av kravene opp mot dagens praksis, og departementet ber om høringsinstansenes syn på dette.

Ordlyden tilbyders produksjon eller formidling av nasjonal elektronisk kommunikasjon må forstås vidt, til også å omfatte tjenesteproduksjon og tillatt lagring i henhold til lov. Forskriften omfatter også tilfeller der tilbyderen med kundeforholdet til sluttbruker produserer tjenesten ved hjelp av underleverandører. I slike tilfeller må tilbyder med kundeforholdet til sluttbruker selv ha oversikt over underleverandørens ruting og produksjon, for å kunne benytte seg av unntaket fra taushetsplikten som bestemmelsen oppstiller.

Begrepet tilhørende fasilitet er definert i ekomloven § 1-5 nummer 12 og departementet viser til merknaden til denne. Begrepet inkluderer element som inngår i, foranlediger eller understøtter etablering og drift av elektroniske kommunikasjonsnett og produksjon og leveranse av elektroniske kommunikasjonstjenester, men som ikke utgjør sentrale deler av elektroniske kommunikasjonsnett og elektroniske kommunikasjonstjenester. Begrepet tilhørende signaliserer ikke eierskapstilhørighet, men en tilknytning til nett- eller tjenestefasiliteten.

For ruting utenfor EFTA/EØS-området kan Nasjonal kommunikasjonsmyndighet ved enkeltvedtak gi tillatelse til at bestemmelsen skal gjelde tilsvarende utenfor EFTA/EØS-området, jf. annet ledd. Krav til tillatelse gjelder også planlagt omruting utenfor EFTA/EØS-området ved transmisjonsbrudd i de regulære forbindelsene. Krav til tillatelse gjelder ikke ved kortvarig omruting utenfor EFTA/EØS-området ved uforutsette transmisjonsbrudd i de regulære forbindelsene. Ved de uforutsette transmisjonsbruddene kan det i forbindelse med hendelseshåndtering være behov for kortvarig å rute trafikken utenfor EFTA/EØS-området for å unngå unødig forsinkelse med å gjenopprette normal drift. Departementet forutsetter at det i disse tilfellene ikke vil være mulig å gjenopprette tjenester eller funksjonalitet innen rimelig tid uten å omrute utenfor EFTA/EØS-området.

Departementet viser til at vedtakskompetansen først og fremst er tenkt på begrensede unntak fra taushetsplikten etter ekomloven § 3-2, og under forutsetning av at sluttbruker blir gjort oppmerksom på unntaket. Abonnenten eller brukeren vil da selv kunne foreta et informert valg om benyttelse av ekomtjenesten.

Hvorvidt det skal gis adgang til å rute nasjonal trafikk utenfor EFTA/EØS-området beror blant annet på en avveining av risikoen for inngripen i kommunikasjonsvernet opp mot

ekommyndighetens tilrettelegging for innovasjon og utvikling av nye tjenester. Hvilke momenter det skal eller kan legges vekt på, vil være gjenstand for en helhetsvurdering. Det er relevant å vektlegge hvilke type tjeneste som rutes, og hvordan denne er planlagt realisert, om det foreligger kontraktsfestede plikter vedrørende leverandørens tilgang til og behandling av tilbyderens data, og tilbyderens rettigheter for innsyn og kontroll. Et annet relevant moment som vil måtte vurderes er risikoaspektet rundt hvilket land tjenesten opereres eller driftes fra, og hvilket sikkerhetsmessig samarbeid Norge har med det aktuelle landet. I tillegg må landets beskyttelsesnivå for behandling av personopplysninger måtte vurderes for å redusere risikoen for konfidensialitetsbrudd og dermed redusere de potensielle negative konsekvenser av å gi unntak fra taushetsplikten etter ekomloven § 3-2.
Etter *tredje ledd* skal tilbyder som nevnt i første ledd informere Nasjonal kommunikasjonsmyndighet om forhold som nevnt i første og annet ledd.
Etter fjerde ledd er bestemmelsen avgrenset mot satellittelefontjeneste og omfattes ikke.

Til § 8-5 Unntak fra sletteplikt og taushetsplikt for nummeruavhengige person-til-person kommunikasjonstjenester

Formålet er å gjennomføre EUs interim forordning om prosessering av personlige og andre data med formål å bekjempe seksuelt misbruk av barn, nærere bestemt om unntak fra sletteplikt og taushetsplikt for behandling av personopplysninger og andre data ved levering av nummeruavhengige person-til-person kommunikasjonstjenester.
Regelverket skal sikre at tilbydere av nummeruavhengige elektroniske person-til-person kommunikasjonstjenester kan videreføre sin praksis med å avdekke materiale med seksuelt misbruk av barn på nettet. Dagens praksis ikke lenger i tråd med kommunikasjonsverndirektivet fordi ekomdirektivet definerer tilbydere av nummeruavhengige elektroniske person-til-person kommunikasjonstjenester som tilbydere av elektroniske kommunikasjonstjenester. Disse omfattes dermed av forbudet i kommunikasjonsverndirektivet om å behandle persondata og annen data på den måten den de har gjort til nå ved å avdekke, fjerne og rapportere materiale med seksuelt misbruk av barn på nettet.
Det midlertidige unntaket i interim forordningen er ment å gjelde inntil ny kommunikasjonsvernforordning som avløser kommunikasjonsverndirektivet 2002/58/EC er på plass.

Til kapittel 9 sikkerhet og beredskap

Til § 9-1 Sikkerhetsstyring

Forslag om ny bestemmelse om sikkerhetsstyring er gitt med hjemmel i ekomloven § 3-8 sjette ledd, og utdyper kravet til systematisk oppfølging av sikkerhet i nett og tjenester.
Etter bestemmelsens *første ledd første punktum* skal tilbyder etablere og vedlikeholde et styringssystem for sikkerhet som beskriver virksomhetens sikkerhetsarbeid. Tilbyder kan ikke velge å la være å etablere sikkerhetsstyringssystem, jf. ordlyden "skal". Styringssystemet må etableres for den konkrete virksomheten, det er således ikke tilstrekkelig å vise til at moderkonsernet eller et søsterselskap har etablert slike.
Med sikkerhetsstyring menes et styringssystem for sikkerhet. Et slikt styringssystem for sikkerhet innebærer systematiske aktiviteter med betydning for forebyggende sikkerhetsarbeid, og omfatter planlegging, etablering, gjennomføring og forbedring av det

forebyggende sikkerhetsarbeidet. Dette er nødvendig for å oppnå og opprettholde forsvarlig sikkerhet i nett og tjenester. Styringssystemet kan f.eks. etableres med grunnlag i anerkjente standarder for styring som ISO 9000-serien og ISO 27000-serien. Forutsetningen er at styringssystemet dekker hele det forebyggende sikkerhetsarbeidet.
I operasjonalisering av kravet til forsvarlig sikkerhet og sikkerhetsstyring, legger departementet til grunn følgende elementer som vil utgjøre minstekrav i vurderingen av om forsvarlig sikkerhet og sikkerhetsstyring foreligger:

