

Høringsnotat - forslag til endringer i ekomforskriften - IP-adresser

1. Innledning

Forslag til endringer i ekomforskriften er ment å utfylle bestemmelsene om plikt for ekomtilbydere til å lagre og utlevere IP-adresser i ekomloven §§ 2-8 a og 2-8 b. Plikten til å lagre IP-adresser ble vedtatt ved en lovendring til ekomloven 18. juni 2021 nr. 131, jf. Prop.167 L (2020-2021). Bestemmelsene i loven er et verktøy i politiets kriminalitetsbekjempelse ved etterforskning av alvorlig kriminalitet.

Tilbyder av elektronisk kommunikasjonsnett som anvendes til offentlig elektronisk kommunikasjonstjeneste og tilbyder av slik tjeneste skal etter ekomloven § 2-8 a lagre de opplysninger som er nødvendige for å identifisere abonnenter. Lagringsplikten gjelder uavhengig av aksessteknologi, og inkluderer tilbydere av internettaksess over både fast- og mobilnett.

Identifiseringen av abonnenter skal skje med utgangspunkt i offentlig IP-adresse og tidspunkt for kommunikasjonen, og også portnummer der det er tilgjengelig dersom samme offentlige IP-adresse er tildelt flere abonnenter samtidig. Det skal ikke lagres destinasjonsinformasjon. Informasjonen skal lagres i 12 måneder fra kommunikasjonen avsluttes, uavhengig av om abonnentens kundeforhold er avsluttet før utløpet av lagringspliktig periode. Etter langringspliktig periode er avsluttet, inntretr hovedregelen om sletteplikt.

Det er videre en plikt til å utlevere slik informasjon til politi- og påtalemyndighet når det er nødvendig for å etterforske alvorlig kriminalitet, jf. ekomloven § 2-8 b. Alvorlig kriminalitet anses å være handlinger med strafferamme på 3 år eller mer, eller handlinger som omfattes av straffebestemmelsene som er listet opp i § 2-8 b.

Lagringsplikten kan gi grunnlag for å identifisere abonnenten, ikke den faktiske brukeren. Det vil være informasjon om tilknytning mellom abonnent og IP-adresse, sammenholdt med ytterligere etterforskningsskritt som eventuelt kan indentifisere faktisk bruker.

Det fremgår også av lovbestemmelsene at tilbydere skal dekke investerings- og driftskostnader som påløper for å oppfylle lagringsplikten. Staten skal dekke kostnader som påløper i forbindelse med utlevering av informasjon.

Bestemmelsene i ekomloven §§ 2-8 a og b trådte i kraft 1. januar 2022. Siden disse regulatoriske endringene krever utvidelser, endringer og utvikling i tilbydernes systemer, er det vedtatt en overgangsordning for å gi tilbyderne tilstrekkelig tid til å gjennomføre nødvendige endringer i sine tekniske og administrative løsninger. De nye reglene skal være operasjonalisert hos tilbyderne senest 1. januar 2023.

2. Mandat og oppdrag knyttet til implementering av reglene om IP-lagring

Kommunal- og distriktsdepartementet og Justis- og beredskapsdepartementet gav 12. oktober 2021 hhv. Nasjonal kommunikasjonsmyndighet (Nkom) og Politidirektoratet (POD) et mandat for å legge til rette for implementeringen av reglene om IP-lagring i ekomloven.

Kripos har i etterkant overtatt POD sin rolle. Av mandatet fremgikk det at de to etatene skulle:

- Sikre god og ensartet regelforståelse hos aktørene og politiet.
- Sikre at tilbydersiden utvikler nødvendige løsninger og systemer for effektiv implementering av de nye reglene om IP-lagring, herunder vurderer innføringen av automatiserte prosesser
- Avklare om det er grunnlag/interesse blant tilbydere for felles løsninger for lagring og utlevering av informasjon, og hvordan det eventuelt kan tilrettelegges for slike løsninger
- Understøtte en sentralisert og enhetlig løsning hos politiet for oversendelse av anmodninger, mottak av informasjon, statistikk mv, herunder utforming av anmodningene.
- Sikre nødvendig samarbeid mellom tilbydere og politiet om grensesnitt og rutiner
- Gi innspill til utfyllende forskriftsregulering
- Avklare relevante forhold knyttet til kravene til politiets årsrapportering

Nkom skulle i tillegg utarbeide utkast til forskriftsbestemmelser og høringsnotat som tilrettelegger for gjennomføringen av reglene om IP-lagring.

Arbeidet som er gjort danner grunnlaget for dette høringsbrevet.

3. Behov for utfyllende forskriftsbestemmelser

Det er behov for utfyllende bestemmelser i forskrift blant annet for å operasjonalisere lagringsplikten nærmere, fastsette regler for hvordan informasjonen skal utleveres, fordele merkostnadene som oppstår, og gi nærmere regler for politi- og påtalemyndighetens årlige rapportering. Forskriftshjemlene fremgår av ekomloven § 2-8 a fjerde ledd og § 2-8 b femte ledd.

