Samferdselsdepartementet
Postboks 8010 Dep
0030 Oslo

Oslo, 20.01.2010

# Høring - datalagring

# Innledning

IKT-Norge ønsker med dette å redegjøre for bransjens synspunkter knyttet til en evetuell implementering av EUs datalagringsdirektiv. IKT-Norge representerer hovedtyngden av norske teleoperatører og ISP'er. Representanter for alle de store tele- og internettleverandørene har bidratt i utformingen av dette høringssvaret.

IKT-Norge mener EUs datalagringsdirektiv ikke bør implementeres i Norge. Som IT-næringens interesseorganisasjon er vi først og fremst bekymret for at direktivet vil bidra til å svekke folks tillit til teknologi. Vi frykter dette vil kunne føre til at bruken av elektronisk kommunikasjon reduseres og dermed også bruken av teknologi reduseres. Dette vil kunne få en rekke utilsiktede negative konsekvenser for det norske samfunn.

Direktivet er svært omstridt internt i EU og land Sverige og Tyskland har ikke innført det. EUs nye kommissær for indre annliggende, Cecilia Malmström, har sagt at hele direktivet må tas opp til fornyet vurdering etter at den pågående evalueringen er konkludert. IKT-Norge mener Norge må avvente resultatene av EUs evaluering av direktivet. Denne evalueringen vil høyst sannsynelig føre til at direktivet blir vesentlig endret. Det vil derfor være uklokt om Norge implementerer direktivet i sin nåværende form.

IKT-Norge mener at det fremlagte høringsnotatet ikke i tilstrekkelig grad belyser relevante problemstillinger og at det ikke er lagt frem noe holdbar dokumentasjon som kan forsvare å implementere direktivet nå.

# Ekomtilbyderens rolle i samfunnet

Ekomtilbyderene er de viktigste tilretteleggerne for en fri og åpen debatt og samfunnsdeltagelse i det digitaliserte samfunnet. En betydelig andel av all kommunikasjon gjøres via en ekomtilbyder. Dermed besitter denne alene både muligheten og forpliktelsen til å ivareta og sikre personvern, informasjonsfrihet osv. Kommunikasjonsstjenestene er altså av stor viktighet for å ivareta og videreutvikle et velfungerende demokrati, noe som også gjenspeiles i "Human rights guidelines for Internet service providers", utviklet i regi av Europarådet, hvor det bla. sies:

> "Access-providers facilitate entry to the Internet and therefore to a diversity of information, culture and languages; they are often the first point of contact and trust for users. Their role is a prerequisite for enabling and empowering users to access the benefits of the information society, in particular to seek and impart information and ideas, to create and to access knowledge and education."[1]

Et resultat av teknologienes egenskaper er at det produseres spor i ekomtilbyderenes nettverk, det er disse sporene eller dataene som vil bli forsøkt registrert dersom direktivet implementeres. Det er nettopp disse dataene som gjør at ekomtilbyderne har et så bevisst forhold til egen rolle og hvilken garantier, friheter og rettigheter ekomtilbyderne forvalter på vegne av samfunnet og hvert enkelt individ. Det er sentralt at dataene som oppstår som biprodukter av tjenesteproduksjon ikke misbrukes og settes inn i ny kontekst slik det ønskes med datalagringsdirektivet. En illustrasjon på dette kan være de dataene som genereres i forbindelse med bruk av mobile enheter som for eksempel mobiltelefoner eller ebøker som Kindle. I studien "Limits of Predictability in Human Mobility"[2] utført ved Center for Complex Network Research ved Northeastern University i Boston kommer det frem at "the most detailed information on human mobility across a large segment of the population is collected by mobile phone carriers". Det er opplagt hvilket betydelig ansvar mobiloperatørene forvalter for ivareta brukere av mobiltjenester og at fremtidige bruksmønstere utvikles uten misbruk av dataene med potensielt store negative konsekvenser. Studien viser at med tilstrekkelig tilgang på data om mobilbrukere er det forholdsvis enkelt mulig med lett tilgjengelige matematiske modeller å fastslå med 93% til 97% sikkerhet hvor et enkelt individ vil befinne seg en hvilken som helst dag i nær fremtid.

I forlengelsens av datalagringsdirektivet og andre initiativ, blant annet i forbindelse med ulovlig fildeling, er det økt bevissthet og fokus på behovet for å sikre tilliten til internett og at ekomtilbyderne ikke tvinges til å utfordre denne tillitten gjennom feks. lovgivning. Forpliktelsene som hviler på enkelte lands myndigheter for å sikre dette kommer klart til uttrykk i Lambridinis rapport "on strengthening security and fundamental freedoms on the Internet":

> "Member States to ensure that freedom of expression is not subject to arbitrary restrictions from the public and/or private sphere and to avoid all legislative or administrative measures that could have a "chilling effect" on all aspects of freedom of speech;"[3]

En undersøkelse av Forsa Institute i Tyskland[4] viser at 11% sier de allerede har latt være å bruke telefon til noen typer samtaler, og 52 % mener at de antagelig ikke kommer til å bruke telekommunikasjon for å komme i kontakt med for eksempel narkotikarådgiver, psykoterapeut eller ekteskapsrådgiver. Denne nevnte ”chilling effect” kan være en trussel mot demokratiet, og er en av de faktorene både "Lambrinidis

---

*1.* Human rights guidelines for Internet service providers Developed by the Council of Europe in co-operation with the European Internet Services Providers Association (EuroISPA); http://www.coe.int/t/dghl/standardsetting/media/Doc/H-Inf(2008)009_en.pdf

2. http://www.bibsonomy.org/bibtex/2a89330f8eb32ce62b5f5c9a2b4909f25/stumme

*3.* Lambridinis rapport "on strengthening security and fundamental freedoms on the Internet" http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+REPORT+A6-2009-0103+0+DOC+XML+V0//EN

4. http://www.vorratsdatenspeicherung.de/images/forsa_2008-06-03.pdf

rapporten" og EMK søker å unngå.

