UTKAST TIL ENDRINGER I EKOMLOVEN - HØRINGSNOTAT

Fordeling av kostnader ved gjennomføringen av datalagringsdirektivet, uthenting av data i nødssituasjoner og endring i reglene for lagring og utlevering av enkelte taushetsbelagte data, PUK-kode og kundereskontro som ikke er lagringspliktige.

Innholdsfortegnelse

1. Sammendrag

Dette høringsnotatet inneholder forslag til bestemmelser som skal regulere fordelingen av kostnader knyttet til datalagring etter ekomloven § 2-7 a, mellom ekomtilbydere og Staten, forslag til lovbestemmelse som regulerer politiets uthenting av elektronisk kommunikasjon i nødssituasjoner og regler vedrørende utlevering av PUK-koder og informasjon fra kundereskontro.

Det foreslås en modell hvor etablerings- og driftskostnader knyttet til klargjøring for lagring av lagringspliktige data dekkes av den enkelte lagringspliktige tilbyder, og at staten dekker kostnadene knyttet til selve lagringen, tilgjengeliggjøring og mottak av data. Departementene tar sikte på at reglene som nå sendes på høring vil tre ikraft 1. januar 2014. Departementene legger opp til at alle nødvendige endringer i lov og forskrift for å få gjennomført datalagringsdirektivet i norsk rett blir vedtatt innen 1. januar 2014. Dette innebærer at alle krav til ekomtilbyderne som følger av lagringsplikten vil være klare innen nevnte dato. Av hensyn til tilbydernes behov for å tilpasse seg de krav som lagringsplikten i ekomloven § 2-7 a første ledd medfører, foreslår departementene at ikrafttreden av selve lagringsplikten blir fra 1. januar 2015. Tilbyderne vil da ha ett år på å tilpasse seg de nye kravene som følger av lagringsplikten. Den etablerte ordning etter ekomloven § 2-8 hvor ekomtilbyder plikter å tilrettelegge for kommunikasjonskontroll og utleveringspålegg etter straffeprosessloven (strpl.) § 210 mv., påvirkes ikke av forslaget. For mer bakgrunnsinformasjon, se også Samferdselsdepartementets hjemmeside[1] og dokumentene under kapittel 2.1.

Stortinget ba i Innst. nr. 275 L (2010-2011) regjeringen også om å utforme en lovbestemmelse som regulerer politiets uthenting av elektronisk kommunikasjon i nødssituasjoner. Forslag til ny slik bestemmelse fremmes som ny § 2-9 a i ekomloven. Samferdselsdepartementet foreslår regler vedrørende utlevering av PUK-koder og informasjon fra kundereskontro som ny § 2-9 tredje ledd i ekomloven. I forslaget presiseres det at denne type opplysninger er taushetsbelagt, samtidig som det åpnes for at opplysningene kan utleveres til politi- og påtalemyndighet i bestemte tilfeller.

Samferdselsdepartementet og Justis- og beredskapsdepartementet har samarbeidet om høringsnotatet.

2. Forslag til ny modell for fordeling av kostnader ved gjennomføring av datalagringsdirektivet

[1] http://www.regjeringen.no/nb/dep/sd/tema/telekommunikasjon/datalagringsdirektivet.html?id=666723

2.1. Innledning

EUs datalagringsdirektiv (direktiv 2006/24/EF) pålegger en plikt for tilbyder av ekomnett og -tjenester å lagre data som fremkommer ved bruk av elektronisk kommunikasjon. Stortinget besluttet 15. april 2011 at EUs datalagringsdirektiv (DLD) skulle gjennomføres i norsk rett. Regler for gjennomføringen fremgår av Innst. nr. 275 L (2010-2011). Av Prop. 49 L (2010-2011) *Endringer i ekomloven og straffeprosessloven mv. (gjennomføring av EUs datalagringsdirektiv i norsk rett)*, fremgår det at det skal utarbeides en modell for hvordan kostnader skal beregnes og fordeles mellom ekomtilbydere og justismyndighetene.

Direktivet pålegger lagring av abonnements-, lokaliserings- og trafikkdata for ulike typer telefoni, e-post og Internett-tilgang. Lagringsplikten knytter seg til historiske opplysninger om hvem som har foretatt kommunikasjonen og tidspunktene for denne. I tillegg skal lokaliseringsdata for mobil kommunikasjon lagres. Hvem det kommuniseres med, kommunikasjonens endepunkt, skal lagres for e-post og telefoni, men ikke for internett-tilgang. Data som røper innholdet i kommunikasjonen skal ikke lagres. Av artikkel 6 i DLD fremgår det at det enkelte medlemsland kan fastsette lagringstid på mellom seks måneder til to år. For Norges vedkommende vedtok Stortinget en lagringstid på seks måneder.

Reglene skulle etter planen tre i kraft 1. april 2012, men har blitt utsatt flere ganger. En av årsakene til dette har vært usikkerhet rundt kostnader forbundet med innføring av direktivet, særlig på grunn av de særnorske kravene. Det foreligger nå en økonomisk utredning av de økonomiske konsekvensene ved innføringen av datalagringsdirektivet i Norge, foretatt av Nexia International DA. Direktivet har ingen bestemmelser om kostnader, og det er opp til nasjonale myndigheter å bestemme hvem som skal betale for gjennomføringen av plikten til å lagre data innenfor elektronisk kommunikasjon.

Det følger av Prop. 49 L (2010-2011) at eksisterende regler for kostnadsdeling mellom tilbyder av ekomnett og -tjenester skal gjelde inntil en ny modell for beregning og fordeling av kostnader er på plass. Eksisterende regler er knyttet til ovennevnte tilretteleggingsplikt. Når det nå tas sikte på at alle nødvendige endringer i lov og forskrift for å innføre en lagringsplikt i norsk rett skal være på plass til 1. januar 2014, er det påkrevet med regler for fordeling av kostnader knyttet til denne nye lagringsplikten.

2.2. Gjeldende rett og praksis

Etter gjeldende rett har tilbyder av elektronisk kommunikasjonstjeneste og -nett ingen lagringsplikt, men en plikt til å tilrettelegge for lovbestemt tilgang til informasjon om sluttbruker og deres bruk av elektronisk kommunikasjon. Tilbydere av elektronisk kommunikasjonstjeneste og -nett lagrer i dag trafikkdata, lokaliseringsdata, abonnements-/ brukerdata mv. hovedsakelig for eget bruk. Behovet for lagring hos den enkelte tilbyder kan tilskrives kundeadministrasjon, opplysningstjeneste, faktureringsformål, samtaleavregning, feilretting i egne systemer mv. Opplysningene

skal kun lagres i henhold til konsesjon gitt av Datatilsynet, jf. personopplysningsloven § 31 og personopplysningsforskriften § 71. Generelt påligger det tilbyder en plikt til å slette eller anonymisere opplysninger som ikke lenger har betydning for formålet. Opplysninger skal således i regelen slettes når faktura er gjort opp, eventuelt når klagefristen er utløpt. Datatilsynets konsesjon oppstiller en maksimal lagringstid på fem måneder etter at opplysningene ble registrert ved kvartalsvis fakturering, og tre måneder etter opplysningene ble registrert ved månedlig fakturering. Det er månedlig fakturering som er praksis i dagens marked. I tilfeller hvor formålet med lagringen er knyttet til teknisk drift og ikke fakturering, har Datatilsynet kun tillatt vesentlig kortere lagringstid. Det samme gjelder internettsesjoner om koblingen mellom IP-adresse og sluttbrukers internettrafikk hvor tilsynet ikke har tillatt lengre lagring enn tre uker.

Ekomloven § 2-8 pålegger tilbydere en tilretteleggingsplikt for å sikre politiets lovbestemte tilgang til sluttbruker og dennes bruk av elektronisk kommunikasjon. Kostnadsmodellen som brukes for tilgang til denne informasjonen er en delingsmodell, hvor ekomtilbyderne skal tilrettelegge nett og tjenester for lovbestemt tilgang til informasjon om sluttbruker og sluttbrukers bruk av elektronisk kommunikasjon. Tilbyder forutsettes å dekke investeringskostnadene knyttet til denne lovbestemte tilgangen, mens driftskostnader knyttet til oppfyllelse av tilretteleggingsplikten dekkes av staten. Gjeldende praksis er at politiet betaler for uthenting av informasjonen i henhold til avtaler inngått med tilbyder, jf. ekomloven § 2-8 annet ledd, denne ordningen foreslås ikke endret ved innføringen av datalagringsplikten i ekomloven § 2-7 a.

2.3. Utredninger og analyser

2.3.1. Kostnadsfordelingsutvalget

Departementet etablerte i juni 2011 et offentlig utvalg som fikk i oppgave å utrede forslag til ny kostnadsmodell for datalagring. Det var forutsatt i Prop. 49 L at både politiet, tilbydere av ekomnett og -tjenester og de respektive myndigheter skulle involveres i prosjektet. For departementene var det viktig å sette sammen utvalget slik at de ulike parter og synspunkter ble ivaretatt i utredningen.

Kostnadsfordelingsutvalget leverte sin rapport "*Forslag til kostnadsfordelingsmodell i forbindelse med innføring av datalagringsdirektivet i norsk rett*" 1. februar 2012. Utvalget vurderte seks modeller for kostnadsdeling (modell A, B, C, D, E og F). For mer detaljert informasjon vises til rapporten, høringen og høringssvarene, alt tilgjengelig på Samferdselsdepartementets hjemmeside. Nedenfor under pkt. 2.3.2 gis en kort oppsummering av modellene og høringsinnspillene.

Fra utvalgets rapport siteres anbefalingen:

"Utvalget har vurdert seks alternative kostnadsfordelingsmodeller. Disse varierer fra ikke noe godtgjørelse til full godtgjørelse av kostnadene tilbyderne påføres. Fire av disse innbefatter en form for kostnadsdeling mellom staten og tilbyderne, hvorav tre tar utgangspunkt i deling etter

kostnadskategoriene investeringskostnader, faste driftskostnader og uthentingskostnader. Den fjerde tar utgangspunkt i en deling av kostnader etter en gitt fordelingsnøkkel uavhengig av kostnadskategori.

Et samlet utvalg finner den samfunnsøkonomisk mest kostnadseffektive modellen å være den som tar utgangspunkt i kostnadsdeling etter en fordelingsnøkkel, uavhengig av kostnadskategori. Denne modellen ivaretar følgende hensyn, som utvalget har sett på som viktige:

- *Kostnadsfordelingsmodellen skal bidra til kostnadseffektivitet ved at krav som staten stiller påvirker kostnaden som staten skal dekke.*
- *Kostnadsfordelingsmodellen skal bidra til å minimere negative virkninger i ekommarkedet.*
- *Kostnadsfordelingsmodellen skal gi tilbyderne insentiver til å implementere kostnadseffektive løsninger.*
- *Kostnadsfordelingsmodellen skal understøtte formålet med datalagringen, nemlig å være et verktøy til bruk for etterforskning, oppklaring og straffeforfølging av alvorlige straffbare forhold."*

Det har ifølge utvalget ikke vært mulig å si noe konkret om fastsettelsen av fordelingsnøkkelen, all den tid de konkrete kravene i datalagringforskriften og konsesjonen for lagring av personopplysninger på dette tidspunktet ikke forelå. Utvalget mener at myndighetene bør ta en betydelig andel av kostnadene. Utvalget anså at selv en beskjeden andel tillagt tilbyderne, ville være tilstrekkelig for å gi nødvendige insentiver til kostnadseffektivitet. På tidspunktet for utvalgets anbefaling forelå det ingen konkret kostnadsberegning hvor kravene fra Stortingets beslutning 15. april 2011 var inkludert for gjennomføring av DLD i Norge.

Samferdselsdepartementet sendte 22. mars 2012 forslagene til utvalgets ulike modeller på offentlig høring.

2.3.2. Oppsummering av høringsinnspillene
Departementet mottok 36 høringssvar om kostnadsdelingsmodeller for datalagringsdirektivet, hvorav 15 ikke hadde merknader. Nedenfor gis en kort fremstilling av modellene, oppsummering av innkomne høringsinnspill, inndelt i kategoriene myndigheter, tilbydere av ekomnett- og tjenester og andre.

De ulike modellene
I rapporten vurderes seks ulike modeller for kostnadsfordeling (modell A, B, C, D, E og F). Modell A representerer det ene ytterpunktet av alternative kostnadsfordelings-modeller, nemlig at tilbyder dekker alle kostnader forbundet med datalagringen uten kompensasjon fra staten. Modellene B, C og D er modeller som innebærer kostnadsdeling mellom staten og tilbyderne etter kategoriene investerings-, drifts- og uthentingskostnader. I modell B dekker staten uthentingskostnadene, og tilbyderne de øvrige kostnadene. I modellene C og D dekker staten i tillegg til uthentingskostnadene, henholdsvis de faste driftskostnadene og investeringskostnadene. Modell C ligger nær opptil dagens praktisering av kostnadsfordeling. Modell E skiller seg fra modellene B, C og D i den forstand at kostnadsdelingen er uavhengig av kostnadskategori.