- Ledelsesforankring
- Verdivurdering
- Risikovurdering
- Tiltak og handlingsplaner for å beskytte verdier
- Beredskapsplanlegging og øvelser
- Revisjon
- Overholdelse av oppfølgingsplikt (påseplikt)
- Informasjonssikkerhet
- Dokumentasjon

Forebyggende sikkerhetsarbeid starter med en verdivurdering der virksomheten kartlegger sine verdier. En slik verdivurdering er en forutsetning for riktig prioritering av ressurser virksomheten har til rådighet for sikkerhet, og for å kunne gjennomføre effektive sikringstiltak. Verdivurderinger må dokumenteres, jf. kravet i bestemmelsens tredje ledd.
Tilsvarende krav til gjennomføring av verdivurdering er gitt i sikkerhetsloven og virksomhetsikkerhetsforskriften kapittel 3.
Det følger av bestemmelsens *første ledd annet punktum* at systemet skal sikre at virksomheten oppfyller krav gitt i eller med hjemmel i lov. Her siktes det til krav gitt i ekomloven eller andre relevante lover f.eks. personopplysningsloven når det gjelder sikring av personopplysninger, samt til forskriftshjemmelen i ekomloven § 3-8.
Etter bestemmelsens *annet ledd første punktum* skal virksomhetens leder jevnlig foreta en gjennomgang av virksomhetens styringssystem for sikkerhet. Forebyggende sikkerhetsarbeid skal gjennomgås av virksomhetens leder. Denne skal gjøre prioriteringer og avsette nødvendige ressurser til arbeidet med den forebyggende sikkerheten. Som en del av forankringen hos virksomhetens leder må det utarbeides sikkerhetsmål, gjerne en sikkerhetsstrategi, og et styringsdokument. Leders evaluering bør formaliseres som et møte og dokumenteres skriftlig. Lignende krav til ledelsesforankring er gitt i virksomhetsikkerhetsforskriften § 10 og finnes gjennomgående i standarden NS-EN ISO 9001:2015. Arbeidet med sikkerhet er en kontinuerlig prosess, jf. at virksomhetens leder jevnlig skal gjennomgå sikkerhetsstyringen. Dette innebærer bl.a. at lederen minst én gang årlig må gjennomgå sikkerhetsmål, sikkerhetsstrategi, organisering og vurderinger. Lederen skal kontrollere at disse er i samsvar med virksomhetens behov og eventuelt oppdatere dokumentene. Gjennomgangen bør utføres etter rutinebeskrivelse.
Etter bestemmelsens *annet ledd annet punktum* skal styringssystemet gjøres kjent for virksomhetens ansatte. Dette kan f.eks. gjøres i form av sikkerhetsinstruks, taushetserklæring, rutiner og sjekklister, og opplæring. Styringssystemet skal også gjøres kjent for underleverandører i den grad det er hensiktsmessig for å oppfylle krav gitt i eller med hjemmel i lov. Departementet viser i denne forbindelse til at virksomheten har ansvaret for oppfyllelse av plikter gitt i lov eller i medhold av lov også der deler av virksomheten er tjenesteutsatt/utkontraktert. Det bør derfor foreligge en skriftlig avtale som sikrer dette.

Etter bestemmelsens *tredje* ledd skal tilbyders styringssystem for sikkerhet dokumenteres fortløpende. Kravet til dokumentasjon innebærer et krav til skriftlighet. Dokumentene skal oppbevares hos tilbyder.
Etter bestemmelsens *fjerde ledd* skal tilbyder 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.

Til § 9-2 Risiko- og sårbarhetsvurdering

Ny forskriftsbestemmelse om risiko- og sårbarhetsvurdering er gitt med hjemmel i ekomloven § 3-8 sjette ledd, og utdyper kravet til systematisk oppfølging av sikkerhet i nett og tjenester, jf. § 3-8 annet ledd. Risiko- og sårbarhetsvurdering vil være en sentral del av en virksomhets sikkerhetsstyring.
Etter bestemmelsens *første ledd første punktum* skal tilbyder utarbeide og vedlikeholde risiko- og sårbarhetsvurderinger (heretter kalt ROS) for å ivareta forsvarlig sikkerhet i elektronisk kommunikasjonsnett og elektronisk kommunikasjonstjeneste.
Hvem som regnes som tilbyder fremgår av ekomloven § 3-8, jf. definisjoner i ekomloven § 1-5. Tilbyder kan ikke velge å la være å utarbeide og vedlikeholde ROS, jf. ordlyden *skal*. ROS skal utarbeides og vedlikeholdes for den konkrete virksomheten, det er således ikke tilstrekkelig å vise til at moderkonsernet eller et søsterselskap har etablert slike. ROS handler om å identifisere konsekvenser ved ulike hendelser eller scenarier, og å vurdere hvor sannsynlig eller lett en uønsket hendelse kan inntreffe. ROS begynner med en kartlegging av verdier som bør sikres. Det bør gjøres en trusselvurdering av hvilke aktører som kan være interessert i verdiene og hvilke angrepsvektorer de ulike trusselaktørene benytter. Deretter gjøres en vurdering av om verdiene er sårbare for de gitte truslene. Resultatet av ROS vurderes opp mot toleransenivå for sikkerhet, dvs. hvor stor risiko virksomheten skal ta ved ulike scenarier. Dersom risikonivået er høyere enn fastlagt nivå for akseptabel risiko, skal det iverksettes tiltak for å redusere risikoen. Det er virksomhetens ledelse som avgjør toleransenivået for sikkerhet.
Det følger av *første ledd annet punktum* at ROS skal være av et slikt omfang at tilbyder kan identifisere organisatoriske, fysiske, logiske og menneskelige sikkerhetstiltak. Med ordlyden *av et slikt omfang* menes at ROS både skal omfatte tilstrekkelig kvantitative og kvalitative vurderinger.
Eksempler på organisatoriske sikkerhetstiltak er prosedyrer, sikkerhetsstrategi, rutiner og opplæring.
Eksempler på fysiske sikkerhetstiltak er adgangskontroll, skap, dører, rom og bygninger.
Eksempler på logiske sikkerhetstiltak er konfigurering av elektroniske systemer, kryptering og tilgangsstyring basert på tjenstlig behov – gjennom passord, autentisering, tilgangsnivå og brukerroller. Et annet eksempel er identitetsforvaltning, som innebærer å håndtere opplysninger om hvem noen er og hvilken rolle denne personen har. Logging av autorisert og uautorisert bruk for drifts- og sikkerhetsformål (klientbasert logging) og nettverksbasert logging for å kunne oppdage datainnbrudd og virus er tiltak som innebærer å etterkontrollere informasjonssystemet.
Eksempler på menneskelige sikkerhetstiltak er kompetanse, kultur, taushetserklæringer, fullmakt og klarering.
Etter bestemmelsens *annet ledd* skal tilbyder ved endringer som kan påvirke sikkerheten vurdere hvilken risiko endringene medfører. Bestemmelsen angir ikke størrelse eller karakter

på endringen, bare at det må påvirke sikkerhetsarbeidet. I så fall må tilbyder vurdere hvilken risiko endringene medfører.
Etter bestemmelsens *tredje ledd* skal tilbyders risiko- og sårbarhetsvurderinger dokumenteres fortløpende. Kravet til dokumentasjon innebærer et krav til skriftlighet. Dokumentene skal oppbevares hos tilbyder.

