Høring – utkast til forskrift om lagringsplikt for bestemte data og om tilrettelegging av disse data (datalagringsforskriften)

Korrigert versjon 8.2.2012 : Rettelse av siste avsnitt i punkt 3.3.2.
(Avsnittet før rettelse er inntatt i sluttnote)

Post- og teletilsynet

Innhold

Høring – utkast til forskrift om lagringsplikt for bestemte data og om tilrettelegging av disse data (datalagringsforskriften)

1. Innledning

Ved lov 15. april 2011 nr. 11 ble det vedtatt endringer i lov av 4. juli 2003 nr. 83 om elektronisk kommunikasjon (ekomloven) og lov av 22. mai 1981 nr. 25 om rettergangsmåten i straffesaker (straffeprosessloven) mv. som gjennomfører EUs datalagringsdirektiv i norsk rett. Vedtaket har sitt grunnlag i Prop. 49 L (2010-2011) (proposisjonen) og Innst. 275 L (2010 – 2011) (innstillingen), og innebar at Norge implementerte direktiv 2006/24/EF om lagring av data fremkommet ved bruk av offentlig elektronisk kommunikasjonstjeneste og offentlig elektronisk kommunikasjonsnett med endring av direktiv 2002/58/EF (datalagringsdirektivet eller DLD) med visse små endringer.

Formålet med datalagringsdirektivet og implementeringen av direktivet i norsk rett har vært å harmonisere lagring av nærmere bestemte data fremkommet ved bruk av elektronisk kommunikasjon. Hensikten er å gi justismyndighetene et verktøy for å avdekke, etterforske og straffeforfølge alvorlig kriminalitet, samtidig som hensynet til personvernet ivaretas best mulig.

Det fremgår av proposisjonen og innstillingen at det skal utarbeides nærmere regler om datalagring i forskrift. Post- og teletilsynet (PT) er, i brev av 8. april og 1. juni 2011 fra Samferdselsdepartementet, gitt i oppdrag å utarbeide og sende på høring forslag til slik forskrift med hjemmel i ekomloven.

PT har på denne bakgrunn utarbeidet forslag til forskrift om datalagring. Tilsynet har vurdert behovet for nærmere regulering for så vidt gjelder hva som skal lagres, hvem som skal lagre og ulike forhold knyttet til selve lagringen av data, herunder autorisasjon av personell som skal håndtere lagrede data, kvaliteten på data, forholdet mellom lagring og tilrettelegging mv.

Det ble i proposisjonen forutsatt at forskrift om datalagring skulle utarbeides på bakgrunn av et samarbeid mellom representanter fra politimyndigheter, representanter fra tilbydere av ekomnett og -tjenester og PT. PT har under arbeidet hatt et godt samarbeid med representanter fra justissektoren, Datatilsynet og tilbydere.

PT sender med dette utkast til forskrift om lagringsplikt for bestemte data og om tilrettelegging av disse data (datalagringsforskriften) på høring.

2. Statistikk om dagens bruk av trafikkdata m.v. i etterforskingsøyemed

PT har i 2011 behandlet 1 894 anmodninger om fritak fra tilbyders taushetsplikt etter ekomloven § 2-9. PT har innhentet ytterligere informasjon for 198 av disse anmodningene. Reelt antall anmodninger som PT har mottatt anslås derfor til å være 1 696[1].

[1]Dette korrigerte tallet er funnet ved å trekke fra antall tilfeller hvor PT har innhentet ytterligere informasjon skriftlig fra antall anmodninger som PT har registrert. Årsaken til at dette tallet må korrigeres, er at PTs statistikkverktøy er utarbeidet for å vise den totale arbeidsmengden som anmodningene om fritak fra taushetsplikten utgjør. Dette tallet gir uttrykk for det reelle antallet anmodninger som PT har mottatt, fordi i nesten alle saker hvor PT innhenter ytterligere informasjon skriftlig, vil den som anmoder om fritak, komme med en ytterligere anmodning om fritak. Når PT mottar svar etter en skriftlig innhenting av ytterligere informasjon, vil det vises som en ny anmodning i PTs statistikk.

Av de innkomne anmodningene har PT gitt fritak fra tilbyders taushetsplikt 1 619 tilfeller. 112 anmodninger har resultert i avslag. I 27 tilfeller ble anmodningen avskrevet før realitetsavgjørelse. Normalt avskrives saker etter tilbakemelding fra den eller de som anmodet om fritak fra tilbyders taushetsplikt.

Det er anmodet om fritak fra tilbyders taushetsplikt for å få tilgang til trafikk- og lokasjonsdata fra bestemte telefonnumre i 1 408 tilfeller. PT har gitt fritak fra tilbyders taushetsplikt for utlevering av trafikk- og lokasjonsdata fra bestemte telefonnumre for 2 944 telefonnumre. Av disse har det blitt gitt fritak for hele lagringsperioden i 47 prosent av tilfellene.

Det er anmodet om fritak fra tilbyders taushetsplikt for å få tilgang til informasjon fra basestasjonssøk i 332 tilfeller. PT har i 2011 gitt fritak fra tilbydernes taushetsplikt for å utgi resultat fra basestasjonssøk på 390 lokasjoner. Gjennomsnittlig tid for disse basestasjonssøkene er på 2,3 timer per lokasjon, totalt 911 timer.

Det er anmodet om fritak fra tilbyders taushetsplikt for å få utlevert PUK-kode i 184 tilfeller. PT har gitt fritak fra tilbyders taushetsplikt for utlevering PUK-kode til 198 telefonnumre.

PT har registrert 85 anmodninger hvor strafferammen for det angitte straffbare forholdet er under tre år, eller det straffbare forhold ikke omfattes av opplistingen av lovbrudd som er foreslått som alternativer til det generelle kravet om at handlingen skal kunne medføre fengsel i tre år eller mer.

PT har mottatt fem anmodninger hvor begrunnelsen er behov for tilgang til trafikkdata fra IP-adresser.

PT har gitt fritak fra tilbyders taushetsplikt i 54 tilfeller der den taushetsbelagte informasjonen gjelder den fornærmede i et straffbart forhold. Slike fritak gis nesten utelukkende når den fornærmede ikke selv er i stand til å samtykke.

PT har innhentet ytterligere opplysninger per telefon 236 ganger.

PT har ikke statistikk som viser andel fritak og avslag fordelt på hvilken kategori anmodningen blir sortert under.

PT har ikke registrert noen anmodninger fra andre enn politiet i hele 2011.

3. Hvem skal lagre

3.1. Bakgrunn

I forbindelse med implementeringen av datalagringsdirektivet er det vedtatt en ny § 2-7a i ekomloven. Det fremgår av første ledd i bestemmelsen at det er tilbyder av elektronisk kommunikasjonsnett som anvendes til offentlig elektronisk kommunikasjonstjeneste, eller tilbyder av slik tjeneste som omfattes av lagringsplikten. Definisjonene i ekomloven § 1-5 nr. 1, 2, 4 og 7 gir en nærmere anvisning på hvem dette omfatter.

Myndigheten er i ekomloven § 2-7a annet ledd siste punktum gitt kompetanse til å gi forskrift eller treffe enkeltvedtak om helt eller delvis å frita fra plikten til å lagre data. Videre kan myndigheten helt eller delvis pålegge andre enn de som er angitt i første ledd lagringsplikt dersom dette må til for å oppnå formålet med bestemmelsen. PT har derfor vurdert om det er

---

En anmodning kan gjelde flere telefonnummer eller områder. Dermed kan en anmodning resultere i ulike resultat. Derfor er tallene i avsnittet under høyere samlet enn dette tallet.

behov for å avgrense eller utvide kretsen av hvem som skal ha plikt til å lagre trafikkdata, lokaliseringsdata og abonnementsinformasjon.

3.2. Pliktsubjekter etter loven

Plikten til å lagre data påhviler "*tilbyder av elektronisk kommunikasjonsnett som anvendes til offentlig elektronisk kommunikasjonstjeneste og tilbyder av slik tjeneste*", jf. ekomloven § 2-7a første ledd.

Med *elektronisk kommunikasjonsnett* forstås system for elektronisk kommunikasjon der radioutstyr, svitsjer, annet koplings- og dirigeringsutstyr, tilhørende utstyr eller funksjoner inngår, jf. ekomloven § 1-5 nr. 2. Med *offentlig elektronisk kommunikasjonstjeneste* forstås tjeneste som helt eller i det vesentlige omfatter formidling av elektronisk kommunikasjon og som normalt ytes mot vederlag og som er tilgjengelig for allmennheten, eller beregnet til bruk for allmennheten, jf. ekomloven § 1-5 nr. 4 og 7.

For at en tjeneste kan sies å være offentlig, må tjenesten altså være tilgjengelig eller beregnet for bruk for allmennheten. En ren språklig forståelse av " tilbys allmennheten" i ekomloven, tilsier at tjenesten må være tilgjengelig for enhver som kan tilbys tjenesten innenfor nettets geografiske område. Det følger imidlertid av forarbeidene til ekomloven at allmennheten ikke må være "alle", men at man må se hen til antallet brukere og interessefellesskapet mellom dem, jf Ot.prp. nr. 58 (2002-2003) side 87. I proposisjonen på side 71 er det uttalt følgende om hva som ligger i at en tjeneste er tilgjengelig for allmennheten:

> *"Ved vurderingen av om tjenesten tilbys allmennheten, skal det blant annet legges vekt på antall brukere og interessefellesskapet mellom disse. Det legges til grunn at for eksempel borettslag med private nett normalt ikke vil være omfattet av tilbyderbegrepet. Andre eksempler på virksomheter som normalt faller utenfor dette tilbyderbegrepet er bedrifter, sykehus, hoteller, kafeer og lignende som utelukkende stiller elektroniske kommunikasjonstjenester til rådighet for sine kunder eller ansatte."*

Etter PTs syn må man se hen til om tjenesten tilbys en vid krets av brukere i et åpent marked for at den skal kunne anses som tilgjengelig for allmennheten. Det vil ikke være det aktuelle antallet kunder hos tilbyder som vil være avgjørende for om tilbudet anses for å være rettet mot allmennheten, men muligheten for brukere til å inngå avtale med tilbyderen. En tilbyder som retter sitt tilbud mot en bestemt brukergruppe, kan fortsatt anses som en tilbyder av offentlig elektronisk kommunikasjon hvis brukergruppen er vid nok. For eksempel vil en tilbyder som retter tjenestene sine mot bedriftsmarkedet, anses som offentlig tilbyder. Det at tjenesten er forbeholdt en avgrenset brukergruppe, er imidlertid et argument som kan peke i retning av at tjenesten ikke tilbys allmennheten. Begrenses kretsen tilbudet retter seg mot tilstrekkelig, vil tilbyderen ikke regnes som en tilbyder av offentlig elektronisk kommunikasjon, Dette vil være i tråd med uttalelsen i proposisjonen om at for eksempel bedrifter, sykehus, hoteller og kafeer normalt ikke anses som tilbydere av offentlig elektronisk kommunikasjonstjeneste, fordi slik tjeneste er forbeholdt virksomheten selv eller dens kunder som vil befinne seg i virksomhetens lokaler og benytte seg av virksomhetens øvrige tjenester.

PT har oversikt over de registreringspliktige tilbyderne i ekombransjen, men denne listen gir ikke en komplett oversikt over alle tilbydere av elektronisk kommunikasjonsnett som anvendes til offentlig elektronisk kommunikasjonstjeneste og tilbyder av slik tjeneste. Hvorvidt en tilbyder faller inn under denne kategorien vil bero på en konkret vurdering.

Etter en gjennomgang av tilbyderne som danner grunnlag for PTs statistikk over ekommarkedet for første halvår 2011, er antall tilbydere av offentlige elektroniske kommunikasjonstjenester i de ulike kategoriene som lagringspliktige data anslått til:

- Fasttelefoni – 13 stk
- Mobiltelefoni – 26 stk
- Internettelefoni – 60 stk
- Internettaksess – 142 stk

Flere lagringspliktige tilbyr tjenester innenfor flere av de lagringspliktige kategoriene. Samlet sett anslås det å være 169 unike lagringspliktige subjekter. Det presiseres at dette tallet er et overslag av antall tilbydere av offentlige kommunikasjonstjenester innenfor de ulike kategoriene. Vurderingen har vært begrenset til informasjon fra åpne kilder.

Enkelte av disse tilbyderne har felles underliggende tjenesteleverandør for de tjenester som utløser lagringsplikt. Det må antas at disse virksomhetene kan gå sammen for å redusere administrative og økonomiske konsekvenser av lagringsplikten.

3.3. Behovet for å endre kretsen av lagringspliktige subjekter

3.3.1. Prinsipielle utgangspunkter for å endre kretsen av lagringspliktige subjekter

Det fremgår av proposisjonen på side 75 at departementet er bevisst at ikke all kommunikasjon vil bli lagret som følge av forslaget om å pålegge lagringsplikt for tilbyder av elektronisk kommunikasjonsnett som anvendes til offentlig elektronisk kommunikasjons-tjeneste og tilbyder av slik tjeneste. Eksempelvis vil leverandører av innholdstjenester tilby kommunikasjonsløsninger som ikke underlegges lagringsplikt. Videre er det som nevnt over i punkt 3.2 gitt flere eksempler på leverandører av elektroniske kommunikasjonstjenester som faller utenfor hovedregelen om hvem som er lagringspliktig. Datalagringsdirektivet har også denne avgrensningen. Det ble ikke ansett nødvendig med en lovfastsatt utvidelse av hvem som underlegges lagringsplikt. Dette indikerer at det er akseptert at implementeringen av datalagringsdirektivet ikke vil medføre at alle data som kan være relevante ved kriminalitetsbekjempelse, blir lagret. PT mener derfor at det bør foreligge særlige grunner før kompetansen til å endre kretsen av lagringspliktige subjekter gjennom forskrift bør anvendes.

Innføringen av datalagringsdirektivet medførte en bred diskusjon og bygger på kompromiss der ulike hensyn og interesser er ivaretatt. Dette tilsier også at PT bør være varsom med å endre kretsen av lagringspliktige subjekter gjennom forskrift, før man har fått noe erfaring med hvordan ordningen virker.

3.3.2. Behov for å utvide kretsen av lagringspliktige subjekter

Private nett

Slik PT vurderer tilbudet av elektroniske kommunikasjonsnett og -tjenester i Norge i dag, er det naturlig å vurdere om private elektroniske kommunikasjonsnett skal omfattes av lagringsplikten. Private elektroniske kommunikasjonsnett er blant annet regulert i ekomforskriften kapittel 9.

Private elektroniske kommunikasjonsnett varierer i størrelse fra meget små nett etablert i husholdinger, til store nett som det er knyttet flere tusen brukere til. Eksempler på store private elektroniske kommunikasjonsnett kan være universitetenes nett, Nødnettet, GSM-R og interne nett for store bedrifter.