Fordelingsnøkkelen kan enten være fast, og dermed den samme for alle tilbydere, eller gradert avhengig av tilbyderkategorisering. Modell F representerer ytterpunktet til modell A ved at staten skal godtgjøre alle tilbyders kostnader. Dette innebærer at tilbyder i utgangspunktet ikke bærer noen kostnader forbundet med datalagringen.

Et samlet utvalg finner den samfunnsøkonomisk mest kostnadseffektive modellen å være den som tar utgangspunkt i kostnadsdeling etter en fordelingsnøkkel, uavhengig av kostnadskategori (modell E).

Myndigheter
Fornyings-, administrasjons- og kirkedepartementet (FAD) deler utvalgets oppfatning om at samfunnsøkonomiske kostnader som etableringshindring, konkurransevridning og svekkede muligheter for fremtidige investeringer må minimeres, og påpeker det uheldige ved innføring av ordninger som medfører at konkurransen i ekommarkedet svekkes. Utover dette tar ikke FAD stilling til modell.

Post- og teletilsynet (PT) deltok i utvalget og støtter utvalgets konklusjon om modell E. PT legger vekt på at den lagringspliktiges konkurranseevne ikke må svekkes sammenlignet med konkurrerende virksomheter som ikke er lagringspliktige.

Kripos deltok i utvalget og legger vekt på at det bør velges kostnadsløsninger som sikrer at det er dataenes potensielle betydning som etterforskningsmateriale i den konkrete sak må avgjøre spørsmålet om disse skal innhentes fra datalagringsbasen, ikke kostnadene med dette. Kripos vektlegger de administrative følgene ved valg av modell, og at kostnadsmodellen bør gjelde både for kommunikasjonskontroll og datalagring i henhold til DLD.

Politidirektoratet (POD) anbefaler pga. likhetshensynet til virksomheter som en forutsetning for å drive næring modell A. POD mener politiet bør kunne innhente data vederlagsfritt, og at dersom politiet skal betale for uthenting av data, bør dette skje gjennom standardpriser fastsatt av myndighetene.

Riksadvokaten har ingen merknader til utvalgets rapport, og mener det er for tidlig å komme med merknader til valg av modell når PTs forskrift ikke er vedtatt.

Politiets sikkerhetstjeneste (PST) mener at valg av kostnadsdelingsmodell ikke må få negative konsekvenser for muligheten til å hente ut trafikkdata. Uthentingskostnadene må ikke være styrende for bruk av trafikkdata. PST avviser at modell A vil føre til risiko for økt bruk av trafikkdata.

Finanstilsynet er enige med Kostnadsfordelingsutvalget i valg av kostnadsmodell.

Datatilsynet anser det som rimelig at staten dekker de totale, eller deler av, tilbydernes investeringskostnader, men har utover det ingen synspunkter på valg av modell.

Tilbydere av ekomnett og -tjenester
Telenor deltok i utvalget og støtter i hovedsak rapportens vurderinger og anbefalinger. Primært ønsker Telenor modell F og eventuelt valg av modell E bør modifiseres slik at staten dekker alle kostnader knyttet til uthenting. Begrunnelsen for dette er at tilbyderne i svært liten grad kan påvirke volum på uthenting, krav til responstid og følgelig kostnader til dette. Grunnlaget for kostnadsdekning bør baseres på de faktiske kostnader til tilbyder, og det bør legges opp til en prosentvis andel av kostnadene.

TeliaSonera mener prinsipalt at modell F bør velges, subsidiært modell E. TeliaSonera legger vekt på at det mest kostnadseffektive vil være å etablere en eller flere store databaser. Få databaser vil kunne gi bedre sikkerhet og personvern.

Tele2 mener at man bør velge modell F, subsidiært modell E. Tele2 legger vekt på en felles bransjeløsning som gjør det mulig for aktørene å velge kostnadseffektive løsninger.

Telio mener modell F er riktig og legger vekt på at belastningen ikke må bli uforholdsmessig stor for små tilbydere med små ressurser og antatt få henvendelser fra politi og påtalemyndighet.

TDC og Ventelo har gitt innspill gjennom IKT-Norge.

Andre
IKT-Norge deltok i utvalget og anser at disse kostnadene må bæres av myndighetene (modell F og E). Dette begrunnes i de særkrav norske myndigheter stiller til ekomtilbydere for tilgang til data som kun er i myndighetenes interesse. Dersom myndighetene ikke dekker kostnadene vil dette være en betydelig konkurranse-vridning med fare for avvikling og etableringshindring. Prinsipalt anbefaler IKT-Norge modell F, men dersom valg av modell E velges, mener de det er avgjørende å begrense tilbydernes andel til 0,5-1 % av kostnadene.

Forbrukerrådet har som prinsipielt utgangspunkt at kriminalitetsbekjempelse er et offentlig ansvar og at kostnadene ved slike oppgaver ikke bør belastes forbrukere.

NHO mener at modell F bør velges. NHO finner det vanskelig å skulle ta stilling til modell E fordi det ikke fremgår hvordan fordelingsnøkkelen mellom staten og tilbyderne skal være.

Spekter mener det vil være naturlig å velge modell F. NTNU foretrekker modell F, fordi dette er krav som staten stiller til bekjempelse av kriminalitet. Sikkerhetskravene vil føre til betydelige investeringskostnader som vil slå uheldig ut for små og mellomstore tilbydere, selv med en kostnadsdeling mellom stat og tilbyder.

Elektronikkbransjen og NTE (Nord-Trøndelag elektrisitetsverk) støtter modell E.

Virke støtter modell F, begrunnet med faren for konkurransevridning dersom tilbyderne må dekke kostnadene. Videre vil denne modellen fremme kostnadseffektivitet og bidra til å sikre personvernet ved å hindre overforbruk.

Kabel Norge mener modell F er riktig fordi datalagringen utelukkende er et verktøy for kriminalitetsbekjempelse. Høringsinstansen peker også på at det ikke er godt nok begrunnet at modell E vil gi større kostnadseffektivitet og mener den vil innebære stor risiko for negative konkurransemessige virkninger.

FriBit og Elektronisk Forpost Norge mener modell F bør velges, fordi DLD er et verktøy for politiet. Modell F vil føre til at politiet må vurdere dette verktøyet opp mot andre verktøy, og synliggjøre om DLD er kostnadssvarende (kost/nytte).

Oppsummering
Et gjennomgående argument fra de aller fleste som har gitt innspill er at siden føringene fra stortingsvedtaket er så spesielle med sine mange særnorske krav og på grunn av at tilbyderne må etablere nye og adskilte systemer for lagring av data, som ikke kan utnyttes i egen kommersiell virksomhet, bør staten dekke alle kostnader ved datalagringen. Det er kun Politidirektoratet av høringsinstansene, som uttalte at ekombransjen bør betale for hele datalagringen.

2.3.3. Økonomiske utredninger
Samferdselsdepartementet og Justis- og beredskapsdepartementet har fått gjennomført fire utredninger om kostnader forbundet med DLD, henholdsvis i 2006, 2008, 2010 og 2012. De tre første utredningene ble utført av Teleplan og er av mindre relevans i dag, blant annet på grunn av at utredningene ikke omfattet alle lagringspliktige data etter direktivet. Det kan imidlertid nevnes at fra Teleplans analyser fremkommer det at dersom alle små tilbyderne utvikler en enkel løsning som kan gjenbrukes, med lokale tilpasninger hos hver enkelt tilbyder, vil en kunne få en betydelig kostnadsreduksjon. Det ble ikke gjort noen kartlegging av om en slik løsning ville bli benyttet av tilbyderne, men for tilbydere som ikke har lagringsløsninger i dag kan det være en mulighet dersom det gir kostnadsmessige besparelser i forhold til å utvikle en egen løsning. Av analysen fremgår det ikke hvilken kostnadsreduksjon som kan ventes dersom også mellomstore og store tilbydere utvikler løsninger som kan gjenbrukes. Analysen viser videre at lagringstid i liten grad påvirker kostnadene for lagring. Hovedkonklusjonene fra Teleplan var at med de systemkrav og forutsetninger som ble gitt den gang om tilgang og sikkerhet, vil tilbyderne måtte utvikle og implementere nye systemer for lagring. For tilbyderne samlet ble kostnaden den gang anslått til å bli 217 mill. kr. over en femårsperiode, basert på at de små tilbyderne vil implementere en felles standardisert løsning. Det fremkom videre at det kunne ventes liten kostnadsreduksjon som følge av delvis bortfall av dagens ordning for lagring og uthenting. Merkostnader

er således i størrelsesordenen tilsvarende de samlede kostnadene. Utredningene fra Teleplan kan lastes ned på Samferdselsdepartementets hjemmeside[2].

Den fjerde og i dag mest relevante økonomiske utredningen ble foretatt av Nexia høsten 2012, etter at Datatilsynets konsesjonsvilkår av 15. mai 2012 ble offentliggjort og Post- og teletilsynets Datalagringsforskrift hadde vært på offentlig høring.

Hovedpunkter fra Nexia-rapporten[3]
Nexia anslår at dersom alle lagringspliktige tilbydere (omlag 169) etablerer egne løsninger, vil de totale etableringskostnadene overstige en milliard kroner (1 170 mill.kr.). I et slikt tilfelle vil det også sannsynligvis påløpe høyere driftskostnader, spesielt for offentlige myndigheter, sammenlignet med en såkalt "to-systemløsning". Ved en "to-systemløsning" hvor Telenor, med ca. 50 % markedsandel, etablerer en egen løsning og de resterende tilbyderne går sammen om en annen felles løsning, estimeres etableringskostnadene til å bli på rundt 353 mill. kr. og de årlige drifts- og vedlikeholdskostnader på 70 mill. kr. Etableringskostnadene avskrives i begge tilfellene over en femårsperiode. De særnorske kravene for innføring av DLD representerer en merkostnad på rundt 170 mill. kr.

Fordelingsmodell og kostnadseffektivitet
Nexia konkluderer med at modell E *kan* være en fornuftig løsning forutsatt at det gjennomføres tiltak for å redusere de negative ringvirkningene i tilbydermarkedet. En viktig del av dette vil være å akseptere en eller flere fellesløsninger. Dette vil redusere totalkostnadene og belastningen på særlig de små tilbyderne.

Nexia understreker imidlertid at de ikke kan se de sterke argumentene som gjør at utvalget foretrekker modell E fremfor modell F. Nexia strekker seg enda lenger i å hevde at hensynet til at markedet ikke rammes av konkurransevridning eller andre negative ringvirkninger, burde veie så tungt at staten bør dekke alle kostnader knyttet til DLD. Det vises til at nivået på totalkostnadene ikke er forventet å bli betydelig påvirket selv om kostnadsansvaret delvis påhviler tilbyderne, fordi kravene staten stiller uansett vil være hoveddriveren for de totale kostnadene knyttet til DLD.

Nexia viser til at kostnadsfordelingsutvalget også er tydelig i sin rapport om at modell F er den eneste som forhindrer negative ringvirkninger i markedet, men viser til at de negative effektene vil være begrenset også med modell E, under forutsetning av at tilbydernes andel begrenses tilstrekkelig. Det vises for øvrig til utvalgets rapport som henviser til SDs brev til transport- og kommunikasjonskomiteen, samt EUs ekspertgruppe for datalagringsdirektivet som ifølge utvalget anbefaler at staten dekker alle kostnader forbundet med DLD, for å forhindre uheldige markedsmessige konsekvenser.

---

[2] http://www.regjeringen.no/upload/SD/Vedlegg/Telekommunikasjon/teleplan_utdyping.pdf#search=teleplan

[3] http://www.regjeringen.no/pages/36532538/dld-sluttrapport.pdf

Av Nexia-rapporten fremgår det videre at det er store forskjeller mellom de nordiske landene med hensyn til både tolkning og nasjonal innføring av DLD. Den største forskjellen ses i kravene til sikkerhet og kryptering. Det er kun Norge som har satt krav om spesifikke krypteringsløsninger. Sverige, Danmark og Finland opererer med normen "tilfredsstillende krav" til sikkerhet.

2.3.4. EU-kommisjonens ekspertgruppe

Av andre dokumenter og anbefalinger vises det til ekspertgruppen nedsatt av EU-kommisjonen Data Retention Expert Group. Gruppen har publisert flere dokumenter som kan lastes ned her[4]. Ekspertgruppen har vært bredt sammensatt med blant annet representanter fra påtalemyndighet, politi og datatilsyn, ekomindustrien, parlamentarikere, med flere.

Når det gjelder spørsmålet om hvem som bør bære kostnadene ved implementeringen av DLD, omhandles dette spesielt av gruppen i Position Paper No. 15.

