

KOMMUNAL- OG MODERNISERINGS-
DEPARTEMENTET
Postboks 8112 DEP
0032 OSLO

Deres referanse
21/3980-2

Vår referanse
21/02527-2

Dato
15.10.2021

Høringssvar - Forslag til ny ekomlov, ny ekomforskrift og endringer i nummerforskriften

Vi viser til Kommunal- og moderniseringsdepartementets høringsbrev av 2. juli 2021 vedrørende høring om forslag til ny ekomlov, ny ekomforskrift og endringer i nummerforskriften, samt vedlagte høringsnotat.

Innledende bemerkninger

Forslagene skal blant annet gjennomføre EUs ekomdirektiv (2018/1972), forordningen om BERIC (2018/1971), deler av tilgjengelighetsdirektivet (2019/882) og flere andre EU-rettsakter som er innlemmet i EØS-avtalen.

Datatilsynet har sammen med Forbrukertilsynet levert et felles høringssvar knyttet til forslaget til regulering av bruk av informasjonskapsler i den nye ekomloven § 3-7. Dette høringssvaret gjelder de øvrige delene av forslaget.

Mange av pliktene i ekomloven angår behandling av personopplysninger, og har betydelige konsekvenser for personvernet. Ekomregelverket henger derfor tett sammen med personvernregelverket som Datatilsynet fører tilsyn med. Datatilsynet har jevnlig kontakt- og saksbehandlingsmøter med Nasjonal kommunikasjonsmyndighet (Nkom) vedrørende de områdene der regelverkene våre grenser mot hverandre eller overlapper.

Oppsummert vurderer Datatilsynet at flere av forslagene viderefører bestemmelser fra gjeldende ekomlov som er uklare og problematiske, uten å bidra til å klargjøre rettstilstanden. Disse uklarhetene har personvernkonsekvenser som etter vårt syn ikke er godt nok vurdert i høringsnotatet.

Når det gjelder forslagens bestemmelser om lagring og utlevering av IP-adresser, vurderer vi at disse er i strid med kommunikasjonsvernet og siste praksis fra EU-domstolen. Personvernkonsekvensene ved forslagene ikke er godt nok vurdert. Dette har vi tidligere

redegjort for i egen høringsuttalelse 18. januar 2021 til forslaget om endringer i ekomloven, (lagring av IP-adresser mv.), og vi viser til dette høringssvaret. Departements referanse er 20/3645-1.

I det følgende vil vi redegjøre for våre innspill.

Datatilsynets kommentarer

Høringsnotatets punkt 3.2 – Formidling av viktig melding – Forslagets ekomlov § 3-10

Forslaget innebærer at plikten til å formidle viktig melding fra statsmyndighet i gjeldende ekomlov § 2-10, videreføres i ny ekomlov § 3-10. Departementet vil komme tilbake med nærmere forslag til forskriftsbestemmelse på et senere tidspunkt.

Datatilsynet har det siste året undersøkt lokasjonsbasert SMS-varsling, som i økende grad ble tatt i bruk under pandemien.¹ Med lokasjonsbasert SMS-varsling mener vi tjenester for befolkningsvarsling hvor offentlige myndigheter gjennom teleoperatørene sender ut SMS til alle som befinner seg i et bestemt geografisk område som myndigheten definerer. Dette skiller seg fra andre former for SMS-varsling som er basert på registrert adresse eller øvrige opplysninger. Datatilsynet har mottatt flere klager på bruk av disse tjenestene, og vi mottar også spørsmål fra offentlige myndigheter som lurer på om lokasjonsbasert SMS-varsling er lov å ta i bruk.

Hensikten med undersøkelsene har vært å få klarhet i hvordan disse varslingstjenestene behandler personopplysninger, hvordan ansvaret er fordelt mellom de involverte partene, og hvordan de registrertes rettigheter ivaretas. Disse tjenestene reguleres av både ekomregelverket og personvernregelverket, og Datatilsynet har derfor hatt dialog med Nkom i forbindelse med våre undersøkelser.