Til § 9-3 Grunnsikring

Forslaget til ny forskriftsbestemmelse om grunnsikring utdyper kravet til forsvarlig sikkerhet i nett og tjenester.
Etter *første ledd* skal tilbyder utarbeide, iverksette og vedlikeholde grunnsikringstiltak for å ivareta forsvarlig sikkerhet i elektronisk kommunikasjonsnett og elektronisk kommunikasjonstjeneste.
Hvem som regnes som tilbyder fremgår av jf. definisjonen i ekomloven § 1-5. Tilbyder kan ikke velge å la være å utarbeide, iverksette og vedlikeholde grunnsikringstiltak, jf. ordlyden *skal*.
Grunnsikringstiltak vil være de barrierene virksomheten har til rådighet for å beskytte mot utfall og sikre tilgjengeligheten for nett og tjenester ved andre hendelser. Dette gjelder både tilsiktede og utilsiktede hendelser.
En nærmere beskrivelse av hva grunnsikring innebærer er gitt i *første ledd annet punktum*. En slik kombinasjon av barrierer, deteksjons-, verifikasjons- og reaksjonstiltak må planlegges, gjennomføres og vedlikeholdes som permanent grunnsikring for objekter og infrastruktur. Aktuelle tiltak vil kunne være påbyggingstiltak, tiltak for skadebegrensning og gjenoppretting og tiltak for å oppnå redundans. Grunnsikringen skal tilpasses den til enhver tid gjeldende risiko. Dersom risikoen øker må man vurdere om det skal utføres påbygningstiltak for å komplementere grunnsikringstiltakene for å oppnå forsvarlig sikkerhet. Dersom den økte risikoen vedvarer, skal tilbyderne vurdere om påbyggingstiltakene skal bli en del av grunnsikringen.
Kravene til grunnsikringstiltak vil måtte tolkes strengere der det er tale om å tjenesteutsette deler av virksomhetens drift til leverandører/produsenter som ikke er hjemmehørende i Norge. I tillegg til å vurdere tjenestetilbyderen, bør tilbyderen vurdere vertslandet der leverandøren har tilhold og hvor tjenesten tilbys fra. Nasjonale forhold kan påvirke en leverandørs mulighet til å levere tjenester, eksempelvis gjennom kvaliteten på nasjonal infrastruktur eller nasjonal lovgivning som gir rett til innsyn i data lagret i vertslandet. Risikoen knyttet til vertslandet kan dermed gi avgjørende føringer på behovet for kompenserende sikringstiltak og hvilke tjenestetilbydere som bør vurderes. Landvurderingen bør inngå som en del av den totale risikovurderingen ved tjenesteutsettingen. Kravene til tiltak vil måtte tilpasses trusselen det enkelte land utgjør eller vil kunne utgjøre i utstyrets levetid.
Etter *annet ledd* skal tilbyder planlegge skadebegrensende tiltak som kan iverksettes i situasjoner som ikke fullt ut kan håndteres med grunnsikringstiltakene. Dette kan for eksempel være tiltak for å oppnå redundans.
Tredje ledd innebærer krav til at tilbyder skal ha en plan for gjenoppretting for å sikre forsvarlig sikkerhet og hindre unødig nedetid.
Etter bestemmelsens *fjerde ledd* skal tilbyders tiltaksplaner dokumenteres. Kravet til dokumentasjon innebærer et krav til skriftlighet. Dokumentasjonen skal oppbevares hos tilbyder.

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

Ny forskriftsbestemmelse om krav til sikring av informasjons- og styringssystemer er gitt med hjemmel i ekomloven § 3-8 sjette ledd, og utdyper kravet til systematisk oppfølging og forsvarlig sikkerhet i nett og tjenester, jf. ekomloven § 3-8 annet ledd.

I henhold til *første ledd* skal tilbyder utarbeide, iverksette og vedlikeholde konkrete planer for sikring av informasjon, informasjonssystemer og styringssystemer. Hvem som regnes som tilbyder fremgår av ekomloven § 3-8 jf. definisjonen i ekomloven § 1-5. Tilbyder kan ikke velge å la være å utarbeide, iverksette og vedlikeholde sikringsplaner, jf. ordlyden *skal*.

Planer for sikring skal utarbeides og vedlikeholdes for den konkrete virksomheten, det er således ikke tilstrekkelig å vise til at moderkonsernet eller et søsterselskap har utarbeidet slike.

Forskriften *første ledd annet punktum* oppstiller hva slike planer for sikring av informasjon, informasjonssystemer og styringssystemer minimum innebærer. Departementet henviser i denne sammenheng generelt til overholdelse av anerkjente standarder for planverk, jf. direktiv 2018/1972 fortalepunkt (94) siste setning, som et minstekrav for sikkerhet.

Forskriften stiller krav til prosedyrer for tilgangsstyring som er metoder for å tildele, endre, slette og føre kontroll med autorisasjon for tilgang til IT-ressurser. Slik tilgangsstyring bør være basert på tjenstlig behov, og kan i praksis skje gjennom bruk av eksempelvis passord, autentisering, tilgangsnivå og brukerroller. Utvikling, testing og opplæring bør separeres for å redusere risiko for uautorisert tilgang eller uønskede endringer. Departementet viser her til viktigheten av gode rutiner for opprettelse og vedlikehold av brukere. Logging av autorisert og uautorisert bruk for drifts- og sikkerhetsformål (klientbasert logging) og nettverksbasert logging for å kunne oppdage datainnbrudd og virus vil være tiltak som innebærer å etterkontrollere informasjonssystemet.

Sikring av informasjons- og styringssystemer innebærer krav til redundans for sentrale elementer i informasjons- og styringssystemer for å ivareta forsvarlig sikkerhet.

Sikkerhetskopiering må anses for å være nødvendig for å sikre at ikke viktig informasjon går tapt. Departementet viser til at sikkerhetskopiering også er i henhold til god bransjepraksis, jf. f.eks. A.12.3 i ISO 27001.

Prosedyrer for vedlikehold og testing vil kunne gi grunnlag for å vurdere effektiviteten av sikkerhetstiltakene.

Det følger av *første ledd in fine* at hensikten med planer for sikring er å sikre vedvarende tilgjengelighet, autentisitet, integritet og konfidensialitet i informasjon, informasjonssystemer og styringssystemer, som ligger til grunn for tilbyders nett og tjenester.

Tilgjengelighet innebærer at tjenester er tilgjengelige. Autentisitet betyr at kommunikasjon og data er opprinnelig og ekte. Integritet innebærer at kommunikasjon og data ikke blir endret utilsiktet eller av uvedkommende for å sikre fullstendighet, nøyaktighet og gyldighet. Med konfidensialitet menes at kommunikasjon og data ikke blir kjent for uvedkommende, men kun at den autoriserte får tilgang.