Ekspertgruppen anbefaler at medlemsstatene vurderer alternativer for å sikre full refusjon av alle rimelige kostnader som tilbydere pådrar seg som følge av gjennomføringen av DLD. Kostnadene som dekkes av staten bør ifølge gruppen sees i sammenheng med nivået av ytelser som myndighetene i det enkelte land krever. Formålet er å skape en ordning som ikke bidrar til konkurransevridning mellom store og små tilbydere i ekombransjen. Ekspertgruppen fraråder en refusjonsordning basert på antall registrerte anmodninger fra politiet hos den enkelte tilbyder. Ekspertgruppen har vurdert en slik ordning, men kommet til at den kan være uheldig med tanke på konkurransevridning mellom ekomtilbydere av ulike størrelser og typer.

Videre anbefales det at tjenestenivået som skal kreves av tilbyderne, blir utformet i samarbeid mellom myndighetene og ekombransjen. En god og balansert ordning for dette vil ifølge ekspertgruppen kunne være en nasjonal styringsgruppe som ledes av myndighetene, og hvor ekomtilbyderne er representert. En slik styringsgruppe vil kunne vurdere innholdet i de forskjellige operative kravene, og kostnadene forbundet med disse.

2.4. Kostnadsfordeling i andre land

2.4.1. Innledning

DLD gir ikke noen anvisning på hvordan kostnadene skal fordeles. I tillegg gir direktivet en betydelig grad av frihet med hensyn til hvordan kravene kan gjennomføres nasjonalt. De nasjonale valgene av fordeling av kostnadene mellom tilbydere og stat vil også i stor grad avhenge av hvilke løsninger de ulike lands tilbydere

[4] http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/police-cooperation/data-retention/experts-group/index_en.htm

hadde i utgangspunktet, og hvor nært opptil disse løsningene de respektive landene la seg etter gjennomføringen av direktivet. Noen land har tilpasset kravene innenfor eksisterende løsninger, mens andre har etablert nye løsninger som er adskilt fra, og kommer i tillegg til, eksisterende løsninger. Videre kan det stilles ulike krav til sikkerhet, responstid, antall tilbydere som omfattes av lagringsplikt, utnyttelse av data til egen kommersiell nytte osv. De samlede kostnadene som følge av innføringen av datalagringsdirektivet vil derfor variere betydelig fra land til land. Den norske løsningen innebærer etablering av en separat løsning for datalagring med betydelige sikkerhetskrav hvor tilbyderne ikke skal kunne utnytte dataene i egen virksomhet. EU-kommisjonens evalueringsrapport[5] fra april 2011 problematiserer de store forskjellene i de ulike lands kostnadsfordelingsmodeller, da dette skaper ulike vilkår i ekommarkedene. Det anses som spesielt problematisk at små tilbydere pålegges betydelige økonomiske byrder om følge av datalagringen. Kommisjonens *Data Retention Expert Group* har sett nærmere på problemstillingen reist i evalueringsrapporten. Kommisjonen annonserte revisjon av DLD i 2012, denne er nå utsatt til etter revisjonen av EUs personvernregelverk, som er varslet vedtatt i løpet av sommeren 2014. Det gjenstår således fortsatt noe tid før Kommisjonen vil ta stilling til hvordan en eventuell harmonisering kan gjennomføres i EU.

2.4.2. Danmark

Danmark implementerte datalagringsdirektivet i 2006 og reglene trådte i kraft 15. september 2007. Det ble innført en lagringstid på 12 måneder, se nærmere om reglene i den såkalte logningsbekentgørelsen[6] (Bekendtgørelse nr. 988 af 28. september 2006). Forskriftens formål er å sikre at nærmere bestemte data er tilgjengelige dersom politiet skal ha tilgang til dem, men regulerer ikke selve tilgangen til dataene. Forskriften stiller heller ingen spesielle sikkerhetskrav knyttet til datalagringen. Det åpnes i forskriften for at andre tilbydere eller annen tredjepart kan lagre data på vegne av en tilbyder. Dette gjør at for eksempel små tilbydere, videreselgere, MVNOer[7] osv. kan tjenesteutsette lagringsforpliktelsen.

Tilbyderne i Danmark er pålagt å dekke investerings- og driftskostnadene knyttet til DLD, men staten betaler for selve uthentingen etter et stykkprissystem. Investerings- og driftskostnadene knytter seg til tilpasninger i egne drifts- og faktureringssystemer. De samlede uthentingskostnadene for politiet utgjorde i 2010 ca. 78 mill. dkk. og i 2011 ca. 81 mill. dkk. Disse tallene inkluderer også utgifter til kommunikasjonskontroll og kan således ikke sammenlignes direkte med andre lands kostnader med innføring av DLD. Etter hva departementene kjenner til er imidletid stykkpris per uthenting av DLD - data ca. 800 dkk, per "nummer" eller forespørsel. Den danske ekombransjen har selv

---

[5] http://ec.europa.eu/commission_2010-2014/malmstrom/pdf/archives_2011/com2011_225_data_retention_evaluation_en.pdf

[6] https://www.retsinformation.dk/Forms/R0710.aspx?id=2445

[7] Virtuell mobiltilbyder (Mobile Virtual Network Operator), tilbyder som benytter en annen operatørs nettverk til å produsere ekomtjenestene til sine kunder, men som for øvrig har egne sentraler og teknisk tjenesteproduksjon.

beregnet de samlede investeringskostnadene til å være i størrelsesorden 100 til 200 mill. dkk, og har antydet at de årlige samlede driftskostnader anslagsvis vil ligge på rundt 50 mill. dkk. Dette er imidlertid anslag og ikke bekreftede tall og knytter seg i stor grad til tilpasninger i tilbydernes egne drifts- og faktureringssytemer.

2.4.3. Sverige

Sverige implementerte DLD i 2012 og fastsatte lagringstiden til 6 måneder. Forskrift om kostnadsfordeling ventes å foreligge innen utgangen av 2013. Lagringspliktige data skal håndteres særskilt og sikkert, og være kryptert både når de lagres og når de overføres til lager. Flere av tilbyderne har diskusjoner om en fellesløsning for små og mellomstore tilbydere.

Tilbyderne er pålagt selv å dekke investerings- og driftskostnaden. Prissettingen av kostnadene per utlevering til politiet antas å kunne foreligge ved fastesettelsen av forskriften innen utgangen av 2013 ifølge Post och Telestyrelsen (PTS)[8]. Tilsvarende håndtering i dag koster 2 000 sek per utlevering, med ca. 10 000 forespørsler per år har politiet et budsjett på ca. 20 mill. sek. Dersom tilbyder kan påvise at det koster mer å ta frem data, kan tilbyder søke om å få utbetalt beløp ut over 2 000 sek. Per i dag finnes det i Sverige ca. 440 lagringspliktige tilbydere.

2.5. Departementenes vurderinger

2.5.1. Sentrale hensyn

Det er særlig tre hensyn som har stått sentralt i departementenes vurdering ved valget av kostnadsfordelings- modellen som foreslås. Modellen skal ivareta hovedformålet som er kriminalitetsbekjempelse, ivareta konkurransen i ekommarkedet, samtidig som den skal understøtte en samfunnsøkonomisk kostnadseffektivitet. I tillegg skal personvernhensyn vektlegges i vurderingen. Formålet med DLD er å gi politiet et effektivt verktøy i kampen mot alvorlig kriminalitet. Det har derfor vært sentralt for departementene å få på plass en kostnadsfordeling og finansieringsordning som sikrer at politiet får et godt og hensiktsmessig samarbeid med ekomtilbyderne.
Departmentene har også lagt vesentlig vekt på at ordningen som foreslås ikke skal skape unødige etableringshindringer eller konkurransevridning i ekomsektoren og da særlig med tanke på de mindre tilbyderne. Samtidig har departementene ønsket å legge til rette for til at det etableres ordninger hvor ekomtilbyderne gis insentiv til å innrette seg etter de nye kravene som følger av datalagringsdirektivet på en kostnadseffektiv måte.

2.5.2. Rammer for vurderingen av kostnadsmodel

Utgangspunktet er at private pålegges å dekke kostnader med å etterkomme offentligrettslige pålegg. Pålegg som lagring og tilrettelegging av informasjon til bruk for kriminalitetsbekjempelse er heller ikke enestående i denne sammenhengen. Blant

[8] http://www.pts.se/sv/Bransch/Internet/Integritet/Regler/Trafikdatalagring/PTS-arbete-med-trafikdatalagring/

annet legger hvitvaskingsloven opp til et til dels omfattende kontroll- og rapporteringsregime for finansforetakene for å forebygge og avdekke transaksjoner knyttet til straffbare handlinger og terrorhandlinger. Et hovedmål er her å sikre tilliten til den norske finanssektoren ved å vise til at disse bidrar til å bekjempe hvitvasking av transaksjoner på en effektiv måte. Foretak som driver valutavirksomhet plikter også å rapporte om valutaveksling og overføring av betalingsmidler inn og ut av Norge i henhold til valutaregisterloven. Hensikten er å forebygge alvorlig kriminalitet. Det er ikke lagt opp til noen form for kompensasjon fra staten for kostnadene som finansforetakene har i forbindelse med disse kravene. Eksempelvis påføres finansnæringen årlige kostnader på om lag 160 mill. kr og 24 mill. kr. for å håndtere pliktene etter henholdsvis hvitvaskingsregelverket og valutaregisterloven.

Føringene fra stortingsvedtaket med de særnorske datalagringskravene er imidlertid svært spesielle, også sammenlignet med andre land som har innført DLD. Det kreves svært omfattende sikkerhetstiltak, inkludert autorisering av personell som skal behandle lagrede data, identitets- og adgangskontroll til lagringslokaler, fysisk sikring av lagringslokaler, brannmur og kryptering av data. Sikkerhetskravene følger ikke av direktivet, men er en konsekvens av at Stortinget av personvernmessige hensyn ønsket å styrke sikkerheten ved lagring. Det vises videre til at tilbyderne selv ikke skal kunne nytte dataene i egen virksomhet.

Departementene har derfor etter en nøye vurdering kommet til at man i dette tilfellet bør kunne foreslå å gjøre et unntak fra utgangspunktet om at private parter fullt ut skal betale ved offentligrettslige pålegg. Departementene foreslår således at Staten skal dekke de anslåtte kostnadene knyttet til lagring og uthenting av data som omfattes av datalagringsdirektivet, mens tilbyderne henvises til å dekke kostnadene med å tilpasse egne systemer for å forberede lagring av lagringspliktige data etter § 2-7 a. I denne vurderingen har departementene lagt vesentlig vekt på at gjennomføringen av direktivet i liten grad bør skape etableringshindringer eller konkurransevridning i ekommarkedet. De særnorske kravene som ble vedtatt, jf. endringene i ekomloven og straffeprosessloven mv. av Stortinget i 2011, har bidratt til at det fremmes et forslag om at staten bør kompensere en større andel av kostnadene for gjennomføringen av direktivet.

2.5.3. Nærmere om kostnadsmodell

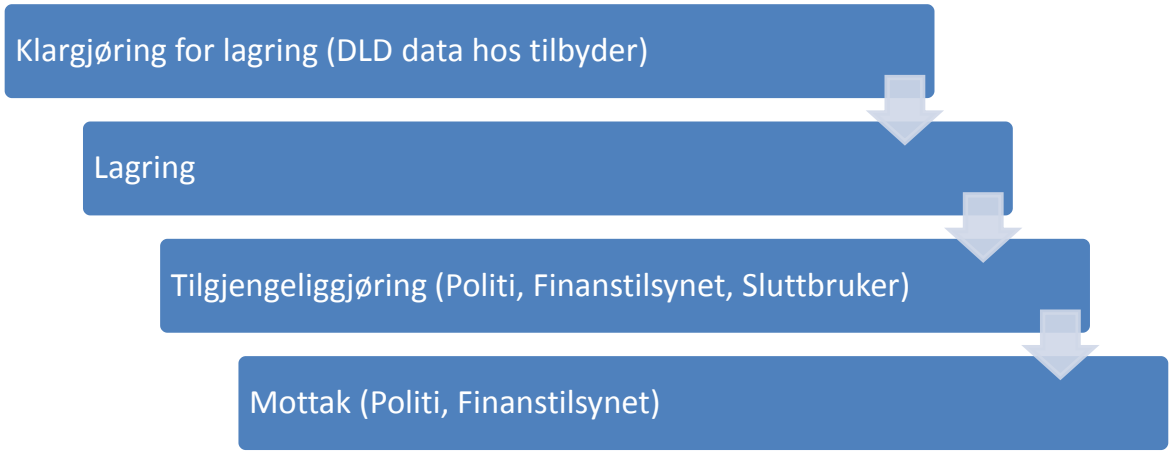
Kostnadsfordelingsmodellen som nå foreslås følger i stor grad de samme linjer som hovedelementene i anbefalingen kostnadsfordelingsutvalget. Nexia som utarbeidet den siste kostnadsberegningen i 2012 sluttet seg også til utvalgets anbefaling. Modellen som utvalget anbefalte var at staten skulle finansiere hoveddelen av kostnadene ved gjennomføringen av direktivet etter en fordelingsnøkkel, mens tilbyderne skulle dekke en mindre andel. Departementene vil imidlertid presisere at Kostnadsfordelingsutvalget la til grunn som en forutsetning at kostnadene ville bli svært høye. I tillegg ble det tillagt stor vekt i utvalgets konklusjon at

kostnadsfordelingsmodellen ikke måtte utgjøre en etableringshindring eller være konkurransevridende.

