HØRINGSNOTAT

Endring av forskrift om behandling av personopplysninger (personopplysningsforskriften)

A. Data som faller inn under lagringsplikten i datalagringsdirektivet

1. Innledning

Den 4. april 2011 vedtok Stortinget at direktiv 2006/24 EF (datalagringsdirektivet) skulle implementeres i norsk rett. Vedtaket innebærer at tilbyder av offentlig kommunikasjonsnett og -tjeneste blir pliktig til å lagre såkalte trafikkdata i 6 måneder. Av beslutningen fremgikk videre flere krav til gjennomføringen av implementeringen, bl.a. særlige krav til kryptering av lagringspliktige data, samt konsesjonsplikt for behandling av personopplysninger i ekomsektoren.

I forbindelse med oppfølgingen av gjennomføringsbeslutningen foreslår Fornyings-, administrasjons- og kirkedepartementet en endring av personopplysningsforskriften § 7-1, jf. personopplysningsloven §§ 13, 14, 31 og 35 nytt annet ledd (ikke iverksatt). Endringen innebærer konsesjonsplikt etter personopplysningsloven for behandling av personopplysninger for kommunikasjons- og faktureringsformål i ekomsektoren. Den gir videre Datatilsynet en plikt til, ved konsesjonstildeling, å vurdere og eventuelt pålegge kryptering av data som faller inn under lagringsplikten i ny § 2-7a i lov om elektronisk kommunikasjon (lagringspliktige data). Videre angis at Datatilsynet i pålegget skal fastsette nærmere vilkår for krypteringen, herunder om omfanget. Forslaget stiller også krav til nødvendig sikring (lukket lagring).

2. Bakgrunn

Beslutningen om implementeringen av datalagringsdirektivet har sitt grunnlag i Prop. 49 L (2010-2011) om Endringer i ekomloven og straffeprosessloven mv. (gjennomføring av EUs datalagringsdirektiv i norsk rett) og Innstilling 275 L (2010-2011) om gjennomføring av EUs datalagringsdirektiv i norsk rett. I Innstilling 275 L gjengir komiteens flertall en felles avtale mellom Arbeiderpartiet og Høyre (heretter benevnt "avtalen"). Stortinget har i anmodningsvedtak besluttet at denne avtalen skal legges til grunn for regjeringens arbeid med implementeringen av direktivet.

Fornyings-, administrasjons- og kirkedepartementet er bedt om å følge opp avtalen i innstillingen punkt 5 a) om endring av personopplysningsforskriften § 7-1 og punkt 5 c) vedrørende kryptering og lukket lagring. Bestemmelsene som gis i avtalen vedrørende disse punktene danner grunnlag og angir norm for den forskriftsendring Fornyings-, administrasjons- og kirkedepartementet foreslår i dette høringsnotatet.

Parallelt med denne høringen utarbeider Post- og teletilsynet en forskrift om lagringsplikt for bestemte data og om tilrettelegging av disse data (datalagringsforskriften). Videre har Datatilsynet utarbeidet utkast til konsesjon, med bakgrunn i føringene i Innstilling 275 L.

3. Endringsforslag og vurderinger

3.1. Konsesjonsplikt

I avtalen fastslås det at all behandling av personopplysninger for kommunikasjons- og faktureringsformål, samt for å oppfylle lagringsplikten iht. datalagringsdirektivet, skal være konsesjonspliktig. Dette medfører at det samlede antall virksomheter som omfattes av personopplysningslovens konsesjonsplikt, vil øke i forhold til dagens regel. Årsaken er at de gjeldende konsesjonene i sektoren, utstedt med hjemmel i personopplysningsforskriften § 7-1, har vært avgrenset til fast- og mobiltelefontilbydere. I det nye regelverket vil også tilbydere av internettilgang, IP-telefoni og visse former for e-post kunne omfattes. Det vises til Post- og teletilsynets høringsutkast til datalagringsforskriften for en ytterligere redegjørelse.

