Fornyings-, administrasjons- og kirkedepartementet
Postboks 8004 Dep
0030 Oslo

Oslo, 10. oktober 2012

Sendt per e-post til: postmottak@fad.dep.no

# HØRINGSSVAR - UTKAST TIL ENDRINGER I PERSONVERNFORSKRIFTEN § 7-1

## 1. Bakgrunn

Tele2 Norge AS (**Tele2 Norge**) og Network Norway AS (**Network Norway**) viser til e-post fra Fornyings-, administrasjons- og kirkedepartementet (FAD) 26. juni 2012 vedrørende endringer i § 7-1 i personvernforskriften. Tele2 og Network Norway ønsker med dette å kommentere forslaget til endringer i § 7-1 i personvernforskriften.

Som kjent kjøpte Tele2 Sverige AB (**Tele2**) Network Norway med datterselskap i 2011. Det innebærer at Tele2s norske virksomhet nå omfatter Network Norway AS, Mobile Norway AS og Tele2 Norge. Dette høringsinnspillet er å anse som et innspill på vegne av hele Tele2s norske virksomhet.

## 2. Nærmere om Tele2 Norges virksomhet

Tele2 Norge og Network Norway er i eiet av Tele2 AB, et selskap med ca. 32 millioner kunder i flere land. Omsetningen var i 2010 på SEK 40.2 milliarder med en EBITDA på SEK 10.3 milliarder.

Tele2s kjøp av Network Norway er et industrielt viktig kjøp. Norge får en tredje aktør med 15-17 % markedsandel. Selskapets investering i Norge er langsiktig. Målet på sikt er å bli Norges nest største mobiloperatør.

Etter kjøpet har Tele2 AB utpekt Norge som ett prioriterte satsningsland hvor selskapet skal bygge og eie sin egen nasjonale infrastruktur som grunnlag for mobilvirksomheten.

Tele2 AB er en dedikert industriell aktør med tilgang til kapital, som vil sikre utbyggingen av det tredje mobilnettet. Selskapet har som ambisjon å bygge et landsdekkende mobilnett i

Norge. Den viktigste forutsetningen for å lykkes er markedstilpassede, stabile og forutsigbare rammebetingelsene.

## 3. Kommentarer til forskriftsforslaget

### *3.1 Overordnete kommentarer*

Datatilsynets har publisert et detaljert forslag til konsesjon som har blitt hørt i bransjen. Tele2 Norge og Network Norway kommenterte 25. april 2012 på sentrale punkter i det reviderte utkastet, herunder på valg av krypteringsmekanisme, sikkerhetsnivå mv. Våre innspill er også relevante for utformingen av ny § 7-1 i personvernforskriften. Selskapene vil derfor som et utgangspunkt vise til våre kommentarer i dette dokumentet (vedlagt). Tele2 Norge og Network Norway vil likevel fremheve enkelte forhold som har særlig betydning for forskriftsutkastet.

### *3.2 Sikkerhetsnivået bør kobles til hvor sensitiv informasjonen er, ikke mengden data*

I tilknytning til FADs vurdering av kryptering uttaler FAD på side 3 i høringsnotatet

> "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." (Vår understrekning)

På side 4 fremgår det:

> "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."

Tele2 Norge og Network Norway ber departementet om å presisere samt å klargjøre disse uttalelsene.

Selskapene vil peke på at data som omfattes av den lovpålagte lagringsplikten er svært sensitiv i sin natur. Selv mindre tilbydere vil oppbevare opplysninger om mange tusen kunder. Et sikkerhetsbrudd hos en mindre aktør vil dermed raskt få like store konsekvenser som hos en større aktør. Med unntak av Telenor som lagrer data om anslagsvis 50 % av alle sluttbrukerne i Norge er det dessuten vanskelig å avgjøre hva som kvalifiserer til en "stor mengde opplysninger". Sikter man med dette for eksempel til et høyt antall MB eller at det er snakk om opplysninger om en "stor mengde" sluttbrukere? Tele2 Norge og Network Norway vil i denne forbindelse peke på at mengden opplysninger varierer med hva slags tjeneste det er snakk om.

Datatilsynets siste utkast til konsesjon legger opp til at samtlige tilbydere pålegges strenge krav til lagring. Forutsatt at forskriften åpner for å skjerpe pliktene ytterligere ber Tele2 Norge og Network Norway om at FAD presiserer hva slags tiltak det er snakk om og gjør en vurdering av om dette er hensiktsmessig. Selskapene vil i denne forbindelse advare mot å åpne for vilkår som er så strenge at det ikke er mulig for aktørene å oppfylle dem teknisk eller på grunnlag av kostnadene. Dette vil hindre effektiv lagring av de opplysningene som er nødvendig for å fremme kriminalitetsbekjempelse. Tele2 Norge og Network Norway ber også om at FAD ikke legger opp til å lette på kravene til sikring av data utelukkende fordi en liten aktør lagrer mindre opplysninger enn en stor. Utover den økte risikoen for sikkerhetsbrudd vil dette kunne være konkurransevridende.