Etter bestemmelsens *annet ledd* skal tilbyders planer for sikring dokumenteres. Kravet til dokumentasjon innebærer et krav til skriftlighet. Dokumentasjonen skal oppbevares hos tilbyder.

Til § 9-5 Beredskapsplanlegging og øvelser

Ny forskriftsbestemmelse om beredskapsplanlegging og øvelser er gitt med hjemmel i ekomloven § 3-8 sjette ledd, og utdyper kravet til systematisk oppfølging og forsvarlig sikkerhet i nett og tjenester, jf. ekomloven § 3-8 annet ledd. Bestemmelsen er en videreføring av gjeldende ekomforskrift § 8-2 beredskapsplaner og øvelser mm., men bestemmelsen har fått ny struktur. Risiko- og sårbarhetsvurderinger, som er tatt ut av bestemmelsen, har fått en egen forskriftsbestemmelse i ekomforskriften § 9-2. Nytt i ekomforskriften § 9-5 er at ordlyden i større grad vektlegger dokumentasjon av beredskapsplaner og plan for gjennomføring av beredskapsøvelser. Departementet viser til at dokumentasjon innebærer et krav til skriftlighet. Nytt er også at forsvarlig sikkerhet skal ivaretas i elektroniske kommunikasjonstjenester i tillegg til elektronisk kommunikasjonsnett.
I bestemmelsens *annet ledd* fremgår det at tilbyder jevnlig skal gjennomføre beredskapsøvelser med det innhold og omfang som er nødvendig for å vedlikeholde og utvikle virksomhetens kompetanse og evne til å håndtere uønskede hendelser. Virksomheten må ha et oppdatert beredskapsplanverk tilpasset virksomhetens art og omfang. Beredskapsplanleggingen skal bl.a. omfatte forberedelser til tiltak det kan bli nødvendig å iverksette.
Ekomforskriften § 9-5 tredje ledd er en videreføring av gjeldende ekomforskrift § 8-2 tredje ledd, og setter krav til at tilbyder skal delta i beredskapsøvelser arrangert av myndigheten.

Til § 9-6 Sikkerhetsrevisjon

Bestemmelsen er ny, og gjennomfører ekomdirektivet artikkel 41 nummer 2. Den gir grunnlag for å kunne vurdere om sikkerhetskravene i ekomloven § 3-8 med tilhørende forskrift er oppfylt, departementet viser til omtalen i kapittel 3.2.2.
Bestemmelsen hjemler at tilsynsmyndigheten i særlige tilfeller kan pålegge tilbyder av offentlig elektronisk kommunikasjonsnett eller tilbyder av offentlig tilgjengelig elektronisk kommunikasjonstjeneste å foreta en sikkerhetsrevisjon av hele eller deler av virksomheten. Ordlyden "særlige tilfeller" er valgt for å poengtere at sikkerhetsrevisjon ikke skal ilegges regelmessig eller erstatte myndighetens eget tilsyn. Sikkerhetsrevisjon vil kunne være aktuelt der myndigheten allerede har innhentet opplysninger eller gjennomført tilsyn, men hvor dette ikke har vært tilstrekkelig for å fullstendig besvare nødvendige spørsmål om virksomhetens sikkerhet.
Pålegg fra myndigheten skal regnes som en prosessledende avgjørelse, og ikke som et enkeltvedtak. Det gjøres med andre ord unntak fra forvaltningslovens regler. Unntaket gjøres med hjemmel i forvaltningsloven § 1.
En sikkerhetsrevisjon kan bli pålagt for hele eller deler av virksomheten, f. eks. for deler av virksomheten som trenger ytterligere granskning eller som er spesielt sårbare. Eksempler kan være behov for å teste sikkerheten til internettilgang til viktige noder eller fasiliteter, eller tiltak som er iverksatt for å løse sårbarheter i kommunikasjonsprotokoller.
Etter bestemmelsens *annet punktum* skal revisjonen foretas av en uavhengig, kvalifisert tredjepart, og resultatet av revisjonen skal sendes Nasjonal kommunikasjonsmyndighet. Det forutsettes at revisjonsrapporten sendes så snart den foreligger. Med uavhengig, kvalifisert tredjepart legger departementet opp til at det utførende revisjonsfirmaet ikke på noen måte er nært forbundet med tilbyderen. Firmaer med sertifisering innen revisjon vil fylle vilkåret om kvalifisert, men også andre kan være kvalifisert, eksempelvis en offentlig myndighet.

Etter *tredje punktum* skal tilbyderen dekke alle kostnader ved revisjonen. Dette omfatter både direkte og indirekte kostnader.
Etter *fjerde punktum* skal pålegget regnes som en prosessledende avgjørelse. Dette er et unntak fra forvaltningsloven bestemmelser om enkeltvedtak. Begrunnelsen for å anse dette som en prosessledende avgjørelse, er at forvaltningslovens bestemmelser om klagerett på en beslutning om å iverksette en sikkerhetsrevisjon vil kunne medføre at et tilsyn trekker unødvendig ut i tid. Det forutsettes imidlertid likevel at pålegget om sikkerhetsrevisjon begrunnes i det enkelte tilfellet.
De nærmere vurderinger som ligger til grunn for bestemmelsen er gitt i kapittel 3.2.2.

Til § 9-7 Oppfølgingsplikt

Forslag til forskriftsbestemmelse om oppfølgingsplikt utdyper kravet til systematisk oppfølging og forsvarlig sikkerhet i nett og tjenester, jf. ekomloven § 3-8 annet ledd. Bestemmelsen pålegger tilbyder å følge opp at leverandører, entreprenører og andre kontraktører som utfører arbeid på virksomhetens vegne etterlever sikkerhetskrav fastsatt i eller med hjemmel i lov. Dette gjelder også ved tjenesteutsetting utenfor Norge. Om denne problemstillingen viser departementet til merknaden til § 9-3. Men også kontraktører og underleverandører som driver sin virksomhet i Norge og som leverer tjenester til tilbyder, er det viktig at tilbyder følger opp at etterlever sikkerhetskravene. Tilbyderen har således en plikt til å følge opp sikkerhet gjennom hele verdikjeden når man setter ut arbeid på oppdrag.