I avtalen i innstillingen pkt. 5 a) angis endring av § 7-1. I avtalen fastsettes at ny § 7-1 skal lyde:

"§ 7-1 Konsesjonsplikt for behandling av personopplysninger i ekomsektoren

Behandling av personopplysninger for kommunikasjons- og faktureringsformål, samt for å oppfylle plikten til å lagre data i medhold av lov 4. juli 2003 nr. 83 om elektronisk kommunikasjon (ekomloven) § 2-7 a første ledd hos tilbydere av elektronisk kommunikasjonsnett som anvendes til offentlig elektronisk kommunikasjonstjeneste og tilbydere av slik tjeneste, er konsesjonspliktig etter personopplysningsloven."

Fordi avtalen i innstillingen angir hvorledes bestemmelsen skal lyde, og dette må anses som en instruks fra Stortinget, anses høring av denne endringen som åpenbart unødvendig, jf. Utredningsinstruksen pkt. 5.4. Endringen tas likevel med av informasjonshensyn og for å få en god sammenheng med de andre foreslåtte endringene. Fornyings-, administrasjons- og kirkedepartementet legger videre til grunn at også de som blir pålagt å lagre data i medhold av § 2-7 a andre ledd siste punktum, er ment å skulle omfattes av konsesjonsplikten. Dette må anses i tråd med intensjonen i avtalen. Bestemmelsen endres derfor i samsvar med dette ved at henvisningen til "første ledd" tas ut.

3.2. Kryptering

I forbindelse med Stortingets behandling av Innst. 275 L (2010-2011) ble det besluttet et nytt annet ledd i personopplysningsloven § 35. Det følger av den nye bestemmelsen at det skal vurderes om data som skal lagres med hjemmel i ekomloven § 2-7 a, skal krypteres. Det følger av Stortingets anmodningsvedtak at det er Datatilsynet som skal gis myndighet til å gi pålegg om kryptering av lagringspliktige data. Avtalen sier om dette:

"Partene er enige om at kryptering er et godt tiltak for å sikre dataenes konfidensialitet. Partene er enige om at Datatilsynet gis myndighet til å gi pålegg til tilbydere om å foreta kryptering av data som faller under lagringsplikten etter (ny) ekomlov § 2-7 a. Omfanget av krypteringen, herunder knyttet både til lagring og forsendelse, fastsettes nærmere av Datatilsynet i det enkelte pålegg. Det skal utarbeides forskriftsbestemmelser for kryptering, som skal tilfredsstille etablerte internasjonale standarder."

Fornyings-, administrasjons- og kirkedepartementet foreslår at dette fastsettes i person-opplysningsforskriften § 7-1 andre ledd slik at Datatilsynet ved tildeling av konsesjon også skal vurdere om kryptering bør pålegges. Departementet mener at denne plasseringen på en god måte synliggjør forholdet til lagringspliktige data i henhold til datalagringsdirektivet. Forskriften er teknologinøytral og gir Datatilsynet mulighet til å endre pålegg i takt med teknologisk utvikling og andre faktorer som ev. får konsekvenser for egnet kryptering av data.

Innstillingen gir ingen direkte veiledning om hva som skal vektlegges i vurderingen av om kryptering skal pålegges. Fornyings-, administrasjons- og kirkedepartementet mener imidlertid at det fremgår av sammenhengen at sikring av personvernet var en forutsetning for vedtaket om implementering av datalagringsdirektivet. Departementet viser til at avtalen har et eget punkt (punkt 12) om "*Styrking av det generelle personvernet"*. Videre er personvern trukket frem i avtalens innledning hvor det bl.a. står:

"*Regelverket partene har blitt enige om vil styrke personvernet på dette og andre områder."*

Og videre står det:

"For å ivareta personvernet innføres det strenge regler for uthenting, oppbevaring og sletting av data."

Datatilsynet må med utgangpunkt i dette vurdere om kryptering er nødvendig for å ivareta personvernet jf. personopplysningsloven § 35. Proporsjonalitetsbetraktninger må også inngå i vurderingen, og Datatilsynet må se på tiltakets effekt i forhold til ivaretakelse av personverninteressene. Yttergrensene for hvor tyngende vilkår som kan settes, vil følge av alminnelige forvaltningsrettslige regler sammenholdt med personopplysningslovens formål.