I vurderingen av om lagringsplikten skal utvides til å omfatte private elektroniske kommunikasjonsnett, må det foretas en avveining av hensynet til etterforsking av de forbrytelser som kvalifiserer til uthenting av lagringspliktige data og følgelig behovet for å

lagre slike data for å oppnå formålet med lagringen på den ene siden, opp mot personvernet for de som dataene gjelder og kostnadene for de som vil bli pålagt lagringsplikt på den andre siden. Kostnadselementet må vurderes i et samfunnsmessig perspektiv. I relasjon til en eventuell forskriftsmessig utvidelse av lagringspliktige subjekter vil det etter PTs oppfatning være særlig aktuelt å vurdere antallet brukere nettene har, ikke hvilke brukere de forskjellige nett måtte ha.

Private elektroniske kommunikasjonsnett med få brukere vil ha liten økonomisk evne til å kunne ivareta de sikkerhetskrav som er, og vil bli satt, for lagringspliktige data. Videre legger PT til grunn at behovet for tilgang til lagrede data i private nett med få sluttbrukere normalt er lite. På denne bakgrunn finner PT ikke grunn til å forskriftsfastsette lagringsplikt for eiere av små private nett. Dette er også i tråd med de signaler som proposisjonen gir om lagringsplikt for små private nett som tilbyr internettaksess.

Store private elektroniske kommunikasjonsnett kan imidlertid ha så mange brukere at det kan være ønskelig, fra et etterforskings- og påtaleståsted, å pålegge lagringsplikt for å oppnå formålet med lagringsplikten. Hensynet til etterforsking av de forbrytelser som kvalifiserer til uthenting av lagringspliktige data kan derfor, til tross for kostnadene dette medfører, tale for at private elektroniske kommunikasjonsnett med et høyt antall brukere bør omfattes av lagringsplikten. Dette vil særlig gjelde dersom brukergruppen ikke utelukkende er ansatte eller lignende. PT mener derfor at kun private elektroniske kommunikasjonsnett som hovedsakelig har andre brukere enn egne ansatte, bør vurderes underlagt lagringsplikt.

En lagringsplikt vil i slike tilfeller minske mulighetene til å omgå at data blir lagret.

PT har ikke mottatt begjæringer hvor det eksplisitt bes om fritak for taushetsplikt vedrørende private nett. Private nett tilbyr imidlertid i hovedsak internettaksess, og politiet har kunnet få utlevert abonnementsinformasjon direkte uten PTs forutgående samtykke, jf. ekomloven § 2-9 tredje ledd. PT har derfor ikke oversikt over hvor ofte politiet har innhentet denne type informasjon.

Spekteret av private elektroniske kommunikasjonsnett er bredt og med stor forskjell i brukergrupper, antall brukere, geografisk spredning osv. Dette medfører at det vil være vanskelig og lite hensiktsmessig å regulere lagringsplikt gjennom forskrift som angir hvilke private elektroniske kommunikasjonsnett som eventuelt skal omfattes av lagringsplikten. PT vil kunne regulere dette gjennom enkeltvedtak, hvor de overfor nevnte momenter vil være sentrale i vurderingen om det skal pålegges lagringsplikt for private elektroniske kommunikasjonsnett.

Hvis ikke lagringsplikt pålegges, står det tilbydere av private nett fortsatt fritt til å lagre denne type informasjon dersom det foreligger behandlingsgrunnlag for personopplysningene og eventuell nødvendig konsesjon. Det kan dermed ikke etableres tilgang til slik informasjon som nevnt i dette avsnittet i medhold av straffeprosessloven §§ 210b og 210c.

Innholdstjenester
Kripos har overfor PT uttrykt behov for at lagringsplikten utvides til også å gjelde leverandører av innholdstjenester. Eksempler på slike tjenester kan være ”chat”, søkemotorer og nettsamfunn. Slike tjenester er ikke lagringspliktige etter direktivet, proposisjonen eller innstillingen. Videre kan en lagringsplikt for slike tjenester være svært problematisk da man vil kunne komme i konflikt med forbudet mot å lagre innhold. Selv om det ut fra formålet med regelverket kan være gode argumenter for å lagre data fra slike tjenester, er det PTs oppfatning at det på nåværende tidspunkt ikke er aktuelt å utvide kretsen av lagringspliktige subjekter til å omfatte leverandører av innholdstjenester.[i]

3.3.3. Behov for å innskrenke kretsen av lagringspliktige subjekter

Virksomhetene som omfattes av lagringsplikten etter ekomloven § 2-7a varierer sterkt i størrelse. Det kan stilles spørsmål om tilbydere med få brukere, ut fra en totalvurdering, bør unntas fra lagringsplikten. En slik vurdering vil imidlertid måtte foretas basert på antall abonnenter tilbyderen har innenfor kategoriene fasttelefoni, mobiltelefoni, internettelefoni, internettaksess og e-post, fordi det ikke nødvendigvis bør settes samme terskel for unntak for de forskjellige plattformer.

De følgende tall er hentet fra PTs markedsstatistikk for første halvår 2011. Det understrekes at det ikke er foretatt noen konkret vurdering av hvorvidt alle tilbyderne inkludert i statistikken vil omfattes av lagringsplikten. Videre understrekes at tilbyder er et videre begrep enn tilbyder av offentlig elektronisk kommunikasjonstjeneste.

Når det gjelder **mobiltelefontjeneste**, har PT registrert at det er 26 tilbydere med totalt 5 699 924 abonnement. Gjennomsnittelig antall abonnenter pr. tilbyder er 219 228, men mediantallet er 16 006. De ti største tilbyderne har 98,1 prosent av alle abonnenter og 98,5 prosent av all trafikk. Av det totale antallet abonnement registrert ved utgangen av 2011, vil altså kun ca. 94 000 abonnement falle utenfor lagringsplikten hvis lagringsplikten begrenses til de ti største tilbyderne. For å inkludere 99,5 prosent av abonnentene, vil de 14 største tilbydere av mobiltelefoni måtte omfattes.

I kategorien **fasttelefontjeneste**[2] har PT registrert at det er 17[3] tilbydere med totalt 1 097 872 abonnement. Gjennomsnittelig antall abonnenter pr. tilbyder er 63 522, men mediantallet er
2 295. De ti største tilbyderne har 99,9 prosent av alle abonnenter og 99,3 prosent av all trafikk. Av det totale antallet abonnement registrert ved utgangen av 2011, vil altså 13 504 abonnement falle utenfor lagringsplikten hvis lagringsplikten begrenses til de ti største tilbyderne.

For **internettelefontjeneste** har PT registrert at det er 61[4] tilbydere med totalt 511 852 abonnement. Gjennomsnittelig antall abonnenter pr. tilbyder er 8 256, men mediantallet er 1 540. De ti største tilbyderne har 80,3 prosent av alle abonnementene og 83,8 prosent av all trafikk. Av det totale antall abonnement registrert ved utgangen av 2011, vil 101 049 abonnement falle utenfor lagringsplikten hvis lagringsplikten begrenses til de ti største tilbyderne.

Når det gjelder **internettaksess** er de tall PT har tilgjengelig delt mellom fast og mobil internettaksess. PT har registrert at det er 150 tilbydere av fast internettaksess og 16 tilbydere av mobil internettaksess[5]. Gjennomsnittelig har tilbydere av mobil internettaksess 40 112 abonnenter, mens mediantallet er 7 947 abonnenter. Når det gjelder fast internettaksess er de tilsvarende tallene henholdsvis 11 622 og 1 145 abonnenter. De ti største tilbydere av fast internettaksess har 83,3 prosent av alle abonnenter, mens de tilsvarende tallet for mobil internettaksess er 99,6 prosent.

For **e-pos**t har ikke PT tilgjengelige tall som kan vise hvor mange som tilbyr dette og som er lagringspliktig etter ekomloven § 2-7a første ledd.

Lagringsplikten medfører kostnader. På det nåværende tidspunkt er det ikke avklart hvem som skal dekke disse kostnadene. Hvis de lagringspliktige pålegges å dekke noe av disse kostnadene, vil konkurransen i markedet kunne påvirkes fordi små tilbydere har færre

[2] I denne sammenheng omfatter fasttelefoni PSTN, ISDN 2B+D og ISDN 30B+D
[3] Tallet inkluderer fire mindre tilbydere som ikke er lagringspliktige.
[4] Tallet inkluderer en tilbyder som ikke er lagringspliktig etter forslaget.
[5] Tallene inkluderer 22 tilbydere som ikke er lagringspliktige etter forslaget.

abonnenter å fordele kostnadene på. Samtidig vil et eventuelt unntak fra lagringsplikten for de minste tilbyderne kunne gi disse konkurransefortrinn fremfor de som ikke unntas fra lagringsplikten.

PT ser det ikke som hensiktsmessig å vurdere forskriftsfastsatte unntak for mindre tilbydere av mobiltelefontjeneste, fasttelefontjeneste, internettelefontjeneste, mobil internettaksess eller e-post. PT ser imidlertid at det er argumenter for at mindre tilbydere av fast internettaksess ikke nødvendigvis bør underlegges lagringsplikt.

Flere internettaksesspunkter, som hoteller og kafeer, vil ikke omfattes av lagringsplikten i § 2-7a første ledd, dermed er det allerede ved hovedregelen "hull" i lagringen av internettaksess. Kostnadene som påføres ved at mindre tilbydere av fast internettaksess underlegges lagringsplikt, kan oppfattes som uforholdsmessig i forhold til nytten for å oppnå formålet med lagringen. Den informasjon lagringspliktige for fast internettaksess skal lagre, se utkastet § 2-5, taler også for forsiktighet med hensyn til omfanget av hvem som blir underlagt lagringsplikt.

På den annen side vil det kunne uthule formålet med lagringsplikten dersom man gjennom forskrift fastsetter at tilbydere som er mindre enn et gitt nivå, skal være unntatt lagringsplikt. En slik bestemmelse vil kunne berede grunnen for forretningsvirksomhet basert på at virksomheten er unntatt lagringsplikt. En slik profilering vil kunne medføre dårligere måloppnåelse av det formålet som loven søker å oppnå. Videre vil lagringsplikt for alle som tilbyr fast internettaksess sikre at all internettaksess fra en abonnent gjennom fast tilkobling blir lagret.

Endelig må det sees hen til de konsekvenser som ny straffeprosesslov §§ 118a, 210b og 210c har for politiets med flers mulighet til å innhente trafikk- og lokasjonsdata. Hvilke data som kan innhentes er i straffprosessloven §§ 210b og 210c begrenset til å gjelde data som angitt i ekomloven § 2-7a første ledd *og* som en *tilbyder* er pliktig å lagre. Dette har to viktige konsekvenser.

For det første vil tilgangen til trafikk- og lokasjonsdata etter straffeprosessloven §§ 210b og 210c kun gjelde for lagringspliktige data i medhold av ekomloven § 2-7a. Eventuelle data som en tilbyder måtte lagre for kommunikasjons- eller fakturaformål, som ikke også er lagringspliktige data etter ekomloven § 2-7a vil det ikke kunne gis lovlig tilgang til etter straffeprosessloven §§ 210b og 210c.

For det andre begrenser straffeprosessloven §§ 210b og 210c tilgangen ytterligere til å gjelde data som en tilbyder har plikt til å lagre etter ekomloven § 2-7a. Dette må forstås slik at tilgangen etter nevnte bestemmelser kun kan gis for lagringspliktige data hos pliktsubjekter etter § 2-7a første ledd og eventuelle andre tilbydere, jf. ekomloven § 1-5 nr. 14, som pålegges lagringsplikt etter ekomloven § 2-7a annet ledd.

Av proposisjonen punkt 12.6 fremgår det at PT ikke lenger skal ha en rolle ved opphevelse av taushetsplikten etter ekomloven § 2-9 i medhold av straffeprosessloven § 118. Slik PT forstår rettstilstanden etter innføringen av straffeprosessloven § 118a, vil derfor PT ikke lenger kunne oppheve taushetsplikten i medhold av straffeprosessloven § 118 for taushetsbelagt informasjon etter ekomloven § 2-9. Således vil § 118 ikke kunne anvendes for å gi fritak fra taushetsplikt for blant annet trafikk- og lokasjonsdata lagret i medhold av ekomloven § 2-7 hos tilbydere som ikke er pålagt lagringsplikt i medhold av ekomloven § 2-7a.

Ved å unnta en lagringspliktig etter ekomloven § 2-7a første ledd fra lagringsplikt, vil konsekvensen være at politiet og påtalemyndigheten avskjæres fra tilgang til slike data etter straffeprosessloven §§ 210b og 210c. Formålet med lagringsplikten tilsier derfor at PT bør

være forsiktig med å anvende kompetansen til å frita pliktsubjekter etter ekomloven § 2-7a første ledd fra lagringsplikten.

I lys av at kompetansen kun skal anvendes for å oppnå formålet med bestemmelsen, mener PT at det bør foreligge tungtveiende kostnadsmessige og konkurransemessige hensyn før kompetansen til å innskrenke kretsen av lagringspliktige subjekter kan benyttes.

Etter PTs oppfatning vil det på nåværende tidspunkt ikke være hensiktsmessig å fastsette en innkrenking av kretsen av lagringspliktige subjekter i forskriften basert på virksomhetens størrelse. PT anser det mest hensiktsmessig å innskrenke kretsen av lagringspliktige subjekter gjennom enkeltvedtak dersom det etter en konkret helhetsvurdering viser seg nødvendig.

3.3.4. Momenter som vil bli vektlagt ved eventuell endring av kretsen av lagringspliktige subjekter

Selv om PT på nåværende tidspunkt ikke finner grunn til å foreslå utvidelser eller innskrenkninger i kretsen av lagringspliktige subjekter, så mener PT at det likevel er grunn til å angi hvilke momenter som kan bli vektlagt ved et eventuelt pålegg om, eller dispensasjon fra lagringsplikt. Det presiseres at disse signalene ikke må oppfattes som en uttømmende liste av hvilke momenter som kan bli tillagt vekt.

PT mener at det må vurderes konkret hvilken type tjeneste den lagringspliktige tilbyr, behovet for lagring av den aktuelle informasjon, herunder oppnåelse av formålet med lagringen, de relative kostnadene ved lagring, mengden abonnenter som den lagringspliktige representerer og konkurransemessige virkninger et eventuelt pålegg eller fritak vil kunne gi.

PT vil også se hen til om tilbyder kan vise til at det er truffet effektiviseringstiltak for å begrense kostnadene forbundet med lagringsplikten. Eksempelvis vil det ikke bli gitt dispensasjon fra lagringsplikten dersom den lagringsløsning som den aktuelle tilbyder har valgt kan gjøres billigere ved felleslagring eller andre effektiviserende tiltak med tilsvarende effekt.