Når det gjelder sitatet på side 4 antar Tele2 Norge og Network Norway at FAD sammenlikner krypteringsbehovet ved en samlet database med mindre databaser, ikke basestasjoner. Mobilaktørene lagrer ikke trafikkinformasjon og liknende i basestasjonene. Dataene blir dessuten først lagringspliktige og dermed omfattet av lagringsplikten når samles i form av Call Detail Records (CDR) i en eller flere sentrale databaser i nettet.

### *3.3 Forholdsmessighet og vektlegging av kostnadene ved tiltaket*

På side 3 i høringsnotatet gir FAD veiledning når det gjelder proporsjonalitet og Datatilsynets valg mellom ulike tiltak:

> "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.
>
> [...]
>
> Dersom personvernet kan ivaretas tilfredsstillende ved flere forskjellige alternative krypteringsmåter, skal Datatilsynet pålegge det minst kostbare tiltaket for den lagringspliktige og staten."

Tele2 Norge og Network Norway er enig i denne innfallsvinkelen. Selskapene er ikke kjent med om Datatilsynet gjorde noen kost-nytte vurdering av mulige alternative krav under utformingen av konsesjonen. Vi legger til grunn at dette blir gjort før endelig vedtagelse.

### *3.4 Utformingen av omfanget av krypteringen*

FAD beskriver på side 3 i høringsnotatet det foreslåtte omfanget av krypteringen:

> "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."

Tele2 Norge og Network Norway mener i likhet med FAD at det kan være hensiktsmessig å presisere omfanget av krypteringen direkte i forskriften. Selskapene vil samtidig advare mot at denne hjemmelen benyttes til å pålegge konkrete sikkerhetsløsninger heller enn å foreskrive et ønske sikkerhetsnivå. Det er allerede komplisert å etablere gode lagringsløsninger basert på forslaget til datalagringsforskrift og utkastet til konsesjon.

Dersom Datatilsynet på bakgrunn av denne hjemmelen regulerer omfanget av lagringen i for store detalj, vil dette i praksis forsinke gjennomføringen av datalagringsdirektivet fordi konsesjonsvilkårene gjør det teknisk umulig eller for kostnadskrevende å etablere den nødvendige løsningen. Dette er for eksempel aktuelt dersom Datatilsynet stiller ytterligere krav til lokalisering utover det som allerede fremgår av utkastet til konsesjon. Tele2 Norge og Network Norway vil her spesielt peke på at forskriften ikke må åpne for krav som forhindrer aktørene i å etablere felles lagringsløsninger, se punkt 3.6 under. Selskapene stiller for øvrig spørsmål ved hvilke sikkerhetsmessig gevinst konkrete vilkår knyttet til lagringssted vil gi.

Tele2 Norge og Network Norway ber om at departementet klargjør disse spørsmålene og om nødvendig endrer forskriftsforslaget. Selskapene vil i denne forbindelse peke på de føringer departementet peker på i tilknytning til kravet om lukket lagring:

> "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."

### *3.5 Nærmere om håndtering av innsynsretten og bruk av personnummer*

På side 4 i høringsnotatet peker FAD på at vilkårene for kryptering må være kompatible med andre rettigheter:

> "Det må videre sikres at vilkårene for kryptering er kompatible med andre rettigheter, slik som retten til innsyn i egne opplysninger, retten til å kreve retting og retten til å bli informert."

Departementet problematiserer ikke innsynsretten andre steder i høringsnotatet.

Tele2 Norge og Network Norway har ved flere anledninger tatt opp med Datatilsynet at gjennomføringen av datalagringsdirektivet aktualiserer en rekke nye utfordringer på dette punktet.

Frem til i dag har aktørene oppbevart de opplysningene som er påkrevet for å produsere tjenesten samt å administrere og fakturere kunden midlertidig. Når lovendringen trer i kraft vil tilbyderne måtte systematisere og lagre en stor mengde sensitive opplysninger i seks måneder. De negative konsekvensene av å gi ut DLD-data til feil person vil være omfattende. Regelverket tar samtidig ikke høyde for denne utviklingen. Dagens konsesjon for teletilbydere tillater for eksempel ikke at operatørene lagrer fødselsnummer etter at kundeforholdet er opprettet. Ettersom dette er den eneste entydige form for identifikasjon av en enkeltperson oppstår det dermed en risiko for at data registreres på eller utleveres til feil individ.