Dette innebærer at Datatilsynet i sin vurdering blant annet må vurdere ivaretakelse av datakvalitet, opplysningenes sensitivitet og aktuelle sikringstiltak som kan iverksettes. Andre viktige hensyn vil være personvernkonsekvenser dersom opplysninger kommer på avveie og risiko for misbruk, og konsekvensen for den enkeltes personvern som helhet. Det må for eksempel kunne fastsettes strengere vilkår for lagringspliktige som lagrer store mengder opplysninger enn for andre.

Kostnader ved krypteringen og andre ulemper som pålegget kan medføre for ekomtilbydere, må også inngå i den samlede vurderingen. Datatilsynet må se hen til alle relevante momenter og foreta en avveining mellom disse, sett i forhold til personvernet. Vurderingene vil kunne falle ulikt ut for forskjellige lagringspliktige tilbydere og for forskjellige lagringspliktige data. Dersom personvernet kan ivaretas tilfredsstillende ved flere forskjellige alternative krypteringsmåter, skal Datatilsynet pålegge det minst kostbare tiltaket for den lagringspliktige og staten.

Dersom Datatilsynet kommer til at kryptering skal pålegges, skal det fastsettes nærmere omfang av krypteringen i konsesjonen. Departementet foreslår at også dette reguleres i § 7-1 andre ledd. I avtalen i innstillingen nevnes om omfanget av krypteringen: "*herunder knyttet både til lagring og forsendelse*" av data. Fornyings-, administrasjons- og kirkedepartementet foreslår at dette presiseres nærmere i § 7-1 andre ledd som "*herunder vilkår knyttet til lagringsmåte, -tidspunkt og lokalisering, samt krav til sikker overføring"*. Opplistingen er imidlertid kun en pekepinn med hensyn til hva som regnes som "*omfang*" og er ikke ment å være uttømmende.

Vilkår knyttet til "lagring" kan inneholde krav både til lagringstidspunkt, lagringsmåte og lokalisering av dataene. Vilkår knyttet til lokalisering vil normalt innebære konkrete bestemmelser om hvilket punkt som skal danne utgangspunkt for sikring av lagringsstedet (f.eks. i et nærmere angitt samlingspunkt), og ikke være knyttet til geografisk plassering. Gjeldende regelverk er ikke til hinder for at lagringspliktige data lagres utenfor landets

grenser, såfremt angitte konsesjonsvilkår oppfylles og Datatilsynet gis mulighet til å føre tilsyn med dette. Oppfyllelse av konsesjonsvilkår vil imidlertid indirekte kunne sette krav til geografisk plassering ved at oppfyllelse og tilsyn ikke er tilstrekkelig sikret på et gitt sted. Vilkår knyttet til lagringstidspunkt vil normalt være frister for når kryptering av dataene senest skal skje. Det må her ses hen til tekniske muligheter og kostnader ved disse, sammenholdt med behovet for kryptering. Generelt legges til grunn at krypteringsbehovet øker i takt med mengden data, slik at behovet er mindre i de enkelte basestasjoner sammenholdt med en samlet database. Vilkår knyttet til lagringsmåte vil omfatte alt fra krypteringsstyrke, tekniske krav, kvalitetskrav og nærmere krav til sikkerhetskopiering og tilgang.

På samme måte som ved vurderingen av *om* kryptering skal pålegges, må tilsynet ved vurderingen av de enkelte krypteringsvilkår, også se hen til vanlige proporsjonalitets- og nødvendighetsbetraktninger. Det må videre sikres at vilkårene for krypteringen er kompatible med andre rettigheter, slik som retten til innsyn i egne opplysninger, retten til å kreve retting og retten til å bli informert. Krypteringspålegg må også være egnet til å ivareta dataenes beviskvalitet (integritet), og ikke være til unødvendig hinder for tilgjengelighet for politiet.

Datatilsynets pålegg om kryptering skal tilfredsstille etablerte internasjonale standarder der slike foreligger. Der etablerte standarder ikke finnes, må en søke å finne en løsning som i størst mulig grad ivaretar de samme hensyn til sikkerhet. Mangel på etablert standard kan ikke i seg selv medføre en lempning av krypteringskravet, hvis Datatilsynet vurderer at kryptering er nødvendig.

Departementet legger til grunn at Datatilsynet vil ha dialog med og konsultere Nasjonal sikkerhetsmyndighet (NSM). Det vises til at NSM representerer et allerede veletablert kryptomiljø nasjonalt.