Departementet ønsker i utgangspunktet en finansieringsordning som dekker kostnader etter kategori, jf. figur 1 nedenfor. Bakgrunnen for en slik ordning er at det vil bidra til å bedre oversikt over de forskjellige kostnadselementene i ordningen, identifisering i hvilke kategori kostnadene påløper, bidra til en enklere administrasjon og gi insitamenter til at at flere tilbydere kan gå sammen om noen få felles lagringsløsninger for DLD-data. Det må legges til grunn, bl.a. basert på Nexias rapport, at felles lagringsløsninger trolig vil ha langt lavere kostnader, høyere kvalitet og minst like høyt sikkerhetsnivå som separate løsninger. Et godt eksempel på at norske tilbydere i samarbeid med ekommyndigheten har evnet å etablere kostnadseffektive og gode systemer er systemet for nummerportering og opprinnelsesmarkering, hvor Norsk Referansedatabase (NRDB), opprettet i 2001 og eid av de sju største norske ekomtilbyderne, har etablert en fellesløsning som trolig både er mer effektiv operasjonelt sett, og til lavere kostnader enn lignende løsninger i andre europeiske land. Dersom staten skulle finansiert etter en fordelingsnøkkel basert på en prosentandel av totalbeløpet er departementene av den oppfatning at tilbyderne ikke ville fått tilstrekkelig insentiv til å innordne seg på den mest kostnadseffektive måte. Nexia gir også uttrykk for i sin rapport at det vil være hensiktsmessig å tillate en eller flere fellesløsninger for å redusere totalkostnadene, samtidig som man vil forebygge en konkurransevridende effekt mellom store og små tilbydere.

Ved etablering av felles lagringsløsninger for tilbyderne vil det også bli enklere å skille mellom klargjøringskostnader i egne systemer og lagringskostnader. Tilbyderne vil få klarere insentiver til å lage kostnadseffektive løsninger til forberedelse for lagring av data i egne drifts- og faktureringssystemer, og staten vil enklere kunne føre kontroll med kostnadseffektiviteten med noen få større felles lagringsløsninger.

Etter departementenes vurdering kan man for å synliggjøre hovedaktivitetene og kostnadselementene i et DLD system fremstille det skjematisk slik:



Figur 1. Hovedaktiviteter og kostnadselementer i et DLD-system

En modell hvor tilbyderne må dekke alle sine kostnader til klargjøring for lagring uten kompensasjon, er en løsning som er i overensstemmelse med utgangspunktet for andre næringer som har blitt pålagt kriminalitetsbekjempende tiltak, slik som finansnæringen som ble pålagt å tilrettelegge data uten kompensasjon ved opprettelsen av valuttaregisteret og hvitvaskingsregisteret. En modell som den som her foreslås ligner også mest på den eksisterende ordningen i ekomloven jf. § 2 – 8, og modell C i kostnadsfordelingsutvalgets rapport. Som følge av Stortingets omtale i Innst. 275 L (2010-2011) til lovvedtaket er det imidlertid ikke aktuelt at staten skal eie og administrere et DLD-register, slik ordningen er med for eksempel valutaregisteret og hvitvaskingsregisteret. Det har for DLDs del vært et bevisst valg av Stortinget at ekomtilbyderne selv skal være ansvarlig for lagringen selv om dataene kun er til offentligrettslige formål og tilbyderne ikke vil ha noen eierbeføyelser over dataene som skal lagres. Dette kan likevel ikke anses å være til hinder for at staten kompenserer for kostnader som ellers ville påløpt dersom staten selv sto som ansvarlig for registeret. Det foreslås derfor en kostnadsfordelingsmodell som innebærer at tilbyderne dekker tilrettelegging kostnadene (fase 1) fullt ut, mens staten dekker kostnadene knyttet til lagring og uthenting av data (fase 2, 3 og 4 i figur 1).

I modellen som nå foreslås vil etableringskostnadene for systemer til å forberede eller tilrettelegge for lagring etter DLD bli omlag 120 mill. kr. som en engangsinvestering for ekomtilbyderne samlet sett. Årlige driftskostnad for denne delen vil bli på omlag 18 mill. kr. Departementene mener at ordningen som foreslås ikke vil skape nevneverdige negative effekter for konkurransen i markedet.

Med bakgrunn i funn identifisert i ovennevnte utredninger er det også ønskelig å legge til rette for en ordning med noen få lagringsløsninger, som tilbyderne i ekombransjen selv står ansvarlig for. Departementene er kjent med at det har vært gjort enkelte forsøk på å få etablert en felles bransjestandard om felles format for tilrettelegging og utlevering av lagringspliktig data. Etter det departementene kjenner til eksisterer det per i dag ingen slik felles bransjestandard, noe som øker sannsynligheten for at kvaliteten ikke vil oppleves som tilfredsstillende for brukerne av dataene, dersom disse skal mottas fra opp til ca. 170 pliktsubjekter.

Staten kan, slik rammene nå er utformet, ikke legge føringer for hvordan den enkelte aktør velger å etterkomme kravene som DLD oppstiller. Departementene vil imidlertid presisere at beløpet som skal bevilges over budsjettet til kostnadsdekning er basert på at det etableres to sentrale databaser for lagring av DLD-data. Beløpet som bevilges vil bli fordelt mellom tilbyderne. Dette omtales nærmere under neste punkt om stykkprisfinansierng.

Det foreslås derfor en ordning der tilbyderne stimuleres til å velge en felles lagringsløsning, både for å sikre kostnadseffektivitet og at data som politiet etterspør kan utleveres med kort responstid i et lesbart format.

Ved valg av kostnadsfordelingsmodell har det vært viktig for departementene å sikre en kostnadsdeling som ivaretar balansen mellom hensynene til kriminalitetsbekjempelse og personvern, samt sikre like konkurransevilkår og levedyktigheten for ekombransjen. Etableringshindringer og konkurransevridninger kan være en stor samfunnsøkonomisk kostnad. Modellen som nå foreslås ivaretar etter departementetenes syn disse utfordringene på en god måte, spesielt for de små og mellomstore tilbyderne.

2.5.4. Stykkprisfinansiering

Departementene foreslår en modell hvor tilbyder får kostnadsdekning for lagring og tilgjengeliggjøring av lagringspliktige data basert på antall abonnenter tilbyder har. Departementenes forslag følger her en av tre anbefalte modeller (Modell 3) som anbefales av ekspertgruppen (Data Retention Expert Group) nedsatt av EU-kommisjonen. Forslaget til modell er i tråd med de prinsipper som ekspertgruppen har nedfelt for kostnadsdekning. Departementene har søkt å få i stand en finansieringsordning som ivaretar både ekomtilbydernes og politiets interesser. Det har vært spesielt viktig å unngå konkurransevridning mellom små og store tilbydere.

En finansieringsordning hvor det spesifiseres en stykkpris for lagring og uthenting av data knyttet opp mot antall abonnenter hos tilbyder, antas også å kunne gi tilbyderne større insentiver til å gå sammen med andre tilbydere for å etablere felles og kostnadseffektive lagringsløsninger. En slik ordning antas også å kunne bidra til å utjevne belastningen mellom store og små tilbydere med hensyn til kapitalkostnader mv.

Gjennomføring av lagringsplikten for trafikkdata, lokaliseringsdata og abonnements-/brukerdata ved bruk av elektronisk kommunikasjon som fasttelefoni, mobiltelefoni, internettaksess, e-post og bredbåndstelefoni vil kunne ha ulik kostnad knyttet til lagring for den enkelte ekomtjeneste. Modellen innebærer at ekomtilbyderne får dekket sine kostnader gjennom en tilskuddsordning basert på antall abonnenter for hver tjeneste som er underlagt pliktig datalagring. Satsene vil bli av sjablongmessig karakter som igjen vil måtte bli differensiert etter faktiske kostnader knyttet til lagring for den enkelte ekomtjeneste. Dette innebærer at det må beregnes en flat sats per abonnent for hver enkelt lagringspliktig tjeneste. Disse satsene må beregnes nærmere på et noe senere tidspunkt. Det vil bli satt ned en arbeidsgruppe under ledelse av Post- og teletilsynet for å beregne disse satsene.

Departementene har særskilt vurdert om tilbyderne burde få kostnadsdekning for tilgjengeliggjøring av data for politiet, basert på antall henvendelser. En ordning basert på antall anmodninger kan etter departementenes mening i større grad skape konkurransevridning mellom store og små tilbydere enn den ovennevnte. Departementenes forslag følger EUs ekspertgruppes anbefaling på dette punktet, men det inviteres særskilt til innspill fra høringsinstansene. Ordningen som foreslås vil også ivareta politiets behov for å holde de administrative kostnadene lave. De lovmessige

begrensningene for politiets bruk av data som er underlagt lagringsplikt vil etter departementenes mening være tilstrekkelig for til å begrense politiets anmodninger om trafikkdata. Politiets anmodning om trafikkdata bør uansett bare foretas etter forsvarlige faglige prioriteringer.

For å sikre at ekomtilbyderne får dekket kostnader for lagring og tilgjengeliggjøring vil det bli foretatt kostnadsberegninger av ekombransjens totale kostnader forbundet med DLD. Departementene vurderer på nåværende tidspunkt at dette vil være tilstrekkelig for å sikre ekomtilbyderne kostnadsdekning for lagring og tilgjengeliggjøring av data. EUs ekspertgruppes anbefaling om etablering av en nasjonal styringsgruppe har man kommet til vil bli svært ressurskrevende i forhold til behovet på nåværende tidspunkt. Departementene utelukker imidlertid ikke at dette kan bli aktuelt på et senere tidspunkt. Det bes imidlertid om særlige innspill på dette punktet. Satser og regler for utmåling av kostnadsdekning til tilbyderne vil bli regulert i forskrift fastsatt av Post- og teletilsynet. Politidirektoratet vil få ansvaret for å administrere ordningen. Direktoratet vil kunne holde tilbake finansiering av kostnader dersom tilbyderen ikke oppfyller de krav som stilles i lov og forskrift som følger av DLD.

Samlet sett mener departementene at modellen i liten grad vil påvirke konkurransen i ekommarkedet. Bekymringen har vært rettet mot de små og mellomstore tilbyderne, og svekkelsen av mulighetene for fortsatt å kunne legge til rette for innovasjon i tillegg til å opprettholde relativt lave etableringshindringer i markedet. I løsningen som nå foreslås, kommer etter departementenes syn alle disse forholdene relativt godt ut.

Uavhengig av flat sats eller differensiering mener departementene at tilbydere bør stimuleres til å inngå samarbeid om lagring for å redusere egenandelen.

Det forventes at de tilbydere som er omfattet av lagringsplikten vil trenge noe tid til å få gjort de nødvendige tilpasninger og innført de nødvendige systemer etter at kravene er på plass. Departementene foreslår derfor å legge opp til at ikrafttredelsen for selve lagringsplikten som følger av ekomloven § 2-7 a, blir 1. januar 2015. Tilbyderne vil således få tiden frem til 1. januar 2015 til å tilpasse seg de nye kravene.

2.6. Nærmere om lovforslaget

Det foreslås at staten skal dekke kostnader knyttet til lagring og uthenting av data som omfattes av datalagringsdirektivet, mens tilbyderne skal dekke kostnadene med å tilpasse egne systemer for å forberede lagring av lagringspliktige data etter § 2-7 a. Departementet foreslår at den nye kostnadsdelingsmodellen kun skal omfatte lagringspliktige data etter ekomloven § 2-7a.

Dette medfører at den etablerte ordningen for kostnadsdeling når det gjelder tilrettelegging for lovbestemt tilgang til informasjon om sluttbruker og elektronisk kommunikasjon videreføres. Tilretteleggingsplikten ekomtilbyderne har overfor politiet

med hensyn til kommunikasjonskontroll og tilhørende trafikkdata mv. i medhold av § 2-8, holdes ved dette forslaget adskilt fra lagringsplikten i § 2-7a.