Norske ekomtilbydere ser meget alvorlig på det ansvaret som følger av rollen de har for å sikre viktige byggesteiner i demokratiet som bla. informasjonsfrihet, kommunikasjonsfriet, kildevern etc. Det er med stor bekymring at vi registrerer at det i høringsnotatet legges opp til lovfestede plikter for ekomtilbydere som går på tvers av dette. IKT-Norge er bekymret over hvor lett problemstillinger rundt juridisk kompetanse hos ekomtilbydere er berørt i høringsnotatet. Et betydelig antall av for eksempel internettleverandører i Norge er meget små organisasjoner med få og primært tekniske ansatte, som har teknisk drift og utvikling som spisskompetanse. Slike organisasjoner ikke rigget for en situasjon der noen kutter svinger og øver et betydelig press for tilgang til taushetsbelagt informasjon. Et eksempel er en sak hvor NAV mente de hadde krav på tilgang trafikkdata. NAV presset på og benyttet en fremgangsmåte det er grunn til å frykte ville ført ført frem til utlevering av data fra en aktører med liten eller ingen juridisk spisskompetanse og erfaring på området.

Høringsnotatet klargjør ikke ansvarsforhold på en rekke sentrale områder. Det er mye uavklart knyttet til ekomtilbydere sitt ansvar for data de evt. pålegges å lagre, og ved feks. lekasjer, feil utlevering, mangler på data når de etterspøres, misbruk av data etc. Alle disse forhold må avklares før en beslutning om å implementere direktivet kan fattes.

*IKT-Norge mener ansvaret som vil pålegges ekomtilbydere ved en implemenering av datalagringsdirektivet i norsk lov ikke er forenlig med den rollen og nøytraliteten en ekomtilbydere har i vårt samfunnet.*

# Datalagringsdirektivets effektivitet

Datalagringsdirektivets effektivit er avgjørende for vurderingen om hvorvidt direktivet skal implementeres i norsk lov. IKT-Norge mener det er to konkrete vurderinger som må gjøres i denne sammenhengen.

1. Vil direktivet være et verktøy som gir merverdi i seg selv og utover alternative verktøy for "relevante myndigheter"?
2. Vil direktivet og dets intensjon være mulig å omgå for å unngå registrering?

Når det gjelder alternativer til direktivet kan ikke IKT-Norge se at dette er tilstrekkelig utredet i forbindelse med høringsporessen. IKT-Norge mener at dette i seg selv gir grunnlag for å vurdere å sette prosessen på vent. I tråd med god forvaltningsskikk burde alternativer vært utredet. Både som reelle alternativer til direktivet, men også som nødvendige elementer å vurdere direktivet opp i mot.

Direktivet og det norske høringsnotatet er tilsynelatende basert på en forutsetning om at informasjon direktivet krever registrert alltid vil være tilgjengelig for ekomtilbydere. En

slik forutsetning er ikke riktig. I flere sammenhenger vil ikke ekomtilbyderen kunne vite hva brukeren gjør, hvem brukeren er osv. Dermed fremstår det som opplagt at ekomtilbyderen heller ikke vil kunne lagre de høyst personlige dataene datalagringsdirektivet spesifiserer. Det er et tydelig trekk ved noen av de teknologiene direktivet omhandler at en bruker med enkle metoder vil kunne bruke teknologien slik at andre (inkl. ekomtilbyder) ikke får tilgang til data. Utover de teknologiske mulighetene for å unndra seg registering vil det alltid foreligge betydelige muligheter til å bruke utstyr/ tjenester som er registrert på/koblet til andre enn den som benytter utstyet og dermed skjule brukerens identitet.

Når det gjelder direktivets effektivitet med tanke på muligheter til å omgå direktivet ved å unngå registering av egne trafikkdata er IKT-Norge av den klare oppfattning at direktivet er så enkelt å omgå, både bevisst og ubevisst, at det ikke vil kunne fungere etter intensjonen og dermed fremstår som et betydelig inngrep ovenfor relevante bransjeaktører og kundene som rammes av den omfattende registreringen av data. EuroCop (European Confederation of Police) sier om effektiviteten til direktivet at "a vast effort is made with little more effect on criminals and terrorists than to slightly irritate them" [5] .

Mulighetene for å omgå er så utstrakte at det gir grunn til å frykte at direktivet kun vil fremstå som symbol på handling uten nødvendig real verdi til å forsvare kostnadene, både de økonomiske og ikke-økonomiske. Eurocop har beskrevet en av direktivets klare svakheter slik: "Activities like these are unlikely to boost citizens' confidence in the EU's ability to deliver solutions to their demand for protection against serious crime and terrorism."

*IKT-Norge mener det ikke er tilstrekkelig sannsyneliggjort og/eller dokumentert at en implementering av Datalagringsdirektivet i norsk lov vil gi den forespeilede effekten. Dermed fremstår det som uforenlig med hensiktsmessig vurderingskriterier i forhold til bla. inngripen i teknologiutviklingen, personvernet, kostnader, tilliten til ekomtilbydere etc. å innføre et slikt lovverk.*

## Noen enkle metoder for å unngå registrering

Noen av metodene for å unngå registrering er kort beskrevet under, IKT-Norge kan utdype dette på et senere tidspunkt om departementet skulle ønske det.

Det er viktig å merke seg at det ikke er noe spesielt og/eller avansert med teknologien som benyttes til å unngå registrering av egen data. Den samme nøytrale teknologien som beskytter og sikrer oss, brukes også til å unngå registrering. Mange helt vanlige internettbrukere benytter antagelig løsninger, bevisst og/eller ubevisst, som bidrar til å unngå registrering allerede i dag. En av de vanligste metodene blir bla. anbefalt av

---

5. Pressemelding fra EuroCop om datalagringsdirektivet, http://www.eurocop-police.org/pressreleases/2005/05-06-02%20PRESS%20JHA%20Council_E.pdf

Nettvett (http://www.nettvett.no) som en fornuftig metode for å sikre bedrifters kommunikasjon. Det er med andre ord snakk om helt standard sikkerhetsteknologi som vanlige internettbrukere blir anbefalt å bruke av både relevante offentlige myndigheter og private sikkerhetseksperter. Eksemplene her er altså teknologi det er ønskelig at norske internett- og teknologibrukere benytter, og som det i all hovedsak ikke vil være mulig å registere data fra selvom myndigheter og/eller andre skulle ønske det og tilpasse lovverket for å forsøke.

**Vanlige brukere vil unngå registering ved å**

1. bruke åpne, eller dårlig sikrede nettverk, i nabolaget de bor eller andre steder de befinner seg.
2. bruke nettverk på hotell, kafeer eller for eksempel arbeidsplassen.
3. bruke webbaserte eposttjenester utenfor Norge som for eksempel Gmail eller Hotmail.
4. bruke Skype og lignende tjenester til "telefonsamtaler".
5. bruke tjenester som Google Talk, Facebook osv. til å chatte
6. bruke online spill som World of Warcraft til "telefonsamtaler"

Det blir umiddelbart helt opplagt at potensialet for å unngå registrering er betydelig selv om det ikke en gang skulle være bevisste handlinger. Dette er viktig i en vurdering av direktivets proporsjonalitet sett i lys av dets opplagt lave effekt.

