

Samferdselsdepartementet
Postboks 8010 Dep
0030 Oslo

Vår dato
24.03.2017

Vår referanse

Deres dato
02.03.2017

Deres referanse
17/482

Vår saksbehandler
Henriette Holt-Francati

EU-kommisjonens forslag til ny kommunikasjonsvernforordning

EU-kommisjonen offentliggjorde den 10. januar 2017 et forslag til ny kommunikasjonsvernforordning (COM(2017) 10 final), som skal erstatte dagens kommunikasjonsverndirektiv (2002/58/EC). 2. mars inviterte Samferdselsdepartementet til å gi innspill til *'dei foreslåtte endringane, til andre element høyringsinstansane er opptekne av, eller til forordninga som heilheit, inkludert økonomiske og administrative konsekvensar som følgje av deler av eller heile forordninga.'*

Dette høringssvaret oppsummerer Telenor Norges synspunkter på EU-kommisjonens forslag til ny kommunikasjonsvernforordning.

Revisjonen av EUs regelverk for person- og kommunikasjonsvern har pågått over flere år, og Telenor Norges innspill til prosessen har primært skjedd gjennom Telenor Group og europeiske bransjeorganisasjoner bidrag direkte inn i EU-lovgivningsprosessene, jvf. tidligere oversendte posisjonspapirer og høringssvar. Telenor Norges bidrag til EU-kommisjonens utkast til ny kommunikasjonsvernforordning er utformet i tråd med Telenor Groups og ETNOs posisjonspapirer, som begge vedlegges til orientering. Nedenfor gis en oppsummering av hovedbudskapene i disse satt inn i en norsk kontekst.

Utilstrekkelig regelverksforenkling og hindring av konkurranse på like vilkår

Generelt støtter Telenor harmonisert regulering av ekomsektoren på tvers av EU/EØS, og anser i så måte at regulering av kommunikasjonsvern i form av en forordning normalt er et hensiktsmessig lovgivningstiltak. Telenor mener samtidig at det hadde vært en vesentlig mer fremsynt løsning å avvike dagens sektorspesifikke kommunikasjonsverndirektiv i sin helhet og i stedet samle all regulering av personvern – inkl. taushetsbeskyttelse av kommunikasjon – i ett generelt regelverk (GDPR), underlagt ett tilsyn.

Den foreslåtte kommunikasjonsvernforordningen vil utvide særreguleringen av elektroniske kommunikasjonstjenester til å gjelde alle former for person-til-person kommunikasjon, inkl. OTT-produserte meldingstjenester, webbasert e-post og VoIP. Dette er isolert sett et bra forslag, forutsatt at lovgiver mener at det er nødvendig å videreføre særregulering av ekomområdet.

Telenor mener imidlertid at EU/EØS forspiller en viktig mulighet til regelverksforenkling ved å videreføre denne særreguleringen: Elektroniske kommunikasjonsnett og -tjenester realiseres i stadig

større grad basert på generisk informasjonsteknologi og internett frem for dedikert telekommunikasjonsteknologi. Det gir derfor lite mening å videreføre særregulering av akkurat de offentlige nett og tjenester som bærer person-til-person-kommunikasjon, men ikke andre sammenlignbare digitale plattformer og tjenester (f.eks. app'er) som formidler tilsvarende beskyttelsesverdige personopplysninger. Dette vil gi en rekke uheldige virkninger i forhold til konkurranse, kostnader og investeringer, f.eks. oppnår globale digitale plattformaktører som GAFA en rekke fordeler både knyttet til kundedialog og compliance-relatert ressursbruk sammenholdt med ekomtilbyderne. Under det foreslåtte regelverket vil f.eks. lokasjonsopplysninger, som kan knyttes til en person, bli regulert av ulike forordninger avhengig av om opplysningene genereres av en pulsklokke (GDPR) eller en mobiltelefon (kommunikasjonsvernforordningen). Dette vil for en vanlig bruker fremstå som ulogisk – særlig hvis selvsamme pulsklokke også kan brukes til å sende meldinger, sjekke e-mailen og foreta anrop.