Datatilsynets vedtak om krav i konsesjon til å behandle personopplysninger vil kunne påklages til Personvernnemnda på vanlig måte, jf. personopplysningsloven § 42 siste ledd og personopplysningsforskriften § 10-1.

3.3. Lukket lagring

Det følger av avtalen at lagrede data skal undergis nødvendig sikring, såkalt "lukket lagring". Departementet legger til grunn at det med "lukket lagring" skal forstås tiltak som iverksettes for å sikre at informasjon ikke er tilgjengelig uten autorisasjon. Begrepet er ikke vanlig brukt og er heller ikke nærmere definert i avtalen, foruten at avtalen angir nærmere konkrete krav som må tilfredsstilles for at kravet til lukket lagring skal oppnås. Det antas at disse kravene er minimumskrav, og at alle krav må oppfylles. Datatilsynet vil, innenfor disse rammene, kunne vurdere tilpasninger og ytterligere krav i konsesjon dersom dette anses nødvendig for å sikre lukket lagring. Dette vil være særlig aktuelt for å kunne følge den teknologiske utviklingen.

Fornyings-, administrasjons- og kirkedepartementet foreslår at kravene til lukket lagring opplistes i personopplysningsforskriften § 7-1 tredje ledd. Kravene angis som minimumskrav som Datatilsynet skal pålegge i konsesjonen. Videre gis Datatilsynet anledning til å fastsette nærmere krav, dersom tilsynet anser det som nødvendig.

I bokstav a) og b) oppstilles krav til identitetskontroll og behovsbegrenset adgang til de lokaler hvor lagringspliktige data lagres. Departementet antar at den enkelte lagringspliktige selv som hovedregel er godt egnet til å finne en tilfredsstillende metode for identitetskontroll,

slik at det vil være tilstrekkelig å fastsette i konsesjonen at identitetskontroll skal finne sted. Det er en forutsetning at metoden som velges er velegnet for å oppnå formålet om en god sikring av dataene. Dersom det anses nødvendig, vil Datatilsynet, etter en konkret vurdering i det enkelte tilfellet, kunne spesifisere kravene til tilstrekkelig identitetskontroll ytterligere i den enkelte konsesjon.

Vurdering og fastsettelse av hvem som har behov for adgang til de lokaler hvor lagrings-pliktig data oppbevares samt tilgang til dataene, antar departementet likeledes best kan ivaretas av lagringspliktige selv, slik at det vil være tilstrekkelig å fastsette krav om behovsbegrensning i konsesjonen. Det forutsettes at lagringspliktige undergir behovet en grundig vurdering, og at det vurderes jevnlig. På samme måte vil kravet til behov for adgang og tilgang måtte vurderes strengt og individuelt. Det vil ikke være anledning til å fastsette at en nærmere gruppe ansatte har "behov" for adgang eller tilgang, for eksempel at "rengjøringspersonell" har behov for adgang til lokalet. Behovsvurderingen må foretas individuelt for hver enkelt ansatt og/eller andre som skal ha tilgang. Videre innebærer kravet at gruppen med tilgang bør gjøres så liten som mulig sett i lys av behovet. Regulering av krav til den som gis autorisasjon og nærmere bestemmelser om dette, faller utenfor forskriften og kravene til lukket lagring. Det følger imidlertid av avtalen punkt 5 b) at slike krav skal følge av retningslinjer som utarbeides av Datatilsynet og Post- og teletilsynet i fellesskap.

Bokstav c) og d) fastsetter krav til elektronisk og fysisk sikring av lagringsmediet og området rundt, og bokstav e) fastsetter forbud mot tilgangsløsninger som innebærer at data kan hentes ut direkte "on-line". Bestemmelsene omfatter krav til sikring fra det tidspunkt krypteringsplikten inntrer. Fysisk sikring er tiltak som er egnet til å hindre at uvedkommende får adgang til området eller mediet uten at det etterlates spor. Vilkårene henger tett sammen med krav til identitets- og adgangskontroll i bokstav a) og b). Elektronisk sikring vil typisk omfatte krav om brannmur mv.