**Avanserte brukere vil unngå registrering ved å**

Politiets Fellesforbund har beskrevet den teknologiske bevisstheten og adferden til kriminelle. "Erfaring viser at kriminelle i stor grad benytter seg av stjålne eller uregistrerte telefoner. Ofte kastes en telefon etter at en samtale er gjennomført. Igjen viser det seg at kriminelle kjenner til begrensninger i politiets metodebruk og benytter seg av denne kunnskapen i sin kriminelle virksomhet."[6] .

Det er viktig å merke at aktiviteten til terrorister og organiserte kriminelle, som er direktivets målgruppe, vil være vanskelig å registere nettopp fordi de med letthet vil benytte bla. metodene beskrevet her for å unngå registering.

1. bruke VPN, det vil si at man etablerer en tunnel som er sikret mot innsyn til en annen maskin på internett og kan gå videre derfra med annen identitet.
2. Anonymiserende proxyservere gjør at brukerne med enkle verktøy/midler kan undra seg å bli registrert av direktivet
3. bruke anonyme kontantkort fra andre land.
4. bruke norske kontantkort med en annen persons identitet
5. endre IMEI kode på mobiltelefon

---

6. http://www.pf.no/asset/2092/2/2092_2.doc

6. bruke anonymiserende tjenester som for eksempel Tor[7] .
7. bruke zombier og botnet, dvs. datamaskiner under kontroll av tredjepart uten at eieren er kjent med dette[8] .
8. benytte andres identiten og dermed også legge igjen spor som peker på andre enn den som evt. har utført en handling.

*IKT-Norge mener det vil være så enkelt å unndra seg registrering at de direktivet er ment å avdekke kommunikasjonsmønsteret til med letthet vil kunne unngå dette.*

# Merknader til høringsnotatets forslag

IKT-Norge er av den klare oppfattning av direktivet ikke må implementeres i Norge. Vi velger likevel å kommentere viktige enkeltelementer i høringesnotatet. Delvis fordi dette er poeng vi mener en bør være kjent med i forkant av en eventuell videre utredning og fordi det er sider ved høringsnotatets forslag som i seg selv er sentrale argumenter mot direktivet.

## Avveining av hensynet kriminalitetsbekjempelse – personvern – konkurransehensyn

IKT-Norge er enig i at disse tre hensyn må avveies ved en eventuell innføring av datalagringsdirektivet. Vi kan ikke se at det foreligger tilstrekkelig dokumentasjon på at innføringen av direktivet vil bidra i bekjempelse av alvorlig kriminalitet. IKT-Norge viser til at en slik dokumentasjon har blitt etterspurt fra flere instanser i flere år. Hensynet til personvernet er utførlig redegjort for av Personvernkommisjonen i deres betenkning om datalagringsdirektivet og av Datatilsynet i deres høringssvar i denne saken. IKT-Norge mener disse to dokumentene viser at innføringen av datalagringsdirektivet vil gi klare negative konsekvenser for personvernet. IKT-Norge vil særlig vektlegge hensynet til konkurransen. Vi ønsker i den forbindelse å kommentere flere forhold knyttet til konkurranseforholdene på ekommarkedet.

### Konkurransen på ekommarkedet i Europa

Siden direktivet er utformet på en måte som gir rom for store nasjonale tilpasninger kan vi ikke se at det bidrar til å harmonisere regler og styrke konkurransen på ekommarkedet i Europa. Ulike land innenfor EU/EØS opererer med ulik lagringstid, ulike typer data som skal lagres, ulike lagringsformater og ulike regler for hvem som skal ha tilgang til data. Det opereres også med svært forskjellige regler for hvem som skal betale for lagring og utlevering av data. For selskaper som operer i ulike land stilles det

7. http://www.torproject.org/
8. http://en.wikipedia.org/wiki/Zombie_computer, http://en.wikipedia.org/wiki/Botnet og http://www.youtube.com/watch?v=BRhauoXpNSs

krav til at de skal forholde seg til alle disse ulike nasjonale regelverkene. Etter vår mening har direktivet dermed bidratt til å svekke konkurransen framfor å harmonisere regelverk slik intensjonen med direktivet hevdes å være.

**Konkurransen mellom store og små aktører**

IKT-Norge frykter implementeringen av direktivet vil føre til en særlig konkurransemessig ulempe for de små ekomtilbyderne. I Norge finnes det i overkant av 200 ekomtilbydere og av disse er det store flertallet små og ofte regionale aktører. Disse selskapene har ingen erfaring eller kompetanse knyttet til utlevering av trafikkdata til politiet, slik de største aktørene har. IKT-Norge er redd for at kostnadene knyttet til implementering kan føre til store problemer for mange av de små lokale ekomtilbyderne i Norge. Dette vil i så fall kunne føre til at de store etablerte selskapene vinner økte markedsandeler som en følge av implementeringen. IKT-Norge mener dette vil være svært skadelig for konkurransen på det norske ekommarkedet og for utbredelsen av høyhastighets bredbånd i disktriktene.

**Konkurransen mellom ulike teknologier**

Datalagringsdirektivet er utformet på en måte som gjør at det alt før ikrafttredelse. Som høringsnotatet helt korrekt beskriver er en rekke teknologier for elektronisk kommunikasjon unntatt direktivets lagringsplikt. Dette gjelder alle applikasjoner som ikke er definert som offentlige ekomtjenester etter Ekomloven og tjenester som tilbys fra land utenfor EU/EØS. Høringsnotatet lister opp Skype - som i dag står for 13 prosent av all teletrafikk på tvers av landegrenser[9] . MSN, som har både tekst, tale og videokommunikasjon innebygget. Vi har beskrevet flere teknologier som går utenfor direktivet i kapitellet om direktivets effektivitet. Tilveksten av slike tjenester er stor, og det vil i praksis ikke være mulig å omfatte alle disse med direktivet selv om det skulle være en målsetning. IKT-Norge mener direktivets effekt på konkurransen mellom teknologier er meget bekymringsfull. Disse applikasjonsbaserte ekomtjenestene blir stadig mer avanserte, kvalitativt bedre og de tar stadig større markedsandeler på bekostning av tradisjonell elektronisk kommunikasjon. Innføringen av direktivet vil gi de applikasjonsbaserte ekomtjenestene en kraftig konkurransefordel og vil kunne føre til en markant konkurransevridning over på denne type tjenester. Markedet for applikasjonsbaserte ekomtjenester domineres av store internasjonale selskaper med base utenfor Europa. Direktivet vil dermed også kunne føre til en konkurransevridning over fra norske og europeiske ekomselskaper til internasjonale applikasjonsbaserte ekomtjenester.