Til § 9-8 Varsel

Bestemmelsen viderefører, utvider og presiserer tilbydernes varslingsplikt.
I *første ledd* foreslås en utvidelse av tilbyders varslingsplikt til å omfatte sikkerhetshendelser som har medført eller kan medføre brudd på tilgjengelighet, autentisitet, integritet eller konfidensialitet. Gjeldende bestemmelse omfatter kun varsling om brudd på tilgjengelighet. I henhold til ekomdirektivet artikkel 40 nummer 2 skal medlemsstatene sikre at tilbydere varsler myndighetene om sikkerhetshendelser. Direktivets definisjon av sikkerhetshendelse er ny og omfatter brudd på både tilgjengelighet, autentisitet, integritet og konfidensialitet. Varslingen skal i henhold til direktivet skje uten ugrunnet opphold. Utvidelsen av varslingsplikten er dermed i tråd med ordlyden i direktivet. Bestemmelsen fastsetter i tillegg at varsling skal skje senest innen en halv time etter at tilbyder er kjent med hendelsen, og innfører dermed en absolutt grense for hvor lenge tilbyder kan vente med å varsle. Direktivet fastslår at det ved vurderingen av når det skal varsles skal ses hen til konsekvenser for funksjoner i nett og tjenester, innvirkning på økonomiske og samfunnsmessige aktiviteter, antall berørte kunder, geografisk omfang og, varighet. Dette vil være momenter tilbyderne skal vurdere ved hendelser som kan medføre sikkerhetsbrudd og dermed varsling.
Annet ledd presiserer terskler for varsling om brudd på tilgjengelighet. Tilbydere skal varsle ved ustabilitet eller bortfall av nett eller tjenester for mer enn halvparten av kundene eller basestasjonene i en kommune eller alternativt på et tettsted med mer enn 20 000 innbyggere. Myndighetene skal også varsles ved ustabilitet eller bortfall av nett eller tjenester for mer enn ti prosent av kundemassen eller basestasjonene på landsbasis. Det skal også varsles ved ustabilitet eller bortfall av nett og tjenester for brukere med ansvar for liv og helse, eller i situasjoner som innebærer høy risiko for tap av liv og helse, for eksempel ved ekstremvær, flom og jordras.

Tersklene i bestemmelsens *annet ledd* har tatt utgangspunkt i tersklene gitt i Nasjonal kommunikasjonsmyndighets vedtak om varsling av 2. februar 2016.
I bestemmelsens *tredje ledd* foreslås en presisering av krav til innhold i varselet. Varsel til myndigheten skal som et minimum inneholde opplysninger om hendelsens årsak, konsekvenser for funksjoner i nett og tjenester, innvirkning på økonomiske og samfunnsmessige aktiviteter, geografisk omfang, antall berørte kunder, varighet, tiltak og tilbyders kontaktinformasjon. Krav til innhold er utledet av oppstillingen i ekomdirektivet artikkel 40 nummer 2 som fastslår hvilke momenter som skal vektlegges i vurderingen av hendelsens alvorlighetsgrad. Momentene som inngår i vurderingen av hendelsens alvorlighetsgrad bør gjenspeiles i terskler for varsling og innhold i varsel til myndighetene.
I henhold til bestemmelsens *fjerde ledd* skal tilbyderen også informere om aktuelle avhjelpende tiltak som bidrar til at kunden kan sikre sin egen kommunikasjon.
I bestemmelsen *femte ledd* er det foreslått inntatt en varslingsplikt overfor tilbyderens egne kunder om planlagte bortfall av nett eller tjenester. Ved å varsle egne kunder om planlagte bortfall, f. eks. i forbindelse med vedlikeholdsarbeid på infrastruktur og systemer, kan kundene iverksette egne tiltak for å sikre sin kommunikasjon og dermed redusere konsekvensene av planlagt bortfall av nett eller tjenester.
I bestemmelsens *sjuende ledd* videreføres myndighetens kompetanse til å fastsette prosedyrer for varsling.

Til § 9-9 Nasjonal autonomi

Forslaget til bestemmelse er en videreføring av gjeldende ekomforskriften § 8-3. Bestemmelsen er ikke i kraft, men kan tre i kraft når departementet bestemmer.
Nasjonal autonomi innebærer at tilbydere av elektroniske kommunikasjonsnett og -tjenester i en krise- og beredskapssituasjon skal ha evne til å drifte og vedlikeholde tjenestetilbudet, med personell og tekniske løsninger som er lokalisert på norsk territorium.
Den omfattende internasjonaliseringen utfordrer både evnen og muligheten til å kunne innføre nasjonal autonomi. Likevel tilsier samfunnets stadig økende avhengighet av elektroniske kommunikasjonsnett og -tjenester, og endringer i det sikkerhetspolitiske landskapet, at en viss grad av nasjonal autonomi er viktig for Norges beredskapsevne. Elektronisk kommunikasjon er så grunnleggende viktig for landet, at det må være mulig å innføre nasjonal kontroll med denne infrastrukturen i visse alvorlige situasjoner.
De kommersielle ekomnettene får også en stadig viktigere rolle i totalforsvaret. Dersom de nødvendige ressursene for å sikre de kritiske kommunikasjonstjenestene ikke kan underlegges nasjonal lovgivning og kontroll i en krise- eller krigssituasjon, kan dette få svært alvorlige følger for den nasjonale styringsevnen.
Bestemmelsen er ikke til hinder for at tilbyder i daglig drift kan benytte ressurser utenfor norsk territorium for drift og tjenesteproduksjon, men tilbyder må ha beredskap for å kunne opprettholde nødvendig nasjonalt tjenestetilbud uten bruk av ressurser lokalisert i andre land i det tilfelle at bestemmelsen trer i kraft. Bestemmelsen gir myndigheten mulighet til å pålegge tilbyder å iverksette nasjonal autonom drift. Slikt pålegg kan bare gis i krise- og beredskapssituasjoner. Det vises også til forskriftens § 8-4 hvor det fremgår at tilbyder plikter å informere egne kunder dersom trafikkdata rutes over landegrensene.

Til § 9-10 Prioritering av tjenestetilbud

Bestemmelsen er en videreføring av gjeldende ekomforskrift § 8-4 og regulerer prioritering av tjenestetilbud ved driftsstans.
Bestemmelsen stiller krav til hvordan ressurser skal utnyttes i situasjoner hvor det blir knapphet på disse. Dette kan være tilfeller hvor det blir kapasitetsbegrensninger i nettet i forbindelse med driftsstans og man må gi prioritet for noe trafikk fremfor annen trafikk. Det kan også være situasjoner hvor brukere har mistet sitt tjenestetilbud og hvor det blir snakk om prioritering av rekkefølgen brukere skal få tilbake sitt tjenestetilbud.
Av første ledd fremgår det at i gjenopprettingsfasen etter utfall plikter tilbyder å prioritere hensynet til sluttbrukere med ansvar for liv og helse, foran kommersielle hensyn.
Sluttbrukere med ansvar for liv og helse betyr i utgangspunktet nødetatene, men også sykehus, legevakt og andre akuttmedisinske instanser kan være aktuelle.
Av annet ledd følger det at myndigheten i særlige tilfeller kan pålegge tilbyder å prioritere andre viktige samfunnsaktører i gjenopprettingsfasen. Det kan være aktuelt i situasjoner hvor offentlige interesser tilsier en annen rekkefølge i gjenopprettingen.
Plikter som fremgår av forskrift om prioritet i mobilnettene faller utenfor hva som reguleres i denne bestemmelsen.