PT vil konsultere politiet eller påtalemyndigheten ved eventuelle endringer i kretsen av lagringspliktige subjekter, ved utøvelse av kompetansen gitt i ekomloven § 2-7a annet ledd.

3.4. Svalbard

Samferdselsdepartementet følger opp hvorvidt Svalbard skal unntas fra lagringsplikten. Dette vil eventuelt skje gjennom endringer i forskrift 4. juli 2003 nr. 882 om stedlig virkeområde for lov om elektronisk kommunikasjon vedrørende Svalbard, Jan Mayen, Bilandene og Antarktis.

4. Lagringspliktige data

4.1. Innledning

4.1.1. Hovedregelen om hvem som skal lagre hva

Det er den som tilbyr tilgang til offentlige kommunikasjonsnett eller -tjenester til en sluttbruker som skal lagre de dataene denne har tilgang til i egne systemer. Dette betyr for eksempel at når en telefonsamtale settes opp mellom to abonnenter hos ulike lagringspliktige, skal den lagringsplikte A lagre informasjonen om abonnent A og trafikkdata fra samtalen, mens lagringspliktige B skal lagre informasjon om abonnent B og trafikkdata fra samtalen. Hvis telefonsamtalen er en mobiltelefonsamtale skal lagringspliktige A lagre lokaliserings-informasjon om abonnent A og lagringspliktige B skal lagre lokaliseringsinformasjon om abonnent B.

Når det skal fastsettes hvilken informasjon som skal lagres, og dette skal struktureres i ulike kategorier, kan det i enkelte tilfeller se ut til at det kreves at en lagringspliktig skal lagre informasjon som denne ikke har rådighet over. Dette er ikke intensjonen, og dette presiseres også i proposisjonen på side 78.

Eksempelvis vil abonnentsdata for en egen abonnent som er A-nummer finnes i den lagringspliktige (A) sine systemer på tidspunktet for lagringen, men abonnentsdata for et B-nummer, hvis abonnent tilhører en annen lagringspliktig (B), ikke vil være kjent for A. Denne informasjonen kan utleveres mellom A og B, men PT legger til grunn at slik utveksling vil være unødvendig krevende å administrere. Slik overføring er heller ikke nødvendig for å oppnå formålet med lagringen. Politiet kan gå direkte til B og kreve utlevert abonnentsdata i medhold av ekomloven § 2-9 tredje ledd. Det merarbeid som politiet må foreta i de konkrete tilfeller, hvor abonnentsinformasjon ikke er kjent, anses å være mindre enn det merarbeid som eventuelt må pålegges lagringspliktige dersom alle lagringspliktige skal lagre abonnentsinformasjon for alle parter i kommunikasjonen.

For å presisere hvem som skal lagre hvilken informasjon, er det i utkastet til forskrift § 2-1 første ledd tatt inn at den lagringspliktige bare skal lagre data knyttet til egne abonnenter. Således skal den lagringspliktige som hovedregel lagre trafikkdata for kommunikasjonen som egen kunde gjennomfører, samt lokasjons- og abonnentsdata for egne kunder.

Underleverandører av tilgang til nett eller tjeneste skal som hovedregel ikke lagre data som blir generert av kunder hos andre virksomheter. Slik unngås det at samme informasjon lagres hos ulike lagringspliktige.

4.1.2. Særregulering for tjenester over landmobile offentlige kommunikasjonsnett

Ved å følge hovedreglen beskrevet i punkt 4.1.1 over, vil politiet, ved innhenting av lagringspliktige data etter straffeprosessloven § 210c (basestasjonssøk), måtte henvende seg til 27 forskjellige lagringspliktige subjekter for mobiltelefoni og mobil internettaksess for å skaffe seg samlet oversikt all trafikk i det aktuelle området.

Det vil kunne oppnås klare fordeler for politiet om de relevante data er samlet hos færre lagringspliktige. For mobiltelefontjenester og mobil internettaksess finnes det fire lagringspliktige tilbydere av landmobile offentlige kommunikasjonsnett. Disse fire subjektene vil være de eneste virksomhetene som vil kunne fremskaffe samlet informasjon om all bruk av egne basestasjoner.

For gjennomføringen av basestasjonssøk mener derfor PT at det er hensiktsmessig at det er den netteier av det nett hvor trafikk- og lokasjonsdata blir generert, som også er den som utleverer informasjonen. Dette vil være en videreføring av dagens praksis.

Datatilsynet har imidlertid i møter gitt uttrykk for at det er den som har et kundeforhold til abonnenten som bør lagre, og at det vil være problematisk med en løsning hvor netteier skal behandle personopplysninger tilhørende en abonnent til en annen lagringspliktig.

PT ser at en avvikende løsning for mobil kommunikasjon kan være utfordrende, men mener det like fullt er nødvendig å vurdere om det finnes en mer tidseffektiv og kostnadseffektiv løsning for lagringen. PT mener også at man ved etablering av lagring av disse dataene bør ser hen til formålet med at data skal lagres, samt de sikkerhetskrav som er foreslått etablert omkring dataene.

PT har identifisert tre alternative måter å gjennomføre lagringen for mobiltelefontjeneste og mobil internettaksess som ivaretar politiets behov for å få tilgang til slik informasjon enklest mulig.

Alternativ 1 er at den lagringspliktige som har et kundeforhold til abonnenten lagrer abonnementsinformasjon og at eier av landmobilt offentlig kommunikasjonsnett lagrer trafikk- og lokasjonsdata generert i eget nett. Eventuelle trafikk- og lokasjonsdata generert hos roamingpartnere lagres av den lagringspliktige som har kundeforholdet til abonnenten.

Alternativ 2 er at den lagringspliktige som har et kundeforhold til abonnenten lagrer all lagringspliktig data for egne kunder og at eier av landmobilt offentlig kommunikasjonsnett også lagrer all trafikk- og lokasjonsdata generert i eget nett. Eventuelle trafikk- og lokasjonsdata generert hos roamingpartnere lagres av den lagringspliktige som har kundeforholdet til abonnenten.

Alternativ 3 er som alternativ 1, men at eventuell trafikk- og lokasjonsdata generert hos roamingpartnere lagres hos eier av de(t) landmobile offentlige kommunikasjonsnett som den lagringspliktige som har kundeforholdet til abonnenten har avtale med.

Slik PT ser det, vil alternativ 3 medføre at store mengder data generert hos roamingpartnere må overføres fra en tilbyder til en annen. Dette medfører kostnader og utgjør en risikofaktor. Av den grunn velger PT ikke å forfølge dette alternativet videre.

Basert på PTs erfaringstall for politiets bruk av basestasjonssøk og personsøk i 2011, har PT estimert hvor mange henvendelser politiet må rette mot ulike lagringspliktige for å få utlevert lagringspliktige data. Tabellen viser forskjellene mellom de omtalte alternativene.

Mobiltelefoni	**Antall saker 2011**	**Hovedløsning**	**Alternativ 1**	**Alternativ 2**
Basestasjonssøk	390	10 140	1 170	1 170
Personsøk	2 950	2 950	5 900 – 8 850	2 950
Sum		**13 090**	**7 070 – 10 020**	**4 120**

Av tabellen fremkommer at det i 2011 var 390 begjæringer om basestasjonssøk. Hvis disse skulle distribueres til og behandles av 27 forskjellige lagringspliktige ville dette totalt medføre 10 140 behandlinger hos de lagringspliktige. Begjæringer om personsøk vil etter hovedløsningen kun behandles av den lagringspliktige som har avtale med kunden. Totalt vil hovedløsningen dermed medføre 13 090 behandlinger.

Ved alternativ 1, vil kun de fire eiere av landmobilt offentlig kommunikasjonsnett behandle basestasjonssøk. På den annen side, vil flere lagringspliktige bli involvert i personsøk. Dette fordi både den lagringspliktige som har kundeforholdet med den aktuelle personen og minst en, men i noen tilfeller opptil to eiere av landmobilt offentlig kommunikasjonsnett, vil måtte behandle lagringspliktig data. Dette er indikert i tabellen over. Basert på dagens markedsandel for de fire landmobile offentlige kommunikasjonsnett, kan det imidlertid antas at summen behandlinger nødvendig vil ligge i den lavere delen av spennet.

Ved alternativ 2 vil kun de fire eiere av landmobilt offentlig kommunikasjonsnett behandle basestasjonssøk, og kun den lagringspliktige som har kundeforholdet med den aktuelle personen vil bli involvert i personsøk. Dette medfører et vesentlig lavere antall behandlinger.

Tillagt ekstraarbeidet hos politiet med å sammenstille informasjon fra de involverte lagringspliktige, antar PT, etter et forsiktig, anslag at hver behandling vil medføre en arbeidstime i ressursbruk. Forskjellen i medgått resursbruk hos de lagringspliktige vil derfor variere sterkt mellom de forskjellige alternativene. Den estimerte lavere resursbruken i alternativ 2 anses ikke å bli oppveid av økte kostnader til lagringskapasitet.

Hovedløsningen anses som unødig ressurskrevende for politiet ved basestasjonssøk. Videre vil et hvert basestasjonssøk trolig involvere samtlige lagringspliktige for mobiltelefontjenester og trolig også for mobil internettaksess. Den samlede ressursinnsats vil derfor bli meget stor.

PT anser alternativ 2 som den beste løsningen totalt sett. Lagring av trafikk- og lokasjonsdata både hos netteier og tjenestetilbyder vil imidlertid medføre at noe av de lagringspliktige dataene blir lagret av to ulike lagringspliktige. Verken direktivet eller forarbeidene gir et absolutt forbud mot en slik løsning, men uttaler at lagringen bør gjennomføres hos bare en lagringspliktig. PT mener likevel at det på dette punktet er nødvendig å pålegge tilbyder av landmobilt offentlig elektronisk kommunikasjonsnett en lagringsplikt for de data som hentes ut ved basestasjonssøk. Dette gjøres for å oppnå en effektiv måte å benytte seg av virkemiddelet basestasjonssøk sett i forhold til både kostnader og tidsbruk ved uthenting, og samtidig kunne utføre spesifikke søk effektivt. Dette alternativet vil medføre at det totale volumet av lagringspliktige data blir høyt, men vil gi en effektiviseringsgevinst ved uthenting av lagringspliktige data.

PT foreslår derfor at det etableres en løsning i tråd med alternativ 2. Dette gjøres ved å innta i utkast til forskrift bestemmelser om at eiere av landmobilt offentlig kommunikasjonsnett også skal lagre nærmere angitte datatyper når det gjelder mobiltelefoni og mobil internettaksess, samt at eiere av landmobilt offentlig kommunikasjonsnett kun kan behandle denne lagrede informasjonsmengde for utlevering til politiet og påtalemyndighet ved basestasjonsøk. Forslaget vil også innebære at eiere av landmobilt offentlig kommunikasjonsnett skal lagre og behandle data generert av utenlandsk abonnent som roamer i norske nett.

4.1.3. Lagringspliktens subjekt og omfang oppsummert

Lagringspliktige skal altså som hovedregel kun lagre lagringspliktige data i den grad de tilbyr fasttelefontjeneste, mobiltelefontjeneste, internettelefontjeneste, internettaksess og/eller e-post til sluttbruker. En slik hovedregel vil sikre at man unngår lagring to steder ved at tilbyder av elektronisk kommunikasjonsnett og tilbyder av elektronisk kommunikasjonstjeneste lagrer samme informasjon. Se nærmere 4.1.1.

PT mener imidlertid at det er grunn til å utfylle hovedreglen i to tilfeller, se nærmere punkt 4.1.2.

For å få dette frem i utkastets § 2-1 foreslås det i første ledd at de lagringspliktige kun skal lagre de data som er opplistet i kapittel 2 av utkastet for egne sluttbrukeres bruk av de tjenester som utløser lagringsplikt. I annet og tredje ledd foreslås det en ufylling av første ledd hvor det angis konkret når og hva tilbyder av offentlig elektronisk kommunikasjonsnett også skal lagre.

4.2. Strukturell inndeling av lagringspliktige data

Datalagringsdirektivet artikkel 5 lister opp hvilken informasjon som skal lagres etter hva den aktuelle informasjonen skal synliggjøre. I proposisjonen punkt 8.5 er lagringspliktige data listet opp etter hvilken tjenesteplattform som genererer informasjonen. PT foreslår at den opplistingen som proposisjonen inneholder, blir tatt inn i forskriften. En slik systematisering av hvilke data som skal lagres vil gjøre det lettere for den lagringspliktige å identifisere hva som skal lagres.

4.3. Definisjoner

PT foreslår å definere i forskriften de ulike kategoriene som proposisjonen benytter for inndeling de lagringspliktige data. Videre er det nødvendig å definere hva som menes med telefontjeneste i forkriften, da definisjonene av noen av kategoriene er knyttet opp til dette begrepet.

4.3.1. Lagringspliktig telefontjeneste

Begrepet telefontjeneste er definert i direktivet artikkel 2 bokstav c. Utkastets definisjon er ment å ta opp i seg de momenter som direktivets definisjon av begrepet inneholder. Det foreslås likevel en noe annen ordlyd enn direktivet fordi det er ønskelig med tilnærmet lik ordlyd som foreslås som definisjon av ”offentlig telefontjeneste” i Samferdselsdepartementets høringsnotat av 25. juni.2010. I utkastet til forskrift er det bare behov for å definere ”telefontjeneste” fordi tilbyder av telefontjenester som ikke anses å være offentlige etter ekomloven ikke er underlagt lagringsplikt. Definisjonen inneholder derfor, til forskjell fra Samferdselsdepartementets forslag, ikke en avgrensning mot *offentlige* telefontjenester. For å tydeliggjøre at begrepet telefontjeneste brukt i utkastet ikke har samme innhold som det som er foreslått brukt i ekomloven, benevnes dette begrepet *lagringspliktig telefontjeneste*.

4.3.2. Fasttelefontjenester

Fasttelefontjenester er i proposisjonen telefontjenester som benytter ISDN eller PSTN for overføring av tale.[6] Det er ikke ønskelig å knytte definisjonen opp til teknologi, da definisjonen ikke vil kunne ta opp i seg teknologisk utvikling. Videre vil man ved å knytte definisjonen til disse teknologiene møte utilsiktede virkninger ved at intern kommunikasjon gjennom sentralt plasserte hussentraler vil omfattes av lagringen. Slik kommunikasjon er ikke ment å omfattes av lagringsplikten. PT er kjent med de endringer som Telenor foretar i PSTN og ISDN-nettet, og mulig overføring til annen teknologi for tjenesten.

Det særegne med fasttelefontjeneste er at terminalen er knyttet til en fast geografisk adresse. Derfor er definisjonen knyttet opp til denne særegenheten. Et fasttelefoniabonnement kan imidlertid flyttes, men dette krever deltakelse fra tilbyder.

