

Samferdselsdepartementet  
Postboks 8010  
0030 Oslo

Gjøvik, 12. april 2010

Vår ref.: NorSIS/2010-34/TLO

Deres ref.:09/585-HK  
08.10.2010

## Høring om datalagring

Norsk senter for informasjonssikring (NorSIS) viser til høringsbrev fra Samferdselsdepartementet 8. januar 2010 om EUs Datalagringsdirektiv (DLD) skal innlemmes i EØS-avtalen.

### *Sammendrag*

Formålet med datalagring av trafikkdata vil etter vårt syn være kriminalitetsbekjempelse, derav også kriminalitetsforebyggende. Spørsmålet er om dette sikkerhetstiltaket er et hensiktsmessig tiltak?

Ved en eventuell innføring av DLD må det tas grundig hensyn til å sikre personvern slik at den norske borgers personvern ikke blir tilsidesatt for å kunne innehente trafikkdata i enkeltsaker. NorSIS mener at det må rettes stor fokus på å sikre trafikkdata på en slik måte at personvernet ikke blir krenket. Tilbydere behandler i dag også store mengder trafikkdata, og med en innføring av datalagringsplikt vil man også kunne innføre strengere sikringstiltak.

Trafikkdata for mange av de kriminelle sakene vil være grenseoverskridende data. Trafikkdata vil kunne være lagret i annet land enn trafikken skjer i og annet land enn hvor tilbyder har tilhold. Det vil være vesentlig for om Norge skal innføre krav om datalagring at også andre land innfører det, spesielt land vi er nært knytte til i forhold til utveksling av data og samhandling. Det bør tilstrebes like krav til lagringstid, sikring av data og innføring av datalagring som disse landene. I den grad andre og sammenlignbare land innfører datalagring bør det være høy fokus på:

- Sikring av trafikkdata, med tanke på konfidensialitet, integritet, tilgjengelighet og driftsstabilitet hos tilbydere og hos politiet.
- Tilsyn av sikkerhet og av om formål og krav i direktivet overholdes
- Forhold knyttet utlevering av trafikkdata over landegrensene.

En viktig forutsetning for innføring av DLD bør etter vårt syn også baseres på erfaringer fra de som allerede har tatt i bruk DLD på om en innføring av direktivet faktisk har gitt de ønskede effekter. NorSIS finner ikke at slike erfaringer er godt beskrevet i høringsnotatet.

## NorSIS Kommentarer til høringsnotatets kapitler

### 2.4.4 Metodekontrollutvalgets utredning

5. – 9. avsnitt

Teletilbydere som bryter taushetsplikt kan ikke straffes. Dette vil også i dag kunne være en stor utfordring. Høringsnotatet viser at de største tilbydere i Norge allerede gjennomfører store deler av trafikkdataagringen. Det er et forslag om å skjerpe disse reglene slik at brudd på taushetsplikt blir straffbart for både teletilbydere, personer som ikke er i tjeneste eller arbeid for statlig eller kommunalt organ. NorSIS støtter at brudd på taushetsplikt blir straffbart også for disse. NorSIS mener også at disse endringene må legges til grunn for iverksettelse av datalagringsdirektivet.

### 2.5 Praksis for utlevering av trafikkdata fra tilbyderne til politiet

NorSIS mener at dagens lovformulering om at ” ... utsette staten eller allmenne interesser for skade eller virke urimelig overfor den som har krav på hemmelighet ” virker som en vag formulering som kan være utfordrende å vurdere. Videre virker det som Post- og teletilsynet gjennomfører en restriktiv praksis på bakgrunn av personvern hensyn.

NorSIS merker seg at politiet mener det har vært vanskeligere å etterforske internettrelaterte saker vedrørende overgrep mot barn, pga kort lagringstid. Lagringstid er derfor et viktig avklaringspunkt for direktivet. Når det gjelder identitetstyverisaker har NorSIS gjennom sitt eget prosjekt erfaring med at den rammede ofte ikke selv blir gjort oppmerksom på at de er utsatt for dette før lang tid etter at selve ID-tyveriet har funnet sted. I følge Gartner group er det ikke unormalt med 12-15 måneder fra ID-tyveriet starter til svindelen begynner og offeret blir gjort oppmerksom på dette i form av gjenparts brev fra kredittvurderingsselskaper og lignende.

