

Samferdselsdepartementet  
Postboks 8010 Dep  
0030 OSLO

Dato: 12.04.2010  
Vår ref.: 10-24 BKA/TAH  
Deres ref.: 09/585 - HK

## **Høring - norsk gjennomføring av EUs datalagringsdirektiv (2006/24/EF)**

### **1. Innledning**

Finansnæringens Fellesorganisasjon (FNO) – som har overtatt de oppgaver som tidligere ble ivaretatt av FNH og Sparebankforeningen – viser til Samferdselsdepartementets høringsbrev 8. januar 2010 om eventuell norsk gjennomføring av EUs datalagringsdirektiv (2006/24/EF). Fristen for gjennomføring av direktivet for EUs medlemsland var 15. september 2007.

Samferdselsdepartementet skriver i høringsbrevet at det ikke er enighet i regjeringen om datalagringsdirektivet skal innlemmes i EØS-avtalen og at dette spørsmålet først vil bli avgjort etter at høringsrunden er gjennomført 12. april. Som grunnlag for høringen har Samferdselsdepartementet utarbeidet et høringsnotat i samarbeid med andre berørte departementer som Justisdepartementet og Fornyings-, administrasjons- og kirkedepartementet.

For det tilfellet at datalagringsdirektivet innlemmes i EØS-avtalen og således gjennomføres i norsk rett, er det i høringsnotatets kapitler 8 til 10 inntatt forslag til endringer i lov om elektronisk kommunikasjon (ekomloven), ekomforskriften og straffeprosessloven.

Datalagringsdirektivet innebærer en plikt for tilbydere av offentlig elektronisk kommunikasjonstjeneste eller telekommunikasjonsnett å lagre trafikkdata, lokaliseringsdata og andre data som identifiserer bruken av slike tjenester. Det omfatter blant annet data som er nødvendige for å spore og identifisere avsender og mottaker (kilden og bestemmelsesstedet), tidspunkt og kommunikasjonens varighet og kommunikasjonstype, ved anvendelse av fasttelefon, mobiltelefoni, bredbåndtelefoni, internettaksess og e-post. Direktivet omfatter ikke opplysninger og annet innhold i den elektroniske kommunikasjonen.

Finansnæringens Fellesorganisasjon (FNO) tilrår at:

- Datalagringsdirektivet innlemmes i EØS-avtalen og gjennomføres i norsk rett.
- Myndighetene fastsetter behandlingsregler og andre tiltak i det norske regelverket som sikrer at enkeltindividenes krav på personlig integritet og kommunikasjonsfrihet blir ivaretatt på en god måte.
- Det fastsettes:
  - en maksimal lagringstid for trafikkdata og andre lagringspliktige data på 12 måneder,
  - begrensninger i retten til innsyn og utlevering av trafikkdata mv,
  - strenge krav til datasikkerhet og internkontroll hos tjenestetilbyderne, og
  - krav om domstolsbeslutning for utlevering av trafikkdata mv til politi og påtalemyndighet.

## 2. Kriminalitetsbekjempelse

Også i dag lagres trafikkdata i Norge, riktignok av kommersielle hensyn. Det er særlig kommunikasjonsformål og mulighetene for å kunne dokumentere korrekt faktureringsgrunnlag som begrunner lagringen hos den enkelte tjenestetilbyder. Politiet har, med visse begrensninger som følge av tilbydernes lovbestemte taushetsplikt, mulighet til å få tilgang til disse dataene som lagres i 3 til 5 måneder, for å forebygge eller etterforske straffbare handlinger.

Formålet med datalagringsdirektivet (jf. artikkel 1) er å sikre harmoniserte regler om lagring og anvendelse av trafikkdata mv i forbindelse med etterforskning, oppklaring og rettsforfølgelse av grov kriminalitet slik dette er definert i nasjonal lovgivning. Som nærmere redegjort for i høringsnotatet pkt. 4.3, er utvikling og utbredelse av ny teknologi med på å endre rammebetingelsene for samhandling og kommunikasjon mellom mennesker nasjonalt og internasjonalt. Utbredelse av internett, e-post og mobiltelefoner er eksempler på dette.

Banker, forsikringsselskaper og andre finansforetak er storbrukere av IKT, både for levering av kundetjenester og for egen virksomhet. Dette gjør slike foretak svært utsatte for alle typer av datakriminalitet som er økonomisk motivert. Både foretakene og kundene kan rammes sterkt av kriminelle handlinger, som gjerne skjer over internett, for eksempel dokumentfalsk, identitets- og informasjonstyveri, ulovlig inntrengning i nettbanker, manipulering av sikkerhetskoder og nettbaserte betalingskortbedragerier.