I takt med økt digitalisering av samfunnet integreres i tillegg (særregulerte) elektroniske kommunikasjonstjenester stadig tettere med andre former for elektroniske nett, tjenester og funksjonalitet som ikke lar seg definere som person-til-person-kommunikasjon. Slike 'smarte' tjenester produseres og distribueres dessuten stadig oftere gjennom ulike former for samarbeid mellom flere leverandører – noe som vil gjøre det enda mer upraktisk, komplekst og kostbart for alle parter – inkl. regulerende myndigheter – å måtte forholde seg til ulike regelsett. Særreguleringen står dermed i veien for nyskapende digitale tjenester og samhandlingsbasert innovasjon. Dette er dårlig nytt for norsk og europeisk næringsliv generelt, og for ekomtilbydere spesielt, men også for potensielle kunder av innovative digitale løsninger som kanskje aldri blir utviklet innenfor EU/EØS, eller som må utvikles med mindre brukervennlig funksjonalitet og større kostnad (f.eks. under forutsetning av store antall samtykker som må fornyes halvårlig) pga. særkravene i kommunikasjonsvernforordningen.

Med GDPR vedtaket implementeres i disse dager modernisert, felleseuropeisk regulering av personvernområdet på tvers av alle sektorer for å etablere likeverdige rammer for beskyttelse av personopplysninger og brukernes rettigheter til nytte for så vel innbyggere som næringsliv i EU/EØS. I lys av GDPRs grundige tilblivelsesprosess og brede omfang, formål og anvendelsesområde har Telenor vanskelig for å se nødvendigheten av å videreføre sektorspesifikke regler vedrørende personopplysninger (metadata og innhold) knyttet til elektroniske kommunikasjonsnett og -tjenester – men uten den tilsvarende muligheten til å utøve fleksibilitet i lovanvendelsen, som er innebygget i GDPR, for nettopp å sikre digital innovasjon.

Med utsikten til at ny kommunikasjonsvernforordningen skal tre i kraft samtidig med GDPR allerede i mai 2018 erkjenner Telenor at det antakelig neppe er realistisk å gjennomføre den ønskede regelverksforenklingen innen person- og kommunikasjonsvern, slik vi hittil har argumentert for overfor så vel europeiske som norske myndigheter.

Gitt at videre lovgivning på området vil skje med utgangspunkt i EU-kommisjonens forslag til kommunikasjonsvernforordning, viser vi til Telenor Groups og ETNOs høringssvar for detaljerte innspill til hvilke endringer som i så fall bør gjennomføres i forordningsforslaget. Hensikten med disse innspillene er i størst mulig grad å redusere negative effekter av videre særregulering av ekomnett og -tjenester. Målet bør være å bringe kommunikasjonsvernforordningen mest mulig i samsvar med GDPR, slik at denne kun avviker fra GDPR på punkter som anses som absolutt nødvendige og forholdsmessige. Oppsummert anses følgende grep som helt nødvendige:

However, the proposed ePrivacy Regulation does not foresee the desired alignment with the GDPR in terms of recognition of **additional legal grounds for processing e-communications metadata**.

- Therefore, ETNO calls for EU Legislators to include in the future ePrivacy Regulation **“legitimate interest” as a legal basis for processing metadata** in line with GDPR.
- In addition, the future ePrivacy Regulation should also recognize, in line with GDPR, the right to further process metadata for other purposes **compatible with the initial purposes** for which the data was initially collected, provided that appropriate safeguards like **pseudonymisation** are put in place.

These principles are essential to ensure a level playing field in data protection, to encourage innovation in big data and to enable responsible e-communications providers to provide trusted and secure innovative data driven services in an accountable manner.

Hindrer europeiske telekomaktører i å delta i samfunnsnyttig stordataanalyse

Enhver behandling av personopplysninger må være formålsstyrt og ha et legalt grunnlag. Som redegjort for i ETNOs høringssvar er den største utfordringen med EU-kommisjonens forslag til kommunikasjonsvernforordning at denne mangler GDPRs fleksibilitetsmekanismer som skal sikre en balansert interesse- og rettighetsavveining mellom henholdsvis *den registrerte* (data subject), *behandlingsansvarlig* (data controller) og *databehandler* (data processor) ved behandling av personopplysninger. GDPR legger i så måte til rette for at både personvern og innovasjon tilgodeses. I den forbindelse er det naturlig å vise til EU Commission Communication ‘*Building a European Data Economy*’ som peker ut den veien EU ønsker å gå med tanke på å benytte de muligheter bl.a. stordata åpner for, samt EU Commission Communication ‘*Exchanging and Protecting Personal Data in a Globalised World*’ hvor det fremheves at slik innhenting, benyttelse og flyt av data må skje innenfor EUs sterke personvern.