Som tidligere nevnt i punkt 2 ble Nkom gitt et oppdrag om å utarbeide forslag til forskriftsbestemmelser som tilrettelegger for gjennomføringen av reglene om IP-lagring. Nkom har i perioden fra departementets oppdrag ble gitt, hatt dialog med tilbyder- og politisiden både gjennom fellesmøter og bilaterale møter. Hovedfokuset for møtene har vært tilbydernes implementering av nødvendige interne systemer for logging og lagring, samt dialog om funksjonelle og tekniske behov knyttet til standardisering av datautveksling mellom tilbydere og politi. Møtene har imidlertid også avdekket problemstillinger som det er relevant å vurdere i tilknytning til et behov for utfyllende forskriftsbestemmelser. Departementet mottok et innspill fra Nkom 4. juli 2022.

På nåværende tidspunkt er det ikke ferdige produksjonssatte løsninger for logging og lagring hos tilbyderne eller produksjonssatte løsninger for standardisert datautveksling hos verken tilbyderne eller politiet. Det foreligger ikke praktisk erfaring med gjennomføring av reglene i ekomloven §§ 2-8 a og b, og enkelte regulatoriske behov vil først kunne vise seg senere. Departementet foreslår derfor å utvise en viss forsiktighet med for omfattende og detaljert kravsetting på det nåværende tidspunkt.

På dette grunnlag foreslår departementet at det fastsettes en bestemmelse som presiserer og utfyller krav knyttet til tilbydernes lagrings- og utleveringsplikt etter ekomloven §§ 2-8 a og b, i ekomforskriften. Videre foreslås en bestemmelse som gir nærmere regler om politi- og

påtalemyndigheten sin plikt til årlig rapportering til Nkom knyttet til uthenting av IP-adresser. I tillegg foreslås en mindre justering i ekomforskriften § 10-3 om tilsyn og sanksjoner for å sikre at myndigheten skal kunne pålegge ekomtilbydere overtredelsesgebyr ved brudd på bestemmelsene i forslaget til ny § 7-6 i ekomforskriften. Forslag til forskriftsbestemmelser fremgår av punkt 7. Departementet vil redegjøre nærmere for noen utvalgte temaer i punktene 4 - 6.

4. Standardisering av datautveksling

I Prop. 167 L (2020-2021) er det en ambisjon om at utlevering av lagringspliktig informasjon til politi- og påtalemyndighet skal skje på en mest mulig kostnadseffektiv måte.

Automatisering og forenkling av både uthenting av data i tilbyders systemer og overføringen av opplysningene til politisiden nevnes som eksempler. Det fremgår også av lovproposisjonen at man forventer at antall anmodninger om informasjon fra politiet vil øke betydelig, sammenliknet med volumet knyttet til dagens spørringer etter ekomloven § 2-9 fjerde ledd, jf. tredje ledd. Dette tilsier også at det er behov for å utvikle løsninger for effektiv datautveksling.

Av mandat til Nkom og Politidirektoratet, jf. punkt 2, fremgår det at etatene skal sørge for et samarbeid mellom tilbydere og politiet for å utvikle slike løsninger. I denne forbindelse er det igangsatt et arbeid med å utvikle standardiserte og automatiserte løsninger for datautvekslingen. Kripos, Politiets IKT-tjenester (PIT), Nkom, Telia, Telenor, Altibox, ICE, NextGenTel og Global Connect har deltatt i dialogmøter og PIT har påtatt seg å utvikle forslag til tekniske utvekslingsløsninger.

For å kunne legge til rette for en effektiv datautveksling er det en forutsetning at det utformes standarder for ulike alternativer til spørringer og svar, slik at alle anmodninger fra politiet og svarene fra tilbyderne er like og skåret over samme ledd. Dette inkluderer blant annet standardisering av hvilket innhold de ulike alternative spørringer og svar skal ha, struktur på innholdet og alle nødvendige formater knyttet til innholdet.

Videre må det utvikles løsninger for overføringen av anmodninger og svar. Det legges opp til å utvikle to alternative overføringsmåter med utgangspunkt i Digitaliseringsdirektoratets sine nasjonale fellesløsninger; Maskinporten og ID-porten. Det første alternativet innebærer en maskinell datautveksling ved bruk av API. Det andre alternative tilrettelegger for en med mer manuell behandling. Begge løsninger vil ivareta hensynet til «sikker overføring», gjennom blant annet kryptering, autentisering og autorisasjon.

Det legges videre opp til at man i politiets nye sentraliserte internsystem for spørringer bygger inn en funksjonalitet for å ivareta formkravene i ekomloven § 2-8 b annet ledd. Det legges blant annet opp til at anmodninger ikke kan sendes til tilbyder fra den sentraliserte løsningen med mindre det i forkant deklarerer nødvendig informasjon om aktuelt straffebud, at nødvendighetsvurdering er foretatt mv. Det legges derfor opp til at de individuelle anmodningene som sendes tilbyder fra politiets sentraliserte løsning skal inneholde informasjon om at anmodningen er en «Ekomloven § 2-8 b-sak» og ikke inneholder detaljer om hva saken gjelder, aktuelt straffebud mv. En slik løsning vil begrense distribusjon av sensitive opplysninger samtidig som at hensynet til at formkrav følges og notoritet rundt dette sikres.