Disse utviklingstrekkene representerer store utfordringer for samfunnet. Teknologit utviklingen har gitt nye muligheter til å utføre kriminelle handlinger og til å unndra seg kontroll og straffeforfølgning. Men når lovbrudd dokumenteres og distribueres elektronisk, etterlates det også elektroniske spor. Slik sett representerer

kommunikasjonsteknologien også muligheter for å forebygge, avdekke og etterforske lovbrudd effektivt.

Banker og forsikringselskaper opplever i økende grad at anslagene kommer fra utlandet gjennom nettverk som ikke kjenner geografiske grenser. Dette understreker etter vårt syn at både forebyggende tiltak og etterforskning må ha solid internasjonal forankring. Effektiviteten av tiltakene vil utvilsomt økes dersom lovverket i de enkelte land blir rimelig godt harmonisert.

Fra finansnæringens side vil det ikke være ønskelig at Norge stiller seg på siden av felles europeiske tiltak på dette området.

### **3. Forholdet til EØS-avtalen**

I en betenkning av 2008 fra professorene Arnesen og Sejersted konkluderes det med at det ikke kan gis noe klart juridisk svar på om datalagringsdirektivet må anses EØS-rettslig relevant. Vi noterer oss dette, men vil likevel påpeke at direktivet henger materielt sammen med flere direktiver om datasikkerhet som allerede er innlemmet i EØS-avtalen. Som påpekt av Arnesen og Sejersted (s. 10 flg.) vil konsekvensen av en norsk reservasjon mot direktivet kunne bli at tilsluttede deler av EØS-regelverket (avtalens vedlegg XI) suspenderes eller settes ut av kraft.

FNO ser det svært lite ønskelig om Norge skulle påbegynne en prosess med EU med et slikt utgangspunkt og mulighet for et slikt utfall.

### **4. Lagringstid**

Etter direktivets artikkel 6 skal medlemsstatene sørge for at trafikkdata mv lagres i minst 6 måneder, maksimalt 2 år. Statene har med andre ord valgfrihet når det gjelder fastsetting av lagringstidens lengde.

Både Danmark og Finland har valgt en pliktig lagringstid av trafikkdata mv på 12 måneder fra kommunikasjonstidspunktet. Etter vår mening tilsier rettslikhet innenfor Norden at også Norge fastsetter en lagringstid på 12 måneder.

### **5. Personverntiltak**

Som nevnt i direktivets fortale pkt 15 gjelder personverndirektivet (95/46/EF) og direktiv (2002/58/EF) fullt ut ved lagring av trafikkdata og andre personopplysninger etter datalagringsdirektivet. Datalagringsdirektivet legger klare føringer på nasjonalstaten for å sikre forsvarlig lagring av trafikkdata (artikkel 16) samt pålegg om tiltak for å sikre fortrolighet og behandlingssikkerhet (artikkel 17). Videre skal statene gjennom nasjonal

lovgivningen sørge for at lagrede trafikkdata kun utleveres til kompetente myndigheter i tråd med formålet med direktivet (artikkel 4).

Lagring, utlevering og annen behandling av trafikkdata mv vil medføre negative konsekvenser for personvernet og kommunikasjonsfriheten. Gjennomføres direktivet i norsk rett vil dette kreve tiltak som gir en rimelig balanse mellom hensynet til enkeltindividets krav på personlig integritet og samfunnets behov for forebygging, etterforskning og bekjempelse av alvorlig og organisert kriminalitet.

Etter FNOs mening bør derfor de norske reglene for lagring og behandling av trafikkdata mv utformes slik at de ivaretar hensynet til personvern på en god måte. Direktivet overlater til nasjonale myndigheter å ta nærmere stilling til omfanget av personvernforemmende tiltak, og de norske reglene bør derfor inneholde klare begrensninger i lagringstid (maksimalt 12 måneder), krav til datasikkerhet og internkontroll, begrensninger i utleveringsadgangen samt tydelige vilkår i ekomloven og straffeprosessloven om domstolsprøvelse av politiets og påtalemyndighetens beslag- og utleveringsbegjæringer.

Med vennlig hilsen

**Finansnæringens Fellesorganisasjon**



Arne Hyttnes

administrerende direktør



Tore A. Haugje  
fagdirektør