Til § 9-11 Planer for konkursvern

Forslag til bestemmelse viderefører gjeldende ekomforskrift § 8-6. Presiseringen av tilbyderbegrepet i forhold til gjeldende rett følger av at definisjonen av elektronisk kommunikasjonstjeneste er endret, jf. § 1-5 nummer 4. Endringen innebærer ingen materiell endring og tilbyderne som er pliktsubjekter etter bestemmelsen er de samme som før endringen.
Formålet med bestemmelsen er å rettlede tilbyderne om gjennomføring av ekomloven § 2-12 om sikring av fortsatt levering ved konkurs m.v. Bestemmelsen inneholder en opplisting av minimumsinformasjonen som skal inngå i tilbyders planer for sikring som pålegges etter § 2-12.
Det fremgår av annet ledd at Nasjonal kommunikasjonsmyndighet kan frita fra plikten til å utarbeide planer for konkursvern i særlige tilfeller.

Til § 9-12 Gjennomføring av forordning om ENISA

Bestemmelsen viderefører gjeldende ekomforskrift § 8-7.
Europaparlamentet og rådet har vedtatt en ny forordning 2019/881 om ENISA (den europeiske unions byrå for nett- og informasjonssikkerhet) og om cybersikkerhetssertifisering av informasjons- og kommunikasjonsteknologi. Denne forordningen opphever forordning nr. 526/2013. Norske myndigheter er medlem uten stemmerett i ENISA.
Den nye forordningen er ennå ikke innlemmet i EØS-avtalen. Departementet foreslår derfor to alternative bestemmelser. Den ene viderefører inkorporeringen av ENISA forordningen forordning (EU) nr. 526/2013 fordi denne fremdeles er en del av EØS-avtalen, og det andre alternativet foreslår å inkorporere den ne forordningen som har erstattet denne og som er EØS- relevant.
Ordlyden i alternativ 2 foreslås med andre ord endret i tråd med den ny forordningen for det tilfellet at forordningen innlemmes i EØS-avtalen før den foreslåtte forskriften trer i kraft.

Den nye forordningen innebærer at ENISA får et styrket budsjett og et styrket og permanent mandat. ENISA vil få en større rolle i EUs cybersikkerhetslandskap. Organisering og styring av ENISA forandres i liten grad.
ENISA skal etter anmodning kunne bistå medlemslandene med grenseoverskridende hendelseshåndtering, herunder blant annet rådgivning, analyse og tekniske undersøkelser. ENISA skal også særlig bistå og legge til rette for medlemslandenes kapasitetsutbygging, operativt samarbeid og forskning og utvikling.
Forordningen etablerer også et felleseuropeisk rammeverk for sikkerhetssertifisering av IKT-produkter, tjenester og prosesser for å understøtte det digitale indre markedet. ENISA får oppgaver i forbindelse med å utvikle og administrere dette rammeverket. Forordningen innebærer at det skal utpekes en tilsynsmyndighet for sertifiseringen i hvert land.

Til kapittel 10 Private elektroniske kommunikasjonsnett

Til § 10-1 Tilkobling til private elektroniske kommunikasjonsnett

Det er fremdeles behov for å regulere tilgang til privateide elektroniske kommunikasjonsnett for å sikre kompatibilitet til de ordinære elektroniske kommunikasjonsnettene og sikre konkurransen om levering av tjenester. Forslag til § 10-1 viderefører de konkurransemessige aspektene av gjeldende ekomforskrift § 9-1.
I *første ledd* defineres private elektronisk kommunikasjonsnett som elektronisk kommunikasjonsnett som eies av bedrifter, eiere av næringsbygg, en eller flere eiere i næringsparker og eiere av ulike boligsammenslutninger, og dekker et område fra tilkoblingspunkt i et større elektronisk kommunikasjonsnett og frem til nettermineringspunktet. Det er gjerne ordinære tilbydere av elektronisk kommunikasjon som eier eller disponerer nettene som private elektroniske kommunikasjonsnett kobler seg til. Et privat elektronisk kommunikasjonsnett kan for eksempel være et nett som en bedrift har bygget ut til eget bruk mellom forskjellige geografiske lokasjoner eller et nett som et borettslag har bygget ut til hver enkelt boenhet/beboer. Det er slike private nett som skal reguleres etter bestemmelsen her. Det avgrenses imidlertid mot nett innad i et privat hjem som en nedre grense. Ettersom definisjonen av nettermineringspunkt og offentlig elektronisk kommunikasjonspunkt gjør at det offentlige elektroniske kommunikasjonsnettet nærmest går helt til sluttbrukers terminal, vil ikke definisjonen av privat elektronisk kommunikasjonsnett utfordre disse på noen måte, men fungere som en logisk definisjon av slike nett som er privateide og hvor eierne ikke vanligvis er profesjonelle i relasjon til elektronisk kommunikasjon. Av konkurransemessige hensyn er det nødvendig at slike private elektroniske kommunikasjonsnett er kompatible med resterende offentlige elektroniske kommunikasjonsnett, derfor skal det, om mulig, sikres at tilkoblingen skjer gjennom ett fysisk tilkoblingspunkt. Terskelen for at slik tilkobling gjennom ett punkt ikke er mulig, skal være høy.
Tilbyder av offentlig elektronisk kommunikasjonsnett skal etter *annet ledd* informere eier av privat elektronisk kommunikasjonsnett om muligheten til tilkobling. Med lokalt område menes for eksempel boligsammenslutning, næringspark og nabolag.
Tredje ledd slår fast at selve tilkoblingspunktet skal utformes slik at det enkelt kan skiftes signalleverandør. Formålet med bestemmelsen er at grensesnittet mellom privat elektronisk kommunikasjonsnett og annet offentlig elektronisk kommunikasjonsnett fungerer slik at det er raskt og enkelt å bytte tjenesteleverandør på et senere tidspunkt. Videre skal tilkoblingen gjøres på en slik måte at det ikke brukes mer kapasitet enn nødvendig. Dette er også av

hensyn til at så mange tilbydere som ønskelig kan levere tjenester i det private elektroniske kommunikasjonsnettet.

Til § 10-2 Tjenestetilbud i privat elektronisk kommunikasjonsnett

Forslag til § 10-2 viderefører gjeldende ekomforskrift § 9-2.
Etter *første ledd* skal privat elektronisk kommunikasjonsnett anlegges slik at tjenester fra ulike tilbydere kan føres frem til bruker. Dette innebærer at private elektroniske kommunikasjonsnett ikke skal utformes på en måte som vanskeliggjør, enten teknisk eller økonomisk, at andre tjenestetilbydere kobler seg til tilkoblingspunktet.
Etter *annet ledd* er det eier av det private elektronisk kommunikasjonsnettet som har ansvar for at de tjenestene som leveres i nettet har samme kvalitet som de som blir levert ved tilkoblingspunktet mellom privat elektronisk kommunikasjonsnett og offentlig elektronisk kommunikasjonsnett. Eier har også ansvar for at sluttbrukere i det private elektroniske kommunikasjonsnettet får tilgang til leveringspliktige tjenester og funksjoner.