4. Økonomiske og administrative konsekvenser

Implementering av datalagringsdirektivet medfører økning i Datatilsynets arbeidsoppgaver. Ved at det pålegges en plikt til å vurdere kryptering, og kretsen av konsesjonspliktige øker, vil Datatilsynet få flere konsesjonssøknader til behandling. I tillegg vil implementeringen av datalagringsdirektivet medføre økte veilednings- og tilsynsoppgaver som følge av at Datatilsynet får tilsynskompetansen. Behovet for økte ressurser til å ivareta oppgavene er ivaretatt i budsjettet for 2012, hvor Datatilsynet har fått midler til å ivareta det ekstra tilsynsansvaret som ligger i implementeringen av datalagringsdirektivet. Bevilgningen til Datatilsynet er styrket med 1,5 mill. kroner, jf. Prop. 1 S (2011-2012) Fornyings-, administrasjons- og kirkedepartementet.

Når det gjelder kostnadene ved kryptering, er kostnadsbildet komplisert, og avhenger av flere, uavklarte faktorer. Flere av de faktiske forutsetningene ved implementering av datalagringsdirektivet er ennå ikke tilstrekkelig klargjort. Det er derfor på det nåværende tidspunkt vanskelig å tallfeste hvor store de økte kostnadene som følge av krav til kryptering og lukket lagring blir. Kostnadene vil avhenge av hvilke krav Datatilsynet pålegger i konsesjonen, hvilke krav som vil stilles i datalagringsforskriften (som ennå ikke er fastsatt) og tilbydernes valg av løsninger.

Krav om behandling og tilrettelegging av lagringspliktige data vil kunne medføre betydelige kostnader for virksomhetene. Videre kan autorisasjon av personer bli kostbart. Disse

kostnadene påvirkes av krav som stilles i medhold av datalagringsforskriften, og vil også få følger for krypteringskostnadene. Datalagringsforskriften regulerer i tillegg responstid, som også kan påvirke kostnadene for mindre virksomheter.

Videre vil ekomtilbydernes valg av krypteringsløsning, mulighet for samarbeid om felles løsninger og regler for utlevering av data, få følger for kostnadene. Virksomhetens størrelse, tjenester som tilbys og hvilken intern kompetanse virksomheten har, er også av betydning.

Bransjens valg må videre antas å kunne påvirkes ved valg av kostnadsfordelingsmodell, dvs. modell for fordelingsnøkkel mellom ekomtilbyderne og staten for utgifter knyttet til gjennomføring av datalagringsdirektivet. Valg av kostnadsmodell utredes av Justisdepartementet og Samferdselsdepartementet, og er ennå ikke sluttført.

Alle disse faktorene gjør en utregning av kostnadene ved kryptering og lukket lagring vanskelig og uhensiktsmessig på det nåværende stadiet, da det vil være svært mange variabler. Da forslaget kun omhandler *utformingen* av en krypteringsbestemmelse, og ikke *om* Datatilsynet skal gis myndighet til å pålegge kryptering, antar departementet likevel at kostnadene ved krypteringen i denne sammenheng ikke er avgjørende for høringsforslaget.

B. Kameraovervåking

1. Innledning

Den 16. desember 2011 la Justis- og politidepartementet frem Prop. 47 L om endringer i personopplysningsloven, lov 14. april 2000 nr. 31. Endringsforslaget ble vedtatt 22. mars 2012, og trådte i kraft 20. april 2012. Det ble blant annet vedtatt endringer i personopplysningslovens bestemmelser om kameraovervåking. Disse endringene nødvendiggjør visse tilpasninger i personopplysningsforskriftens, forskrift 15. desember 2000 nr. 1256, kapittel 8 om fjernsynsovervåking.

2. Bakgrunn

Personopplysningsloven kapittel VII regulerer kameraovervåking (tidligere fjernsynsovervåking). I medhold av lovens § 36 er det gitt forskrifter om fjernsynsovervåking i personopplysningsforskriften kapittel 8. Reglene i forskriften supplerer personopplysningslovens bestemmelser om behandling av personopplysninger gjort ved fjernsynsovervåking. Slik personopplysningsloven § 37 lød før endringen 20. april 2012, gjaldt bare enkelte av bestemmelsene i loven for billedopptak gjort ved fjernsynsovervåking. Reglene som kom til anvendelse var bestemmelsene om vilkår og grunnkrav til behandling av opplysninger i §§ 8, 9 og 11, samt bestemmelsene i §§ 31 og 32 om meldeplikt. Sentrale bestemmelser om sikring av personopplysninger, innsynsrett for den registrerte og sletting av opplysninger gjaldt ikke for billedopptakene.