For å legge til rette for en effektiv gjennomføring av utleveringsplikten foreslås det å forskriftsfeste et krav om at de standardiserte løsninger for datautveksling skal benyttes så langt mulig. Et slikt krav kan imidlertid først tre i kraft når det pågående standardiseringsarbeidet er ferdigstilt og tilbyderne er gitt tilstrekkelig tid til å implementere løsningene. Forbeholdet om at løsningene skal benyttes «så langt mulig» er ment å ta høyde for de tilfeller der politiets anmodning kommer på annen måte enn via en av de to standardiserte løsningene. I slike tilfeller vil ikke tilbyder kunne benytte en av disse til å besvare anmodningen.

5. Driftskrav knyttet til lagring og utlevering

5.1 Lagring

Når det gjelder generelle krav til hvor og hvordan IP-informasjon skal lagres er dette nærmere beskrevet i Prop. 167 L (2020-2021) kapittel 8.3. Reglene i ekomloven §§ 2-7 og 2-9, om taushetsplikt og vern av kommunikasjon og data i tilbydernes nett og tjenester, omfatter også logging, lagring og utlevering av informasjon som gjøres i medhold av ekomloven §§ 2-8 a og b. I tillegg vil regler om blant annet informasjonssikkerhet i personvernlovgivningen som Datatilsynet forvalter, gjelde. Vurderingen i lovproposisjonen var at det ikke er behov for særlige regler for hvordan og hvor de lagringspliktige dataene lagres utover de overnevnte regelsett. Regelsettene gjelder for tilbydernes virksomhet i dag og bør være godt kjente.

For at formålet med lagringsplikten i ekomloven § 2-8 a skal oppnås, må bestemmelsen forstås slik at den setter kvalitative krav til tilbydernes gjennomføring av logging og lagring. Det vil si at logging og lagring av informasjon må skje med tilstrekkelig kvalitet for at plikten skal anses oppfylt. For å tydeliggjøre dette foreslår departementet å presisere kravene i forskriften om at logget informasjon skal lagres uten ugrunnet opphold og med tilstrekkelig sikring for at lagringspliktig informasjon ikke går tapt. Videre foreslås det en bestemmelse om plikt til å bevare dataintegritet fra informasjon logges til den utleveres. Det foreslås også en klargjøring knyttet til at tidssonen for de lagrede klokkeslett skal angis.

5.2 Utlevering

Når det gjelder behovet for presiseringer av driftskrav knyttet til utleveringsplikten i ekomloven § 2-8 b foreslår departementet en forskriftsbestemmelse om at anmodninger fra politi- og påtalemyndighet skal besvares uten ugrunnet opphold. Videre at tilbyder plikter å sørge for sikker utlevering av etterspurt informasjon og benytte standardiserte løsninger for datautveksling. Vi viser til punkt 4 for en nærmere beskrivelse av bakgrunnen for forslaget om sikker og standardisert datautveksling.

Når det gjelder forslaget om responstid har Nkom innhentet informasjon om hvordan disse spørsmålene er regulert i hhv. Finland og Sverige. I Finland er det ingen regulatoriske krav til responstid når det gjelder anmodninger fra finsk politi i tilsvarende saker. Det er imidlertid utarbeidet et responstidsdokument som en del av operative retningslinjer som er avtalt på frivillig basis mellom politi- og tilbydersiden. Nkom har videre fått opplyst at alle anmodninger sendes fra en sentralisert enhet i det finske politiet (Unit Special operations – Telecommunications unit) og at denne enheten i utgangspunktet kun prosesserer slike anmodninger innenfor normal kontortid. I den grad finske etterforskere har behov for at

anmodninger sendes fra den sentraliserte enheten utover dette, eksempelvis i nødrettssituasjoner, må den sentraliserte enheten i politiet kontaktes særskilt.

I Sverige vil det fra 1. august 2022 gjelde et krav om at all informasjonsinnhenting fra politiet knyttet til teledata skal besvares «uten drøjsmål». Kravet har tidligere vært gjeldende for innhenting av blant annet sanntidsinformasjon. Det har imidlertid vært ønskelig at samme regel for responstid skal tydeliggjøres for all informasjonsinnhenting, også historiske data knyttet til abonnementsinformasjon, herunder IP-adresser.

Utgangspunktet for departementets forslag om at anmodninger skal besvares uten ugrunnet opphold er å sikre at tilbydernes tidsbruk ikke trekker ut i tid, slik at formålet med anmodningen blir «virkningsløs». Dette tilsier at etterspurt informasjon skal gis ut så fort den er tilgjengelig hos tilbyder. På den annen side er det ulik kompleksiteten i politiets anmodninger, noe som tilsier at noen anmodninger kan ta lengre tid å svare ut enn andre. Eksempelvis vil det ved anmodninger knyttet til IP-informasjon hvor tilbyder har benyttet NAT-teknologi (delt IP) ved abonnentens kommunikasjon, kunne være et betydelig informasjonsvolum som skal tilgjengeliggjøres hos tilbyder, som igjen vil påvirke responstiden. Videre vil et eventuelt behov for klargjørende dialog mellom tilbyder og politi før anmodninger kan besvares, også påvirke responstiden, jf. beskrivelse knyttet til behov for kontaktpunkt i punkt 6 nedenfor.