### 2.6 Andre myndigheters tilgang til trafikkdata i dag

NorSIS merker seg at gjeldende praksis er streng mht til å gi andre myndigheter enn politiet tilgang til trafikkdata. NorSIS mener at Norge bør opprettholde en streng praksis på hvem som vil få utlevert trafikkdata.

## 3 Rettstilstanden og implementeringen av datalagringsdirektivet i andre land

NorSIS merker seg at det er satt fokus på lagringstid og hvilke lovbrudd som er gjeldende for å hente ut trafikkdata. NorSIS savner informasjon om hvilke krav det stilles til sikringstiltak, tilgangskontroll og tilsyn med datalagring i de nevnte land. Danmark iverksatte direktivet i 2007, Finland i 2008. NorSIS savner erfaringer fra disse årene i disse landene. Hvilken bistand har direktivet hatt for politiet og påtalemyndighetene. Hvilke svakheter og styrker ser man allerede av gjennomføringen av direktivet. Dette kan være nyttige erfaringer for Norge før en beslutning om for eller mot innføringen av DLD tas, og evt. hvordan detaljene i direktivet skal utformes til det beste for personvern og kriminalitetsbekjempelse.

### 3.1 Danmark

NorSIS merker seg at Danmark har annen strafferamme til grunn for mulighet til å hente ut trafikkdata (strafferamme på minst 6 år) enn det Norge foreslår.

NorSIS merker seg også at overskuddsinformasjon kan brukes av politiet i etterforskning. NorSIS er skeptisk til at det gis åpning for at trafikkdata kan lagres hos politiet over lengre tid og eventuelt benyttes i relaterte saker. Erfaringsmessig vil åpning for utvidet bruk bli benyttet og faren for at grensene ytterligere flyttes er stor.

Danske myndigheter har satt ned arbeidsgruppe for å se på ulike nettbaserte tjenester. Slike tjenester, som f eks gratis wlan, vil være teknologiske løsninger som typisk de kriminelle vil tas i bruk for å hindre lagring av egne trafikkdata. Dette vil være et typisk problem knytte til den stadige kampen mellom de kriminelle og myndighetene, der de kriminelle vil være i forkant av utviklingen og utnytte ”huller i lovverk / teknologi for å omgå lovverket.

### 3.2 Finland

Den finske reguleringen legger til grunn en annen strafferamme enn Danmark.

Finland har også en annen kostnadsmodell for inndekning til tilbyderne enn det Danmark har og det som anbefales i Norge. NorSIS mener dette kan ha betydning for effektiviteten og implementering av datalagringen.

### 3.3 Sverige

Diskusjonene i Sverige, spesielt knyttet til FRA-reguleringen har vist at direktivet skaper debatt om overvåkning av alle innbyggere sett opp mot kriminalitetsbekjempelse og at dette er vanskelige avgjørelser.

### 3.4 Andre EU-land

I Tyskland har man kommet frem til at direktivet «er et svært alvorlig inngrep mot personvernet» og har bedt teleselskapene slette arkivene over e-poster og telefonsamtaler. – Det er en del av den tyske konstitusjonelle identitet at innbyggernes oppfatning av frihet ikke skal tas til fange og registreres fullstendig var domstolens formann Hans-Jürgen Papier sin begrunnelse. Det må tillegges at lovverket også er forskjellig fra det norske.

## 4 Nærmere om lovforslaget

Elektronisk kommunikasjon benyttes av de aller fleste i dagens samfunn, både de ærlige og de kriminelle. I denne utviklingen er det et stadig sterkere behov for å unngå nye typer elektronisk kriminalitet.

Det er viktig at politiet får de nødvendige verktøy for å følge med i den generelle samfunnsutviklingen. Vi kan ikke redusere mulighetene til å utføre politiarbeid fordi den teknologiske utviklingen går fremover. På samme måte som politiet har gjennomført forebyggende og håndhevende politiarbeid i tidligere tider med f eks å patruljere det offentlige rom, må det tilrettelegges for patruljering i de nye offentlige rommene. Ny teknologi bør gi politiet de samme muligheter som de har i dag.