---

9. http://www.itwire.com/it-industry-news/strategy/30579-13-percent-of-international-calls-now-go-via-skype

**Inngangsbarrierene til markedet**

Innføringen av direktivet vil på to sentrale områder bidra til å heve inngangsbarrierene til ekommarkedet og dermed til å svekke konkurransen. For det første vil direktivet føre til at kostnadene ved å etablere seg på markedet øker. De initielle investeringskostnadene øker siden ekomtilbyderne må etablere egne lagringsløsninger tilpasset direktivets krav. For det andre bidrar direktivet til at reguleringsregimet blir mer komplekst og byråkratisk. Et tilbyder som ønsker å etablere seg på ekommarkedet får ytterligere nye reguleringer å forholde seg til. IKT-Norge mener begge disse forhold vil bidra til å øke inngangsbarrierene til det norske ekommarkedet og dermed svekke konkurransen. Hvor sterk denne effekten vil være er det vanskelig å anslå, men IKT-Norge mener det er grunn til å være bekymret for denne effekten på markedet.

*IKT-Norge mener hensynet til konkurransen på ekommarkedet taler klart mot implementering av direktivet.*

# Forholdet til EMK

IKT-Norge har ingen direkte bemerkninger til forholdet mellom datalagringsdirektivet og EMKs artikkel 8. Vi registrerer imidlertid at Datatilsynet og dets europeiske søster organisasjoner sier direktivet er i konflikt med artikkel 8. Vi ønsker her å knytte noen kommentarer til enkelte av argumentene høringsnotatet tar opp under dette kapittelet. I høringsnotatet argumenteres det med at lagringsplikten i direktivet representerer "et mindre inngripende inngrep for den enkelte enn for eksempel telefonavlytting...og "at dette ikke vil gjelde informasjon som er direkte knyttet til folks identitet". IKT-Norge mener dette er en uriktig framstilling av hvilke rolle teknologien i dag spiller i våre liv. Vi lever en stadig større del av våre liv på en måte som innebefatter bruk av teknologi. Mer og mer av vår kommunikasjon med omverdenen foregår ved hjelp av elektronisk kommunikasjon. Disse teknologitrendene vil øke i årene som kommer. Det vil stilles krav om at vår kontakt med offentlige myndigheter i større grad skal foregå elektronisk. Våre kjøp av varer og tjenester vil i større grad foregå elektronisk og vår kommunikasjon med familie, venner og kolleger vil i større og større grad foregå elektronisk. I tillegg vil flere og flere av våre eiendeler selv knyttes opp mot elektronisk kommunikasjon "the internet of things". Alle disse teknologitrendene vil i sum gjøre at dette dette direktivet representerer det mest inngripende og altomfattende overvåkningsregimet i europeisk historie. Innholdet i og omfanget av data som samles inn vil i sum kunne gi et svært presist bilde av en persons identitet, historiske bevegelser og vil også kunne gi et ganske presist bilde av en persons framtidige bevegelser.

Videre argumenteres det i høringsnotatet under dette punktet for at "en praksis hvor kriminalitetsbekjempelse og varetakelse av den nasjonale sikkerhet beror på tilfeldigheter må i det lange løp betegnes som utilfredstillende...og...dette kan således tale for at lagringsplikten er nødvendig for å bekjempe kriminalitet og vareta den nasjonale sikkerheten". IKT-Norge mener denne formuleringen representerer et skremmede samfunnssyn. I et demokrati vil det aldri være slik at politiets etterforskning

kan baseres på noen annet enn de "tilfeldige" spor som til enhver tid finnes. Dersom analogien i resonementet over skal være konsistent må det i så fall bety at en mener vi må innføre en lignende lagrings/overvåkningsplikt også for all annen informasjon som kan være nyttig for politiets etterforskning. I så fall beveger vi oss farlig nære grensen for å kunne kalle oss et demokratisk samfunn.

To roller i vårt samfunn som er lett kan komme under sterkt press dersom direktivet implementeres er pressens kilder og varslere. Risikoen for at disse og andre mister den nødvendige tillitten til ekomtjenestene er høyst reell og kan dermed bidre til den tidligere nevnte "chilling effect". IKT-Norge registrerer at både Norsk Presseforbund[10] og Norsk Journalistlag[11] går mot direktivet på denne bakgrunn.

Videre registrerer IKT-Norge at både Advokatforeningen[12] og Den internasjonale juristkommisjon – norsk avdeling[13] gjør et poeng av at direktivet etter all sannsynelighet er i strid med EMK.

*IKT-Norge er opptatt av at folk skal kunne ha tillit til at tilbydre av elektronisk kommunikasjon opererer innefor grensene av EMKs artikkel 8. Etter vår mening kan direktivet skape tvil om så er tilfelle.*

## Kriminalitetsbekjempelse i en ny teknologisk hverdag

IKT-Norge mener det forelagte forslaget vitner om en grunnleggende svikt i forståelsen av hvordan teknologi fungerer, og tidligere nevnte eksempler på hvordan et individ kan unngå registrering. Videre er det påfallende at det ikke er gjort noen utredninger av alternativer til direktivet. I høringsnotatet vises det til udokumenterte påstander fra politiet om behov for lagringstid og bruksverdi. Disse påstandene tåler ikke en sammenligning med funnene i EUs egen evalueringsprosess som fremdeles pågår. Videre er det meget problematisk at regjeringen simelthen konkluderer med at det ikke finnes noe alternativ til direktivet (side 28 i høringsnotatet) all den tid det er helt opplagt at alle som ønsker det enkelt vil unngå registrering.