4.3.3. Mobiltelefontjeneste

Mobiltelefontjeneste er definert til å gjelde telefontjeneste som benytter landmobile kommunikasjonstjenester. Basestasjoner som er plassert på mobile enheter, slik som skip, fly eller lignende, og som benyttes til landmobile kommunikasjonstjenester vil omfattes av definisjonen.

---

[6]Dette samsvarer ikke med den begrepsbruk som ellers benyttes for fasttelefoni, da slik telefoni og bredbåndstelefoni normalt omtales som fasttelefoni.

Landmobile tjenester omfatter mer enn hva som defineres som mobiltelefontjenester, men tilleggskravet om at tjenesten må benytte nasjonal eller internasjonal nummerplan for gjennomføringen av kommunikasjonen, vil begrense definisjonen til å gjelde det som i dagligtale oppfattes som mobiltelefontjeneste.

Dersom en mobiltelefon benyttes for mobil internettaksess, så vil slik bruk ikke inngå i begrepet *mobiltelefontjeneste* i utkastet til forskrift, men som *internettaksess*. Se vedlagte forslag til § 1-3. Dette vil også gjelde selv om den mobile internettaksessen benyttes for å gjennomføre internettelefontjeneste. I slike tilfeller må lagringspliktig lagre data for internettaksess og internettelefontjeneste hver for seg.

Etter utkastet § 2-3 første ledd nr. 9 skal det lagres data om forhåndsbetalte anonyme mobiltelefontjenester. Slike tjenester selges ikke i Norge, men tas inn for å oppnå direktivets formål om harmonisering på europeisk nivå. Det bes om innspill på om en slik regulering er nødvendig. Særlig bes det om tilbakemelding på om norske netteiere for landmobile offentlige kommunikasjonsnett vil kunne lagre relevant informasjon ved internasjonal roaming i deres nett.

4.3.4. Internettelefontjeneste

I proposisjonen fremgår det at forslaget inneholder annen begrepsbruk for bredbåndstelefontjeneste enn hva bransjen og PT tidligere har benyttet. PT vil i denne forskriften benytte begrepet fra proposisjonen, men vil utdype begrepet med bransjens normale begrepsbruk.

PT har i rapporten «Regulering av bredbåndstelefoni etter lov om elektronisk kommunikasjon» av 14. juni 2006, definert tre forskjellige hovedkategorier av bredbåndstelefoni.

Bredbåndstelefontjeneste som ikke er tilrettelagt for alle-til-alle kommunikasjon omtales som kategori 1. Ett eksempel på slik bredbåndstelefontjeneste er basisversjonen av Skype. I kategori 2 er bredbåndstelefontjeneste som delvis er tilrettelagt for alle-til-alle kommunikasjon. Bredbåndstelefontjeneste som er tilrettelagt for alle-til-alle kommunikasjon inngår i kategori 3. For denne kategorien bredbånd kan man både motta samtaler og anrope brukere av tradisjonelle telefontjenester.

Bredbåndstelefontjenester av kategori 1 omfattes ikke av definisjonen, mens de to andre kategoriene vil omfattes av definisjonen da disse må anses som en telefontjeneste, jf. § 1-3 nr. 1 i utkastet til forskrift.

Lagringspliktig bredbåndstelefontjeneste kan teknisk gjennomføres på ulike måter. En fellesnevner for disse metodene er at IP-protokollen anvendes for gjennomføringen av telefontjenesten. Derfor har PT valgt å knytte definisjonen opp til bruk av IP-protokollen.

I utkastet § 2-4 første ledd nr. 5 er det foreslått at man skal lagre hvilken tjeneste som er benyttet for internettelefontjeneste. Dette kravet fremgår fra direktivet, men PT er usikre på hvilken relevans informasjonen vil ha slik direktivet foreslås implementert i Norge. PT ber om tilbakemelding på hvilke ulike tjenester som den lagringspliktige for internettelefontjeneste vil kunne identifisere som tilbyder av internettelefontjeneste alene.

4.3.5. Internettaksess

I forskriften er det tilgang til Internett gjennom kablet eller radiobasert tilkobling som er avgjørende. Med dette vil enhver tilkobling til Internett omfattes av definisjonen.

Dette medfører videre at definisjonen ikke avgrenser mot internettaksess oppsatt av eksempelvis bedrifter, hoteller, kafeer, eller lignende som utelukkende stiller internettaksessen til rådighet for sine kunder eller ansatte. Det er bevisst at definisjonen ikke avgrenser mot slik internettaksess, da denne avgrensningen blir foretatt gjennom hvilke subjekter som er lagringspliktige.

4.3.6. E-posttjeneste

Det følger av ekomloven § 2-7a første ledd at visse data knyttet til bruk av en e-posttjeneste skal lagres.

Elektronisk kommunikasjonstjeneste er definert i ekomloven § 1-5 nr. 4 som en "*tjeneste som helt eller i det vesentlige omfatter formidling av elektronisk kommunikasjon og som normalt ytes mot vederlag*". Videre er *elektronisk kommunikasjon* definert i ekomloven § 1-5 nr. 1 som "*overføring av lyd, tekst, bilder eller andre data ved hjelp av elektromagnetiske signaler i fritt rom eller kabel i et system for signaltransport*". En e-posttjeneste er en applikasjon som benytter Simple Mail Transfer Protocol (SMTP) for å overføre informasjon fra en bruker til en annen i et elektronisk kommunikasjonsnett. Dersom protokollen skal fungere i et elektronisk kommunikasjonsnett forutsetter det at e-posttjenesten anvender en underliggende elektronisk kommunikasjonstjeneste som kan formidle de elektroniske signaler som e-posttjenesten ønsker å formidle. De aktører som tilbyr tjenester som kun utnytter og er avhengig av funksjoner i underliggende elektronisk kommunikasjonstjenester, formidler ikke elektronisk kommunikasjon slik ekomloven krever. Således vil e-posttjeneste ikke være en elektronisk kommunikasjonstjeneste.

Tilbudet av kun en e-posttjeneste medfører ikke at tilbyderen av denne blir å regne som "*tilbyder av elektronisk kommunikasjonsnett som anvendes til offentlig elektronisk kommunikasjonstjeneste og tilbyder av slik tjeneste*". Dette medfører at kun de som omfattes av ekomloven § 2-7a første ledd første punktum som tilbyr en e-posttjeneste skal lagre visse data knyttet til bruk av e-posttjenesten.

PT har vurdert om lagringspliktige som tilbyr aksessen til eller for en e-posttjenesten kan lagre de lagringspliktige data knyttet til bruk av e-posttjenesten. Slik PT vurderer dette vil dette innebære at disse vil måtte overvåke all datastrøm i eget nett for å kunne identifisere relevant lagringspliktig informasjon. PT vil ikke anbefale en slik løsning for å sikre lagring av data knyttet til e-posttjenester tilbudt av noen som ikke er lagringspliktige.

PT foreslår dermed at alle lagringspliktige som tilbyr e-posttjenester, skal lagre data knyttet til bruk av denne tjenesten. Det avgjørende for lagringsplikten knyttet til bruk av e-posttjenesten vil være om man er tilbyder av offentlig elektronisk kommunikasjonstjeneste eller er pålagt lagringsplikt av myndigheten med hjemmel i ekomloven § 2-7a annet ledd.

Nærmere om visse problemstillinger

4.3.7. Network Address Translation (NAT)

Det fremgår av direktivet artikkel 1 nr. 2 at innhold ikke skal lagres. Ved implementeringen har det vært sentralt å ikke lagre innhold. PT er kjent med at det for mobil internettaksess foregår bruk av NAT fordi tilgangen til IP-adresser er begrenset[7]. Gjennom bruk av NAT vil

[7] Det vil også benyttes NAT som de lagringspliktige ikke kan se. Typisk vil dette skje i routere plassert hos den enkelte sluttbruker.

mange brukere benytte samme IP-adresse utad. Ut fra de opplysninger som PT sitter med kan så mange som 2 000 brukere av mobil internettaksess kunne benytte samme IP-adresse samtidig.

Bruk av NAT vil kunne uthule formålet med lagring ved internettaksess, da dette vil medføre at mange brukere vil fremstå med samme IP-adresse i de lagringspliktige data. Det bør derfor vurderes om de lagringspliktige skal pålegges å lagre informasjon som er nødvendig for å identifisere brukeren.

Slik PT ser det, omfattes ikke opplysninger om hvilke domenenavn/IP-adresser en bruker har besøkt/kommunisert med på Internett, av kravene til hva som skal lagres. Videre vil slik informasjon ikke anses for å være tildelt når abonnenten *abonnerer på eller registrerer seg hos en Internettilgangstjeneste eller en internettkommunikasjonstjeneste*, jf. direktivet artikkel 2 nr. 2 bokstav d.

Netteier vil kunne identifisere hvilken bruker som har benyttet den aktuelle IP-adressen i det relevante tidsrommet ved å lagre informasjon om hvilke domenenavn eller IP-adresser som den enkelte bruker har besøkt/kommunisert med. For å kunne identifisere den aktuelle informasjonen må imidlertid den lagringspliktige overvåke all kommunikasjon som foregår, også hva som er innholdet i kommunikasjonen. Blant annet basert på det som er nevnt i ekspertgruppens posisjonspapir nr. 10[8] og de signaler som har kommet vedrørende lagring av e-post, så legger PT til grunn at det ikke er akseptabelt at lagringsplikten medfører at den lagringspliktige må overvåke all datakommunikasjon som foregår over Internett.

Til tross for de negative konsekvensene for formålsoppnåelsen, vil PT på nåværende tidspunkt ikke foreslå at det pålegges lagring av informasjon som er nødvendig for å identifisere abonnenten når den lagringspliktige benytter NAT.

Ved fullstendig overgang til IPv6 vil dette problemet løses.

4.3.8. Mislykkede og tapte telefontjenesteanrop

I proposisjonens punkt 8.4.3 har departementene vurdert lagringsplikt for mislykkede og tapte telefontjenesteanrop. PT foreslår av den grunn å forskriftsfastsette at data om slike telefontjenesteanrop kun skal lagres såfremt slik data blir behandlet, logget og lagret. Avgjørende blir altså *om* slike data blir behandlet, logget og lagret.

PT ber om tilbakemelding på hvilke virksomheter som i dag behandler, logger og lagrer slik informasjon.

Eventuelle ulikheter i omfanget av lagringspliktige data dette kan medføre, vil eventuelt bli avhjulpet i den endelige forskriften.

4.3.9. Lokaliseringsinformasjon ved kommunikasjonens begynnelse og slutt

Av datalagringsdirektivet artikkel 5 nr. 1 bokstav f nr. 1 fremgår at det skal lagres lokaliseringskoden (Celle ID) som benyttes av mobilt kommunikasjonsutstyr ved kommunikasjonens begynnelse. Etter definisjonen i direktivet artikkel 2 nr. 2 bokstav e vil dette gjelde uavhengig av om kommunikasjonen originerer eller terminerer i det mobile kommunikasjonsutstyret.

[8] Position Paper No 10, Closer understanding of the terms ”Internet Email” and ”Telephony ” in relation to its application in Directive 2006/24/EC. Utarbeidet av Experts Group “ The platform for electronic data retention for the investigation, detection and prosecution of serious crime” (DataRet/EXPGRP (2010) 10- 16 3 2010)

I proposisjonen på side 77 foreslås det at det for *mobiltelefontjeneste* skal lagres lokaliseringsinformasjon ved kommunikasjonens begynnelse *og* avslutning. Dette medfører at det skal lagres mer enn hva direktivet krever. Proposisjonens forslag er tatt inn i utkastet § 2-3 første ledd nr. 10.

Det er naturlig å reise spørsmål om utvidelsen av hva som skal lagres også skal gjøres gjeldende for annen mobil kommunikasjon enn mobiltelefoni. Dette vil særlig være aktuelt for mobil internettaksess. Proposisjonen behandler ikke dette. PT antar imidlertid at det ikke er tilsiktet at Norges gjennomføring av direktivet skal fravike direktivets løsning på dette punktet. I og med at proposisjonen ikke nevner lagring av lokaliseringsinformasjon, tar PT direktivets opplistning som utgangspunkt for hva som skal lagres.

For mobil internettaksess vil utvidelse av hva som skal lagres til også å omfatte lokaliseringsinformasjon ved kommunikasjonens slutt, medføre en merkbar økning i det totale datavolumet som skal lagres. Grunnen til dette er at det genereres langt flere sesjoner ved mobil internettaksess enn ved bruk av mobiltelefontjeneste. Denne økningen vil medføre økte kostnader.

På denne bakgrunn legger PT til grunn at det for mobil internettaksess kun skal lagres lokaliseringsinformasjon ved *oppstart* av kommunikasjonen. Dette betyr at det ikke skal lagres lokaliseringsinformasjon ved kommunikasjonens avslutning.

4.3.10. Cellens geografiske lokalisering

Etter direktivet skal man for å lokalisere mobilt kommunikasjonsutstyr blant annen lagre ”opplysninger som identifiserer cellens geografiske lokalisering ved å vise til deres lokaliseringskode (celleidentitet) i det tidsrommet kommunikasjonsopplysningene lagres.”

Med cellens geografiske lokalisering forstår PT det arealet som basestasjonen/senderen dekker.

Det har vært diskusjon om hvordan man skal vise til det tidsrommet kommunikasjons-opplysningene lagres. Særlig er det uttrykt bekymring fra tilbyderne og Datatilsynet om bestemmelsen medfører at det skal lagres forflytning mellom basestasjoner under en enkelt kommunikasjon.

PT forstår direktivets bestemmelse på dette punkt slik at det kun er cellens geografiske posisjon på det tidspunkt kommunikasjonen ble opprettet, som skal lagres. Etter proposisjonen og utkastet til forskrift skal imidlertid også cellens geografiske posisjon ved tidspunket for når mobiltelefonikommunikasjonen ble avsluttet lagres ved mobiltelefontjeneste. Eventuelle posisjoner fra andre celler som har blitt benyttet under bruk av tjenesten skal ikke lagres.

Henvisningen til at det skal lagres i det tidsrommet kommunikasjonsopplysningene blir lagret, må forstås som en presisering av at cellens geografiske lokalisering på tidspunkt for start og eventuelt slutt av kommunikasjonen ikke skal endres dersom man senere i lagringstiden endrer cellens geografiske lokalisering. Slik vil det være mulig å hente ut korrekt data fra den aktuelle kommunikasjon uavhengig om cellens geografiske lokalisering har blitt endret i ettertid.

4.3.11. Tidsformat

For å sikre mulighet til å analysere de lagrede data er det viktig at tidsangivelse er entydig. Derfor er det foreslått at all tidsangivelse skal vise hvilken tidssone dataene er angitt i.