I kommunikasjonsvernforordningen er det kun pekt på samtykke fra bruker som det eneste legale grunnlaget for å behandle personopplysninger i form av metadata og innhold knyttet til ekomnett og -tjenester til alle formål som faller utenfor produksjon og leveranse av selve ekomnettet eller ekomtjenesten. Listen over lovlige formål er i tillegg konkret og uttømmende – dvs. alt annet enn fleksibel og fremtidssikret.

I sin nåværende form vil den praktiske konsekvensen av forslaget bli at europeiske ekomtilbydere i fremtiden stilles konkurransemessig vesentlig dårligere enn aktører, som kun omfattes av den generelle personvernforordningen, GDPR, når det gjelder muligheten til å utnytte tilsvarende data både kommersielt og til gagn for storsamfunnet. Dette står i skarp kontrast til EU-kommisjonens egen målsetning om å legge til rette for fremveksten av en sterk datadrevet europeisk økonomi, jf. igjen f.eks. *Communication on Building a European Data Economy*, hvor hovedforslaget er at den videre vei er å forenkle, redusere og likebehandle med målsetning om å sette næringsvirksomheter i EU/EØS i stand til å ta opp konkurransen med næringsvirksomheter i USA og Asia.

I forordet til publikasjonen Status Teknologi Norge¹, som Telenor presenterte 31. januar i år på MESH i Oslo med bl.a. Statsminister Erna Solberg til stede, skriver Berit Svendsen:

¹ <https://www.telenor.no/om/teknologi-norge/>

‘Til tross for store endringer i samfunnet, står tilliten, likeverdet og felleskapstanken støtt. Disse kulturelle verdiene tjener til godt utgangspunkt for å mestre det den digitale agendaen krever: Fangst og forvaltning av nyttige data, i store mengder og umiddelbart tilgjengelig.’

Samme publikasjon inneholder også en beskrivelse av Telenors forskning og satsing innen stordataområdet *mobilty analytics*², dvs. analyse av bevegelsesmønstre:

‘Som mobiloperatør ser vi hvilken basestasjon mobilen er koblet opp mot. Når mobilen så kobler seg opp til en ny basestasjon vet man at det har skjedd en forflytning mellom områdene som dekkes av disse to basestasjonene. Ved å telle totalt antall forflytninger, så kan man estimere hvordan folkemengder beveger seg i geografien. Det har vist seg at disse bevegelsesmønstrene har stor anvendelsesverdi innenfor mange områder’

Telenor frykter at denne typen ekombasert stordataanalyse av bl.a. bevegelsesmønstre ikke lenger vil være mulig under ny kommunikasjonsvernforordning, når bruk av slike data vil være avhengig av å innhente gyldig samtykke fra hver enkelt bruker. Dette vil ikke bare være uheldig for Telenor, men for hele det norske samfunnet som vil kunne gå glipp av uvurderlig innsikt og verdi for de områdene vi kan underbygge, herunder transport, turisme, helse og smittevern. Alternativet vil være at utvikling og nyttiggjøring av slike nyvinninger legges andre steder enn i Norge.

Ved innsamling av stordata er ikke bare kvaliteten på dataene viktig men også tidspunktet for når innsamling av data er utført. Det er viktig å ha en forståelse for at man ikke alltid vet hva man trenger av innsikt i fremtiden. Mye av det som har med innsikt å gjøre er målinger, ofte over tid, hvorpå man ønsker historiske data å måle opp i mot. Da må man kunne lagre data før man kjenner til hva bruksområdet er, men selvsagt samtidig ivareta personvernet. Her vil sikkerhetsteknikker som pseudonymisering av data, som GDPR åpner opp for, men som altså ny kommunikasjonsvernforordning utelukker, kunne være en løsning som trygger person- og kommunikasjonsvernet samtidig som det blir mulig å gjennomføre stordataanalyse.