I tillegg til ulikheten i kompleksiteten i anmodninger, vil også det faktum at det er store ulikheter i pliktsubjektenes størrelse/kundemasse måtte vurderes ved utformingen av krav til responstid. Størrelsen på kundemassen vil ha betydning både for totalvolumet av anmodninger tilbyderen kan forvente å få og også skaleringen av en kostnadseffektiv driftsorganisasjon for politisvar, herunder ulikheter i stordriftsfordeler. Idet man ikke ennå har praktisk erfaring med utleveringsplikten etter ekomloven § 2-8 b, herunder bruk av standardiserte løsninger, tilsier dette at et regulatorisk krav om responstid må utformes med tilstrekkelig fleksibilitet for å ivareta de overnevnte ulikheter.

Videre vil graden av «servicenivå» også være direkte avgjørende for uthentingskostnadene som skal dekkes av politiet. For høye krav til tilgjengelighet og responstid vil være kostnadsdrivende.

Selv om den klare hovedvekten av anmodninger vil sendes og besvares på dagtid, vil det kunne være situasjoner der politiet vil ha behov for opplysninger raskt uavhengig av tidspunkt på døgnet. Dette kan for eksempel være tilfelle i situasjoner som gjelder fare for liv og helse eller andre akutte saker. I slike situasjoner vil kravet til at opplysningene skal utleveres uten ugrunnet opphold innebære at det må etableres løsninger som sikrer at anmodningene kan håndteres raskere, herunder utenom normal kontortid.

6 Ruting av anmodninger

Det fremgår av merknaden til bestemmelsen i ekomloven § 2-8 b at politiets anmodninger kan ta utgangspunkt i både IP-adresse og abonnent (fysisk og juridisk person). Det vil si at det både kan innhentes opplysninger om hvilken abonnent som var tildelt en gitt IP-adresse på et gitt tidspunkt, og også om hvilke IP-adresser en gitt abonnent var tildelt i en tidsperiode.

Når det gjelder anmodninger med utgangspunkt i abonnent eksisterer det ikke en felles samlet oversikt over hvilke tilbydere abonnenter i det norske markedet har avtale med. Når anmodningene tar utgangspunkt i fysiske eller juridiske personer, må politi- og påtalemyndighet sende anmodningen til flere, eventuelt alle lagringspliktige tilbydere for å finne relevant tilbyder. Dette er også situasjonen i dag for politiets forespørsler med utgangspunkt i opplysninger fra tilbyders «driftslager» i medhold av ekomloven § 2- 9 fjerde ledd, jf. tredje ledd.

Når det gjelder politiets anmodninger i dag¹ som tar utgangspunkt i IP-adresser, foretar politiet oppslag i RIPE² sin database for å finne hvilken tilbyder som er tildelt den aktuelle IP-adressen. RIPE³ er et organ som har ansvar for å tildele og registrere tildelingen av IP-adresser i Europa.

RIPE-databasen skal fremdeles danne utgangspunktet for ruting av politiets anmodninger etter ekomloven § 2-8 b når disse tar utgangspunkt i IP-adresser. Dette er også ordningen i Sverige og Finland. For å legge til rette for effektiv gjennomføring av utleveringsplikten er det imidlertid behov for å sikre at informasjonen i RIPE-databasen om tildelt IP-adresserom og eventuelt videre tilordning av IP-adresseblokker til grossistkunder eller partnere er tilstrekkelig oppdatert. Departementet foreslås derfor å forskriftsfeste en slik oppdateringsplikt for tilbyderne som er tildelt IP-adresserom.

I arbeidet med standardisering av datautvekslingen mellom tilbyder- og politisiden har det videre fremkommet synspunkter fra både tilbydere og Kripos om at det vil kunne være behov for dialog mellom tilbyder og politi, i tillegg til selve informasjonsutvekslingen basert på standardiserte løsninger, jf. punkt 4. Det kan blant annet være behov for klargjørende dialog knyttet til de mer komplekse spørringene. Slik klargjørende dialog er vanlig også i dag når det gjelder spørringer etter ekomloven § 2- 9 fjerde ledd, jf. tredje ledd. For å legge til rette for gjennomføring av utleveringsplikten foreslås det derfor at lagringspliktig tilbyder skal ha plikt til å opprette et kontaktpunkt i sin politisvarfunksjon. Det antas å være behov for et fast kontaktpunkt i tilbyderens organisasjon selv om maskinell utveksling via API benyttes. Departementet foreslår at kontaktpunkt og endringer skal meldes inn til Nkom.

7 Økonomiske og administrative konsekvenser

Departementet viser til Prop. 167 L (2020-2021) kapittel 11 om økonomiske og administrative konsekvenser av bestemmelsene i ekomloven §§ 2-8 a og b om logging, lagring og utlevering av IP-adresser. Forslaget til nye bestemmelser i ekomforskriften § 7-6 første og tredje ledd er i hovedsak en klargjøring og presisering av kvalitative krav i hjemmelsbestemmelsene og medfører på dette punkt ingen endring sammenliknet med vurderingen i overnevnte kapittel 11.