Kriminaliteten har med ny teknologi et mye større internasjonalt samarbeid. Det er derfor svært viktig at politiet i de ulike land har tilgang til de samme kriminalitetsbekjempende tiltakene. Det er viktig at Norge ikke blir en nasjon det er lettere å være kriminell i, men samtidig en nasjon med sterkt fokus på personvern.

#### *Personvern*

Når man vurderer samfunnets overvåkningsnivå er det som høringen beskriver viktig å vurdere det totale bildet. Det er lett å stadig utvide mulighetene til overvåkning uten at noen reagerer på dette. Man ser at videoovervåkning var noe omstridt i starten, for så å øke veldig, uten at borgerne reagerer på dette. De fleste synes dette skaper en trygghet. Videoovervåkingen er i dag ofte gjennomført uten at bedrifter og behandlingsansvarlige har nevneverdig fokus på sikring og personvern.

Gitt en stor grad av innsamling av ulike persondata uten tilstrekkelig sikring kan disse komme uvedkommende i hende og dersom datamengden er stor vil sammenstilling kunne medføre skader for personvernet. NorSIS mener det er av vesentlig betydning at ved innsamling av persondata må man legge stor vekt på gode sikringstiltak for å kunne avveie konsekvensene mtp personvernet.

NorSIS mener det er særdeles viktig at det blir satt strenge krav til sikring av trafikkdata for alle tilbydere og for politiet. Kravene må gjennomgås jevnlig slik at de demmer opp for trusselbilde. Det må også følges nøye opp at alle tilbydere overholder sikringskravene, med f eks bruk av periodisk tilsyn. Det er også viktig at det er en straff knyttet til at sikringstiltak ikke blir gjennomført som står i forhold til kostnaden ved å ikke implementere sikringstiltakene.

NorSIS hadde gjerne sett at erfaringer fra Danmark og Finland hadde blitt vurdert i forhold til valg av kriterium for å benytte lagret datatrafikk. Har flere forbrytelser blitt avdekket og er flere kriminelle dømt på grunn av tilgang til trafikkdata?

Dersom datalagring gjennomføres i Norge, bør man også etter en gitt erfaringsperiode evaluere effekten av dette. Har politiet fått et bedre verktøy? Har flere forbrytere blitt pågrepet, er bevisene som datatrafikk gir effektive nok?

Trafikkdata kan som definert i denne høringen også være starten på å innhente data fra andre kilder, f eks GPS data fra biler, systematiske data fra ulike alarmsystemer, kassesystemer fra butikker og lignende.

#### *Konkurransen innenfor markedet*

Norge er et spesielt land med svært mange små bedrifter. Dette gjelder også for tilbydere. Dersom datalagring blir kostbart for tilbyderne kan noen velge å ikke tilby de ulike tjenestene i distriktene. Det er også viktig at kostnadsdekningen for land vi gjerne sammenligner oss med er tilnærmet lik. Allerede ser vi at Danmark, Finland og Norge legger til grunn ulike kostnadsmodeller for datalagringen. Dette mener NorSIS man bør forsøke å harmonisere. Kostnadene knyttet til f eks tilsyn og sikring av datalagring er også et element som ikke må glemmes og ikke nedprioriteres.

## 4.2 Forholdet til den europeiske menneskerettighetskonvensjonen (EMK)

Høringen beskriver at ”statene må ha en stor skjønnsmargin” Det er derfor viktig at man kan måle i hvilken grad man har brukt trafikkdata til å bekjempe kriminalitet. Dette bør hittil kunne måles i land som allerede har innført datalagringsplikt.

## 4.3 Kriminalitetsbekjempelse i en ny teknologisk hverdag

Teknologien er i svært rask utvikling og det er utfordrende å holde tritt på alle nivåer og på alle områder, f eks er det alltid vært en kamp mellom de kriminelle og politiet i forhold til metode og verktøy. NorSIS mener at kompetansehevende tiltak også må prioriteres for å følge med på denne utviklingen.