Etter endringen gjelder alle personopplysningslovens regler for behandling av personopplysninger innsamlet gjennom kameraovervåking. Dette følger av ny bestemmelse i personopplysningsloven § 3 første ledd c). Behovet for spesialregulering i forskrift vurderes nå som noe mindre enn tidligere. Bestemmelsen i nåværende § 8-2 om sikring av opptak foreslås derfor opphevet. Av samme grunn foreslås bestemmelsen i nåværende § 8-5 delvis opphevet, og delvis flyttet og justert.

3. Endringsforslag og vurdering

3.1. Begrepsbruk

Kapitteloverskriften i lovens kapittel VII ble endret ved lovendringen som trådte i kraft 20. april 2012. Begrepet *fjernsynsovervåking* ble erstattet med det mer moderne begrepet *kameraovervåking*. Som en følge av dette foreslås kapitteloverskriften i forskriften kapittel 8 endret tilsvarende, slik at begrepsbruk i lov og forskrift er den samme. Tilsvarende foreslås at begrepet *fjernsynsovervåking* i § 8-1 endres til *kameraovervåking*

Ved lovendringen ble også begrepet *billedopptak* endret til *opptak*. Begrepet *billedopptak* foreslås derfor gjennomgående endret til *opptak* i forskriften, slik at det er samsvar med begrepsbruken i personopplysningsloven.

3.2. Sikring av opptak - § 8-2

Nåværende bestemmelse inneholder en henvisning til personopplysningslovens generelle bestemmelse om informasjonssikkerhet i § 13, og forskriftene gitt i medhold av denne bestemmelsen, slik at disse bestemmelsene også gjelder for sikring av billedopptak. Etter lovendringen gjelder personopplysningsloven § 13 med forskrifter uten videre for sikring av billedopptak gjort ved kameraovervåking. Fornyings-, administrasjons- og kirkedepartementet anbefaler derfor at nåværende § 8-2 i personopplysningsforskriften oppheves. Bestemmelsen erstattes ikke med noen ny bestemmelse.

3.3. Innsynsrett - § 8-5

Gjeldende forskriftsbestemmelse om innsynsrett gir i dag lovens generelle regel om innsynsrett for de registrerte, personopplysningsloven § 18, anvendelse på billedopptak, jf. § 8-5 første ledd. Bestemmelsen vurderes som overflødig all den tid personopplysningslovens alminnelige innsyns- og informasjonsregler etter lovendringen gjelder for all behandling av personopplysninger innsamlet ved billedopptak. Personopplysningsforskriften § 8-5 første ledd foreslås derfor opphevet.
§ 8-5 annet ledd er en særbestemmelse om unntak fra innsynrett i opptak som er utlevert til politiet, eller opptak som kan være av betydning for rikets sikkerhet mm. Fornyings-, administrasjons- og kirkedepartementet vurderer det som hensiktsmessig å videreføre spesialbestemmelsen om innsyn i opptak hos politiet. Bestemmelsen foreslås flyttet til gjeldende § 8-3, som for øvrig regulerer politiets bruk av billedopptak. Reglene om innsyn i opptak hos politiet blir etter dette ny § 8-3 annet ledd. Det foreslås nødvendig språklig justering av bestemmelsen i forbindelse med ny plassering. Første ledd i gjeldende § 8-3 forblir uendret.

Ut over de ovenfor foreslåtte endringene, vurderer departementet ikke at det er påkrevet å foreta endringer i personopplysningsforskriften som følge av de nylig ikrafttrådte endringene i personopplysningsloven.

4. Økonomiske og administrative konsekvenser

Endringene i personopplysningsforskriften kapittel 8 vurderes å ikke ha økonomiske eller administrative konsekvenser.

C. Forslag til forskriftstekst

Endringer satt i kursiv.