Når det gjelder de foreslåtte kravene i annet ledd om responstid og bruk av standardiserte utvekslingsløsninger vil disse kunne medføre økt ressursbruk hos tilbyder. Kravet om

¹ I medhold av ekomloven § 2-9 fjerde ledd, jf. tredje ledd

² RIPE NCC (Réseaux IP Européens Network Coordination Centre)

³ I ICANN blir den konkrete forvaltningen av IP-adresser håndtert av ASO (Address Supporting Organization). Denne forvaltningen er videre distribuert regionalt, og i Europa utføres denne funksjonen av RIPE.

responstid vil blant annet kunne påvirke behovet for ressurser i tilbyders politisvarfunksjon. Krav til et høyt servicenivå vil gjenspeiles i prisene for uthenting av lagringspliktig informasjon.

Når det gjelder krav om bruk av standardiserte utvekslingsløsningene vil tilbyder måtte påregne utviklingskostnader forbundet både med selve tilknytningen til politiets maskinelle løsning basert på Maskinporten, samt også utviklingskostnader i interne systemer for uttak av etterspurt informasjon. På den annen side forventes at en maskinell utveksling av anmodninger og svar på disse, vil gi betydelige effektiviseringsgevinster, både for tilbyder- og politisiden.

Det andre utvekslingsalternativet basert på ID-porten, medfører ingen utviklingskostnader hos tilbyder forutsatt at tilbyder kan benytte en ferdigutviklet portaltjeneste hvor politiet er systemeier. Dette alternativet antas også å gi effektiviseringsgevinster.

Politiets kostnader ved utviklingen av de standardiserte utvekslingsløsningene faller utenfor vurderingen av økonomiske og administrative konsekvenser fordi disse løsningene ikke utvikles som følge av regulatoriske krav i forskriftsutkastene, men er et funksjonelt ønske fra politisiden.

Kravet om å utarbeide en årlig revisorbekreftet kostnadsoversikt, jf. forslaget fjerde ledd, medfører økte kostnader for tilbyderne knyttet til både bruk av internt personell og kostnader til ekstern revisjon. Dokumentasjon av relevant kostnadsgrunnlag er imidlertid nødvendig for å unngå uenighet om prisene for politiets uthenting av lagringspliktig informasjon. Departementet legger derfor til grunn at det også er i tilbyders interesse at et slikt kostnadsgrunnlag sikres.

Den foreslåtte plikten i femte ledd om å etablere et fast kontaktpunkt i tilbyders politisvarfunksjon, gi oppdatert informasjon om dette til Nkom og å sikre at RIPE-databasen inneholder oppdatert informasjon antas å ha en begrenset økonomiske og administrative konsekvenser for tilbyder. Nkom må regne med ressursbruk knyttet til å utarbeide oppdaterte lister over relevante tilbydere, herunder relevant kontaktpunkt hos den enkelte som en del av sitt tilsynsarbeid.

Når det gjelder forslaget om innholdet i politiets årlige rapportering til Nkom i ny § 7-7, viser departementet til Prop. 167 L (2020-2021) kapittel 11.2.2 hvor det fremgår følgende: *Som det fremkommer av kapittel 8.6.4, jf. forslag til bestemmelse i ny § 2-8 b, skal anmodninger fremmes skriftlig i et enhetlig format, og politiet skal utarbeide en årlig oversikt over anmodninger som sendes Nasjonal kommunikasjonsmyndighet. Politiet opplyser at det eksisterende systemet for telefoni kan utvikles til å støtte innhenting og statistikk for IP-anmodninger, og at dette i liten grad vil medføre kostnader for politiet.*

8 Utkast til bestemmelser

§ 7-6 Krav i forbindelse med lagring og utlevering av IP-adresser mv.

Tilbyder som nevnt i ekomloven § 2-8 a første ledd skal uten ugrunnet opphold lagre de opplysninger som går frem av bestemmelsens første ledd. Lagringen skal skje med tilstrekkelig sikring for å unngå at opplysningene går tapt. Det skal fremgå informasjon om

hvilken tidssone lagrede klokkeslett er angitt i. Tilbyder skal sikre at opplysningene ikke endres gjennom innsamling, logging, lagring og utlevering.

På bakgrunn av anmodninger fra politi- og påtalemyndighet etter ekomloven § 2-8 b første ledd, skal tilbyder utlevere lagringspliktige opplysninger uten ugrunnet opphold. Tilbyder skal sørge for sikker utlevering av opplysningene og så langt mulig benytte de standardiserte løsningene for datautvekslingen.

Tilbyder skal utlevere liste over alle abonnenter som har benyttet en IP-adresse på aktuelt tidspunkt når anmodninger ikke inneholder informasjon om portnummer på abonnentssiden. Tilbyder skal utlevere all tilgjengelig abonnementsinformasjon knyttet til identifiserte abonnenter i forbindelse med anmodningen. Tilbyder skal ikke utlevere opplysninger om abonnement og abonnentens utstyr etter bestemmelsen her.