"–Heller ikke i forbindelse med høringen om mulig innføring av datalagringsdirektivet i norsk rett, er det fremlagt noen systematisk analyse av nytten slike data har i etterforskning, påpeker Leif T. Aanensen, avdelingsdirektør i Datatilsynet"[14] . Med den bakgrunn har siv.ing og ph.d. Svein Willassen utarbeidet en rapport på oppdrag fra

---

10. http://presse.no/Arkiv/NP+går+i+mot+implementering+av+datalagringsdirektivet.9UFRvM30.ips
11. http://www.journalisten.no/story/60917
12. http://www.advokatforeningen.no/Aktuelt/Nyheter/DLD-direktivet-strider-mot-EMK/
13. https://docs.google.com/fileview?id=0B2Rh7x7YpF3KZjc1MWY0YjUtNGM3Yy00OTUwLTg2OWEtMGQ5ODVmMDU0ZWNh&hl=en
14. http://www.datatilsynet.no/templates/Page____3387.aspx?utm_source=twitterfeed&utm_medium=laconi

Datatilsynet som viser at politiets nytte av den omfattende registreringen og lagringen av data er høyst begrenset.

IKT-Norge mener det er påfallende at høringsnotatet ikke problematiserer potensialet for effektivisering av politets arbeid med de utstrakte muligheter politiet allerede har. "- Politiet trenger ikke mer informasjon, de trenger å jobbe bedre med det de allerede vet, sier professor Petter Gottschalk ved Handelshøyskolen BI."[15] Det er i denne sammenhengen et poeng å vise til hva Politiets Fellesforbund sa om kriminelles teknolgivalg for å unngå å bli registrert i "Høring: Forebyggende politimetoder"[16] for å unngå registrering. "Telefonsamtaler blir ikke brukt i forbindelse med planlegging av organisert kriminalitet. Deltagerne i nettverkene er helt bevist på å ikke bruke telefoner til slike samtaler." Dette er et syn som også støttes av Heinz Kiefer, President i EuroCOP, som sier: "The result would be that a vast effort is made with little more effect on criminals and terrorists than to slightly irritate them.[17] ".

*IKT-Norge mener teknologien gjør det så enkelt å unngå registrering at man ikke kan benytte hensynet til kriminalitetsbekjempelse i en ny teknologisk hverdag som et argumentere for implementering av direktivet.*

## Hva skal lagres

IKT-Norge mener at det i direktivets formulering; "data generated or processed as a consequence of a communication or a communication service"[18] fremkommer tydelig at ekomtilbyderene kun skal lagre data som fremkommer når de utfører sin tjeneste[19] . Dette innebærer at ekomtilbyderene ved en eventuell implementering ikke skal iverksette tiltak for å fremskaffe data de selv ikke besitter.

IKT-Norge mener høringsnotatet i liten grad bidrar til å oppklare den uklarhet som ligger i direktivet rundt hvilke typer data som skal pålegges lagret. Det råder særlig en uklarhet rundt hvilke krav til kvalitet på data som skal lagres. Denne uklarheten kan ha stor betydning for hvilke omfang lagringsplikten vil gi. IKT-Norge mener denne uklarheten må presiseres langt bedre før saken legges fram til politisk behandling. I følge direktivet pålegges ekomtilbydereer å lagre data som framkommer når de utfører sine tjenester, dvs bare de data de har tilgang til jamfør direktivets punkt 13. Ekomtilbydere har i dag tilgang til data for å dekke egne behov for kundeservice og sikre kvalitet på tjenesten. Disse data kan ha ulik kvalitet da formater er tilpasset det behov de i dag skal dekke. Data som for eksempel kun anvendes til feilsøkingsformål vil typisk

---

15. http://www.idg.no/computerworld/article161438.ece
16. http://www.pf.no/asset/2092/2/2092_2.doc
17. Pressemelding fra EuroCop om datalagringsdirektivet, http://www.eurocop-police.org/pressreleases/2005/05-06-02%20PRESS%20JHA%20Council_E.pdf
18. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2006:105:0054:0063:EN:PDF
19. http://www.regjeringen.no/pages/2281081/hnotat_datalagring.

holde en lavere kvalitet enn data som legges til grunn for fakturering av kunder. Dersom selskapene skal pålegges nye krav som betyr at kvaliteten på dataene må økes vil dette kunne føre til store økte kostander og dermed øke lagringspliktens omfang. IKT-Norge mener at dersom direktivet implementeres skal det ikke legges krav til lagring av data som bidrar til at selskapene må produsere tilleggsdata eller øke kvaliteten på dataene.

Under punkt 4.4.4 siste punkt foreslås det at det ved internettaksess skal lagres informasjon som identifiserer kommunikasjonsutstyret eller kommunikasjonsannlegget. IKT-Norge mener det er behov for å klarlegge hva som menes med dette punktet.

*IKT-Norge mener det fremdeles er stor uklarheten rundt hva som skal lagres. Dette må avklares og det skal ikke stilles strengere krav til kvalitet på data enn hva selskapene selv har i dag.*

## Hvem skal lagre i henhold til lovforslaget

IKT-Norge viser her til de kommentarer vi hadde under punktet om hensynet til konkurransen på ekommarkedet og særlig konkurransen mellom ulike teknologier. Alle applikasjonsbaserte ekomtjenester er unntatt direktivet. Dette vil føre til at kunder flytter over til denne type kommunikasjonsløsninger. Kriminelle kan lett komme seg unna direktivet ved å benytte applikasjonsbaserte kommunikasjonstjenester. Dermed uthules direktivets formål samtidig som det bidrar til en urimelig forskyvning av konkurransen på ekommarkdet.

*IKT-Norge mener direktivet bidrar til å forskjellsbehandle ulike tilbydere av elektronisk kommunikasjon avhengig av hvilken teknologi deres tjenester er basert på.*

## Ulike løsninger for lagringssted

IKT-Norge støtter høringsnotatets forslag om at det skal være valgfritt for selskapene om de ønsker å lagre data lokalt eller om de ønsker å gå sammen om en felles lagringsløsning. Det er imidlertid viktig at samlokalisert lagring må skje i regi av selskapene selv fremfor en myndighetskontrollert lagringsløsning. IKT-Norge støtter at selskaper som opererer i flere land må kunne samlokalisere. IKT-Norge mener at følgende krav fra høringsnotatet viser at dette direktivet ikke bidrar til harmonisering; "Tilbydere som ønsker å lagre data i en sentral database i EU må sørge for at data fra de ulike medlemslandene er fysisk adskilte, sånn at hvert enkelt medlemslands lover og regler når det gjelder lagringstid, vilkår for uthenting m.m. kan ivaretas". Et slikt krav er etter IKT-Norges mening urimelig. IKT-Norge forutsetter videre at valg av lagringssted ikke vil ha implikasjoner for hvem som eventuelt skal bære kostnadene forbundet med lagringsplikten.