4.3.12. Annen informasjon som ikke omfattes av lagringsplikten

Personal Unblocking Key (PUK) er ikke lagringspliktig data etter ekomloven § 2-7a. Videre vil data fra signaleringstrafikk ikke omfattes av lagringsplikten etter ekomloven § 2-7a.

5. Krav til behandlingen av lagrede data

5.1. Innledning

Summen av de lagringspliktige data hos den enkelte lagringspliktige vil utgjøre omfattende informasjon om den enkelte sluttbrukeren. Deler av de lagringspliktige dataene vil kunne bli benyttet som bevis i straffesaker. Stortinget har derfor forutsatt at strenge krav til selve lagringen blir innført. Videre legges det opp til etterprøvbarhet om hvilken behandling som er foretatt under lagringen. Samlet hindrer dette at uvedkommende får tilgang til de lagrede data og bidrar til å sikre beviskvaliteten til de lagrede data.

I innstillingen forutsettes det at det skal innføres konsesjonsplikt for de lagringspliktige, at det skulle innføres autorisering av personell med selvstendig tilgang til de lagrede data, krav om kryptering ved overføring av data over landegrensene og "lukket lagring" av de lagrede data og krav om sporbarhet for enhver bruk av de lagrede data for på denne måten forhindre uautorisert bruk. Stortinget forutsetter at det skal utarbeides forskriftsbestemmelser for kryptering, som skal tilfredsstille etablerte internasjonale standarder.

Samferdselsdepartementet har bedt PT å utarbeide forslag til regler for autorisering av personell og om sporbarhet. Datatilsynet har fått i oppgave fra Fornyings-, administrasjons- og kirkedepartementet å vurdere om det er behov for kryptering ut over Stortingets krav om kryptering ved forsendelse av data over landegrensene, samt ivareta kravene til "lukket lagring". Videre skal Datatilsynet utarbeide en eller flere bestemmelser som hjemler pålegg om kryptering etter særskilte standarder.

PT er kjent med at Datatilsynet foreslår å regulere kryptering og "lukket lagring" gjennom konsesjoner til den enkelte lagringspliktige og at hovedregelen vil bli asymetrisk kryptering i hele lagringsperioden.

Lagringspliktige subjekter etter ekomloven § 2-7a første ledd vil være underlagt pliktene i ekomloven § 2-7 om konfidensialitet og § 2-9 om taushetsplikt. Videre vil personopplysnings-loven § 13 om informasjonssikkerhet og § 14 om internkontroll komme til anvendelse for alle lagringspliktige etter ekomloven § 2-7a første ledd. Konsesjonsplikten nedfelt i person-opplysningsforskriften § 7-1 vil, etter sin ordlyd, kun omfatte de som er lagringspliktige etter ekomloven § 2-7a første ledd. Lagringsplikten kan med hjemmel i ekomloven § 2-7a annet ledd utvides til virksomheter som ikke er lagringspliktige etter første ledd. Slike virksomheter blir ikke underlagt konsesjonsplikt etter personopplysningsforskriften § 7-1.

PT legger til grunn at Datatilsynet har, eller vil skaffe seg hjemler for å kunne pålegge konsesjonsplikt for lagringspliktige som pålegges lagringsplikt med hjemmel i ekomloven § 2-7a annet ledd, slik at behandlingen av dataene vil kunne underlegges strengere vern enn hva kravene til konfidensialitet og taushetsplikt bestemt i medhold av ekomloven § 2-7a annet ledd.

Uansett gir ekomloven § 2-7a annet ledd første punktum hjemmel til å forskriftsfeste konfidensialitetskrav som vil gjelde for alle lagringspliktige.

Kravene til lagring som skal sikre at uvedkommende ikke får tilgang til dataene, vil omfatte fysiske, logiske og personellmessige krav.

5.2. Lagringsmediet

Lagringspliktige data genereres på ulike nivå i nettet og hos ulike aktører. Et spørsmål er da når kravene til sikkerhet for lagringen skal inntre. Dette må sees i sammenheng med når behovet for særskilt beskyttelse oppstår. Verken proposisjonen eller innstillingen er tydelige på når sikkerhetskravene, skal starte å gjelde.

Innføring av særskilte sikkerhetskrav for lagringen, innebærer at den lagringspliktige må ha kontroll på de lagringspliktige data. Dette innebærer blant annet at den lagringspliktige må dedikere et eller flere områder for lagring av lagringspliktige data og beskytte området etter de krav som fastsettes. Det vil ikke være adgang til å lagre lagringspliktige data utenfor det forhåndsdefinerte området.

Teoretisk er det mulig å gjennomføre sikkerhetskravene allerede når dataene genereres. Dette vil imidlertid være svært krevende både praktisk og økonomisk. Videre vil pålegging av sikkerhetskravene allerede fra det tidspunkt dataene genereres, umuliggjøre at fakturerings- og driftsdatabaser[9] adskilles fra databasen for lagringspliktige data. Dette vil også innebære at lagringspliktige vil måtte autorisere langt flere ansatte for tilgang til lagringspliktige data enn det som er nødvendig for å håndtere tilgangsbegjæringer.

Etter PTs oppfatning er begrunnelsen for den særskilte beskyttelsen av de lagringsplikte data at lagringstiden er seks måneder, samt at det skal lagres noe mer informasjon enn i dag. Det er summen av disse to forhold som medfører at dataene må beskyttes bedre.

PT legger til grunn at beskyttelsesbehovet ikke oppstår før de forskjellige informasjonselementene som er angitt i kapittel 0 i høringsnotatet, for det vesentligste er samlet på det sted hvor de kan bli aksessert for tilgjengeliggjøring for de som har rettmessig adgang til lagringspliktige data. Dette vil typisk være at de kan aksesseres fra et punkt eller er samlet i en database, men også andre avgrensningskriterer kan være aktuelle. Først på dette tidspunkt vil det kunne oppstå langt større personvernmessige konsekvenser ved kompromittering av de lagrede data, enn hva som er tilfelle med dagens lagringspraksis. PT legger denne forståelsen til grunn i relasjon til når kravene om sporbarhet og kravet til kun å bruke autorisert personell kommer til anvendelse.

5.3. Taushetsplikt om lagringspliktige data

Ekomloven § 2-9 pålegger tilbyder og installatør med flere taushet om andres bruk av elektronisk kommunikasjon. Bestemmelsen vil ikke komme til anvendelse for virksomheter som pålegges lagringsplikt etter ekomloven § 2-7a annet ledd, og som ikke allerede er omfattet av ekomloven § 2-9.

For å ivareta dataenes konfidensialitet dersom kretsen av lagringspliktige subjekter blir utvidet til å gjelde andre enn de som omfattes av ekomloven § 2-9, er det nødvendig å forskriftsfastsette tilsvarende taushetsplikt som gjelder for bruk av elektronisk kommunikasjon etter ekomloven § 2-9. Ettersom innhold ikke skal lagres, er det ikke nødvendig å etablere identisk taushetsplikt som det som følger av ekomloven § 2-9.

Taushetsplikten gjelder både aktivt og passivt. Det vil si at de som har taushetsplikt skal aktivt hindre uvedkommende i å få tilgang til taushetsbelagt informasjon, eksempelvis ved fysiske sikringstiltak. På dette punktet vil trolig Datatilsynets regulering av ”lukket lagring” oppfylle taushetsplikten. Videre skal de som har taushetsplikt ikke gi ut taushetsbelagt informasjon til uvedkommende.

[9] Slike databaser vil være underlagt lagringsrett for drifts- og faktureringsformål.

5.4. *Taushetsplikt om politiets uthenting av lagrede data*

I innstillingen på side 8 forutsettes det at autorisert personell har taushetsplikt om alt de får kjennskap til under behandling av lagringspliktige data. Videre gis det på side 11 uttrykk for at det er behov for at de som gjennom sitt arbeid, får kjennskap til at politi eller påtalemyndigheten innhenter eller har innhentet lagret informasjon, skal ha taushetsplikt om dette. Ekomloven § 2-9 pålegger ikke taushetsplikt om hvilken behandling lagret informasjon har blitt underlagt.

Både ekomloven §§ 2-9 og 2-7a hjemler forskriftfastsetting av taushetsplikt for å sikre dataenes konfidensialitet. Hjemlene gir imidlertid ikke grunnlag for å pålegge taushetsplikt om hvilken behandling dataene har vært underlagt, herunder om noen har bedt om utlevering av de lagringspliktige data. PT legger til grunn at det er, eller vil bli etablert slik taushetsplikt med hjemmel i annen lov.

5.5. Intern behandling av lagringspliktige data – autorisasjon

Av innstillingen fremgår det at Stortinget la til grunn for sitt vedtak at det personalet som på vegne av den lagringspliktige, skal ha tilgang til lagringspliktig data, skal autoriseres av den lagringspliktige. Denne godkjennelsesprosessen skal skje i henhold til retningslinjer fastsatt av Datatilsynet og PT i fellesskap. Slike retningslinjer skal omtale behovet for politiattest. Videre la innstillingen opp til at det skulle gjennomføres regelmessige autorisasjonssamtaler.

PT mener at det er behov for å tydeliggjøre at de lagringspliktige skal sikre at uvedkommende ikke får tilgang til lagringspliktig data. Det er bare personell som er autorisert for tilgang til lagringspliktige data hos den lagringspliktige som kan behandle eller på annen måte få kjennskap til lagringspliktige data under lagringen. På denne bakgrunn foreslår PT at det settes krav i forskriften om at uvedkommende ikke skal få tilgang til lagringspliktige data så lenge dataene er under den lagringspliktiges kontroll.

PT legger til grunn at Stortinget har ment at det er nødvendig med en mer omfattende godkjenningsordning for personell som skal ha tilgang til lagringspliktige data, enn den godkjenning som i dag gjelder for behandling av trafikkdata etter ekomforskriften § 7-1 annet ledd. Denne bestemmelsen lyder:

"Behandling av trafikkdata hos tilbyder kan bare foretas av personer som arbeider med fakturering, trafikkstyring, kundeforespørsler, markedsføring av elektronisk kommunikasjonstjeneste eller avsløring av urettmessig bruk av elektronisk kommunikasjon. Nevnte personer må ha fullmakt for utførelsen av arbeidet fra tilbyder av elektronisk kommunikasjonsnett eller -tjeneste. Behandlingen skal begrenses til det som er nødvendig for utførelsen av nevnte arbeidsoppgaver."

PT håndhever nevnte bestemmelse slik at det er et krav om forutgående individuell godkjennelse av personer som skal ha tilgang til trafikkdata.

Fordi det kreves en særskilt godkjenningsordning for personell som har tjenstlig behov for tilgang til lagringspliktig data, ser PT det som mest hensiktsmessig at dette reguleres i forskriften om datalagring framfor å endre ekomforskriften § 7-1. PT foreslår derfor at det inntas en særskilt bestemmelse om krav til autorisasjon for personell som skal ha tilgang til lagringspliktige data. Se vedlagte utkast § 3-4.

Se punkt 5.2 for når kravet til å benytte autorisert personell inntrer. PT mener at det ikke er krav til bruk av autorisert personell før dataene er lagret i database som er underlagt "lukket lagring"

Autorisering skal gjennomføres før det gis tilgang til lagringspliktige data som er underlagt lukket lagring. For å opprettholde autorisasjonen skal det avholdes autorisasjonssamtale minst en gang i året. Ved fratredelse av stilling skal vedkommende gjennom en samtale gjøres kjent med at autorisasjonen er opphevet og underrettes om at taushetsplikten fortsatt gjelder. Avholdelse av autorisasjonssamtaler skal dokumenteres skriftlig eller i elektronisk format som ikke kan endres.

PT legger til grunn at en lagringspliktig skal begrense antallet autoriserte personer mest mulig, men ikke i et slikt omfang at det hindrer en forsvarlig og effektiv håndtering av de lagringspliktige data og henvendelser om lovlig tilgang.

Når det gjelder hvem som skal foreta autorisasjonen, legger PT til grunn at dette skal være virksomhetens leder eller en annen som er tildelt fullmakt til å autorisere. Den som er tildelt fullmakt til å autorisere kan ikke delegere denne kompetansen videre. Dette for å unngå pulverisering av ansvaret.

Avholdelse av selve autorisasjonssamtalene og det forutgående arbeidet med selve autorisasjonen vil imidlertid kunne delegeres.

For at en lagringspliktig skal kunne autorisere en person, foreslår PT at det skal kreves fremlagt politiattest i henhold til strafferegisteringsloven § 5 før vedkommende får selvstendig tilgang til lagringspliktige data. Gjennom krav til politiattest settes den lagringspliktige bedre i stand til å foreta en vurdering av egnethet hos den som skal autoriseres. Hvis innhentet politiattest avdekker tidligere straffbare forhold, bør den lagringspliktige forta en konkret vurdering av om vedkommende likevel kan gis tilgang til lagringspliktige data. I denne vurderingen vil selvfølgelig lovbruddets art ha betydning. Lovbrudd som har medført brudd på gitt tillit, manglende overholdelse av profesjonsplikter, overlagte lovbrudd eller alvorlige forbrytelser bør tillegges større negativ betydning enn mindre alvorlige lovbrudd. Det understrekes at vurderingsnormen ikke er uttømmende.

I tillegg til vurderingen av vedkommendes vandel, må den lagringspliktige også vurdere om det foreligger andre forhold som kan medføre at den aktuelle personen ikke er egnet til å behandle lagringspliktige data på vegne av den lagringspliktige. Dette kan være forhold som kan tilsi at vedkommende selv ikke overholder tilgangsreglene eller som kan medføre at vedkommende kan bli presset eller bestukket til å foreta uautorisert behandling og distribusjon av de lagringspliktige data. Relevante forhold kan være eget forhold til alkohol eller andre rusmidler, anstrengt økonomi eller tilknytning til kriminelle. Eksemplifiseringen er ikke uttømmende og ingenting av det nevnte vil automatisk diskvalifisere en person fra å bli autorisert. Det må alltid foretas en konkret helhetsvurdering.

Nærstående skal som hovedregel ikke vurderes i autorisasjonsprosessen. En så omfattende gjennomgang av den som vurderes autorisert vil ikke være forholdsmessig i forhold til hvilke data som skal behandles og det inngrep i den personlige sfære som kreves av arbeidsgiver.

En viktig faktor i en autoriseringsprosess er at vedkommende som skal autoriseres blir gjort kjent med og internaliserer de regler som gjelder for behandlingen av de lagringspliktige data. Gjennom autoriseringsprosessen skal den lagringspliktige ansvarliggjøre sitt personell i forhold til overholdelsen av dette regelverket. Brudd på regelverket må videre kunne sanksjoneres i forhold til personellet.