Tilbyder skal opprette et kontaktpunkt i sin politisvarfunksjon og melde inn kontaktpunkt og eventuelle endringer til Nkom. Tilbyder som er tildelt IP-adresserom av RIPE plikter å ha oppdatert informasjon om dette i RIPE-databasen. Tilbyder som har tilordnet sine tildelte IP-adresser i faste adresseblokker til annen tilbyder plikter å ha oppdatere informasjon om dette i RIPE-databasen.

Tilbyder skal årlig utarbeide oversikt over kostnadene som følge av utleveringsplikten i ekomloven § 2-8 b første ledd. En revisorbekreftet oversikt over kostnadene skal være ferdigstilt innen 30. juni hvert år, for foregående regnskapsår. Nkom skal på forespørsel få tilsendt den revisorbekreftede kostnadsoversikten, og kan kreve dokumentasjon av de prinsipper og vurderinger som er lagt til grunn for den.

§ 7-7 Årlig rapportering om uthenting av opplysninger om IP-adresser

Politi- og påtalemyndigheten skal oversende årlig rapportering om uthenting av lagringspliktig opplysninger etter ekomloven § 2-8 b første ledd. Rapporteringen skal sendes Nkom innen 31. januar hvert år.

Rapporteringen skal inneholde:

- a) oversikt over det totale antallet anmodninger som er sendt lagringspliktige tilbydere per kalenderår, antallet som er besvart av tilbyder og dokumentasjon på at kravene til utlevering i ekomloven § 2-8 b annet ledd er oppfylt for anmodningene,*
- b) det totale antallet abonnenter politiet har fått utlevert informasjon om per kalenderår,*
- c) den årlige fordelingen av besvarte anmodninger med utgangspunkt i henholdsvis IP-adresse eller abonnent og*
- d) oversikt over hvilke straffebud som ligger til grunn for det årlige uttaket av lagringspliktig informasjon.*

§ 10-3 annet ledd skal lyde:

Nasjonal kommunikasjonsmyndighet kan pålegge en fysisk person eller et foretak overtredelsesgebyr dersom personen, foretaket eller noen som handler på vegne av foretaket, forsettlig eller uaktsomt overtrer ekomforskriften § 1-2 første og fjerde ledd, § 1-6 til § 1-8, § 2-2 første ledd, § 2-4, § 2-5, § 2-6 første ledd, § 2-7, § 2-8, § 3-1 til § 3-6, § 4-1 første ledd, § 4-2 til § 4-4, § 5-1 første og fjerde ledd, § 5-3, § 5-4, § 5-5 første ledd, § 5-6, § 5-8 første ledd, § 5-10, § 5a-1 til § 5a-5, § 5a-6 første og tredje ledd, § 6-2, § 6-6 fjerde ledd, § 7-1, § 7-2, § 7-6 eller § 8-2 til § 8-4, § 8-5 første ledd.

9 Merknader til utkast til bestemmelser

Til § 7-6 Krav i forbindelse med lagring og utlevering av IP-adresser mv.

Av bestemmelsens *første ledd* fremgår det at det er tilbyder som nevnt i ekomloven § 2-8 a første ledd som har plikter etter forskriftsbestemmelsen. Det er således tilbyder av elektronisk kommunikasjonsnett som anvendes til offentlig elektronisk kommunikasjonstjeneste og tilbyder av slik tjeneste som reguleres.

De materielle kravene som stilles til lagringspliktige opplysninger i bestemmelsens første og annet ledd, gjelder både for opplysningene som eksplisitt nevnes i ekomloven § 2-8 a første ledd bokstav a og b, samt abonnementsopplysninger om fysisk eller juridisk person, jf. forskriftsbestemmelsens tredje ledd.

Første ledd fastsetter krav om at tilbyder skal lagre opplysningene uten ugrunnet opphold. Dette betyr at tilbyder skal sørge for at opplysninger lagres så snart som mulig etter at for eksempel opplysninger er logget i tilbyders systemer.

Videre skal lagringen skje med tilstrekkelig sikring for å unngå at opplysningene går tapt. Kravet medfører eksempelvis at tilbyder er ansvarlig for at det legges opp til en hensiktsmessig frekvens for sikkerhetskopiering av informasjonen samt etablering av nødvendige back-up løsninger ved systemfeil osv.

Av første ledd fremgår det også et krav knyttet til dataintegritet og tilbyder pålegges å sikre at opplysningene ikke endres gjennom innsamling, logging, lagring og utlevering. Dersom politiets anmodninger ikke kan besvares fordi de relevante opplysninger har gått tapt eller er feilaktige på grunn av manglende tiltak for å bevare dataintegritet, vil utleveringsplikten ikke anses oppfylt.

I henhold til første ledd skal det også fremgå informasjon om hvilken tidssone lagrede klokkeslett er angitt i.