### 4.4.5 Ved e-post skal følgende data lagres

Ved e-post: Vil data om på- og avlogging være til nytte? Mange er alltid pålogget. Hvordan håndteres meldinger som sendes inne i sosiale medier, lukkede chatterom, og andre tjenester.

Om noen tjenester utelates, vil de kriminelle velge å benytte disse, og da er mye av hensikten bak direktivet borte.

### 4.4.7 Nærmere om innhold

Synkronisering eller ulikhet i klokker vil være en utfordring. Profesjonelle kriminelle vil trolig i stor grad benytte seg av tjenester som ikke har lagringsplikt om dette finnes og er mulig. Dette vil trolig redusere effekten av datalagringsplikten betydelig.

At tjenester er unntatt datalagring vil også kunne bety en vridning av bruk for hele befolkningen. Tjenester med krav til datalagring vil kunne øke i pris pga økte kostnader med lagring av trafikkdata, dvs forbrukeren vil måtte betale for trafikkdatalagring. Det er også fare for at forbrukeren vil benytte tjenester som anonymiserer eller krypterer dersom dette både er vesentlig billigere og at de ikke blir ”overvåket”.

## 4.6 Hvem skal lagre i henhold til lovforslaget

I Norge har vi mange svært små tilbydere av bredbånd. Datalagring vil medføre en relativt stor økonomisk og ressursmessig innsats for disse. Mange store virksomheter som tilbyr wlan til kunder eller gjester vil i mange tilfeller ha flere personer knyttet til sitt nett enn noen av de minste bredbåndstilbydere.

### 4.7.3 Mellomløsninger

I en sentral løsning vil det også måtte stilles strenge krav til sikkerhet, tilsyn m.v.

### 4.7.4 Avveining av ulike hensyn ved valg av lagringsløsning

NorSIS støtter at det ikke velges en sentral datalagringsløsning, slik at alle egg ikke havner i samme kurv. Når det er sagt, er noen av tilbydere så store at deres datalagring vil innbefatte svært store datamengder, med persondata. NorSIS poengterer igjen viktigheten av å sette krav til sikring av data, tilgangskontroll og tilsyn av at data slik at disse blir behandlet etter gjeldende lover og regler.

En felles løsning for de minste tilbydere kan gi økt sikkerhet, da svært små tilbydere kan mangle kompetanse og ressurser til å sikre data tilfredsstillende. En delt løsning mellom flere små tilbydere kan bidra til at dette gir sikrere løsninger.

#### **4.7.4.1 Lagringsstedets betydning for personvernet**

NorSIS er enig i at ulike formål for datalagring bør behandles deretter. Det bør stilles strenge krav til tilgangskontroll slik at tilbyderne ikke kan benytte data lagret i henhold til datalagringsdirektivet til eget bruk.

#### **4.7.4.2 Lagringsstedets betydning for informasjonssikkerhet**

NorSIS mener at et annet formål og flere data som er lagret over lengre tid bør kreve strengere tilsyn enn i dag. Datatilsynets ressurser er begrenset og tilsyn til omfattende lagring bør skje med jevne mellomrom, og ikke med for lange tidsintervaller. Det bør også reguleres strengere straffereaksjoner for de som ikke sørger for tilstrekkelig sikring av dataene eller ved hendelser der data kommer på avveie. Her er også formålet utenfor tilbyders behov, dvs. myndighetsoppnevnt behov, og dette vil kunne medføre at tilbydere ikke ser samme behov eller plikt til å sikre dataene.

NorSIS mener det er viktig å påpeke hvem som har ansvar for sikring av dataene og straffereaksjon ved brudd.

#### **4.7.4.3 Lagringsstedets betydning for uthenting av data**

NorSIS mener at myndighetene må sette krav til tilgjengelighet, sikker overføring og tidskrav av trafikkdata i de tilfeller data skal hentes ut. NorSIS mener at dersom datalagring iverksettes for dette formålet, må funksjonaliteten tilpasses behovet. NorSIS ønsker ikke å kommentere hvem som bør dekke kostnad med dette.