2.7. Administrative og økonomiske konsekvenser

Innføring av datalagringsdirektivet medfører økte kostnader både for staten og for tilbyderne. Post- og teletilsynet har anslått at det vil være 169 lagringspliktige subjekter. Dette er tilbydere av fasttelefoni, mobiltelefoni, internettelefoni og internettaksess. Enkelte av disse tilbyderne har felles underliggende tjenesteleverandører for de tjenestene som utløser lagringsplikt. Det antas at virksomhetene kan gå sammen for å redusere administrative og økonomiske konsekvenser av lagringsplikten. Forslag innebærer at tilbyderne vil måtte dekke alle etablerings- og driftskostnader i sine respektive systemer for tilrettelegging og oversendelse av lagringspliktige data til den dedikerte datalagringsbasen, og staten dekker alle anslåtte kostnader knyttet til lagring av data i datalagringsbasen og politiets uthenting av data. De samlede etableringskostnadene anslås til å bli 353 mill. kr, med en avskrivningsperiode på fem år. De årlige drifts- og vedlikeholdskostnadene anslås til om lag 70 mill. kr. Kostnadene fordeler seg med ca. 120 mill.kr. til etableringskostnader for ekomtilbydernes forberedende fase hvor data skal hentes fra tilbydernes produksjonssystemer mv, hvoretter ca. 18 mill. kr. vil påløpe til årlig drift, samlet sett for tilbyderne. Disse utgiftene foreslås dekket fullt ut på ekomtilbydernes hånd. Det er videre beregnet at kostnader for etablering av løsninger for selve lagringen, overleveringen til politiet og mottaket hos politiet vil beløpe seg på ca. 233 mill. kr. Deretter omlag 54 mill. kr. i årlige driftskostnader. Disse utgiftene foreslås dekket fullt ut av staten.

Tilretteleggingskostnadene (fase 1 i figuren ovenfor) vil utgjøre ca. 33 prosent av totalkostnadene. Lagringskostnadene vil utgjøre ca. 60 prosent og utleveringskostnadene ca. 7 prosent. Med totalkostnadene forstås i denne sammenheng investeringskostnadene for å etablere basene samt kostnadene for tilhørende tilpasninger og systemer hos tilbyderne og politi. De totale kostnadene er i denne sammenheng estimert til omlag 353 mill. kr.

Enhver kostnadsdelingsmodell vil medføre administrasjonskostnader. Den anbefalte modellen hvor tilbyder får tilskudd av myndigheten for etablering og drift av datalagringsbasen(e), forutsetter at myndigheten fører tilsyn og kontroll med tilbydernes faktiske og fakturerte kostnader knyttet til oppfyllelse av plikten. Post- og teletilsynet vil måtte dekke sine kostnader til dette tilsynet gjennom gebyrer, jf. forskrift om gebyr til Post- og teletilsynet. Det foreslås videre at det stilles krav om at regnskap for kostnadsdekningen godkjennes av ekstern revisor. Dette vil forenkle tilsynsoppgavene på området.

3. Om politiets uthenting av data i nødssituasjoner

3.1. Innledning

I Innst. nr. 275 (2010-2011) ba Stortinget regjeringen om å se nærmere på utformingen av en lovbestemmelse som regulerer politiets uthenting av elektronisk kommunikasjon i nødssituasjoner.

Hvert år leter politi og andre redningsmyndigheter etter et stort antall personer som av forskjellige årsaker er forsvunnet eller på andre måter er i fare. Informasjon om hvor personens mobiltelefon befinner seg, hvem personen har vært i kontakt med og tidspunktet for kontakten vil være av stor betydning for letearbeidet. I disse sakene vil rask utlevering av opplysninger kunne være helt avgjørende for operasjonens utfall.

I dag hjemler politiet sin uthenting av opplysninger fra ekomtilbyderne i nødssituasjoner i den generelle nødrettsbestemmelsen i straffeloven. En egen bestemmelse i ekomloven vil synliggjøre politiets rett til å hente ut opplysninger fra tilbyderne i disse situasjonene, og således bidra til større forutberegnelighet.

3.2. Beskrivelse av gjeldende rett

3.2.1. Utlevering av data fra ekomtilbyderne

Elektronisk kommunikasjon er taushetsbelagte opplysninger, jf. ekomloven § 2-9. Utlevering av slike opplysninger krever et særskilt hjemmelsgrunnlag.

Foruten i nødssituasjoner kan data i form av elektronisk kommunikasjon utleveres til politiet når kunden samtykker til utlevering, og når straffeprosessloven kapittel 16 og 16a gir hjemmel for utlevering.

Uthenting med hjemmel i straffeprosessloven kan bare skje i forbindelse med avverging eller etterforskning av straffbare forhold. Bestemmelsene i kapittel 16 og 16a angir nærmere hvilke vilkår som må være oppfylt for at utlevering kan skje. Mens reglene for utlevering i straffeprosessloven kapittel 16 kun gir hjemmel for utlevering av *historiske data*, gir reglene for kommunikasjonskontroll i straffeprosessloven kapittel 16a også hjemmel for utlevering av *sanntidsinformasjon* og pålegg om *fortløpende utlevering*.

For å gjennomføre datalagringsdirektivet har Stortinget vedtatt egne bestemmelser i straffeprosessloven for uthenting av data fra ekomtilbyderne. Det er gjort nærmere rede for endringene i Innst. nr. 275 L (2010-2011).

3.2.2. Den generelle nødrettsbestemmelsen i straffeloven

Nødrett rettferdiggjør en utvidelse av handlefriheten i nødssituasjoner. Det er i slike situasjoner tillatt å handle på en annen og avvikende måte enn det normene for en

normalsituasjon krever, dersom slik handling er nødvendig for å redde en person eller et annet rettsgode som befinner seg i en nødssituasjon.

De materielle vilkårene for strafferettslig nødrett er nedfelt i straffeloven § 47. I den nye straffeloven § 17 videreføres hovedsakelig gjeldende rett på dette punkt. Forutsetningen for å bygge på nødrett er at det foreligger en fare som i interesse klart overstiger verdien av det inngrepet avvergingshandlingen medfører. Det legges opp til en forholdsmessighetsvurdering hvor verdien av det som befinner seg i en nødsituasjon veies opp mot normen som brytes. Sannsynligheten for at skade vil inntre og sannsynligheten for at redningshandlingen vil lykkes, vil være relevant i vurderingen.

3.2.3. Eksempler på nødssituasjoner hvor uthenting av data fra ekomtilbyderne vil være et effektivt virkemiddel

Både når det letes etter bestemte personer som er savnet, og når det letes etter overlevende etter en ulykke eller i forbindelse med en katastrofe, vil uthenting av data kunne være et vesentlig og avgjørende virkemiddel.

Personer som er savnet

Oppstart av lete- og redningsarbeid skjer enten etter at andre personer har meldt en person savnet, eller når en person selv har gitt politiet opplysninger som indikerer at vedkommende er i fare. Personen kan meldes savnet fra sitt hjem, fra psykiatrisk institusjon eller fra en institusjon for eldre. Barn kan meldes savnet fra sitt hjem, fra asylmottak eller fra barnevernsinstitusjon. En del personer blir borte på fjellet eller går seg vill andre steder i naturen. Politiet gjør i slike situasjoner en vurdering av om igangsetting av redningsarbeid er nødvendig. Det legges blant annet vekt på personens mentale helse, personens alder og personens tidligere handlingsmønstre. En stor andel av personene som meldes savnet er å regne som suicidale.

En konkret angivelse av hvilket geografisk område savnedes kommunikasjonsutstyr befinner seg i, vil kunne være viktig og ofte helt avgjørende for letearbeidet. Informasjon om hvem personen har vært i kontakt med vil også kunne være av interesse.

Både når det letes etter bestemte personer som er forsvunnet og når det letes etter overlevende etter en ulykke eller i forbindelse med en katastrofe, kan uthenting av elektronisk kommunikasjon være vesentlig og avgjørende for utfallet av redningsarbeidet.

Annet redningsarbeid

I forbindelse med naturkatastrofer eller andre ulykker vil utskrift fra basestasjonssøk kunne være med på å gi redningsmannskapet oversikt over om det befinner seg personer innenfor et område. Flom, jordras eller snøras er eksempler på naturkatastrofer hvor opplysninger fra tilbyderne vil kunne være relevante. Bygg som brenner, skip som havarerer, tog- og flyulykker er eksempler på ulykker hvor slik

informasjon vil kunne være av betydning for politiets arbeid. I slike situasjoner må det selvsagt tas i betraktning at personen og personens telefon ikke nødvendigvis befinner seg på samme sted. En oversikt over kommunikasjonsutstyr som befinner seg innenfor et område vil av denne grunn ikke nødvendigvis gi et sannferdig bilde av hvor mange og hvilke personer som befinner seg der.

Etterforskning i etterkant av en ulykke er ikke å regne som en nødsituasjon. Dersom politiet for eksempel har behov for å finne ut hvem som befant seg innenfor et område innenfor et visst tidsrom, må de benytte andre hjemler for å kreve utlevering.

Gråsonen mellom redningsarbeid og avverging eller etterforskning av et straffbart forhold

Noen redningsaksjoner går fra å være rene redningsaksjoner til å bli avverging eller etterforskning av et straffbart forhold. Et eksempel på en slik situasjon er kidnapping, eller en trussel- eller gisselsituasjon. Straffeprosesslovens regler vil komme til anvendelse når det foreligger mistanke om at et straffbart forhold er begått eller vil kunne bli begått.

3.2.3. Relevante data i nødssituasjoner

Stedsspesifikke og personspesifikke data

I nødssituasjoner vil det primært være stedsspesifikke data, som sier noe om hvor personen befinner seg som er av interesse for politiet. Sanntidsinformasjon vil være av størst interesse, men også historiske data vil kunne være relevante. I redningsarbeidet vil det være behov for å få tilgang til en så korrekt angivelse av kommunikasjonsutstyrets plassering som mulig.

Personspesifikke data vil gi politiet informasjon om hvem personen har vært i kontakt med den siste tiden. Av størst interesse er trafikkdata fra savnedes telefon, men også IP-adresser og epostkommunikasjon vil kunne være relevante.

Når politiet leter etter overlevende i et område, vil utskrifter fra nærmeste basestasjon kunne si noe om hvem som befinner seg innenfor et avgrenset geografisk område innenfor en begrenset tidsperiode.

Kommunikasjonskontroll

Kommunikasjonskontroll, i form av telefonavlytting, vil kunne være et nyttig virkemiddel i nødssituasjoner. Politiet iverksetter i dag telefonavlytting med hjemmel i nødretten. Særlig i situasjoner hvor politiet har indikasjoner på at det har skjedd eller vil kunne skje noe straffbart, men hvor mistankegrunnlaget foreløpig ikke er tilstrekkelig til å iverksette tiltak i medhold av straffeprosessloven, vil dette kunne være aktuelt. Politiet kan for eksempel ha løsere indikasjoner på at en person er utsatt for trusler eller tvang. I flere situasjoner hvor politiet igangsetter kommunikasjonskontroll i medhold av nødretten, utvikler situasjonen seg til å bli en avverging- eller etterforskningssituasjon.

I tilfeller hvor politiet iverksetter kommunikasjonskontroll i form av telefonavlytting uten forhåndsgodkjennelse fra domstolen, skal påtalemyndighetens beslutning forelegges domstolen for etterfølgende kontroll, jf. straffeprosessloven § 216 d. All bruk av kommunikasjonskontroll skal rapporteres til riksadvokaten i medhold av kommunikasjonskontrollforskriften § 3.

Ny ekomlov § 2-9a vil ikke gi hjemmel for igangsetting av kommunikasjonskontroll i form av telefonavlytting. I tilfeller hvor politiet har behov for å iverksette telefonavlytting i nødssituasjoner må dette også i fremtiden hjemles i den generelle nødrettsbestemmelsen.

3.2.4. Beskrivelse av hvordan og hvor hyppig utlevering skjer i dag

Det er politiet som er ansvarlige for iverksetting og organisering av redningsarbeid når menneskers liv eller helse er truet, jf. politiloven § 27 første ledd. I henhold til politiloven, politiinstruksen og organisasjonsplan for redningstjenesten har politiet ansvar for å koordinere og lede redningsinnsats av enhver art.

Redningsmyndighetenes oppgave er å redde menneskeliv. Dette omfatter alt fra innsats ved store katastrofer til søk etter en savnet skiløper i fjellet. Redningsaksjoner ledes og koordineres enten av Hovedredningssentralen (HRS), eller av lokale redningssentraler (LRS). Det finnes to Hovedredningssentraler i Norge, en i Nord-Norge og en i Sør-Norge. Politimestrene i henholdsvis Rogaland og Salten politidistrikt er sentralenes ledere. Lokale redningssentraler er etablert ved alle de lokale politidistriktene. Alle store redningsaksjoner og all sjøredning organiseres fra HRS, mens mindre redningsaksjoner organiseres fra LRS.