Krav til tilbyders responstid fremkommer av *annet ledd*. Bestemmelsen fastsetter krav om at tilbyder skal utlevere lagringspliktige opplysninger til politi- og påtalemyndigheten uten ugrunnet opphold. Kravet skal sikre at tilbyders tidsbruk ikke trekker ut i tid, slik at formålet med anmodningen blir «virkningsløs» og etterspurt informasjon skal gis ut så fort den er tilgjengeliggjort hos tilbyder. Den faktiske tiden det tar å utlevere opplysninger uten ugrunnet opphold kan imidlertid variere noe avhengig av anmodningens størrelse og kompleksitet, behovet for klargjørende dialog, og tilbyders størrelse og kundemasse, jf. punkt 5.2 ovenfor. Når det gjelder tilgjengelighet forutsettes det at hovedvekten av politiets anmodninger besvares på dagtid. Dersom det er fare for liv eller helse eller saken av andre grunner er

akutt, vil dette imidlertid kunne kreve at anmodninger skal besvares raskere, herunder utenom normal kontortid.

Det fremgår også av annet ledd at tilbyder skal sørge for sikker utlevering av opplysningene. Kravet til sikker utlevering omfatter både krav til kryptering av opplysningene ved overføringen til politiet for å ivareta konfidensialitet i denne fasen av datautvekslingen. Videre omfattes også krav til autentisering og autorisasjon av endepunktene for dataoverføringen. Standardene for datautveksling som er utviklet i samarbeide mellom tilbyder- og politisiden skal benyttes så langt mulig.

Ekomloven §§ 2-8 a og b forutsetter at tilbyder skal kunne koble abonnementsinformasjon og en gitt IP-adresse. I forbindelse med bruk av NAT-teknologi (delt IP) klargjøres det i bestemmelsens *tredje ledd* første punktum, at tilbyder skal utlevere liste over alle abonnenter som har benyttet en IP-adresse på aktuelt tidspunkt, i de situasjoner hvor politiet ikke har kjennskap til det aktuelle portnummeret på abonnentssiden og anmodningen følgelig ikke inneholder slik informasjon.

Når det gjelder øvrig abonnementsinformasjon fremgår det av tredje ledd annet punktum at tilbyder skal utlevere all tilgjengelig abonnementsinformasjon knyttet til identifiserte abonnenter. I tillegg til navn/firmanavn, fødselsdato, fødselsnummer, eller organisasjonsnummer på den rettslige avtalepart abonnenten, kan tilbyder ha informasjon om fakturaadresse, anleggsadresse, disponent/bruker av abonnementet og kontaktperson i firma. I den grad tilbyder har slik informasjon skal dette utleveres.

I tredje ledd siste punktum fremgår det at tilbyder ikke skal utleveres informasjon om abonnentens abonnement og utstyr etter denne bestemmelsen. Eksempler på slik informasjon som ikke skal utleveres er eventuell tvilling-SIM, MAC-adresse, IMEI- og IMSI-nummer. Utlevering av slik informasjon skal kun følge eksisterende utleveringsgrunnlag, eksempelvis ekomloven § 2-9 fjerde ledd, jf. tredje ledd.

Departementet presiserer videre at kvaliteten på overnevnte informasjon om abonnenter i utgangspunktet er basert på den selvdeklarerende angjeldende abonnent gjør overfor tilbyder i forbindelse med at avtaleforholdet opprettes og/eller endres. Reglene om krav til entydig identifisering av abonnent i ekomregelverket kan medføre økt kvalitet på abonnementsopplysninger, reglene gjelder imidlertid kun for telefonitjenester.

For å legge til rette for effektiv datautveksling etter ekomloven § 2-8 b første ledd, fastsetter bestemmelsens *fjerde ledd* at tilbyder skal ha et fast kontaktpunkt i sin organisasjon knyttet til slik utveksling. Informasjon om kontaktpunkt, herunder kontaktinformasjonen til vedkommende ansatt i selskapet og endringer i slik informasjon skal fortløpende meldes inn til Nkom. Dette vil blant annet legge til rette for at behov for klargjørende dialog mellom tilbyder og politi, i forbindelse med konkrete anmodninger, kan gjøres effektivt.

For å legge til rette for effektiv ruting av politiets anmodninger basert på spørringer med utgangspunkt i IP-adresser oppstiller fjerde ledd videre en plikt for tilbyder til å ha oppdatert informasjon om hvilket/e IP-adresserom tilbyder er tildelt av RIPE NCC (Réseaux IP Européens Network Coordination Centre) dersom dette er tilfelle. RIPE har ansvar for å tildele og registrere tildelingen av IP-adresser i Europa og har informasjon om tildelingene i sin database.

Oppdateringsplikten omfatter både plikt til å ha riktig informasjon i RIPE-databasen om hvilket/e IP-adresserom tilbyder er tildelt, og også at selskapsnavn og norsk organisasjonsnummer er oppdatert til enhver tid. Tilbyder som er tildelt IP-adresserom av RIPE kan ha behov for å tilordne IP-adresser videre til andre tilbydere, eksempelvis grossistkunder eller partnere når tjenesteproduksjonen er basert på ulike partnerkonstellasjoner. Slik tilordning kan skje ved at hele adresseblokker tilordnes annen tilbyder eller ved at kun individuelle IP-adresser innenfor en adresseblokk tilordnes den andre tilbyderen.