Ekomtilbyderne i Europa behandler gjennom sine nett og tjenester daglig store mengder personopplysninger, og nettopp derfor har bransjen historisk sett betydelig erfaring med og fokus på sikkerhet og lovlig behandling av alle slags kundeopplysninger. Som det vil være kjent for norske myndigheter tar Telenor Norge beskyttelse av innhold og kundeopplysninger på største alvor og strekker seg langt for å verne om kundenes rettigheter og integritet uten å forsvare lovbrudd.

Kommunikasjonsvernet er ikke bare et grunnleggende prinsipp i Telenors forretningsvirksomhet, men følger også av både Grunnloven, og Den Europeiske Menneskerettighetskonvensjon. Telenor anerkjenner og støtter viktigheten av å verne privatlivets fred herunder innhold og metadata knyttet til våre kunders elektroniske kommunikasjon. Dette gjelder uansett om kundene er fysiske eller juridiske personer.

Som forvalter av samfunnskritisk infrastruktur er mange europeiske ekomtilbydere underlagt omfattende krav innen sikkerhet og beredskap. Etterlevelse av dette regelverket er både krevende og kostbart, men samtidig nødvendig for å sikre samfunnet og tilliten til våre tjenester – også i forhold til kommunikasjons- og personvern. Gitt dette utgangspunktet fremstår det som lite gjennomtenkt å frata nasjonale og europeiske ekomtilbydere muligheten til å utnytte godt sikrede ekomnett og -

² <https://www.telenor.no/om/teknologi-norge/stordata-samfunnet.jsp>

tjenester til også å tilby nye digitale tjenester i konkurranse med globale internetbaserte tilbydere uten tilsvarende erfaring med etterlevelse av lovpålagte sikkerhetskrav.

I motsetning til EU-kommisjonens erklærte mål om å styrke Europas aktive deltakelse i den globale digitale økonomi fremstår foreliggende forslag til kommunikasjonsvernforordning som et hinder for at tilbydere som Telenor kan utnytte sitt potensial som et viktig både ansvarlig og markedsbasert korrektiv til globale nettgiganter.

Klar ansvarsfordeling og effektivt tilsyn

Ansvar for administrasjon av eksisterende sektorspesifikke og generelle regler om person- og kommunikasjonsvern er i dag delt mellom Datatilsynet, Nasjonal kommunikasjonsmyndighet og Forbrukerombudet, jf. at kommunikasjonsverndirektivet i Norge er implementert gjennom ekomlov og -forskrift, personopplysningslov, -forskrift og konsesjon samt markedsføringsloven. Denne oppdelingen er til dels overlappende og ikke helt skarpt definert, noe som til tider medfører uklarhet for ekomtilbydere i relasjon til sammenhengen mellom ulikt regelverk, tilbydernes forpliktelser og myndighetenes roller og beføyelser. Et eksempel kan være utfordringene forbundet med nødetatens sterke ønske om innføring av Googles AML løsning for ytterligere forbedring av lokalisering av nødtilte.

Telenor noterer seg at tilsyn med reglene i kommunikasjonsvernforordningen foreslås overlatt til de nasjonale datatilsynsmyndigheter – i Norge: Datatilsynet.

Telenor støtter at det skjer en forenkling og fremtidsretting i administrasjonen av lovgivningen relatert til person- og kommunikasjonsvern (*ePrivacy*) og gjerne en reduksjon i antallet av myndigheter, som har en rolle på dette området. Det viktigste for et effektivt og velfungerende tilsyn er likevel at den, eller de, myndigheter som skal forvalte to så krevende og potensielt overlappende regelverk som GDPR og kommunikasjonsvernforordningen, besitter både tilstrekkelig juridisk og IT/telefaglig spisskompetanse. Hvis oppfølging av så vel GDPR og kommunikasjonsvernforordningen samles hos Datatilsynet, slik EU-kommisjonens forslag legger opp til, bør det vurderes om kompetansen og erfaringen som er oppbygget i Nkom innen forvaltning av kommunikasjonsvern evt. bør overføres til Datatilsynet.

Med hilsen
Telenor Norge AS



Siri Kalager,
Regulatorisk direktør

Vedlegg:

- ETNO's views on the Proposal for an ePrivacy Regulation
- Telenor Group: The new e-Privacy instrument – Finding the right balance between data protection and innovation.