*IKT-Norge støtter forslaget om det skal være valgfritt for selskapene om de ønsker lokal lagring eller samlokalisert lagring.*

## Lagringstid

IKT-Norge er av den klare oppfatning at dersom direktivet skal implementeres i Norge må man velge en minimumsløsning. Nasjonale krav i Norge bør ikke gå utover minstekrav i direktivet. Erfaring viser at politiet svært sjelden ber om å få utlevert trafikkdata fra telefoni og mobiltelefon lenger tilbake enn tre måneder. En lagringstid på 6 måneder er således tilstrekkelig. EUs pågående evaluering av direktivet bekrefter at trafikkdatas relevans for etterforskningen synker signifikant med alderen på dataene. I høringsnotatet slås det fast at det ikke foreligger statistikk over hvor gamle data politiet har etterspurt til nå. I EUs evaluering foreligger denne statistikken. I følge EUs egen statistikk benyttes det meste av dataene før de er 3 måneder gamle (omlag 70 prosent). Omlag 85 prosent benyttes før dataene er 6 måneder gamle. I evalueringen heter det at "data utover 6 måneder kun har anekdotisk verdi". Evalueringen kritiserer at det ikke foreligger noe dokumentasjon som forklarer hvorfor 6 til 24 måneder er valgt som grenser for lagringstid i direktivet. Etter IKT-Norges mening er dette så tungtveiende dokumentasjon at det vil være svært oppsiktsvekkende om Norge velger en lengre lagringstid enn 6 måneder. IKT-Norge syntes det er påfallende at politimyndigheten ikke er istand til å dokumentere behovet for den foreslåtte lagringsplikten, samtidig som de argumenter sterkt for at de er avhengig av utvidet lagring.

*Det finnes ingen dokumentasjon som forsvarer en lengre langringstid enn 6 måneder*.

## Krav til lagring og levering av lagrede data

IKT-Norge har ingen særskilte kommentarer til dette punktet utover at det i størst mulig grad bør tilstrebes at dataene kan overleveres i standardiserte formater og at det finnes standardiserte metoder for uthenting av de data i den kvalitet tilbyderne besitter. Disse standardene må være ment å lette tilbydernes arbeid med utlevering av data og ikke komplisere dem eller øke kostnadene og arbeidsmengden forbundet med utlevering.

## Tilsyn med lagringen

IKT-Norge støtter høringsnotatets forslag om å videreføre det delte tilsynsansvaret mellom Post- og teletilsynet og Datatilsynet. En eventuell implementering av direktivet vil som høringsnotatet beskriver føre til et økt tilsynsansvar, økt arbeidsmengde og dermed økte kostnader for Datatilsynet og Post- og teletilsynet. IKT-Norge mener det er høyst urimelig at Post- og teletilsynets økte kostnader knyttet til tilsyn i denne saken skal lastets over på ekomtilbyderne. Disse ekstra kostandene må Post- og teletilsynet få tilført fra Samferdselsdepartementet ved en eventuell implementering.

Samferdselsdepartementet bør i denne anledning gjennomføre en helhetlig studie av Post- og teletilsynets finasieringsmodell for å se på hvilke oppgaver det er naturlig at skal belastes tilbyderne gjennom gebyr og hvilke av tilsynets oppgaver det er naturlig at belastes offentlige budsjetter.

IKT-Norge mener forøvrig at Post- og teletilsynet, som skal ivareta Ekomlovens formål og virke, fortsatt bør ha en rolle i sakene om politiets tilgang til data for etterforskning og forebygging av alvorlig kriminalitet.

## Politiets tilgang til data

IKT-Norge ønsker innledningsvis under dette punktet å påpeke den noe liberale tolkningen høringsnotatet har lagt seg på i sin oversettelse av direktivets formuleringer. I direktivet benyttes begrepet "serious crime" for å beskrive hvilke saker som skal kunne gi politiet tilgang til data også er det opp til medlemslandene å definere rammene for "serious crime". I høringsnotatet brukes det norske begrepet "særlige saker" som oversettelse av direktivets "serious crime". IKT-Norge mener denne merkelige oversettelsen vil kunne bidra til å utvanne direktivets formål og dermed føre til at listen for når data skal utleveres senkes urimelig lavt. IKT-Norge ber om at det utarbeides en mer presis oversettelse av begrepet "serious crime" i det videre arbeidet. Direktivets formål var bekjempelse av terror og alvorlig organisert kriminalitet. Dette bør også være normgivende for den norske implementeringen. Vi mener derfor at kravet om at data skal utleveres dersom det straffbare forholdet har en strafferamme på 3 år eller mer er urimelig lavt. Vi ønsker i den forbindelse også å vise til våre nordiske naboland Finland og Danmark som har lagt seg på henholdsvis 4 år og 6 år. IKT-Norge har ingen konkrete forslag til hvilken strafferamme man bør legge seg på eller til den oppregning av lovbrudd som er foreslått som alternativ til det generelle kravet. Dersom direktivet skal implementeres i Norge mener IKT-Norge at man ikke skal gå ut over direktivets minstekrav. Det betyr at vi anbefaler at Norge legger seg på en restriktiv linje og setter listen høyt for når politiets skal få tilgang til data. Dette skyldes blant annet at vi frykter en "slippery slope" utvikling der listen legges lavere og lavere. Det virker opplagt at forslaget i høringsnotatet er betydelig annerledes enn direktivets opprinnelige tekst. IKT-Norge har også registrert at det i debatten rundt direktivet har blitt vist til blant annet digital mobbing som et problemområde der direktivet vil kunne ha effekt. Allerede nå kan vi registere at Politiets Fellesforbund viser stor mangel på innsikt i direktivet og "mener at intensjonen med direktivet kan bli undergravet om en innfører en strafferamme på fengsel i tre år eller mer"[20] . At noen ønsker en slik dreining av direktivet, eller en utvikling lik den som er i England hvor over 600 offentlige etater har tilgang til tilsvarende data fremstår som gode illustrasjoner på hvordan en implementasjon fort kan få meget alvorlige konsekvenser for det definerte bruksområdet.