#### **4.7.4.5 Lagringsstedets betydning for konkurranse i ekommerket**

For enkelte tilbydere kan det være en gunstig løsning enten av økonomiske årsaker eller andre, at data blir lagret i andre land enn i Norge. NorSIS stiller spørsmål ved i hvilken grad man da kan føre tilsyn med at disse dataene da har tilstrekkelig sikkerhet. Mange andre land har heller ikke samme grad av lovgiving knyttet til personvern som Norge. NorSIS mener at det vil være utfordringer knyttet til å sette relevante og riktige krav til sikring, etterlevelse av disse kravene og tilstrekkelig tilsyn for å kontrollere at kravene er implementert.

### **4.8 Lagringstid**

NorSIS støtter departementenes oppfatning om at lagringstiden bør balansere hensyn til kriminalitetsbekjempelse og hensynet til personvern. NorSIS er av den oppfatning at man bør begynne med en restriktiv lagringstid, dvs minimumskrav. Andre lands erfaringer bør også legges til grunn ved beslutning om lagringstid. NorSIS mener at datalagringstiden heller bør justeres på sikt, enn å settes høyt i utgangspunktet. Høringens syn knyttet til negative konsekvenser for den frie meningsdannelse mener NorSIS vil kunne være faretruende dersom det oppstår hendelser knyttet til brudd på

intensjonene og formålet med direktivet; Data på avveie, misbruk av data til andre formål enten av tilbyder, politiet, andre myndigheter eller uvedkommende eller at politiet ikke oppnår den påståtte intensjonen med direktivet – å bekjempe kriminalitet. NorSIS støtter departementene syn på at like krav til lagringstid i de nordiske landene i utgangspunktet er hensiktsmessig. Imidlertid synes det ikke som om de nordiske landene så langt har et sammenfattet syn på datalagringstid. Vårt nærmeste naboland Sverige, har så langt ikke tatt beslutning om direktivet. NorSIS mener da at vi bør holde oss til minimum, seks måneder.

NorSIS mener det er formålet med tjenesten, dvs. trafikkdata til politiet i gitte saker, som skal ligge til grunn for å bestemme lagringstiden, og ikke i teknologi, dvs. det bør være lik lagringstid for samme behov og formål.

#### **4.9 Krav til lagring og levering av lagrede data**

NorSIS mener det er fornuftig med standardiserte løsninger og dataformater for å sikre korrekt forståelse av datainnholdet, dvs integritet. Dette vil også kunne gjøre at løsningene vil være mer effektive for behovet og i større grad vil tilfredsstille formålet og kunne gi effektive og raske data til politiet i de tilfeller dette gir grunnlag for uthenting.

#### **4.10 Tilsyn med lagringen**

NorSIS stiller spørsmål ved om en deling av tilsynet, kan medføre at noe kan falle mellom to stoler. F.eks. hvem fører tilsyn med at direktivets formål, nødvendighet og proporsjonalitet, bruk av overskuddsinformasjon blir overholdt.

##### **4.10.2 Tilsyn etter personopplysningsloven**

Så langt NorSIS er kjent med er det i liten grad benyttet overtredelsesgebyr og tvangsmulkt, eller at disse er av så lavt beløp at det er billigere å unndra seg ansvar. NorSIS stiller også spørsmål om det bør være spesielle krav til sikring av trafikkdata, utover det personopplysningsloven og dennes forskrift krever. NorSIS påpeker viktigheten av at det er tilstrekkelig kompetanse, uavhengighet og spesielt kapasitet for tilsynsjobben.

#### **4.11 Statistikk**

NorSIS er helt enige med departementene at det er viktig at det blir ført statistikk over, og at politiet og andre myndigheter som må føre statistikken. Direktivets formål er for disse, og de må derfor føre statistikken og på denne måten vise at direktivet et formålstjenlig. Det er viktig at statistikken inneholder data som sier noe om datoen på benyttet informasjon. Hvilken type straffesak som er løst eller belyst. Sannsynlighetsbetraktning vedrørende om dette kunne vært løst uten tilgang på trafikkdata bør også være en del av statistikken.