§ 7-1. *Konsesjonsplikt for behandling av personopplysninger i ekomsektoren*

Behandling av personopplysninger for kommunikasjons- og faktureringsformål, samt for å oppfylle plikten til å lagre data i medhold av lov 4. juli 2003 nr. 83 om elektronisk kommunikasjon (ekomloven) § 2-7 a hos tilbydere av elektronisk kommunikasjonsnett som anvendes til offentlig elektronisk kommunikasjonstjeneste og tilbydere av slik tjeneste, er konsesjonspliktig etter personopplysningsloven.

Ved utferdigelse av konsesjonen skal Datatilsynet vurdere om det skal stilles vilkår om kryptering av de data som faller inn under lagringsplikten etter § 2-7 a. Vilkår om kryptering skal tilfredsstille etablerte internasjonale standarder der slike foreligger. Ved pålegg om kryptering skal Datatilsynet i den enkelte konsesjon fastsette nærmere omfang av krypteringen, herunder vilkår knyttet til lagringsmåte, -tidspunkt og lokalisering, samt krav til sikker overføring.

For tilbydere som er lagringspliktige i henhold til ekomloven § 2-7 a, skal Datatilsynet i konsesjonen pålegge nødvendige vilkår for å sikre lukket lagring. For å sikre lukket lagring skal det blant annet fastsettes nærmere krav om:

a) identitetskontroll ved innpassering til de lokaler hvor data lagres,
b) behovsbegrenset adgang til lokaler hvor lagringspliktige data lagres og tilgang til lagringspliktige data,
c) fysisk sikring av lagringsmediet og omgivelsene rundt,
d) elektronisk sikring av lagringsmediet (brannmur mv.),
e) begrensninger i adgangen til eksternt å koble seg til lagringsmediet, slik at data ikke kan hentes ut direkte, og
f) *kryptering ved forsendelse av data over landegrensene, i henhold til retningslinjer om krypteringsgrad fra Nasjonal sikkerhetsmyndighet.*

Overskriften til kapittel 8 skal lyde:
Kapittel 8. *Kameraovervåking*

§ 8-1. *Virkeområde*

Kapittelet her gjelder for *kameraovervåking*, jf. personopplysningsloven § 36.

§ 8-2. Oppheves

§ 8-3. Politiets bruk av *opptak*

Personopplysningsloven § 11 første ledd bokstav c er ikke til hinder for at politiet bruker *opptak* det er i besittelse av, i forbindelse med forebygging av straffbare handlinger, i forbindelse med oppklaring av ulykker eller i saker om ettersøking av forsvunne personer.

Innsynsrett etter personopplysningsloven kan ikke gjøres gjeldende i opptak som politiet er i besittelse av, eller opptak som kan være av betydning for rikets eller dets alliertes sikkerhet, andre vitale nasjonale sikkerhetsinteresser og forholdet til fremmede makter.

§ 8-4. Sletting av *opptak*

Opptak skal slettes når det ikke lenger er saklig grunn for oppbevaring, jf. personopplysningsloven § 28.

Opptak skal senest slettes 7 dager etter at opptakene er gjort. Sletteplikten etter forrige punktum gjelder likevel ikke dersom det er sannsynlig at *opptaket* vil bli utlevert til politiet i forbindelse med etterforskning av straffbare handlinger eller ulykker. I slike tilfeller kan *opptakene* oppbevares inntil 30 dager.

Opptak gjort i post- og banklokaler skal slettes senest tre måneder etter at opptakene er gjort.

Sletteplikten etter andre og tredje ledd gjelder ikke

a) for *opptak* som politiet er i besittelse av,

b) for *opptak* som kan være av betydning for rikets eller dets alliertes sikkerhet, forholdet til fremmede makter og andre vitale nasjonale sikkerhetsinteresser, eller

c) hvor den som er avbildet samtykker i at *opptakene* oppbevares lenger.

Dersom sletteplikten etter første ledd oppstår for *opptak* som er utlevert til politiet fra andre, kan politiet tilbakelevere opptaket til vedkommende, som snarest skal slette det dersom fristen etter andre og tredje ledd er gått ut.

Dersom det foreligger et særlig behov for oppbevaring i lengre tid enn fastsatt i andre og tredje ledd, kan Datatilsynet gjøre unntak fra disse bestemmelsene.

§ 8-5. Oppheves