I følge HRS er uthenting av data særlig nyttig i redningsaksjoner hvor det søkes etter savnede personer på land. I 2011 har HRS registrert 1233 hendelser av savnet person på land. I 2010 var det tilsvarende tallet 1160. Uthenting av data kan også være nyttig i redningsarbeid på sjøen. I 2011 har HRS registrert 85 hendelser av savnede fritidsbåter, fiskebåter eller kommersielle fartøy. I 2010 var det tilsvarende tallet 75. Tallene er hentet fra Hovedredningssentralens hjemmesider.

Fra HRS opplyses det om at ekomtilbyderne utleverer nødvendig informasjon raskt, gjerne allerede i løpet av få minutter.

I nødssituasjoner henvender politiet og redningssentralene seg direkte til netteierne for utlevering av data. Det er for tiden tre landsdekkende mobilnett i Norge; Telenor, Telia Sonera Norge og Mobile Norway. Telenor har opplyst at de mottok 689 nødrettsanmodninger i 2011. Telia Sonera Norge mottok i samme periode 446 nødrettsanmodninger. Mobile Norway har opplyst at de mottar omtrent en nødrettsanmodning i uken. Opplysningene fra Telenor og Telia Sonera Norge viser at det var HRS som anmodet om utlevering i 80 % av tilfellene, mens lokale politidistrikt sto bak de resterende anmodningene.

3.2.5. Rettstilstanden i Sverige og Danmark

Sverige
Gjennomføringen av EUs datalagringsdirektiv ble vedtatt med virkning fra 1. mai 2012.

Det er foreslått endringer i reglene som regulerer myndighetenes uthenting av data fra ekomtilbyderne. I Prop. 2011/12:55 *«De brottbekämpande myndigheternas tillgång till uppgifter om elektronisk kommunikation»*, som ble vedtatt av den svenske regjeringen 10. februar 2012, har det blant annet blitt foreslått å innføre utvidede muligheter for politiet til å få tilgang til posisjoneringsdata når det letes etter savnede personer.

I Lag om elektronisk kommunikation (2003:389) foreslås det innført et nytt tredje ledd i 22 § i sjette kapittel som gir ekomtilbyderne fritak fra taushetsplikten i disse tilfellene.

Fritaket fra taushetsplikten foreslås å omfatte abonnementsopplysninger og informasjon om hvem personen har vært i kontakt med og når, men ikke informasjon om innholdet av kommunikasjonen, jf. foreslått 22 § kap 6, jf. 20 § kap 6. Fritaket vil også omfatte *«uppgift om i vilket geografisk område en viss elektronisk kommunikationsutrustning finns eller har funnits»,* jf. foreslått 22 § kap 6.

Opplysningene skal utleveres til politiet dersom myndighetene finner at «*uppgiften behövs i samband med efterforskning av personer som har försvunit under sådana omsändigheter att det kan befaras att det föreligger fara för deras liv eller allvarlig risk för deras hälsa.»*

Danmark
Ekomtilbydernes utlevering av opplysninger i nødssituasjoner er ikke lovregulert i Danmark. Den danske retsplejelov kapittel 71 regulerer utlevering av opplysninger i forbindelse med forbindelse med avvergelse eller etterforskning av en straffbar handling. Utlevering av opplysninger i forbindelse med annet redningsarbeid må eventuelt skje på ulovfestet grunnlag.

3.3. Departementenes vurderinger

3.3.1. En reell nødssituasjon
I nødretten legges det opp til at det skal gjøres en forholdsmessighetsvurdering hvor verdien av det som befinner seg i en nødssituasjon veies opp mot normen som brytes. I situasjoner hvor det er fare for personers liv eller helse vil aldri uthenting av opplysninger fra ekomtilbyderne være uforholdsmessig.

Det bemerkes at uthenting av steds- og personspesifikke opplysninger vil være et svært effektivt virkemiddel når det letes etter personer. I mange tilfeller vil uthenting av slike

opplysninger være den eneste måten politiet kan finne og redde personen som er savnet i tide.

I nødssituasjoner vil det særlig være opplysninger fra den savnede personens kommunikasjonsutstyr som er av interesse for politiet. I en del konkrete redningsaksjoner vil det kunne legges til grunn at den savnede personen *stilltiende samtykker* til at opplysningene hentes ut. Uthenting av opplysninger vil i disse tilfellene være helt uproblematisk.

I andre situasjoner vil det kunne være mer uklart om den savnede personen er frivillig eller ufrivillig utilgjengelig. Uthenting av opplysninger fra en person som frivillig har gjort seg selv utilgjengelig, vil ikke være uforholdsmessig hvis uthentingen er nødvendig for å beskytte personers liv eller helse. Det må altså gjøres en vurdering av om personen er i reell fare.

Det er vanskelig å se for seg rene redningsaksjoner hvor man har behov for å hente ut opplysninger fra kommunikasjonsutstyret til andre personer enn den personen man leter etter. I situasjoner hvor politiet har behov for å hente ut opplysninger om eller fra andre personers kommunikasjonsutstyr, vil politiet som regel ha mistanke om et straffbart forhold.

Ved vurderingen av om uthenting skal kreves, er politiet forpliktet til å vurdere hensiktsmessigheten, nødvendigheten og forholdsmessigheten av uthenting som virkemiddel, jf. politiloven § 6.

3.3.2. EUs datalagringsdirektiv

Hensikten med EUs datalagringsdirektiv er å tilrettelegge for lagring av informasjon som vil være av betydning for politiets etterforskning av alvorlig kriminalitet, jf. direktivets artikkel 1. I direktivets artikkel 4 fastslås det at utlevering til kompetente myndigheter kun kan skje i «særlige sager og i overensstemmelse med national lovgivning,» jf. den danske oversettelsen av direktivet.

Det er departementenes oppfatning at nødssituasjoner, hvor utlevering skjer for å redde personer som er i fare, er å regne som «særlige sager», og at direktivet ikke stenger for at opplysninger som lagres i medhold av ny § 2-7a i ekomloven kan utleveres til politiet i nødssituasjoner.

3.3.3. Den europeiske menneskerettighetskonvensjonen (EMK) artikkel 8

EMK artikkel 8 gir rett til vern av privatliv, familieliv, hjem og korrespondanse. Både steds- og personspesifikke opplysninger som stammer fra en persons kommunikasjonsutstyr er å regne som korrespondanse. Inngrep i rettighetene som vernes av artikkel 8 kan bare skje dersom inngrepet har hjemmel i lov, er i samsvar med et av formålene artikkelen oppstiller og er nødvendig i et demokratisk samfunn for å oppnå det aktuelle formålet (inngrepet må ikke være uforholdsmessig).

Hjemmelsgrunnlaget for uthenting av opplysninger i nødssituasjoner vil være ny ekomlov § 2-9a, og formålet med uthentingen er å beskytte personers liv og helse. Departementene mener uthenting av opplysninger fra ekomtilbyderne ikke vil være uforholdsmessig når formålet er å beskytte personers liv og helse.

3.3.4. Straffeprosesslovens regler om uthenting og vitneplikt

Som tidligere nevnt utvikler noen nødssituasjoner seg fra å være rene redningsaksjoner til å bli avverging eller etterforskning av straffbare forhold. Det fremstår som naturlig at påtalemyndigheten i disse tilfellene benytter sin hastekompetanse, og i medhold av straffeprosessloven § 210 annet ledd beslutter at eventuell uthenting som er iverksatt i medhold av ny ekomlov § 2-9a skal opprettholdes. Forutsetningen vil være at vilkårene for uthenting i medhold av straffeprosesslovens §§ 210 b og c er oppfylt. Påtalemyndighetens beslutning må godkjennes av retten i ettertid, jf. straffeprosessloven § 210 annet ledd.

For opplysninger som er uthentet i medhold av straffeprosessloven §§ 210 b og c, har ekomtilbyderne vitneplikt i en eventuell etterfølgende straffesak, jf. straffeprosessloven § 118 a. Det er departementenes syn at også opplysninger som blir uthentet i medhold av ekomloven, vil omfattes av vitneplikten i straffeprosessloven § 118 a, dersom vilkårene for uthenting i straffeprosessloven §§ 210 b og c er oppfylt.

3.3.5. Etterfølgende kontroll

Departementene finner det hensiktsmessig å etablere en ordning for etterfølgende kontroll. Formålet med kontrollen vil være å tilse at politiet ikke misbruker hjemmel for uthenting av opplysninger fra tilbyderne i nødssituasjoner. Den etterfølgende kontrollen kan enten skje ved at et eksternt organ fører tilsyn, eller ved domstolskontroll.

Etter departementenes oppfatning er det tilstrekkelig å innføre en ordning hvor et eksternt organ fører tilsyn. En slik kontroll vil være tilstrekkelig for å oppnå formålet om å tilse at politiet ikke misbruker sin hjemmel. Det legges vekt på at uthenting av opplysninger i nødssituasjoner i utgangspunktet er et mindre inngripende tiltak.

Departementene foreslår at det innføres en ordning hvor lokale politidistrikt rapporterer sin uthenting av opplysninger i nødssituasjoner til Politidirektoratet (POD). Det er naturlig å se for seg at politidistriktene utarbeider samlerapporter og rapporterer til POD en gang i kvartalet eller en gang i halvåret. POD vil måtte utarbeide retningslinjer for hvordan rapporteringen skal skje. Videre foreslås det at POD samler rapportene i en årsrapport, som sendes til et eksternt organ for tilsyn.

Rutiner for eksternt tilsyn finnes i dag for politiets bruk av kommunikasjonskontroll. Kontrollutvalget for kommunikasjonskontroll kontrollerer at politiets bruk av kommunikasjonskontroll skjer innenfor rammen av gjeldende regelverk. Deres mandat

og hvordan kontrollen gjennomføres er regulert i kommunikasjonskontrollforskriften kapittel to.

Det foreslås at kontroll med politiets uthenting av opplysninger fra tilbyderne i nødssituasjoner legges til Kontrollutvalget for kommunikasjonskontroll. En slik løsning nødvendiggjør visse endringer i kommunikasjonskontrollforskriften. Departementene foreslår at ordningen med at Kontrollutvalget for kommunikasjonskontroll fører tilsyn evalueres etter en toårs periode.

Alternativet vil være å innføre etterfølgende domstolskontroll. Det er naturlig å se for seg at domstolskontrollen gjennomføres ved kontorforretning.

Departementene ber høringsinstansene om tilbakemelding på hensiktsmessigheten av etterfølgende kontroll og hvilken form de mener den etterfølgende kontrollen skal ha.

3.4. Nærmere om forslaget til ny ekomlov § 2-9a

Departementene foreslår en ny bestemmelse i ekomloven, § 2-9a, som i nødssituasjoner opphever tilbydernes taushetsplikt og samtidig gir politiet myndighet til å hente ut opplysninger fra tilbyderne. Det vil være politimesteren eller den politimesteren gir myndighet som beslutter utlevering. Avgjørende for om utlevering skal kunne kreves, vil være om nødssituasjonen er reell, altså om det er fare for personers liv eller helse. Departementene foreslår å innføre en ordning hvor et eksternt organ fører etterfølgende kontroll med politiets uthenting av opplysninger fra tilbyderne i nødssituasjoner.

3.5. Administrative og økonomiske konsekvenser

I dag uthentes opplysninger fra tilbyderne i alle nødssituasjoner hvor det er behov for det. Det er ingen grunn til å tro at politiets uthenting av opplysninger fra tilbyderne vil øke ved innføring av ny ekomlov § 2-9 a. Det er således heller ikke grunn til å tro at de utgiftene politiet og tilbyderne har i forbindelse med uthentingen vil øke.

Ordningen med etterfølgende kontroll vil innebære økt arbeidsmengde både for de lokale politidistriktene, POD og det eksterne tilsynsorganet som eventuelt skal føre tilsyn med ordningen.

Departementene ber høringsinstansene, og særlig Hovedredningssentralen, Politidirektoratet og tilbyderne om tilbakemelding på hvilke økonomiske og administrative konsekvenser de ser for seg at innføringen av ny ekomlov § 2-9a vil medføre for egen virksomhet.

4. PUK-koder og kundereskontro

4.1. Innledning

Formålet med denne delen høringen er å få synspunkter på departementets forslag om endring og presisering av reglene for utlevering av enkelte data som er omfattet av taushetsplikten, men som ikke er lagringspliktige etter ekomloven § 2-7 a.

Samferdselsdepartementet foreslår regelendringer som gir politi og påtalemyndighet tilgang til PUK-koder (jf. definisjon nedenfor) og kundereskontro på lik linje med avtalebasert hemmelig telefonnummer og elektronisk kommunikasjonsadresse. Spørsmålet om hvorvidt PUK-koder er taushetsbelagt og politiets tilgang til denne type opplysninger har vært drøftet av ekommyndigheten og bransjen tidligere (se punkt 4.3). Stortingets vedtak om å innføre datalagringsdirektivet i norsk rett har gitt spørsmålet ny aktualitet. Stortingets beslutning om å lovfeste terskelen for tilgang til lagringspliktige data på bakgrunn av dataenes personvernmessige sensitivitet, gjør det naturlig å foreta en ny vurdering av de dataene som ikke er lagringspliktige, men taushetsbelagte, og som politi- og påtalemyndighet har hjemmel til å få tilgang til.