#### **4.12 Politiets adgang til data**

NorSIS er enig i at data kun skal gis de myndigheter, som beskrives i formålet. NorSIS mener også derfor at politi og påtalemyndighet skal ha tilgang til dataene. Det må kreves

god tilgangskontroll slik at dette sikres. Det må føres tilsyn med at tilgangen er i henhold til formålet.

NorSIS mener at dersom andre myndigheter skal gis tilgang må dette reguleres på forhånd, og tilgangskontroll må beskrives.

NorSIS mener det er viktig at data ikke kan benyttes i generelle hensyn verken ved forespørsel, eller når de er i politiets hender.

NorSIS mener at de nordiske land bør tilstrebe en likhet mht hvilken strafferamme som skall være grensen for å hente ut data. Både Sverige og Finland har strengere kriterium for strafferamme enn den norske anbefalingen. For øvrig er det vanskelig å si hva straffegrensen bør være, men den bør overholdes og ikke tøyes.

Når det gjelder ”særlige saker” mener NorSIS dette vil være et vanskelig begrep dersom dette knyttes til saker hvor f eks teknologi er hyppig benyttet i kommunikasjon eller at teknologi er brukt i stor grad. Dette vil i dag gjelde de aller fleste saker. NorSIS mener derfor at en opprømsing av typer saker bør gjøres i forkant. Det vil da være nødvendig med regelmessig gjennomgang og endring da teknologien endrer seg raskt.

NorSIS er enig med departementene om at kun retten skal kunne pålegge besitteren å utlevere data.

NorSIS mener at det er viktig at det også stilles strenge krav til sikring av trafikkdata som er i politiets hende. NorSIS mener det er viktig at datamengden reduseres, og tilsvarende at overskuddsinformasjon til politiet blir minst mulig.

#### **4.13 Andre myndigheters tilgang til data**

NorSIS mener at det beste er om all tilgang til trafikkdata skjer gjennom politiet.

### **6 Administrative og økonomiske konsekvenser**

Departementene forslår at kostnader ved datalagring tillegges tilbyderne. Dette vil indirekte bli en kostnad for forbrukerne.

NorSIS mener at kostnadsmodellene bør forsøkes å være likt i de nordiske land, som tilbyderne i størst grad konkurrerer med.

Høringsnotatet beskriver løsninger og kostnader vurdert av Teleplan fra 2007. Når det gjelder kostnader for f eks datalagring og også teknologiske løsninger mener NorSIS at dette kan ha forandret seg noe siden denne rapporten ble utarbeidet.

NorSIS mener det er viktig at krav til løsning er konkret og spesifikk beskrevet, dvs at det er standardiserte data- og filformater.

Det må settes krav til konfidensialitet, integritet, tilgjengelighet og driftsstabilitet.

Datalagringsdirektivet er omdiskutert med tanke på å sikre personvernet, NorSIS mener derfor det er vesentlig at Datatilsynet får økte og dedikerte ressurser, slik at de kan prioritere tilsyn av at trafikkdata er tilstrekkelig sikret og at tilbyderne sørger for å sikre persondata. Dette tilsynet må heller ikke gå ut over Datatilsynet oppgaver med tilsyn i andre bransjer som behandler personopplysninger. Datatilsynet må også få nødvendige sanksjonsmuligheter for å kunne straffe de som ikke overholder sikring av personopplysninger.

## Konklusjon

NorSIS ønsker at man i forkant av en behandling av innlemmelsen av DLD i EØS avtalen får en oversikt fra land som har implementert DLD på effekten av tiltaket. Gir DLD de ønskede effekter? Dette er etter vår mening ikke godt nok beskrevet i høringsdokumentet.

Hvis DLD blir innlemmet i EØS avtalen er det i vår høringsuttalelse beskrevet forslag og tiltak som er av vesentlig betydning for en nødvendig sikring av trafikkdata, god tilgangskontroll samt momenter vedrørende tilsyn og forhold knyttet til personvern.

Med vennlig hilsen



Tore Larsen Orderløkken  
Administrerende direktør  
NorSIS