Den lagringspliktige vil være forpliktet til, gjennom aktiv ledelsesoppfølgning, herunder gjennom kontroll av sporingsloggene, å følge opp at personellet ikke bryter reglene for tilgang til de lagringspliktige data. Virksomheten er også ansvarlig for at etablerte rutiner for autorisering samt behandling av lagringspliktige data blir overholdt.

5.6. Beviskvalitet

I proposisjonen punkt 8.4.4 uttales:

> *"Datalagringsdirektivet sier ikke annet om kvaliteten på dataene enn at de skal være av samme kvalitet som de har i nettet. Departementet mener følgelig at tilbyderne ikke kan pålegges å skulle utføre kvalitetshevende tiltak på de data som de skal lagre. Et krav om økt kvalitet vil kunne føre til økte kostnader, og departementet finner ikke grunnlag for å skulle påføre tilbyderne denne type ekstrakostnader."*

PT legger til grunn at dette innebærer at det kun skal settes krav om at kvaliteten på dataene ikke blir forringet ved lagringen. Dette må også omfatte krav til at den bevismessige verdien av de lagrede data ikke må forringens gjennom lagringen.

Lagringspliktige skal selv velge løsning for lagring av data. Det vil derfor ikke være mulig å fastsette tekniske krav til hvordan bevisforringing skal unngås. En forskriftsregulering kan derfor kun sette krav til resultatet.

På denne bakgrunn foreslår PT at det settes krav om at lagringen skal skje på en måte som ikke forringer kvaliteten på de lagringspliktige data. Dette innebærer blant annet adekvate sikkerhetstiltak for å unngå uautorisert endring eller sletting av lagringspliktige data. Se utkastet § 3-1.

5.7. Sikkerhetskopiering

Det er behov for å sikre at de lagringspliktige data ikke forsvinner på grunn av datahavari eller av andre årsaker knyttet til feil på lagringsmediet. PT foreslår derfor at det settes som krav at de lagringspliktige regelmessig skal ta sikkerhetskopier av de lagrede data og oppbevare disse under de samme vilkår som hovedlagringsmediet. Problemstillingen omkring lagring av data hos to lagringspliktige er ikke aktuell når en lagringspliktig lagrer sikkerhetskopien i et eget lagringsmedium. Logisk skille er ikke tilstrekkelig.

PT anser det som nødvendig at det tas sikkerhetskopier minst daglig av de lagrede data.

5.8. Sletteplikt

Det følger av ekomloven § 2-7 annet ledd nr. 2 jf. § 2-7a første ledd at lagringspliktige data skal slettes etter 6 måneder. PT tar inn denne forpliktelsen i forskriften for oversiktens skyld.

Ettersom data blir lagret med ulik forsinkelse i forhold til når kommunikasjonen fant sted, kan det problematiseres om lagringstiden på 6 måneder skal gjelde fra det tidspunkt dataene ble lagret, eller om det skal være fra det tidspunkt kommunikasjonen fant sted. Etter PTs syn må det avgjørende være når kommunikasjonen faktisk fant sted. En annen løsning vil trolig være mer krevende å håndtere for den lagringspliktige, samt at det vil gi fragmentert informasjon om elektronisk kommunikasjon som er rundt 6 måneder gammel.

Videre er det behov for en klargjøring av hvordan sletteplikten etter ekomloven § 2-7 annet ledd skal forstås i de tilfeller tilbyder har blitt pålagt sikring etter straffeprosessloven § 215a. Ordlyden i § 2-7 annet ledd nr. 3 vil etter sin ordlyd utsette sletteplikten så lenge det er gitt sikringspålegg etter straffeprosessloven § 215a for data eldre enn seks måneder. For å tydeliggjøre at den generelle sletteplikten for seks måneder gamle lagringspliktige data står tilbake for eventuelle sikringspålegg, så tas dette inn i forskriftsteksten.

5.9. Sporing av behandling av lagringspliktige data

For å sikre at data ikke blir behandlet til andre formål enn hva som er angitt i forskriften som gyldige behandlingsformål, så kreves det at den lagringspliktige oppretter en logg som viser all behandling av data under lagringen. Dette vil også være med på å sikre beviskvaliteten for de lagrede data. Det skal logges hvem som gjør hva og til hvilken tid. Videre skal det loggføres hvem dataene er utlevert til.

Dersom behandlingsgrunnlaget er annet enn samtykke fra den opplysningene gjelder, så skal bare opplysninger om mottaker hos anmodende virksomhet loggføres. Ved samtykke fra den opplysningene gjelder, skal samtykkeerklæring arkiveres.

6. Behandling og uthenting av lagringspliktige data/ tilgjengeliggjøring

6.1. Innledning

Hvordan tilrettelegging og utlevering av de lagrede data håndteres, vil ha stor betydning for politi og påtalemyndighetens effektivitet ved bruk av de lagringspliktige data. Videre vil utformingen av krav til tilrettelegging av data ha direkte innvirkning på kostnadene for alle parter. Det er derfor viktig å regulere på hvilke grunnlag de lagringspliktige data skal kunne behandles, samt omfanget av tilretteleggingsplikten for lagringspliktige data.

6.2. Uthenting av lagringspliktige data

6.2.1. Innledning

PT har sett hen til utformingen av kommunikasjonsvernet i ekomloven, og foreslår en forskriftbestemmelse med uttømmende opplisting av hvilke tilfeller den lagringspliktige kan behandle de lagringspliktige data. En slik opplisting sikrer at den lagringspliktige ikke behandler de lagringspliktige data for ikke-tillatte formål og klargjør hvem som har adgang til å be de lagringspliktige om tilgang til lagringspliktige data. Bestemmelsen åpner kun for behandling av lagret informasjon hvor slik behandling er nødvendig for å gi slik tilgang til informasjon som loven åpner for. Det vil si at dataene bare kan utleveres til den opplysningene gjelder, eller til de som har rettmessig tilgang til lagringspliktige data etter prosedyrene fastsatt i straffeprosessloven §§ 210b, 210c, 216b eller 222d, i politiloven § 17d eller verdipapirhandelloven § 15-3 annet ledd nr. 3.

De sikkerhetstiltak som blir innført for de lagringspliktige data vil i følge noen tilbydere medføre at data for faktureringsformål vil bli lagret i en annen database enn de lagringspliktige data. Slik kan tilbyderne unngå praktiske og økonomiske utfordringer rundt fakturabehandling, kundeservice og autorisering av personell. Imidlertid kan det tenkes at den praktiske og økonomiske fordelen ved å etablere to databaser ikke er tilstede i alle tilfeller.

For å sikre at vernet av de lagrede data ikke vil være dårligere ivaretatt dersom alle data lagres i en database, vil taushetspliktbestemmelsen i forskriften kreve at det i slike tilfeller lages et logisk skille mellom data som er lagret for faktureringsformål og data som er lagringspliktige.

6.2.2. Rett til innsyn for den registrerte

Det følger av personopplysningsloven § 18 annet ledd at den som opplysningene gjelder kan få opplysninger om hvilken informasjon om den registrerte som tilbyderen behandler. PT foreslår å ta inn en bestemmelse i forskriften som tar hensyn til at denne rettigheten også gjelder for opplysninger som lagres etter ekomloven § 2-7a.

6.2.3. Rett til innsyn etter fullmakt fra den registrerte

Den som er part i kommunikasjonen kan gi opplysninger om trafikk til og fra seg selv uten hinder av taushetspliktsbestemmelsen i ekomloven § 2-9. Dette kan tilsi at denne også må kunne gi fullmakt til at andre kan innhente de lagringspliktige data. For eksempel vil politiet kunne be om fullmakt for å få tilgang til lagringspliktige data, men også andre vil kunne ha interesse av å nyttegjøre seg de lagringspliktige data for å kunne yte tjenester til den de lagringsplikte data omhandler.

Lagring av data etter ekomloven § 2-7a, har til formål å være et hjelpemiddel i kriminalitetsbekjempelse. PT er derfor av den oppfatning at bruken av fullmaktsinstituttet for å gi tredjemann fullmakt til å innhente lagringspliktig data, bør begrenses til den krets som likevel har adgang til å innhente data på annet grunnlag. Det er særlig formålet med den særskilte lagringen etter ekomloven § 2-7a som tilsier en slik løsning. En slik begrensning vil også være i tråd med datalagringsdirektivet artikkel 4. En begrenset adgang til å gi fullmakt til behandling og uthenting av data vil også redusere kostnadene knyttet til den særskilte lagringen og redusere faren for at data brukes til kommersielle formål.

Konsekvensen av en slik begrensning i muligheten til å gi tredjemann adgang til opplysningene gjennom fullmakt, er at ingen andre enn den som har vært part i kommunikasjonen selv eller de øvrige som etter forskriftsutkastet § 4-1 har adgang til å be om data som er lagret, vil kunne anmode den lagringspliktige om å hente ut data. Den som har rett til innsyn i opplysninger som er lagret, kan selvfølgelig selv gi videre informasjonen om seg selv til andre.

6.2.4. Lovlig tilgang

I utkastet til forskrift § 4-1 bokstav c til e og annet ledd foreslår PT å ta inn hvilke rettslige grunnlag som etter nytt femte ledd i ekomloven § 2-9 gir grunnlag for behandling av de lagringspliktige data.

I de tilfellene uthenting av lagrede data gjøres etter pålegg med hjemmel i straffeprosessloven § 216b annet ledd bokstav d, er forskriftsbestemmelsen avgrenset til de tilfeller hvor den anvendes for å få tilgang til data som er lagret i den databasen som inneholder de lagringspliktige data.

Oppkobling av sanntidsoverføring av de lagringspliktige data og eventuelle pålegg om bistand for andre data enn de lagringspliktige, reguleres ikke av denne forskriften. Etter det PT kjenner til vil slike data kunne aksesseres gjennom andre systemer enn den database som vil inneholde de lagringspliktige data.

6.2.5. Teknisk vedlikehold

En database vil kunne ha behov for teknisk vedlikehold og derfor må det åpnes for behandling av dataene dersom det er nødvendig. En forutsetning er at de som utfører slikt vedlikehold må være autorisert.

6.3. Retting av data

Dersom det blir aktuelt med retting av data i medhold av personopplysningsloven, så skal det loggføres at det er foretatt retting av dataene, samt hvilke data som var lagret før rettingen fant sted. Det skal også loggføres hva som er årsaken til at dataene rettes.

6.4. Tilretteleggingsplikten

6.4.1. Innledning

Det følger av ekomloven § 2-8 første ledd at tilbyder av elektronisk kommunikasjonsnett som anvendes til offentlig kommunikasjonstjeneste og tilbyder av slik tjeneste skal tilrettelegge nett og tjeneste slik at lovbestemt tilgang til informasjon om sluttbruker og elektronisk kommunikasjons sikres. Da det kan være mulig å utvide kretsen av lagringspliktige til andre som ikke omfattes av ekomloven § 2-8, foreslås en særskilt bestemmelse i utkastet om tilretteleggingspliktens innhold i relasjon til de lagringspliktige data.

6.4.2. Felles format

Etter PTs syn skal de lagringspliktige data gjøres tilgjengelig på et format som er hensiktsmessig å behandle både for tilbyder, den registrerte og øvrige som har krav på å få tilgang til lagringspliktig data. For så vidt gjelder tilgjengeliggjøring av data for den registrerte innebærer dette at dataene blir presentert på en slik måte at den enkelte sluttbruker er i stand til å tolke dataene.

Når det gjelder tilgjengeliggjøring av data for politi, påtalemyndighet eller Finanstilsynet bør det stilles krav til at dataene blir gjort tilgjengelig på et elektronisk format. Ordene "… enkelt kan behandles …" i forskriftsutkastet § 4-2 annet ledd betyr at det skal være enkelt for mottaker å behandle den overleverte informasjonen. Behandlingen skal ikke nødvendigvis kunne gjøres med teknisk enkle hjelpemidler. Det vil eksempelvis oppfylle forskriftskravet dersom mange tilbydere benytter en felles teknisk løsning og det er kjent for politiet hvordan dette formatet skal håndteres. En bransjestandard om et felles format for overlevering av lagringspliktige data til politiet vil kunne oppfylle kravet om et format som ved enkle midler kan prosesseres. PT vil fasilitere arbeidet med etablering av en slik standard med utgangspunkt i mottatt forslag fra Kripos.

6.4.3. Frist for klargjøring og samling av lagringspliktige data

De ulike lagringspliktige data vil genereres på ulike steder i det elektroniske kommunikasjonsnett som den lagringspliktige benytter. Det tar ulik tid å prosessere de enkelte delene av de lagringspliktige dataene slik at de blir lesbare, videre vil fullt datasett først oppnås når samtlige prosesseringer av de lagringspliktige data er ferdigstilt. Spørsmålet er altså hvor oppdatert de lagringspliktige data skal være.

Etter dagens rettstilstand har tilretteleggingsplikten etter ekomloven § 2-7 ved utleveringspålegg etter straffeprosessloven § 210 kun omfattet ferdig prosesserte data. Kripos har under arbeidet med denne forskriften gitt signaler om at det er viktig av hensyn til etterforskningen at det settes minimumskrav til hvor lang tid det kan gå før dataene er ferdig prosessert slik at det er mulig å få tilgang til forholdsvis ferske data om nødvendig. På bakgrunn av dette finner PT grunn til å forskriftsfastsette minimumskrav til hvor raskt de lagringspliktige data skal klargjøres for lagring, altså hvor raskt de lagringspliktige data skal være tilgjengelig for utlevering til politiet.

PT kan ikke se at det foreligger grunner til å kreve raskere prosessering av de lagringspliktige data enn hva som gjøres i dag. I denne sammenheng har PT sett hen til at

det vil medføre økte kostnader å kreve raskere prosessering, uten at det er dokumentert behov for raskere tilgang enn hva som er tilfellet i dag.

PT mener at de lagringspliktige data kun skal gjennomgå nødvendig prosessering, tilrettelegging og eventuell kryptering før de blir lagret i sikret database for oppbevaring frem til sletting. Selve prosesseringen av trafikk- og lokasjonsdata gjøres i dag ferdig innen få timer, i noen tilfeller i underkant av en halvtime.

På bakgrunn av de krav til kryptering som foreslås fra Datatilsynet, vil de lagringspliktige data måtte tilrettelegges, eller klargjøres, før de blir kryptert. Dette, sammen med selve krypteringen, vil medføre at prosesseringen vil ta noe lengre tid enn tidligere.

Når det gjelder lagringspliktige data som genereres hos andre enn den lagringspliktige selv, vil den lagringspliktig være avhengig av å motta CDR-filer fra disse før klargjøring for lagring kan skje. Hyppigheten av oversendelse av CDR-filer vil altså være avgjørende for hvor hyppig lagringspliktige data mottatt fra roaming kan oppdateres i database for oppbevaring frem til sletting. PT ser ikke grunn til å sette særskilte krav til hyppigheten av slik oversendelse.