Til § 10-3 Levering av signaler til andre nett

Forslag til § 10-3 viderefører gjeldende ekomforskrift § 9-3. Departementet viser for øvrig til Menons uttalelse om standardisering i utredningen til lovforslaget § 10-3 om tilgang til nett og fasiliteter i og utenfor bygninger.

Til § 10-4 Taushetsplikt og sikring

Bestemmelsen viderefører gjeldende forskrift i § 9-4.
Taushetsplikt for tilbydere og installatører følger av ekomloven § 3-2. For å sikre at det er helt klart at eiere av private elektroniske kommunikasjonsnett er bundet av taushetsplikt foreslås dette presisert i bestemmelsen. Det er hensiktsmessig med en slik plikt fordi eier av slike nett vil kunne ha kontroll på et nett med betydelig utstrekning. Det er derfor viktig at også eiere av slike nett er pålagt taushetsplikt og sikring. Med eiere av private elektroniske kommunikasjonsnett menes elektronisk kommunikasjonsnett som eies av bedrifter, eiere av næringsbygg, en eller flere eiere i næringsparker og eiere av ulike boligsammenslutninger, og dekker et område fra tilkoblingspunkt i et større elektronisk kommunikasjonsnett og frem til netterminering spunktet.
I *annet ledd* presiseres at det gjelder krav til kommunikasjonsvern også for private nett.

Til kapittel 11 Tilsyn, klage m.m.

Til § 11-1 Brukerklagenemnda for elektronisk kommunikasjon

Bestemmelsen viderefører gjeldende forskrift § 10-1, med enkelte endringer. Blant annet endres begrepet telefontjeneste i første ledd til nummerbasert person-til-person kommunikasjonstjeneste i samsvar med ny definisjon av begrepet elektronisk kommunikasjonstjeneste. Det er tatt inn en henvising til at nemnda også kan behandle saker etter § 2-7, det vil si klager knyttet til fakturering av fellesfakturert tjeneste som leveres over elektronisk kommunikasjonsnett.
Etter *annet ledd* har nye tilbydere en plikt å melde fra til Brukerklagenemnda så snart de tilbyr relevante tjenester som faller inn under første ledd.

I henhold til *tredje ledd* skal tilbyder skriftlig informere sluttbrukere om sluttbrukers rett til å klage til Brukerklagenemnda. En slik plikt bidrar til gi klagen en totrinnsbehandling. Klageadgangen til Brukerklagenemnda blir således subsidiær.
At klageadgangen til Brukerklagenemnda skal være subsidiær er eksplisitt hjemlet i bestemmelsens *fjerde ledd*. Begrunnelsen for dette er at nemnda ikke skal bruke tid på klager som kunne vært løst på en mindre ressurskrevende måte. Dette innebærer at tilbyderen selv først bør behandle klagen. Det er likevel oppstilt to unntak for når Brukerklagenemnda kan behandle klage uten forutgående behandling hos tilbyder. Unntakene gjelder der tilbyder ikke har informert sluttbruker om forventet behandlingstid innen to uker etter mottak av klagen, og der tilbyder ikke har gitt endelig svar innen rimelig tid. Rimelig tid må vurderes konkret og utvikles etter Brukerklagenemndas nærmere praksis. Det følger av Brukerklagenemndas hjemmeside at dette veiledende regnes til å være to til tre uker.
I *femte ledd* oppstilles en regel om såkalt litispendens som tilsier at saker som behandles i Brukerklagenemnda ikke samtidig skal behandles i de alminnelige domstoler.
Nasjonal kommunikasjonsmyndighet kan etter sjette ledd gi nærmere bestemmelser om Brukerklagenemndas organisering og saksbehandling Dette kan for eksempel gjelde Brukerklagenemndas vedtekter.
I *sjuende ledd* vises det til at Brukerklagenemnda skal oppfylle krav etter lov om klageorganer for forbrukersaker som gjennomfører direktiv 2013/11/EU og forordning (EU) nr. 524/2013).

Til § 11-2 Finansiering av Brukerklagenemnda

Bestemmelsen omhandler Brukerklagenemndas finansiering, og viderefører i sin helhet gjeldende § 10-1a.
Brukerklagenemnda skal finansieres av tilbyderne som deltar i ordningen. Etter *første ledd* skal slike bidrag både baseres på et årlig grunnbeløp og klagegebyr per klage behandlet av Brukerklagenemnda. Per i dag operer Brukerklagenemnda med en ordning der tilbyder betaler et klagegebyr per sak som gjelder den relevante tilbyderen, i tillegg til grunnbeløpet. En slik fordeling sikrer en stabil finansiering samtidig som tilbydere med et høyere antall saker til behandling i nemnda betaler mer.
Brukerklagenemnda kan etter *annet ledd* differensiere grunnbeløpet etter første ledd, første punkt for tilbydere med høy relevant omsetning. Dette innebærer at store tilbydere kan betale en høyere andel av finansieringen.
Etter *tredje ledd* skal brukerklagenemnda utarbeide og vedta budsjett for kommende år. Dette skal gjøres før første desember, og baseres på en forsvarlig drift. Nasjonal kommunikasjonsmyndighet skal motta budsjettet til orientering.
I *fjerde ledd* er det regler om klagegebyrene, herunder at disse skal stå i forhold til budsjetterte utgifter. I tilfeller der det er nødvendig med ekstra innbetalinger i løpet av året kan styret i brukerklagenemnda kreve tilleggsinnbetalinger. Departementet forutsetter at eventuelle tilleggsinnbetalinger normalt skal annonseres i tide til at tilbyderne kan budsjettere disse inn i kommende budsjett.

Til § 11-3 Klagenemnd

Departementet kommer tilbake med forslag til bestemmelse og merknad i egen høring.

Til § 11-3a Klageinstans

Bestemmelsen viderefører gjeldende forskrift § 10-2 i en overgangsperiode inntil ny klageordning er opprettet. Departementet kommer tilbake med en egen høring om ny forskriftsbestemmelse som gir detaljene i ny klageordning.

Til § 11-4 Tilsyn og sanksjoner

Bestemmelsen viderefører gjeldende forskrift § 10-3 med enkelte endringer. Bestemmelsen fremgår av loven, og er hovedsakelig foreslått i forskriften av pedagogiske grunner.
I *første ledd* fremkommer det at Nasjonal kommunikasjonsmyndighet skal føre tilsyn med gjennomføringen av forskriften. Det henvises videre til ekomlovens sanksjonsbestemmelser.
I *annet ledd* er det en opplisting av de relevante bestemmelser i forskriften der Nasjonal kommunikasjonsmyndighet kan pålegge overtredelsesgebyr. Overtredelsesgebyr kan ilegges både foretak og fysiske personer.