Det fremgår av fjerde ledd at tilbyder som er tildelt IP-adresser også har plikt til å sørge for at RIPE-databasen er oppdatert med informasjon om slike tilordninger avgrenset til de tilfeller hvor hele adresseblokker er tilordnet annen tilbyder. Kravet gjelder således ikke for de tilfeller hvor et IP-adresserom deles mellom den som er tildelt adresserommet og dennes grossistkunder/partnere. Dette fordi man da ikke vil kunne vite hvilken av disse tilbydere som har benyttet en gitt adresse innenfor det angjeldende IP-adresserommet.

Av bestemmelsens *femte ledd* fremgår det at tilbyder skal utarbeide en årlig oversikt over kostnadene som følge av utleveringsplikten i ekomloven § 2-8 b første ledd. Det er videre et krav at oversikten skal bekreftes av en tredjepart i form av krav om revisorbekreftelse og at Nkom skal kunne få tilsendt oversikten på forespørsel. Kravet skal blant annet sikre dokumentasjon av relevant kostnadsgrunnlag hos den enkelte tilbyder dersom det oppstår uenighet om priser for politiets uthenting av opplysninger.

Det følger av ekomloven § 2-8 a at tilbyderne skal dekke investerings- og driftskostnader knyttet til lagringsplikten. Videre at staten skal dekke kostnadene for utlevering av informasjon etter § 2-8 b første ledd. Dette siste omfatter kostnader knyttet til selve uthenting av opplysningene i tilbyders systemer og også utleveringen til politiet, herunder blant annet personell- og administrasjonskostnaden for behandling av utleveringsbegjæringer.

Hovedresultatene i en slik kostnadsoversikt vil gi Nkom mulighet til å vurdere forholdsmessigheten mellom tilbyders utleveringspris og -kostnader. Dette kan blant annet være til hjelp i en eventuell sak om uenighet knyttet til pris for utlevering. Revisors bekreftelse skal blant annet sikre kvalitet og validitet og vil være tredjepartskontrollen knyttet til alle forhold og detaljer i den årlige kostnadsoversikten som skal utarbeides.

Til § 7-7 Årlig rapportering om uthenting av opplysninger om IP-adresser

Det fremgår av ekomloven § 2-8 b tredje ledd at politi- og påtalemyndigheten skal sende årlig rapport om uthenting av lagringspliktig opplysninger til Nkom. I denne forbindelse er det behov for å fastsette nærmere presiseringer av rapporteringsplikten i forskrift. Av bestemmelsens *første ledd* fremgår det at rapportering skal sendes Nkom innen 31. januar hvert år. Denne skal være basert på uthenting av lagringspliktige opplysninger foregående kalenderår. Idet hovedregelen for datautveksling er å benytte de standardiserte løsningene for dette, forutsettes det at årlige rapportering sendes samlet for alle anmodninger hvor disse løsningene er benyttet.

I *annet ledd* bokstav a-d fremgår kravene til innholdet i rapporteringen. Av bokstav a fremgår det at rapporteringen skal inneholde informasjon om både antallet anmodninger som er sendt per kalenderår og også antallet anmodninger som er besvart av tilbyder. Dette vil gi

informasjon om det årlige uttaket av opplysninger samt også andelen anmodninger som eventuelt ikke besvares. Bokstav a oppstiller også et krav om at rapporteringen skal inneholde generell dokumentasjon for at alle anmodninger som sendes oppfyller kravene i ekomloven § 2-8 b annet ledd. Departementet forutsetter at Nkom og politiet har dialog om hvilken dokumentasjon som bør inngå i rapporteringen. Bestemmelsen medfører at politi- og påtalemyndighet må legge til rette for sporbarhet og notoritet for at anmodningene dekker lovens krav i sine internsystemer.

Av bokstav b fremgår det at rapporteringen skal inneholde informasjon om antall abonnenter politiet har fått utlevert informasjon om. Som følge av at tilbyder kan ha benyttet NAT-teknologi (delt IP), og politiet i slike tilfeller skal få utlevert opplysninger om alle abonnenter som har delt IP-adressen på det aktuelle tidspunktet, vil antallet abonnenter det blir utlevert informasjon om kunne være større enn antallet anmodninger fra politiet.

Politiet kan anmode om utlevering enten på bakgrunn av en gitt IP-adresse eller opplysninger om en gitt abonnent. Etter bokstav c skal rapporteringen inneholde den årlige fordelingen av besvarte anmodninger med utgangspunkt i IP-adresse eller abonnent.

Av bokstav d fremgår det at rapporteringen skal inneholde en oversikt over hvilke straffebud som ligger til grunn for anmodningene.

Til § 10-3 annet ledd

Departementet foreslår at myndigheten skal kunne pålegge ekomtilbyder overtredelsesgebyr ved brudd på bestemmelsene i forslaget til ny § 7-6 i ekomforskriften. Endringen består med andre ord i å liste § 7-6 i oversikten over forskriftsbestemmelser som gir hjemmel til å kunne ilegge overtredelsesgebyr. Forslaget er ment å sikre myndigheten hjemmel til å kunne sanksjonere overtredelser av forskriftsbestemmelsen på en effektiv måte, og vil kunne ha en preventiv virkning.