4.2. Bakgrunn for forslaget

Tilbyder av elektronisk kommunikasjonsnett og -tjenester lagrer i tillegg til trafikkdata, lokaliseringsdata og bruker-/abonnementsdata også andre typer data som er taushetsbelagte i henhold til ekomregelverket. Dette siste er data som genereres ved produksjon av ekomtjenester og som ikke er lagringspliktige data. Per i dag snakker vi om tre typer data i denne sistnevnte kategorien:

1) **PUK- kode** er en tallkode som tilbyder lagrer for å kunne bistå abonnent med å åpne låst SIM-kort ved behov. Dette forutsetter at abonnenten ikke har endret PUK-koden etter mottak av SIM-kortet. Tallkoden i seg selv vil ikke inneholde informasjon om bruk av elektronisk kommunikasjon, og det har vært stilt spørsmål til om PUK-koden isolert sett er omfattet av ordlyden i taushetsplikten etter ekomloven § 2-9. Tilgang til PUK-kode og SIM-kort vil gi tilgang til informasjon om bruk av elektronisk kommunikasjon.

2) **Kundereskontro** er regnskapsinformasjon om fakturahistorikk for et abonnement hos tilbyder. Denne informasjonen vil kunne si noe om bruk/ikke bruk av et abonnement. En kundereskontro kan også inneholde spesifisert fakturaoversikt.

3) **Signaleringstrafikk** er informasjon som genereres i et kommunikasjonsnett for å styre trafikk. Slik informasjon støtter gjennomføringen av elektronisk kommunikasjon. I et mobilnett sørger signalering blant annet for å styre trafikk til riktig mobilterminal. Informasjonen inneholder løpende oppdatering av hvilket lokaliseringsområde og hvilken basestasjon en mobilterminal er knyttet til. Signaleringstrafikk genereres også uten at abonnenten ringer eller blir ringt

opp eller på annen måte bruker sin mobiltelefon, under forutsetning av at håndsettet er slått på. Innenfor hvor nøyaktige områder abonnenten kan bli lokalisert, vil kunne variere noe fra fra tilbyder til tilbyder. Dataene lagres normalt i 10-14 dager.

I proposisjonen om datalagring ble ikke spørsmålet om taushetsbelagte data som ikke er lagringspliktige, drøftet. Verken PUK-kode eller kundereskontro er lagringspliktige data i henhold til datalagringsdirektivet, og omtale av lagring og utlevering av denne type data hørte derfor ikke med i proposisjonen.

Departementene vil i denne høringen fremme forslag til lovendringer som omfatter PUK-koder og kundereskontro. Når det gjelder signaleringsdata vil Samferdselsdepartementet eventuelt komme tilbake til spørsmålet om lagring av denne type data. Det har ikke vært mulig å utrede spørsmålet innenfor gjeldende tidsramme. Uthenting av signaleringsdata følger de alminnelige regler for uthenting av informasjon og kommunikasjonskontroll i straffeprosessloven kapittel 16 og 16a. Departementene har fått opplyst fra Post- og teletilsynets at tilsynet praktiserer en høy terskel for oppheving av taushetsplikt for signaleringsdata. I praksis har det kun blitt utlevert signaleringsdata i situasjoner hvor politiet har tillatelse til å iverksette kommunikasjonskontroll i medhold av straffeprosessloven § 216a. Departementene legger til grunn at denne praksisen kan videreføres inntil videre.

Også uthenting av PUK-koder og kundereskontro følger de alminnelige reglene for uthenting av informasjon og kommunikasjonskontroll i straffeprosessloven kapittel 16 og 16a. Etter departementenes oppfatning vil det være ryddig om reglene for oppheving av taushetsplikt for PUK-koder og kundereskontro følger samme system som reglene for oppheving av taushetsplikten om avtalebasert hemmelig telefonnummer og andre abonnementsopplysninger i ekomloven § 2-9 tredje ledd.

4.3. Nærmere om bakgrunnen for forslaget om regler for PUK-koder

PUK- kode er forkortelse for "Personal Unblocking Key" og er en sikkerhetskode som skal beskytte SIM-kortet mot at det blir brukt av uvedkommende. Dersom politi- og påtalemyndighet gjennom ransaking og beslag er i besittelse av en terminal hvor SIM-kortet er låst, vil de ha behov for PUK-kode for å få åpnet SIM-kortet og få innsyn i kommunikasjonen og de data som er lagret på kortet.

Spørsmålet om PUK-koder er omfattet av taushetsplikten har vært oppe til diskusjon flere ganger tidligere. Post- og teletilsynet varslet ved brev av 19. februar 2008 en praksisendring om behandling av henvendelser fra politiet knyttet til utlevering av PUK-koder fra tilbyderne. Begrunnelsen lå i at en vurdering av taushetsplikten måtte bygge på PUK-kodens faktiske kjennetegn og ikke på hvordan den anvendes. En PUK-kode er ifølge tilsynet ikke en type data som inngår i den reelle bruken av elektronisk

kommunikasjon. Tilsynet mente videre at en PUK-kode kan sammenlignes med et passord for eksempelvis til Internett.

Samferdselsdepartementet og Post- og teletilsynet ga i 2008 lagdommer Ørnulf Røhnebæk i oppdrag å foreta en juridisk betenkning av taushetsplikt etter ekomloven § 2-9 og PUK-koder til SIM-kort. I betenkningen som ble fremlagt 22. august 2008, konkluderer Røhnebæk med at ekomloven § 2-9 første ledd første punktum ikke omfatter PUK-kodene til SIM-kort.

Det fremgår av brev fra Telenor 8. september 2008 at selskapet har flere innvendinger mot betenkningen. Telenor peker blant annet på at tjenestetilbyder ved å overlevere PUK-koden vil bryte den plikt han har til å bevare taushet om den informasjonen som PUK-koden vil gi tilgang til. Telenor presiserer at det ikke bare dreier seg om innholdet som ligger lagret i et SIM-kort, men også tjenester som mobilsvar og innkommende SMS/MMS i sanntid.

Samferdselsdepartementet støttet i brev av 27. mars 2009 langt på vei de vurderinger som er lagt til grunn i den juridiske betenkningen når det gjelder at en ren ordlydsfortolkning av bestemmelsen ekomloven § 2-9 isolert sett taler i mot at PUK-koder kan anses for omfattet av taushetsplikten. Departementet pekte imidlertid på det uheldige ved å innføre en ny tilsynspraksis uten at det er avklart hvor langt en mulig ulovfestet taushetsplikt vil beskytte abonnenten mot urettmessig innsyn i informasjon på SIM-kortet. Departementet understreker videre i sitt brev betydningen av å legge til grunn et forsiktighetsprinsipp dersom myndigheten skal endre sin praksis basert på en endret lovfortolkning. Departementet viste til at en endring av praksis ikke burde iverksettes før spørsmålet er offentlig hørt og eventuelt presisert gjennom en lovendring. Departementene ønsker med lovforslaget å klargjøre at PUK-koder er taushetsbelagt og kan utleveres til politi og påtalemyndighet, jf. ny § 2-9 tredje ledd.

Departementene ber om innspill på forslaget om at PUK-koder skal være taushetsbelagt, men kunne utleveres til politi og påtalemyndighet.

4.4. Nærmere om bakgrunnen for forslaget om regler for kundereskontro

Med" kundereskontro" forstås underkontoer i regnskapet hvor tilbyder av elektronisk kommunikasjon har oversikt over pengetransaksjoner og eventuell annen regnskapsinformasjon og fakturahistorikk for en sluttbruker. Kundereskontro vil kunne si noe om bruk av et abonnement og således være av interesse for politi og påtalemyndighet ved etterforsking av straffesaker og undersøkelser om savnede personer. Enkelte tilbydere lagrer spesifisert fakturaoversikt på kundereskontroen dersom sluttbruker har bedt om dette. Spesifisert faktura inneholder detaljerte trafikkdata knyttet opp til abonnement. Dette er data som er svært sensitive for personvernet og departementet ser derfor behov for å klargjøre regler for utlevering av kundereskontro.

4.5. Gjeldende rett og praksis med PUK-koder *og* kundereskontro

Post- og teletilsynet har i sin forvaltningspraksis hittil lagt til grunn at PUK-koder omfattes av ekomloven § 2-9 første ledd, det vil si at PUK-koder har blitt regnet som taushetsbelagt. Praksis har vært at Post- og teletilsynet har fritatt tilbyder for taushetsplikten i de tilfeller hvor politi og påtalemyndighet har bedt om å få opplyst PUK-koden.

Når det gjelder kundereskontroen har Post- og teletilsynet lagt til grunn at denne ikke avslører for eksempel hvem som har ringt med hvem, hvor lenge og når. Imidlertid vil fakturaens størrelse avsløre om og i hvilken grad elektronisk kommunikasjon har blitt benyttet i fakturaperioden. Dette vil si noe om bruk av elektronisk kommunikasjon og omfattes av taushetsplikten etter ekomloven § 2-9. Post- og teletilsynet har fritatt tilbyder for taushetsplikt i tilfeller hvor politi og påtalemyndighet har bedt om å få utlevert kundereskontro.

4.6. Departementets vurdering av utlevering av PUK-koder

Samferdselsdepartementets forslag om lovendringer knyttet til PUK-koder begrunnes med at spørsmålet om PUK-koder tidligere har blitt utredet og diskutert mellom myndigheter og tilbydere. Departementet har også tidligere varslet at eventuelle endringer i praksis om utlevering av PUK-koder burde høres offentlig. I tillegg har gjennomføringen av datalagringsdirektivet og diskusjonen om politiets behov i den forbindelse gjort det mer påtrengende å avklare praksisen med PUK-koder før ikrafttredese av datalagringsreglene.

Regler om taushetsplikt skal forhindre at uvedkommende får tilgang til informasjon som er omfattet av taushetsplikten. Taushetsplikten har både en passiv og en aktiv side. Den passive plikten innebærer forenklet sagt at man forholder seg taus om taushetsbelagt informasjon. Den aktive plikten betyr at tilbyder skal beskytte taushetsbelagt informasjon og aktivt hindre uvedkommende å få tilgang til den. Dette kan for eksempel gjøres ved fysiske og/eller logiske sikkerhetstiltak. Departementet anser beskyttelse av PUK-kode som en del av den aktive plikten som følger av taushetsbestemmelsen § 2-9.

Ved å utlevere en PUK-kode vil man kunne komme til å utlevere informasjon som er taushetsbelagt, noe som taler for at PUK bør omfattes av taushetsbestemmelsen i ekomloven på samme måte som tilbyder og installatør plikter å bevare taushet om tekniske innretninger og fremgangsmåter etter § 2-9 første ledd.

PUK-kode er i seg selv ikke en type data som kan være sensitive for personvernet, slik som trafikkdata og lokaliseringsdata. Det vises til at Post- og teletilsynet har vurdert PUK-kode som en tallkode som kan sammenlignes med et passord. Slik sett kan det være naturlig å vurdere utlevering av en PUK-kode på samme måte som utlevering av en IP-adresse eller et telefonnummer. Taushetsplikten vil da ikke være til hinder for at

PUK-koder kan gis til politi- og påtalemyndighet og eventuelle andre myndigheter i medhold av lov, jf. § 2-9 tredje ledd.

På den annen side vil som nevnt ovenfor PUK-kode i enkelte tilfeller kunne gi tilgang til personsensitive data som lokaliseringsdata og innhold, noe som taler for at terskelen for tilgang til PUK-kode bør likestilles med terskelen for tilgang til trafikkdata og lokaliseringsdata, jf. § 2-9 nytt femte ledd.

Departementet vurderer det ikke som hensiktsmessig å skulle likestille tilbyders taushetsplikt om PUK-koder med tilbyders taushetsplikt om trafikkdata og lokaliseringsdata. Politiet vil som oftest få tilgang til mobiltelefoner og lignende etter å ha foretatt ransaking og beslag med hjemmel i straffeprosessloven §§ 192 og 203, og hjemmelsgrunnlaget for å kunne få tilgang til innholdet som er på terminalen/kommunikasjonsutstyret er derfor ivaretatt. Utlevering av PUK-kode bør derfor i slike tilfeller kunne etterspørres hos tilbyder direkte og uten at Post- og teletilsynet må oppheve taushetsplikten, jf. § 2-9 nytt tredje ledd.

Det at man potensielt kan få tilgang til lokaliseringsinformasjon og innhold gjennom tilgang til PUK-kode tilsier at man begrenser muligheten for utlevering av PUK-koder til kun å gjelde politi- og påtalemyndighet.