Til § 11-5 Utmåling av overtredelsesgebyrets størrelse

Bestemmelsen viderefører i hovedsak gjeldende forskrift § 10-3a, men foreslås endret som følge av at skyldkravet for foretak foreslås endret i loven, departementet viser til merknad til ekomloven § 15-12. Fysiske personer kan bare ilegges overtredelsesgebyr for forsettlige eller uaktsomme overtredelser. Foretak kan ilegges overtredelsesgebyr når overtredelsen er begått av noen som har handlet på vegne av foretaket, selv om ingen enkeltperson har utvist skyld.
Bestemmelsens *første ledd* viser til at det ved utmåling av overtredelsesgebyr skal legges særlig vekt på overtredelsens grovhet, varighet, utvist skyld og foretakets omsetning.
Bestemmelsens annet ledd lister opp relevante momenter ved vurderingen av overtredelsens grovhet (overtredelsens art, foretakets gevinst, overtredelsens faktiske innvirkning på markedet, størrelsen på markedet og om overtrederen har hatt en ledende eller passiv rolle i overtredelsen). Både subjektive og objektive forhold er relevante.
Når overtredelsens grovhet skal vurderes på bakgrunn av subjektive forhold, vil overtrederens motiv eller insentiv for overtredelsen et relevant moment. Overtredelsens art, herunder måten overtredelsen er begått på, kan også utgjøre et relevant moment. Om overtrederen har hatt en ledende eller passiv rolle i overtredelsen, er videre en sentralt del av denne vurderingen.
I den objektive grovhetsvurderingen vil overtredelsens faktiske innvirkning på markedet og størrelsen på det berørte markedet, utgjøre sentrale momenter.
Foretakets gevinst er et annet sentralt moment i grovhetsvurderingen. En faktisk gevinst hos overtrederen, utgjør et objektivt forhold i grovhetsvurderingen. En potensiell gevinst vil derimot kunne vurderes i sammenheng med overtredelsens art og størrelsen på markedet.
Ved utmålingen skal også det legges særlig vekt på overtredelsens varighet. Dersom overtredelsen har pågått i lang tid bør dette vektlegges i skjerpende retning.
Utvist skyld er et annet relevant moment i utmålingen. En forsettlig eller grov uaktsom handling, tilsier en høy grad av utvist skyld og bør vektlegges i skjerpende retning. Det understrekes at momentet utvist skyld også vil kunne gjelde ved utmålingen av overtredelsesgebyr som ilegges et foretak.
Overtredelsesgebyrets størrelse
Ved utmålingen skal det også legges særlig vekt på foretakets omsetning.
Overtredelsesgebyr kan ilegges inntil 5 prosent av foretakets omsetning. Det er foretakets

omsetning i Norge som er utgangspunktet for beregningen av overtredelsesgebyrets størrelse. Videre skal det beregnes omsetning for hele foretakets virksomhet og ikke bare for det berørte markedet. Dersom foretaket er en del av et større konsern, kan det innenfor overtredelsesgebyret maksimalgrense tas hensyn til konsernets totale omsetning. Overtredelsesgebyrets størrelse vil på den måten kunne justeres opp. Dette kan være tilfellet der konsernets økonomi gir grunn til å tro at overtredelsesgebyret ikke vil ha en tilstrekkelig avskrekkende effekt på overtrederen.
Prosentgrensen er en maksimalgrense, og er ikke ment å være retningsgivende for overtredelsesgebyrets størrelse. Overtredelsesgebyret utmåles etter en konkret vurdering i den enkelte sak og opp mot ovennevnte momenter (overtredelsens grovhet, overtredelsens varighet, utvist skyld og foretakets omsetning). Overtredelsens grovhet er et sentralt moment i vurderingen.
Andre momenter som kan påvirke utmålingen av overtredelsesgebyr er opplistet i bestemmelsens tredje ledd. Dette er momenter som kan vektlegges i både skjerpende og formildende retning.

Til § 11-6 Dispensasjon

Bestemmelsen gir Nasjonal kommunikasjonsmyndighet generell kompetanse til å dispensere fra de enkelte bestemmelser i forskriften, og viderefører gjeldende forskrift § 10-4.
Ordlyden tilsier at terskelen for å gi dispensasjon fra bestemmelser i forskriften skal være høy, og kun benyttes unntaksvis. Det skal foretas en konkret vurdering i hver enkelt sak om vilkåret om «særlige tilfeller» eller «anvendelse virker urimelig» er oppfylt.
Søknad om dispensasjon kan gjelde midlertidig eller varig dispensasjon for regler i forskriften. Dette kan for eksempel særlig være aktuelt med midlertidig dispensasjon ved implementering av nye bestemmelser og tilhørende krav i forskriften. Etter bestemmelsen skal Nasjonal kommunikasjonsmyndighet først vurdere om dispensasjon kan gis, for så å vurdere om dispensasjon bør gis, jf. «kan». Det kan settes vilkår for å gi dispensasjon. Dette foreslås synliggjort i bestemmelsens ordlyd.

Til § 11-7 Prøvedrift

Bestemmelsen viderefører gjeldende forskrift § 10-5. I forbindelse med utprøving og utvikling av elektronisk kommunikasjonsnett eller elektroniske kommunikasjonstjenester kan det i noen tilfeller være hensiktsmessig å kunne unnta prøvedriften fra bestemmelser etter forskriften. Bestemmelsen er ment som en ren unntaksbestemmelse, og det vil normalt ikke være aktuelt å innvilge unntak fra forskriftens bestemmelser for lengre tidsperioder. Nasjonal kommunikasjonsnett kan ved slik tillatelse stille vilkår for unntaket, herunder om krav til utforming, sikkerhet m.m.
Bestemmelsens *andre ledd* inneholder krav til søknaden, Nasjonal kommunikasjonsmyndighet kan også kreve flere opplysninger ved behandling av søknaden. I etterkant av prøvedriften skal det sendes en rapport til Nasjonal kommunikasjonsmyndighet.

Til kapittel 12 – Avsluttende bestemmelser

Til § 12-1 Endringer i andre forskrifter

Gjeldende forskrift om elektroniske kommunikasjonsnett- og tjenester foreslås opphevet når den nye forskriften om elektronisk kommunikasjonsnett- og tjenester trer i kraft. Forskrift om

konsesjon for tilbydere som har fått tillatelse til bruk av frekvenser etter teleloven kapittel 5 til etablering og drift av samfunnsviktige telenett er ikke lengre i bruk og foreslås opphevet. I tillegg foreslås en rekke forskrifter endret som følge av endringer i ekomregelverket.

Til § 12-2 Ikrafttredelse

Departementet tar sikte på at forskriften trer i kraft sammen med ny ekomlov. Det vil bli gjort unntak for ny klageordning som vil tre i kraft når den er på plass.
Det vil bli gitt utsatt ikrafttreden for § 2-16 annet og tredje ledd om likeverdig tilgang for sluttbrukere med nedsatt funksjonsevne. For rettigheter som følger av tilgjengelighetsdirektivet tar sikte på at disse rettigheten trer i kraft 28 juni 2025. Dette vil gi tilbyderne en mulighet til å få tjenestene på plass.
Departementet kommer tilbake med ikraftsettelse på et senere tidspunkt, når det er blitt klart om og når direktivet tas inn i EØS-avtalen.

Til § 12-3 Overgangsbestemmelse

Det er behov for overgangsordninger for å sikre en sømløs overgang mellom gjeldende og nytt regelverk.