---

20. http://www.regjeringen.no/pages/2281080/Politiets_Fellesforbund.pdf

IKT-Norge er svært skeptisk til å gi Kredittilsynet (nå Finanstilsynet) eller andre offentlige etater tilgang til data. Etter vår mening øker dette faren for at data kan komme på avveie og for at data kan bli utlevert uten tilstrekkelig hjemmel. Mange små ISPer har ikke erfaring og kompetanse for denne type utlevering og kan fort komme opp i situasjoner de opplever som vanskelige og ubehagelige dersom de skal forholde seg til krav og press fra en rekke ulike offentlige autoriteter. Dersom direktivet implementeres bør det kun være politiet som gis tilgang til data og reglementet for utlevering bør være klart og tydelig formulert slik at det ikke er rom for misforståelser.

Utover problemstillingen med Kredittilsynet (nå Finanstilsynet) etterlyser IKT-Norge en grundig utredning om direktivets forhold til tvisteloven og eventuell utlevering av data til privateaktører. Det bør være liten tvil at en implementering av direktivet uten dataene er sikret mot tilgang for private aktører potensielt vil utløse et massivt press mot både rettsvesen og ekomtilbydere om tilgang som lett kan lede til store og utilsiktede negative konsekvenser for mange individer.

*IKT-Norge mener listen bør legges høyest mulig for når politiets skal få tilgang til data dersom Norge velger å implementere direktivet. Det bør kun være politiet som gis tilgang til data.*

## Administrative og økonomiske konsekvenser

IKT-Norge mener det vil være totalt urimelig dersom noen av kostandene forbundet med en eventuell implementering av dette direktivet legges på ekomtilbyderene. Dette direktivet er et offentlig pålegg for å dekke det offentliges behov for data. Dataene skal sågar ikke være tilgjengelige for ekomtilbyderene og de skal være fysisk adskilt fra de trafikkdata tilbyderene har til eget bruk og for å dekke egne behov. Dermed vil lagringsløsningene etter en evt. implementering være selvstendige løsninger med kostnader som kun eksisterer som en følge av direktivet. Myndighetene må dekke den enkelte ekomtilbyderene merkostnader i forbindelse med tilrettelegging for utvidet lagring så vel som de løpende merkostnader til lagring og utlevering. Vi anerkjenner ikke at den modell for kostnadsdeling som benyttes i dag ved utlevering av trafikkdata etter ekomlovens § 2-8  andre ledd har noen som helst relevans. Denne bestemmelsen omhandler utlevering av trafikkdata selskapene allerede henter inn til eget bruk for å sikre kvaliteten på de tjeneste de leverer sine kunder. Altså har selskapene en egeninteresse av å framskaffe disse data. Datalagringsdirektivet omhandler noe nytt - en statlig pålagt lagringsplikt for å dekke statens behov for trafikkdata. Selskapene har ingen egeninteresse av at datalagringsdirektivet innføres i Norge og motsetter seg derfor noe som helst økonomisk ansvar for dette. IKT-Norge er opptatt av at de krav som pålegges selskapene oppfattes å være rimelige og at resultatet ikke bidrar til å skade eller svekke våre medlemmers omdømme overfor forbrukerne. Et krav om at selskapene skal ha en tilretteleggingsplikt og dekke kostnadene for dette vil være åpenbart urimelige og vil kunne bidra til å svekke bransjens omdømme. IKT-Norge er redd for at

kostnadene knyttet til implementering kan føre til store problemer for mange av de små lokale ekomtilbyderne i Norge.

Videre er det urimelig at Post- og teletilsynets økte kostander ved økt tilsyn skal pålegges selskapene gjennom økt gebyr.

Dersom kostnader forbundet med implementering av dette direktivet legges på selskapene vil vi oppfordre selskapene til å synliggjøre dette overfor kundene ved å spesifisere den "statlige overvåkningsavgiften" på kundenes faktura.

*IKT-Norge mener alle kostander knyttet til en eventuell implementering av direktivet må dekkes av det offentlige.*

# Bør datalagrinsdirektivet implementeres i norsk lov?

## Konsekvenser for Norge ved å ikke implementere direktivet

For IKT-Norge har det vært viktig å få fram de juridiske aspektene ved denne saken, men vi etterlyste for over to år siden en utredning av både tekniske forhold, økonomiske konsekvenser, personvernspørsmål og markedssituasjonen. IKT-Norge foreslo da at det skulle settes ned en norsk offentlig utredning som skulle være bredt sammensatt og som kunne utrede alle sider ved implementeringen av direktivet. Vi beklager på det sterkeste at en slik helhetelig utredning ikke er funnet sted og mener dette gir oss et svært dårlig grunnlag for å gå videre med denne saken nå.

To av Norges fremste jurister på EU/EØS-rett har på oppdrag fra IKT-Norge utarbeidet en juridisk betenkning om datalagringsdirektivet skal inn i EØS-avtalen. De konkluderer med at det kan argumenteres juridisk for at direktivet ikke er EØS-relevant og at konsekvensene av at Norge bruker EØS-avtalens ”vetorett” i denne saken bør være svært beskjedne.

### Kort om den juridiske betenkningen

Den juridiske betenkningen er utarbeidet av professor dr juris Finn Arnesen og professor dr juris Fredrik Sejersted ved Senter for Europarett ved Universitetet i Oslo. Hele dokumentet ligger som vedlegg til høringsnotatet på Samferdselsdepartementets nettsider.

Problemstillingen de ble bedt om å utrede:

1. *"Er direktivet EØS-relevant, og hva kan konsekvensene være fra EU sin side i en EØS-sammenheng dersom Norge hevder at direktivet ikke er EØS-relevant?"*
2. *"Hvilke konsekvenser vil det kunne få å benytte EØS-avtalens mulighet til å reservere seg fra direktivet?"*
3. *"Finnes det andre måter Norge kan unngå å implementere direktivet på?"*

Rapportens konklusjon:

- Det kan argumenteres materielt for at direktivet etter sitt innhold faller utenfor EØS-avtalens virkeområde, og dersom Norge ønsker å reservere seg er dette den mest naturlige og legitime begrunnelsen.
- Dersom EU ikke er enig i at direktivet faller utenfor EØS-avtalens naturlige virkeområde vil dette kunne medføre suspensjonsvirkninger, men materielt sett synes det bare å være svært beskjedne deler av EØS-avtalens Vedlegg IX som vil bli direkte ”berørt” av dette.
- Utover dette er det et åpent spørsmål i hvilken grad bruk av reservasjonsretten vil kunne føre til mer indirekte politiske virkninger.
- Dersom direktivet inntas i EØS-avtalen vil norsk lovgiver være forpliktet til å gjennomføre det i norsk rett, men man vil ha betydelig valgfrihet med hensyn til hvordan dette nærmere skal gjøres, og hvilke garantier som oppstilles.