PT mener at det må forventes at de lagringspliktige prosesserer og eventuelt krypterer og tilrettelegger de lagringspliktige data uten ugrunnet opphold. Regelverket må imidlertid ta høyde for ulik prosesseringstid slik at reguleringen må inneholde en absolutt minstetid for tilgjengeliggjøring av ferdig behandlede lagringspliktige data. PT foreslår at det som minimumskrav må kreves at data som genereres eller behandles i den lagringspliktiges eller tilgangsleverandørers elektroniske kommunikasjonsnett skal være tilgjengelig for utlevering til de som har rettslig adgang til de lagringspliktige data innen ett døgn etter at kommunikasjonen har funnet sted. Med tilgangsleverandører forstås både MNO og MVNO. Tilsvarende informasjon fra roamingpartnere skal være tilgjengelig for utlevering innen ett døgn etter at den lagringspliktige har mottatt de lagringspliktige dataene.

Det understrekes at bestemmelsen som foreslås i forskriften § 4-2 ikke regulerer når sikkerhetskravene skal inntre.

6.4.4. Responstid

Det bør vurderes om det skal fastsettes krav til hvor raskt den lagringspliktige skal kunne gjøre tilgjengelig lagret informasjon som begjæres utlevert. Et slikt krav er ikke fastsatt i dag. Det må derfor foretas en grundig vurdering av om det er nødvendig å pålegge de lagringspliktige krav til responstid. Her vil blant annet hensynet til etterforsking og medgått tid til å få tilgang til historiske data for å avdekke, etterforske eller straffeforfølge alvorlig kriminalitet være tungtveiende argumenter.

Videre må det vurderes hva som er en rimelig responstid. Avhengig av hvordan et eventuelt slikt krav formuleres, vil det kunne ha store økonomiske konsekvenser for de lagringspliktige og/eller samfunnet. I denne sammenheng må man se hen til variasjonen av størrelsen på de virksomhetene som blir pålagt lagringsplikt. Antall utleveringspålegg vil sannsynligvis være proporsjonalt med antall abonnement innen hver kategori. Således vil virksomheter med få abonnenter kunne utsettes for uforholdsmessige kostnader dersom de plikter å ha høy tilgjengelighet og rask responstid for utlevering av de lagringspliktige data. Samtidig er det rom for små tilbydere til å gå sammen om en felles lagringsløsning som vil redusere de økonomiske konsekvensene av krav til økt tilgjengelighet.

6.4.4.1. Utlevering til den opplysningene gjelder

For utlevering av informasjon til den opplysningene gjelder, jf. personopplysningsloven § 18, legger PT til grunn at regelverket i personopplysningsloven vil være bestemmende for hvor raskt dataene skal gjøres tilgjengelig for vedkommende.

6.4.4.2. Tilrettelegging for politi, påtalemyndighet og Finanstilsynet

I arbeidet med denne forskriften har det kommet signaler fra justissektoren om at de ønsker at det settes et minstekrav om tilgjengelighet hos de lagringspliktige slik at de lagringspliktige data utleveres uten å forsinke etterforskningen unødig.

PT vil imidlertid innledningsvis presisere noen utgangspunkter som det er hensiktsmessig å ha klart når man vurderer behovet for og villigheten til å innføre en beredskapsplikt for lagringspliktige i forhold til tilrettelegging av data.

I høringsprosessen ble det diskutert om PT eller domstolene skulle ha kompetanse til å gi tilgang til de lagringspliktige data. Valg av domstolene som kompetent instans er etter PTs forståelse begrunnet ut fra prinsipielle betraktninger om maktfordeling og økt rettsikkerhet. Hensynet til raskere tilgang til de lagrede data var ikke sentralt i debatten om plassering av slik kompetanse.

Justissektoren var i høringsrunden kritiske til at politiets hastekompetanse etter staffeprosessloven § 210 annet ledd ble foreslått fjernet i høringsnotatet. I proposisjonen og innstillingen ble hastekompetansen videreført. Lovgiver innførte imidlertid en vaktordning ved Oslo tingrett for at politiets hastekompetanse i denne sammenhengen ikke skal bli benyttet i særlig grad. Vaktordningen er således ikke begrunnet ut fra et behov om raskere tilgang til de lagringspliktige data.

Kripos uttaler i sitt høringssvar at den normale behandlingstid med svar innen to døgn, som PT benytter for å besvare anmodning om fritak fra taushetsplikt, ikke anses som et forsinkende ledd i etterforskningen. Videre vises det til at tilbydernes behandlingstid for utleveringspålegg normalt er noen få dager. Kripos viser i sitt høringssvar ikke til at den totale behandlingstid er problematisk av hensyn til å avdekke, etterforske og straffeforfølge alvorlig kriminalitet.

Kripos har, etter direktivet ble vedtatt implementert, ytret behov for at det settes krav til samtlige lagringspliktige om svartid innen en virkedag ved normal etterforsking, og så snart som mulig ved akuttilfeller.

Responstid ved normal etterforsking

Vaktordningen ved Oslo tingrett er innført for å minske saksbehandlingstid for å etablere lovlig tilgang til de lagringspliktige data. Selv om begrunnelsen for ordningen ikke er begrunnet ut fra raskere responstid hos tilbyderne, er det naturlig å legge til grunn at slike tiltak ikke ville blitt gjennomført uten en forventing om rimelig responstid hos de lagringspliktige. Således bør det stilles krav til lagringspliktige om hvor raskt lagringspliktige data skal tilgjengeliggjøres.

Med innføringen av hastekompetanse og vaktordningen ved Oslo tingrett kan fritak fra taushetsplikten etableres raskt. Dette innebærer at av den tiden som går fra politiet begjærer tilgang til lagringspliktig data til disse dataene er i hende på politiet, vil saksbehandlingstiden hos de lagringspliktige kunne utgjøre den lengste perioden.

Basert på det ovennevnte, finner PT ut fra en konkret helhetsvurdering å fremme forslag om at det bør stilles krav om at responsen fra de lagringspliktige skal være skje uten ugrunnet opphold, dog ikke lengre enn to virkedager eller maksimalt tre dager. Maksimums-begrensningen på tre dager er satt for å dekke ordinære helger. Dette betyr at de lagringspliktige ikke må etablere helgevakt i normale helger.

Responstid ved akutt operativt behov
Kripos har under prosessen med utformingen av dette utkastet til forskrift gitt uttrykk for at det i enkelte saken er behov for for raskere responstid hos tilbyderne enn hva som er dagens praksis. Dette vil være tilfeller hvor det eksempelvis forligger en akutt situasjon som krever operativ innsats. PT ser at det vil være slikt behov, men er ikke kjent med i detalj hvilke saker og hvor hyppig dette behovet foreligger.

Etter det PT forstår, har politiet myndighet til å pålegge den lagringspliktige å yte den bistand som er nødvendig for å gi politiet opplysninger om hvilke kommunikasjonsanlegg som i et bestemt tidsrom skal settes eller har vært satt i forbindelse, se straffeprosessloven § 216b annet ledd boksvar b, jf. § 216a fjerde ledd annet punktum. Disse bestemmelsene ble ikke endret ved implementeringen av datalagringsdirektivet. Dette virkemiddelet vil dekke behovet for alle tilfeller hvor det skal gjennomføres basestasjonsøk. Ved behov for spesifikke søk på bestemte telefonnummer eller IP-adresser, vil samme bestemmelse kunne anvendes i saker med strafferamme med fengselstraff på fem år eller mer, herunder omfattes saker med strafferamme med fengselstraff på tre år eller mer hvor straffeloven § 60a kommer til anvendelse. Dermed er det kun i saker med strafferamme på fire år, samt ved overtredelse av bestemmelser som angitt i straffeprosessloven § 210b første ledd bokstav c, at politiet ikke kan pålegge den lagringspliktige å yte bistand.

Etter gjeldende rett har tilgang til taushetsbelagt informasjon etter ekomloven § 2-9 vært betinget av et fritak fra taushetsplikten for saker med lavere strafferamme enn fem år. Dette gjelder også ved bruk av hastekompetansen etter straffeprosessloven § 210. PT har, som fritakende myndighet, ikke blitt kontaktet av politiet utenfor ordinær arbeidstid i slike saker. På denne bakgrunn legger PT til grunn at politiets behov for raskere tilgang til de lagringspliktige data enn hva som foreligger i dag, ikke har vært presserende.

Adgangen til å pålegge bistandsplikt vil imidlertid ikke nødvendigvis være til nytte hvis de lagringspliktige har en så lang reaksjonstid at bistanden i realiteten vil bli ytet for sent for å dekke politiets akutte behov.

Uavhengig av hvilken plikt som pålegges de lagringspliktige, vil nok de store lagringspliktige uoppfordret stille med nødvendig bemanning uavhengig av når på døgnet behovet skulle oppstå i de åpenbare tilfellene. Det åpenbare tilfellet vil være hendelser som det som skjedde den 22. juli 2011. Det kan imidlertid ikke forventes at de lagringspliktige uoppfordret etablerer slik responstid i tilfeller som ikke er like åpenbare.

PT finner det uforholdsmessig å kreve at enhver tilbyder skal kunne etterkomme utleveringspålegg umiddelbart etter at utleveringspålegg er utferdiget. Dette vil kreve en døgnkontinuerlig bemanning, noe som vil være svært kostnadskrevende. Uavhengig av hvem som ender opp med kostnadene med en slik bemanning, vil en døgnbemanning trolig innebære at tre til fem personer vil måtte til for å dekke en stilling hos den enkelte lagringspliktige for å oppfylle arbeidsmiljølovens krav knyttet til arbeidstid. Sett i lys av at mange, om ikke de fleste, lagringspliktige nok aldri eller kun svært sjeldent vil oppleve at noen etterspør lagringspliktige data med krav om umiddelbar respons, anser PT det som uforholdsmessig at det inneføres et generelt krav om dette. Særlig legges det vekt på at flertallet av de lagringspliktige er så små, at sannsynligheten for at det vil oppstå behov for særlig rask uthenting av historisk informasjon er meget liten.

På den annen side, de lagringspliktige kan heller ikke respondere så sent på krav om utlevering av lagringspliktige data at formålet med å innhente dataene forfeiles. At Stortinget har vedtatt et tilgangsregime med døgnkontinuerlig beredskap hos en domstol, tilsier at de lagringspliktige må respondere raskt på utleveringsbegjæringer.

PT ser imidlertid at det kan være aktuelt å pålegge operatører av store databaser en form for forkortet responstid utenom normal arbeidstid. Dette kan eventuelt skje gjennom pålegg om etablering av en tilkallingsordning, hvor politiet kan tilkalle relevant personell hos den lagringspliktige for å håndtere utleveringsbegjæringer når behovet for meget rask respons fra den lagringspliktige oppstår. Stortingets krav om "lukket lagring" innebærer et forbud mot fjernaksess til de lagringspliktige data, noe som vil innebære en lengre behandlingstid hos den lagringspliktige så lenge personellet ikke er tilstede ved de lagringspliktige data. Hvem som eventuelt skulle pålegges en slik forkortet responstid gjennom en innkallingsordning vil måtte avgjøres i samråd med relevant politimyndighet og forutsetter selvfølgelig en avklaring av kostnadsspørsmålet.

6.4.5. Responstid og når data anses tilgjengeliggjort.

Fristen for å respondere starter å løpe fra det tidspunkt den lagringspliktige mottar begjæringen fra politiet, påtalemyndighet og Finanstilsynet og tilretteleggingsplikten anses oppfylt når den lagringspliktige tilgjengeliggjør etterspurte data for politi, påtalemyndighet og Finanstilsynet.

Det er intet i ekomloven § 2-7a eller § 2-8 som pålegger de lagringspliktige å overlevere etterspurt informasjon til politi, påtalemyndighet eller Finanstilsynet. Ekomloven pålegger således ikke de lagringspliktige ansvaret for forsendelsen til politiet, påtalemyndighet eller Finanstilsynet.

7. Overgangsregler

PT har ikke på dette tidspunkt foreslått overgangsbestemmelser. En ber om begrunnede innspill til eventuelle slike i høringsrunden.

8. Økonomiske og administrative konsekvenser

8.1. For Post- og teletilsynet

Selve forskriften antas ikke å medføre økte økonomiske og administrative kostnader for PT i tillegg til det som det ble redegjort for i proposisjonen punkt 16.5.1 og som følger av Stortingets vedtak. Post og teletilsynets økte kostnader vil dekkes gjennom kostnadsriktig justering av gebyrer til tilbyderne

8.2. For statlige enheter som har lovbestemt tilgang til lagringspliktige data

Selve forskriften antas å medføre netto redusert økonomiske og administrative kostnader for disse i forhold til det som det ble redegjort for i proposisjonen og som følger av Stortingets vedtak. Antatte merkostnader knyttet til uthenting av lagringspliktig data knyttet til bestemt person og/eller telefonnummer m m anses mindre enn de besparelser som ligger i forslaget om forenklet tilgang til områdesøk (basestasjonssøk).

Av forslaget fremgår det at personell som skal ha tilgang til lagringspliktige data skal fremlegge politiattest. De økonomiske og administrative kostnadene for politiet med å utferdige slike attester til aktuelle personer anses som nominelle.

8.3. For de lagringspliktige

Forskriftens krav om daglig sikkerhetskopiering av de lagringspliktige data er en naturlig og nødvendig følge av lagringsplikten. Kravet anses som nødvendig for å sikre at lagringspliktige data ikke går til spille som følge av datahavari. Kostnaden knyttet til oppfyllelsen av dette kravet er av betydning. Krav om sikkerhetskopiering anses å ligge implisitt i Stortingets vedtak.

Forslagets krav til responstid for de lagringspliktige vil også medføre mer enn ubetydelige kostnader for de lagringspliktige, da det vil bli behov for å ha dedikert personell tilgjengelig, også i påskeferie og julehelg. Kostnadene er nødvendige for å etablere tilstrekkelig effektivitet i etterforsking av straffbare forhold. Disse kostnadene vil imidlertid kunne reduseres gjennom etablering av felles lagringsløsninger mellom flere lagringspliktige, og det må legges til grunn at de lagringspliktige finner frem til de for seg mest økonomiske løsningene.

Utkastets krav til logging av all behandling av lagringspliktige data hos den lagringspliktige vil medføre etablerings- og driftskostnader. Disse anses samlet over systemenes levetid for å være marginale.

Når det gjelder autorisasjonsordningen antar PT at ekstrakostnadene med denne for det vesentligste vil knytte seg til tidsbruk hos den lagringspliktige for å gjennomføre autorisasjonssamtaler, samt overholde dokumentasjonskravene. PT anser imidlertid disse kostnadene som kun noe mer enn marginale.