Departementene foreslår på bakgrunn av dette at det presiseres at PUK- koder faller inn under taushetsplikten, men at taushetsplikten for PUK-koder kan oppheves ved utlevering til politi og påtalemyndighet med hjemmel i ekomloven § 2-9, tredje ledd på lik linje med avtalebasert hemmelig telefonnummer, andre abonnementsopplysninger og elektronisk kommunikasjonsadresse.

Departementene ber om høringsinstansenes syn på forslaget om at utlevering av PUK-koder likestilles med utlevering av avtalebasert hemmelig telefonnummer, andre abonnementsopplysninger og elektronisk kommunikasjonsadresse, men med den forskjell at PUK-koder kun utleveres til politi og påtalemyndighet og ikke andre myndigheter i medhold av lov.

4.7. Departementets vurdering av utlevering av data om kundereskontro

Tilbyder har i en kundereskontro oversikt over pengetransaksjoner og eventuell annen regnskapsinformasjon og fakturahistorikk for en sluttbruker. Dette er data som vil være nyttige for politiet i etterforskning av kriminalitet. Samferdselsdepartementet vurderer ikke kundereskontro som særlig personsensitive data fordi innsyn i en kundereskontro kun gir en oversikt over transaksjoner og ikke over hvem som har benyttet elektronisk kommunikasjon med hvem, når og hvor lenge (trafikkdata). Mange sluttbrukere ønsker spesifisert faktura fra sin tilbyder, og slike fakturaoversikter lagres gjerne som en del av kundereskontroen. En spesifisert faktura vil blant annet gi en oversikt over når, til hvem, hvor lenge og hvordan en sluttbruker har benyttet elektronisk

kommunikasjon. Det er med andre ord betydelige mengder trafikkdata i en slik oversikt og den bør derfor ikke følge en kundereskontro. Departementet mener utlevering av spesifisert faktura derfor bør følge de samme reglene for tilgang som for trafikkdata. Når det gjelder kundereskontro for øvrig mener departementene taushetsplikten ikke er til hinder for utlevering av denne på lik linje som for PUK-koder, avtalebasert hemmelig telefonnummer, andre abonnementsopplysninger og elektronisk kommunikasjonsadresse.

4.8. Nærmere om lovforslaget

Departementet presiserer at PUK-koder og kundereskontro omfattes av taushetsplikten i ekomloven § 2-9 første ledd. Departementet foreslår at taushetsplikten ikke er til hinder for at PUK-kode og kundereskontro kan gis til politi- og påtalemyndigheten på lik linje med avtalebasert hemmelig telefonnummer eller andre abonnementsopplysninger, samt elektronisk kommunikasjonsadresse, jf. ekomloven § 2-9 tredje ledd. Det presiseres at PUK-kode og kundereskontro kun kan utleveres til politi og påtalemyndigheten, og ikke til andre myndigheter i medhold av lov. Det presiseres videre at spesifisert faktura ikke skal utleveres ved utlevering av kundereskontro.

4.9. Administrative og økonomiske konsekvenser

Departementene kan ikke se at det skulle påløpe noen ekstra administrative eller økonomiske konsekvenser knyttet til forslaget om PUK-koder og kundereskontro. Det bes om innspill fra høringsinstansene på dette.

5. Merknader og lovforslag

5.1. Merknader til de enkelte bestemmelser i lovforslaget

Til § 2-7a annet ledd,

I § 2-7a annet ledd foreslås det å regulere alle kostnader knyttet til oppfyllelse av lagringsplikten etter § 2-7 a. Med kostnader menes investeringskostnader, driftskostnader, kostnader til behandling og uthenting av opplysninger til relevante myndigheter, samt kostnader knyttet til "lukket lagring" og kryptering som tilbyder har for å oppfylle lagringsplikten. Staten dekker anslåtte kostnader knyttet til etablering og drift av lagringsløsningen for å oppfylle lagringsplikten etter § 2-7a, samt for tilbydernes anslåtte kostnader for politiets uthenting av data. Ekomtilbyderne plikter å etablere og å drifte lagringsløsningen. Ekomtilbyderne vil selv måtte dekke kostnadene med å tilpasse egne systemer for å kunne overlevere lagringspliktige data til datalagringsbasen. Med egne system menes for eksempel trafikkstyring og faktureringssystemer.

Det foreslås at den lagringspliktige pålegges å føre et eget kostnadsregnskap hvor kostnadene fremgår. I regnskapet må det fremgå tydelig hvilke utgifter tilbyder har hatt til ulike formål. Innkjøp av for eksempel hardware, Software, etablering av krypteringssystemer, administrative kostnader og lignende skal i tilstrekkelig grad kunne identifiseres. Revisorbekreftelsen krever en revisjonsgjennomgang som minst oppfyller kravene i RS 800 "Revisors uttalelser ved revisjonsoppdrag med spesielle formål". Bekreftelsen skal utarbeides og sendes inn så snart årsregnskapet for fjoråret foreligger, og senest innen 60 dager etter utløpet av andre kvartal i inneværende år. Det foreslås videre at myndigheten kan gi nærmere bestemmelser i forskrift og treffe enkeltvedtak om kostnadsfordeling, føring av regnskap og revisjon. Myndigheten gis adgang til å gi regler om beregning av tilskudd til tilbyderne, samt fastsettelse av satser som gjelder for den enkelte ekomtjeneste.

Nåværende annet ledd blir tredje ledd.

Til § 2-8 annet ledd

Ekomloven *§ 2-8 annet ledd* foreslås endret for å klargjøre at bestemmelsen ikke gjelder kostnadsdekning for lagringsplikten etter § 2-7a. Når § 2-7a trer i kraft vil relevante myndigheter få tilgang til bruker og abonnementsdata, trafikkdata og lokaliseringsdata med hjemmel i denne bestemmelsen. Tilretteleggingsplikten etter § 2-8 omfatter ikke data som lagres i henhold til § 2-7a. Tilretteleggingsplikten omfatter tilgang til annen type informasjon, som kommunikasjonskontroll i sanntid, innhold og trafikkdata om kommunikasjonen. Gjeldende ordninger for kostnadsdeling for tilrettelegging for lovbestemt tilgang til informasjon videreføres.

Til § 2-8 tredje ledd

Plikten til å lagre trafikkdata slik den fremgår av *§ 2-8 tredje ledd annet komma* utgår fordi plikten etter innføring av datalagringsdirektivet, jf. lagringsplikten i § 2-7a, anses som overflødig. Bestemmelsens tredje ledd annet komma er overlappende med § 2-7a annet ledd. *Tredje ledd første komma* foreslås videreført.

Til § 2-9 første ledd

Bestemmelsen foreslås endret slik at det ikke skal være tvil om at opplysninger om PUK-kode og kundereskontro omfattes av tilbyders taushetsplikt. PUK- kode er forkortelse for "Personal Unblocking Key" og er en sikkerhetskode som skal beskytte SIM-kortet mot at det blir brukt av uvedkommende. PUK- kode er i praksis en tallkode som tilbyder lagrer for å kunne bistå abonnent med å åpne låst SIM-kort ved behov.

Med "kundereskontro" forstås underkontoer i regnskapet hvor tilbyder av elektronisk kommunikasjon har oversikt over pengetransaksjoner og eventuell annen regnskapsinformasjon og fakturahistorikk for en sluttbruker.
Denne informasjonen vil kunne si noe om bruk/ikke-bruk av et abonnement.

Til § 2-9 tredje ledd

Bestemmelsen foreslås endret slik at det fremgår at taushetsplikten ikke er til hinder for at opplysninger om PUK-kode og kundereskontro kan gis til politi og påtalemyndighet. Se nærmere om PUK kode og kundereskontro i merknaden til første ledd. Dersom politi- og påtalemyndighet gjennom ransaking og beslag er i besittelse av en terminal hvor SIM-kortet er låst, vil de ha behov for PUK-kode for å få åpnet SIM-kortet og få innsyn i kommunikasjonen og de data som er lagret på kortet.

Kundereskontro skal ikke inneholde spesifisert faktura. Det vil si at informasjon om hvem som har benyttet elektronisk kommunikasjon med hvem, hvor lenge, når og hvorfra ikke skal fremgå av kundereskontro som utleveres til politi og påtalemyndighet. Det er bare politi og påtalemyndighet som kan kreve denne type opplysninger utlevert, til forskjell fra andre abonnementsopplysninger, avtalebasert hemmelig telefonnummer og elektronisk kommunikasjonsadresse, som også andre myndigheter i medhold av lov kan kreve utlevert.

Taushetsplikten er heller ikke til hinder for at PUK-koder og kundereskontro kan gis som vitnemål for retten.

Til *ny § 2-9 a*

Bestemmelsen er ny og gir politiet hjemmel for uthenting av informasjon fra tilbyderne i nødsituasjoner. Hovedkriteriet for utlevering er at «personers liv eller helse er i fare». Vurderingen må sees i sammenheng med de to alternative vilkårene i annet punktum. Det avgjørende vil være om faren er reell. Det må gjøres en individuell vurdering hvor personens mentale helse, alder og tidligere handlingsmønstre vektlegges. Situasjonen må være å regne som en unntakssituasjon, og det må foreligge konkrete holdepunkter som tilsier at personens liv eller helse er i fare. Når barn eller person med svekket mental helse meldes savnet, vil terskelen for å legge til grunn at den oppståtte faren er reell være lavere.

I annet redningsarbeid vil det avgjørende være om det foreligger holdepunkter som tilsier at personers liv eller helse kan være i fare. Dersom politiet mener det er grunnlag for å lete etter mennesker vil vilkåret være oppfylt.

Både opplysninger tilbyderne plikter å lagre i medhold av ny ekomlov § 2-7 a og andre opplysninger de måtte inneha vil være relevante opplysninger. Både samtidige og historiske data vil være relevant. Ved søk etter personer vil tilbyderne kunne pålegges å utlevere så konkrete posisjoneringsdata som mulig. Relevante opplysninger for politiet i nødsituasjoner vil kunne være lokaliseringsdata, signaleringsdata og trafikkdata. Den foreslåtte bestemmelsen i ekomloven gir ikke hjemmel for kommunikasjonskontroll i form av telefonavlytting.

Det er politimesteren eller den han gir myndighet som ved beslutning pålegger tilbyderen utlevering. Departementene foreslår en ordning hvor et eksternt organ fører etterfølgende kontroll med politiets uthenting av informasjon i nødssituasjoner.

5.2 Forslag til lovbestemmelser

§ 2-7 a annet ledd skal lyde:

Kostnader forbundet med lagring og politiets uthenting av data dekkes av staten. Tilbyder dekker kostnader knyttet til forberedelse for lagring av slike data i egne systemer. Tilbyder skal føre særskilt regnskap for de kostnader som etter denne bestemmelse skal dekkes av staten. Regnskapet skal være bekreftet av ekstern revisor. Myndigheten kan gi nærmere regler i forskrift og treffe enkeltvedtak om kostnadsfordeling, føring av regnskap og revisjon.

Annet ledd blir nytt tredje ledd.

§ 2-8 annet ledd skal lyde:

Tilbyders driftskostnader knyttet til oppfyllelse av tilretteleggingsplikten *etter første ledd* dekkes av staten for de merkostnader som følger av disse tjenestene.

§ 2-9 første ledd skal lyde:

Tilbyder og installatør plikter å bevare taushet om innholdet av elektronisk kommunikasjon og andres bruk av elektronisk kommunikasjon, herunder opplysninger om *PUK-kode*, *kundereskontro,* tekniske innretninger og fremgangsmåter. De plikter å gjennomføre tiltak for å hindre at andre enn de som opplysningene gjelder får anledning til selv å skaffe seg kjennskap til slike opplysninger. Opplysningene kan heller ikke utover lovlige behandlingsformål nyttes i egen virksomhet eller i tjeneste eller arbeid for andre, med unntak av statistiske opplysninger om nettrafikk som er anonymisert og ikke gir informasjon om innretninger eller tekniske løsninger.

§ 2-9 tredje ledd skal lyde:

Taushetsplikten er ikke til hinder for at det gis opplysninger til påtalemyndigheten eller politiet om avtalebasert hemmelig telefonnummer eller andre abonnementsopplysninger, samt elektronisk kommunikasjonsadresse. *Taushetsplikten er heller ikke til hinder for at det gis opplysninger til påtalemyndigheten eller politiet om PUK-kode og kundereskontro.* Det samme gjelder ved vitnemål for retten. Taushetsplikten er heller ikke til hinder for at opplysninger som nevnt i første punktum gis til annen myndighet i medhold av lov.

Ny § 2-9 a skal lyde:

Når personers liv eller helse er i fare, er taushetsplikten etter § 2-9 første ledd ikke til hinder for at tilbyder gir politiet relevante opplysninger. Dette gjelder både når det søkes etter en person som er forsvunnet og i annet redningsarbeid.

Det er politimesteren, eller den han gir myndighet, som ved beslutning pålegger tilbyderen utlevering.