IKT-Norge ønsker avslutningsvis å kommentere noen påstander som har framkommet i det offentlige ordskifte rundt direktivet.

## Feil at Norge blir frihavn for kriminelle uten datalagringsdirketivet

Norge blir ingen frihavn for kriminelle dersom vi ikke implementerer datalagringsdirektivet. Direktivet er svært omstridt internt i EU og land Sverige og Tyskland har ikke innført det. EUs egen evaluering viser at av de landene som har tatt direktivet i bruk er den kun Frankrike, UK og Tsjekkia som bruker det i stort omfang. Data flyttes over landegrenser på sekunder uavhengig av dette direktivet. Det er ikke mer kriminalitet i Norge, Tyskland og Sverige enn det er i UK, Frankrike og Tsjekkia. Det er absolutt ikke snev av belegg for å påstå at vi er i ferd med å bli en frihavn for kriminelle.

## Feil at politiet ikke vil få tilgang til trafikkdata uten direktivet

Det er feil at dette direktivet dreier seg om hvorvidt politiet skal få tilgang til trafikkdata eller ikke. Politiet har alt i dag en utstrakt tilgang til trafikkdata og teleselskapene bistår i stor utstrekning politiet i å benytte trafikkdata i etterforskning. Vi har i Norge klare regler og retningslinjer i ekomloven og personopplysningsloven for hvordan denne utleveringen skal foregå. Dette vil bestå uavhengig av om direktivet innføres eller ikke.

## Feil at teleselskapene vil slutte å lagre trafikkdata

Teleselskapene har ingen planer om å redusere lagringstiden på grunn av teknologiske framskritt. Det er gjort milliard-investeringer i dagens tele-infrastruktur. Ekomtilbyderne er avhengig av trafikkdata for å sikre at tjenestene fungerer og vil også være det i framtiden – uavhengig av teknologivalg.

Uavhengig av direktivet vil ekomtilbyderne i framtiden lagre langt mer trafikkdata enn i dag fordi vi alle i større og større grad benytter telefon, mobil og data til kommunikasjon. I tillegg vil elektronisk kommunikasjon i framtiden også bli mer og mer vanlig mellom tingene våre; f.eks. biler, maskiner, hus. Alt i dag har Telenor over 10 millioner gjenstander som kunder. Dette vil generere mer og mer trafikkdata i fremtiden. I 2005 når direktivet ble utformet hadde 20 prosent av Norges husstander bredbånd – i dag har 80 prosent bredbånd – dette er et bilde på det økte omfanget av elektronisk kommunikasjon. Direktiver er, som en følge av teknologiutviklingen, blitt langt mer omfattende enn det i utgangspunktet var tenkt å være.

# IKT-Norges konklusjon

IKT-Norge mener EUs datalagringsdirektiv ikke bør implementeres i Norge. Utredninger viser klare negative konsekvenser for personvernet, blant annet konkluderer Personvernkommisjonen med at personvernet vil bli svekket og at behovet for og nytteverdien av direktivet ikke er godt nok dokumentert. Som det vises til i høringsnotatet har IKT-Norge også tatt initiativ til å få utredet konsekvensene for Norge ved å ikke implementere direktivet. Professor Finn Arnesen og Fredrik Sejersted ved Universitetet i Oslo konkluderer med at konsekvensene vil være svært begrensede og uproblematiske både for Norge og for norske selskaper.

IKT-Norge er først og fremst bekymret for at direktivet vil bidra til å svekke folks tillit til teknologi. Vi frykter dette vil kunne føre til at bruken av elektronisk kommunikasjon reduseres og dermed også at bruken av teknologi reduseres. Dette vil kunne få en rekke utilsiktede negative konsekvenser for det norske samfunn.

Etter IKT-Norges mening er dagens regelverk og praksis for lagring og tilgjengeliggjøring av trafikkdata tilstrekkelig for å dekke politiets behov. Vi kan ikke se at det foreligger dokumentasjon som forsvarer innføring av EUs datalagringsdirektiv. Videre har det fremkommet at merverdien i etterforskningssammenheng utover dagens situasjon er høyst begrenset, spesielt sett i lys av hvor enkelt det er for alle som ønsker det å unngå registrering.

Dersom det skulle oppstå et behov for utvidet tilgang til trafikkdata vil det være å foretrekke å foreta mindre tilpasninger i dagens nasjonale regelverk – framfor å implementere EUs datalagringsdirektiv. IKT-Norge mener ikke datalagringsdirektivet har

bidratt til å harmonisere regelverk og dermed sikre konkurransen i Europa, således er dette ikke noe argument for å innføre direktivet.

IKT-Norge mener at det fremlagte høringsnotatet ikke i tilstrekkelig grad belyser relevante problemstillinger og at det ikke er lagt frem holdbar dokumentasjon som kan forsvare å implementere direktivet i norsk lov. Eksempelvis er det ikke dokumentert at direktivet vil gi noen reell effektivisering av kriminalitetsbekjempelse, mange sentrale momenter er ikke belyst og tilsynelatende overlatt til forskriftsarbeid.

Dersom norske myndigheter likevel skulle konkludere med at direktivet skal implementeres i Norge mener IKT-Norge at saken må forberedes langt grundigere enn hva som er gjort i dette høringsnotatet. Først og fremst må man avvente resultatene av EUs evaluering av direktivet. Denne evalueringen vil høyst sannsynlig føre til at direktivet blir vesentlig endret. Det vil derfor være uklokt om Norge implementerer direktivet i sin nåværende form. IKT-Norge mener Regjeringen i så fall må komme tilbake med et nytt høringsnotat og nytt helhetlig forslag til implementering etter at EUs evalueringsprosess er konkludert. Et slikt helhetlig forslag må inneholde en utredning av juridiske og tekniske forhold, økonomiske konsekvenser, personvernspørsmål og markedsituasjon. Det må også inneholde en konsekvensanalyse og alternativer til implementering.

*IKT-Norge mener at datalagringsdirektivet ikke skal implementeres i norsk lov*

For IKT-Norge

Hallstein Bjerke
Direktør for myndighetskontakt

Torgeir Waterhouse
Direktør internett og nye medier