Utkast til forskrift om lagringsplikt for bestemte data og om tilrettelegging av disse data (datalagringsforskriften)

Fastsatt av Post- og teletilsynet den [dd. måned år] med hjemmel i lov om elektronisk kommunikasjon av 4. juli 2003 nr. 83 §§ 2-7, 2-7a og 2-8

Kapittel 1 Innledende bestemmelser

§ 1-1 Virkeområde

Forskriften gjelder data som skal lagres for å avdekke, etterforske og straffeforfølge alvorlig kriminalitet.

§ 1-2 Lagringspliktige

Tilbyder av elektronisk kommunikasjonsnett som anvendes til offentlig elektronisk kommunikasjonstjeneste og tilbyder av offentlig elektronisk kommunikasjonstjeneste er lagringspliktig.

Myndigheten kan i særlige tilfeller, ved enkeltvedtak, unnta tilbyder helt eller delvis fra lagringsplikt. Myndigheten kan i særlige tilfeller, ved enkeltvedtak, pålegge lagringsplikt for annen virksomhet enn de som omfattes av første ledd.

§ 1-3 Definisjoner

I denne forskrift menes med

1. lagringspliktig telefontjeneste: elektronisk kommunikasjonstjeneste som oppretter og mottar innenlandske eller innenlandske og internasjonale toveis taleforbindelser direkte eller indirekte ved hjelp av et eller flere numre i en nasjonal eller internasjonal telefonnummerplan, samt tilleggstjenester og eventuelle meldings- og multimedietjenester.
2. fasttelefontjeneste: lagringspliktig telefontjeneste som originerer eller terminerer i terminal tilknyttet en fast geografisk adresse.
3. mobiltelefontjeneste: lagringspliktig telefontjeneste som originerer eller terminerer i terminal tilknyttet et landmobilt kommunikasjonsnett.
4. internettelefontjeneste: lagringspliktig telefontjeneste som originerer eller terminerer ved bruk av IP-protokoll.
5. internettaksess: tilgang til Internett over kablet eller radiobasert tilkobling.
6. e-post: elektronisk meldingstjeneste som blir tilbudt av en lagringspliktig.
7. basestasjonsøk: Uthenting av lagringspliktige data generert i landmobile offentlige elektroniske kommunikasjonsnett innenfor et angitt område i et bestemt tidsrom.

Kapittel 2 Lagringspliktige data

§ 2-1 Lagringspliktens subjekt og omfang

Lagringspliktige skal lagre de data som fremkommer i dette kapittel som er knyttet til den lagringspliktiges egne abonnenters bruk som genererer lagringspliktige data.

Lagringspliktige data nevnt i § 2-3 første ledd nr. 1 til 3, 5, 6, 9 og 10 og annet ledd skal også lagres hos tilbyder av landmobile offentlige elektroniske kommunikasjonsnett.

Lagringspliktige data nevnt i § 2-5 første ledd nr. 1 og 2 og annet ledd skal også lagres hos tilbyder av landmobile offentlige elektroniske kommunikasjonsnett.

§ 2-2 Fasttelefontjeneste

Lagringspliktige data for fasttelefontjeneste er

1. anroperens telefonnummer (A-nummer),
2. telefonnummer til den som blir anropt (B-nummer),
3. telefonnummer som anropet viderekobles til (C-nummer),
4. abonnentens og den registrerte brukerens navn og adresse for A-, B- og C-nummer på tidspunktet for den aktuelle kommunikasjonen,
5. dato og tidspunkt for start og avslutning av kommunikasjonen, og
6. den telefontjeneste som benyttes.

Mislykkede anrop og tapte anrop skal lagres i den utstrekning den lagringspliktige logger, lagrer og behandler trafikkdata om slike anrop.

§ 2-3 Mobiltelefontjeneste

Lagringspliktige data for mobiltelefontjeneste er

1. anroperens telefonnummer (A-nummer),
2. telefonnummer til den som blir anropt (B-nummer),
3. telefonnummer som anropet viderekobles til (C-nummer),
4. abonnentens og den registrerte brukerens navn og adresse for A-, B- og C-nummer på tidspunktet for den aktuelle kommunikasjonen,
5. dato og tidspunkt for start og avslutning av kommunikasjonen,
6. den telefontjeneste som benyttes,
7. anroperens og den anroptes internasjonale kjennetegn for mobilabonnenter (IMSI),
8. anroperens og den anroptes internasjonale kjennetegn for mobiltelefoniutstyr (IMEI),
9. ved forhåndsbetalte anonyme tjenester: dato og klokkeslett for første aktivering av tjenesten samt den lokaliseringskoden (celleidentiteten) som tjenesten ble aktivert fra, og
10. lokaliseringskoden (celleidentiteten) ved kommunikasjonens begynnelse og slutt og opplysninger som identifiserer cellens geografiske lokalisering på de tidspunkt dataene blir lagret.

Mislykkede anrop og tapte anrop skal lagres i den utstrekning den lagringspliktige logger, lagrer og behandler trafikkdata om slike anrop.

§ 2-4 Internettelefontjeneste

Lagringspliktige data for internettelefontjeneste er

1. anroperens telefonnummer (A-nummer) eller tildelt brukeridentitet,
2. telefonnummer til den som blir anropt (B-nummer) eller tildelt brukeridentitet til den som blir anropt,
3. abonnentens eller den registrerte brukerens navn og adresse for A- og B-nummer eller tilsvarende ved tildeling av brukeridentitet på tidspunktet for den aktuelle kommunikasjonen,
4. dato og tidspunkt for start og avslutning av kommunikasjonen, og
5. den tjeneste som benyttes.

Mislykkede anrop og tapte anrop skal lagres i den utstrekning den lagringspliktige logger, lagrer og behandler trafikkdata om slike anrop.

§ 2-5 Internettaksess

Lagringspliktige data for internettaksess er

1. abonnentens og den registrerte brukerens bruker-ID eller tilsvarende identifikasjon,
2. tildelt IP-adresse for kommunikasjonen,
3. abonnenten eller den registrerte brukerens navn og adresse på tidspunktet for den aktuelle kommunikasjonen,
4. dato og klokkeslett for på- og avlogging hos Internett-tjenesten, basert på en bestemt tidssone, sammen med den IP-adressen som tilbyderen av Internett-tilgangstjenesten har tildelt kommunikasjonen, og abonnentens eller den registrerte brukerens brukeridentifikasjon,
5. telefonnummer ved oppringt tilgang, og
6. den digitale abonnentlinjen (DSL) eller et annet sluttpunkt for kommunikasjonens avsender.

Lokaliseringskoden (celleidentiteten) ved kommunikasjonens begynnelse og opplysninger som identifiserer cellens geografiske lokalisering på det tidspunkt dataene blir lagret, skal også lages dersom mobilt kommunikasjonsutstyr benyttes for internettaksess.

§ 2-6 E-post

Lagringspliktige data for e-post er

1. avsender og mottakers e-postadresse samt bruker ID eller annen tilsvarende identifikasjon dersom dette er noe annet enn e-postadressen,
2. abonnenten eller den registrerte brukerens navn og adresse på tidspunktet for den aktuelle kommunikasjonen. Slik informasjon skal lagres for både avsender og mottaker, og
3. dato og klokkeslett for på- og avlogging av e-posttjenesten.

§ 2-7 Tidsformat

Det skal angis hvilken tidssone lagrede klokkeslett er angitt i.

Kapittel 3 Krav til lagringen m.m.

§ 3-1 Beviskvalitet

Lagringspliktige skal sikre at beviskvaliteten til de data som lagres ikke forringes gjennom innsamlingen, klargjøringen, lagringen og tilgjengeliggjøringen.

§ 3-2 Sporbarhet

Enhver behandling av lagringspliktige data skal dokumenteres i egen logg. Av loggen skal det fremgå

1. hva som er gjort i et dataanlegg/informasjonssystem,
2. tidspunkt for behandlingen,
3. entydig identifisering av hvem som har behandlet dataene,
4. entydig identifisering av hvem dataene er utlevert til, og
5. entydig identifisering av pålegg om utlevering.

Tilføring eller sletting av lagringsplikte data med hjemmel i ekomloven § 2-7a første ledd eller § 2-7 annet ledd skal ikke loggføres.

Loggen skal oppbevares i tre år.

§ 3-3 Taushetsplikt

Lagringspliktige skal sikre at uvedkommende ikke får tilgang til lagringspliktige data.

Den som behandler lagringspliktige data på vegne av lagringspliktig skal bevare taushet om de lagringspliktige data overfor uvedkommende. Taushetsplikten gjelder også etter fratredelse av stilling.

Som uvedkommende regnes enhver som ikke er autorisert for tilgang til lagringspliktige data etter § 3-4, den opplysningene gjelder eller andre som har lovbestemt tilgang til lagringspliktige data.

§ 3-4 Autorisasjon

Personer som har tjenestelig behov for tilgang til lagringspliktige data som er klargjort etter § 4-2, skal være forhåndsautorisert av den lagringspliktige virksomheten. Autorisasjonen kan bare omfatte behandling som nevnt i § 4-1.

Autorisasjon kan bare gis til personer som den lagringspliktige virksomhet vurderer som skikket til oppgaven.

Den lagringspliktige skal kreve at den som skal autoriseres fremviser politiattest og undertegner en erklæring om taushetsplikt etter § 3-3 under autorisasjonssamtalen.

Autorisasjonssamtale skal gjennomføres før vedkommende gis tilgang til lagringspliktige data. Lagringspliktige skal gjennomføre autorisasjonssamtaler med de autoriserte minst en gang i året.

Når grunnlaget for en autorisasjon bortfaller, skal den som har vært autorisert, gjennom en samtale, gjøres kjent med dette og underrettes om at taushetsplikten etter § 3-3 fortsatt gjelder. Fjerde ledd siste punktum gjelder tilsvarende.

Lagringspliktige skal føre protokoll over autoriserte personer. Protokollen skal inneholde

1. navn på autorisert person,
2. tidspunktet for autoriseringen,
3. tidspunktet for siste autorisasjonssamtale, og
4. tidspunktet for bortfall av autorisasjonen.

Protokollen skal vise komplett oversikt for de siste 4 år.

§ 3-5 Sikkerhetskopiering

Lagringspliktige skal minst daglig ta sikkerhetskopier av de lagringspliktige data. Sikkerhetskopiene skal oppbevares og slettes på tilsvarende måte som lagringspliktige data.

§ 3-6 Sletting

Lagringspliktige data skal slettes når dataene er 6 måneder gamle, jf. ekomloven § 2-7. Ved bedømmelsen av alderen på dataene skal det tas utgangspunkt i tidspunktet for kommunikasjonens slutt.

Sletting av lagringspliktige data skal foretas minst en gang per døgn.

Sletteplikten står tilbake for sikringspålegg med hjemmel i straffeprosessloven § 215a.

Kapittel 4 Behandling og tilrettelegging av lagringspliktige data m.m.

§ 4-1 *Behandling av lagringspliktige data*

Behandling av lagringspliktige data kan bare finne sted

a) for utlevering til den opplysningene gjelder, jf personopplysningsloven § 18 annet ledd,
b) for tilgjengeliggjøring for politi og påtalemyndigheten eller Finanstilsynet etter samtykke, jf. personopplysningsloven § 2 nr. 7 fra den opplysningene gjelder, jf personopplysningsloven § 18 annet ledd,
c) for tilgjengeliggjøring av informasjon i medhold av ekomloven § 2-9 tredje ledd,
d) for oppfylling av pålegg i medhold av straffeprosessloven §§ 210b, 210c, 222d, politiloven § 17d eller verdipapirhandelloven § 15-3 annet ledd nr. 3,
e) for tilgjengeliggjøring av informasjon i medhold av straffeprosessloven § 216b annet ledd bokstav d, eller
f) for nødvendig teknisk vedlikehold av databasen.

Eier av landmobilt offentlig kommunikasjonsnett kan bare foreta behandling av lagringspliktig data om andre enn egne abonnenter som følge av utleveringspålegg for basestasjonssøk i medhold av straffeprosessloven §§ 210c, 222d eller politiloven § 17d.

§ 4-2 *Frist for klargjøring av lagringspliktige data*

Lagringspliktige data skal klargjøres for lagring uten ugrunnet opphold, og ikke senere enn ett døgn etter at dataene ble generert i den lagringspliktige eller tilgangsleverandørens nett.

Lagringspliktige data som innsamles fra andre enn de som er nevnt i første ledd skal klargjøres for lagring uten ugrunnet opphold, og ikke senere enn ett døgn etter at dataene ble mottatt.

§ 4-3 *Tilrettelegging*

Lagringspliktige data skal tilgjengeliggjøres for uthenting etter § 4-1 første ledd bokstavene b til e og annet ledd uten ugrunnet opphold, og ikke senere enn to virkedager eller maksimalt tre dager etter pålegget er kommet frem til den lagringspliktige. Dataene skal tilrettelegges i et elektronisk lesbart format som enkelt kan behandles hos mottaker.

Tilretteleggingsplikten etter første ledd omfatter ikke overføringen av lagringspliktige data til mottaker.

Lagringspliktig skal etablere et kontaktpunkt som politi og påtalemyndighet kan kontakte ved uthenting av lagringspliktige data.

Kapittel 5 Tilsyn, klage og sanksjoner

§ 5-1 Tilsyn

Post- og teletilsynet fører tilsyn med de bestemmelser som er angitt i denne forskriften, jf. ekomloven § 10-1.

§5-2 Klage

Klageinstans på enkeltvedtak fattet av Post- og teletilsynet i medhold av denne forskriften er Samferdselsdepartementet, jf. ekomloven § 11-6.

§ 5-3 Sanksjoner

Brudd på bestemmelser i denne forskriften kan medføre tvangsmulkt, jf ekomloven § 10-7, overtredelsesbot, jf. ekomloven § 10-13 første ledd nr. 2 eller straff jf. ekomloven § 12-4 første ledd nr. 2.

Kapittel 6 Ikrafttredelse og overgangsbestemmelser

§ 6-1 Ikrafttredelse

Forskriften trer i kraft 1.juli 2012.

§ 6-2 Overgangsbestemmelse

[Behovet er fortsatt under vurdering.]

[i] Siste avsnitt under punkt 3.3.2. lød før rettelsen den 8.2.2012 slik:
”Kripos har overfor PT uttrykt behov for at det lagres data for innholdstjenester. Eksempler på slike tjenester kan være ”chat”, søkemotorer og nettsamfunn. Slike tjenester er ikke lagringspliktige etter direktivet, proposisjonen eller innstillingen. Videre vil en lagringsplikt for slike tjenester være svært problematisk da man vil komme i konflikt med forbudet mot å lagre innhold. Selv om det ut fra formålet med regelverket kan være gode argumenter for å lagre data fra slike tjenester, er det PTs oppfatning at det på nåværende tidspunkt ikke er aktuelt å utvide kretsen av lagringspliktige subjekter til å omfatte leverandører av innholdstjenester.”