Tele2 Norge og Network Norway ber på bakgrunn av dette for det første FAD om å åpne for at operatørene tillates å lagre og behandle fødselsnummer for sine sluttbrukere. I motsetning til det som har vært situasjonen tidligere har operatørene nå et saklig behov for sikker identifisering av at den som ber om innsyn i realiteten også er den registrerte. Både operatører og politiet har dessuten behov for å vite at trafikkdata mv. registreres på riktig person når dataene lagres. Tele2 Norge og Network Norway er ikke kjent med at det finnes alternative identifikatorer eller andre metoder som vil gi et like sikkert resultat.[1]

For det annet vil det i mange tilfeller vil være vanskelig å si hvem som regnes som "den registrerte" i personopplysningslovens forstand. Samtidig vil Tele2 Norge og Network Norway peke på at tilsynet fortsatt ikke ønsker å gi veiledning på om hvem som regnes som "den registrerte" hos den enkelte tilbyder. Bruk av Venner&Familie -abonnement, trådløs bedrift og liknende løsninger innebærer at den som er registrert som abonnent/kunde (en bedrift eller enkeltperson i en familie) vil kunne kreve å få tilgang til all data registrert på abonnementet. Dersom tilbyderne oppbevarer informasjon om bruker i tillegg til abonnent, vil slikt innsyn også omfatte brukerens data. I praksis vil for eksempel arbeidsgiver (abonnent) kunne kreve å se hvem de enkelte ansatte (brukerne) har ringt til og når.

---

[1] Sammenstilling av alle andre identifikatorer slik som navn, adresse, fødselsdato mv. vil i beste redusere risikoen for feilidentifisering til ca. 10 %.

Tele2 Norge og Network Norway vil på bakgrunn av dette be om at FAD tar stilling til denne problemstillingen, eksempelvis ved å gi presis veiledning med tanke på hvem som regnes som registrert eller unnta visse grupper fra innsynsretten med hjemmel i unntaksbestemmelsene i personopplysningsloven § 23 første ledd.

### *3.6 Regelverket må åpne for felles lagringsløsninger*

Både kostnadsutvalget, lovgiver, Post- og teletilsynet og Datatilsynet har påpekt at kostnadene ved å innfri krav til lagring og sikring av data trolig blir høye. Det er foreløpig ikke avgjort hvem som skal betale for investeringer i nytt utstyr samt drift og sikring.

Tele2 Norge og Network Norway har begynt arbeidet med å anslå de økonomiske konsekvensene. Foreløpige beregninger viser at investeringer i nødvendig programvare med tilhørende system for kryptering alene vil koste mange millioner. Selv om deler av utgiftene er operatørspesifikke (kartlegging av egne system mv.) vil aktørene kunne oppnå store besparelser ved å samarbeide om blant annet innkjøp og drift av et felles system. Dette vil foruten bedre beredskap og økt kvalitet på personell gjøre det mulig for mindre aktører å ta kostnaden ved å tilfredsstille de lovpålagte kravene.

Tele2 Norge og Network Norway har sammen med IKT Norge nå tatt initiativ til å undersøke felles lagringsløsninger. Prosjektet ligger nå hos NRDB som er i gang med å utrede regulatoriske, tekniske og økonomiske sider ved et slikt samarbeid.

Tele2 Norge og Network Norway opptatt av at personvernforskriften og konsesjonen ikke reduserer tilbydernes handlingsrom når det gjelder å etablere hensiktsmessige felles lagringsløsning. Selskapene ber derfor om at FAD ikke vedtar krav som er til hindre for dette.

### *3.7 Datatilsynet bør ha kompetanse til å fastsette standardiserte konsesjonskrav*

I FADs utkast til forskriftstekst fremgår det:

> "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." (Vår understrekning)

Datatilsynet legger i dag opp til at en standard konsesjon med beskrivelse av en rekke konkrete sikkerhetsmål. Aktørene må på bakgrunn av dette gjøre en vurdering av hvordan deres virksomhet best kan oppfylle kravene. Tele2 Norge og Network Norway mener dette er en fleksibel fremgangsmåte som legger til rette for tilfredsstillende sikkerhet samtidig som det til aktørene handlingsrom til å finne gode tekniske løsninger. Forslaget til ny forskrift gir inntrykk for at Datatilsynet må gå bort fra denne ordningen og i stedet fastsette individuelle krav til kryptering i "den enkelte konsesjon".

Tele2 Norge og Network Norway mener dette er lite hensiktsmessig og ber om at departementet fjerner denne presiseringen slik at Datatilsynet fastsetter omfanget i "konsesjon". For det første vil individuell behandling av konsesjon for mer enn 150 tilbydere ta lang tid og kreve ressurser hos både aktører og myndigheter. For det annet vil en slik fremgangsmåte kunne gjøre det vanskelig å etablere felles lagringsløsninger ettersom Datatilsynet kan tenkes å pålegge ulike aktører ulike krav. Individuell tilpassing vil for det tredje være konkurransevridende.

## 4. Avslutning

Om ønskelig stiller Tele2 Norge og Network Norway gjerne til møte med departementet for å gjennomgå innspillene knyttet til felles lagringsløsning samt problematikken knyttet til innsyn.

Eventuelle spørsmål kan for øvrig også rettes til undertegnede

Med vennlig hilsen
Tele2 Norge AS

Frode Lillebakken
Juridisk direktør