Våre undersøkelser viser at tjenester for lokasjonsbasert SMS-varsling tilbys i dag til offentlige myndigheter som hovedregel gjennom selskapet Everbridge. Everbridge har igjen avtale med teleoperatørene, som behandler lokaliseringsdata om deres respektive kunder. Ut ifra den informasjon vi har fått fra teleoperatørene, får verken Everbridge eller den offentlige myndigheten som bestemmer at meldingen skal formidles, tilgang til identifiserende opplysninger om mottakerne av SMS-varslene. Slike opplysninger er underlagt taushetsplikt etter gjeldende ekomlov § 2-9.

En utvelgelse av personer som befinner seg i et bestemt geografisk område med den hensikt å sende en SMS til dem, går som hovedregel ut over den behandlingen som er nødvendig for teleoperatørenes kommunikasjons- eller faktureringsformål, jf. gjeldende ekomlov § 2-7 femte ledd. Denne konklusjonen fremgår også av Direktoratet for samfunnssikkerhet og beredskap (DSB) sin rapport *Befolkningsvarsling* fra 8. november 2011. En slik behandling av lokaliseringsdata fra teleoperatørene krever derfor normalt samtykke fra sluttbruker eller

¹ <https://www.datatilsynet.no/aktuelt/aktuelle-nyheter-2020/datatilsynet-undersoker-lokasjonsbasert-sms-varsling/>

hjemmel i lov, jf. gjeldende ekomlov § 2-7 femte ledd. Lovhjemmel finnes som kjent i gjeldende ekomlov § 2-10, som pålegger teleoperatørene å formidle viktig melding fra statsmyndighet. I vår dialog med teleoperatørene har de uttalt at den aktuelle behandlingen av sluttbrukernes personopplysninger tilknyttet lokasjonsbasert SMS-varslings har hjemmel i formidlingsplikten for viktig melding fra statsmyndighet i gjeldende ekomlov § 2-10.

Det er Datatilsynets forståelse av gjeldende ekomregelverk at dersom lokasjonsbasert SMS-varslings skal benyttes utover formidlingsplikten i gjeldende ekomlov § 2-10, må det innhentes forutgående samtykke fra sluttbruker i tråd med gjeldende ekomlov § 2-7 femte ledd.

På bakgrunn av undersøkelsene våre, er vårt syn at dagens regelverk for formidling av viktig melding er svært uklart for de involverte aktørene, og at regelverket ikke fungerer etter sin hensikt. Vi vil i det følgende redegjøre for de problemene vi ser med det nåværende regelverket.

For det første vil vi påpeke at gjeldende ekomlov § 2-10 er svært generell, og sier ikke noe ytterligere om hvilke varslingsløsninger som teletilbyderne må ha på plass for å ivareta formidlingsplikten for viktig melding fra statsmyndighet. Uten ytterligere føringer i lovverket er det dermed tilsynelatende teleoperatørene, samt eventuelle private selskap som disse har avtaler med, som i praksis velger og utformer lokasjonsbaserte mobilvarslingssystemer i Norge per i dag. Dette er problematisk fra et personvernpersonvernperspektiv, og vi stiller også spørsmål ved hvorvidt dette kan være problematisk fra et beredskapsperspektiv.

Ved bruk av dagens løsning for lokasjonsbasert SMS-varslings, er det ofte ikke noen direkte kontakt mellom myndigheten som beslutter at den aktuelle meldingen skal formidles, og teleoperatøren som gjennomfører utsendelsen i tråd med plikten i ekomloven § 2-10. Myndigheten inngår kun en avtale med det private selskapet som leverer befolkningsvarslingstjenesten. Ekomloven regulerer virksomhet knyttet til elektronisk kommunikasjon og tilhørende utstyr, og vårt inntrykk er at myndighetene ofte ikke kjenner til vilkårene i gjeldende ekomlov § 2-10 når de inngår avtaler om lokasjonsbasert SMS-varslings. Vårt inntrykk er at det heller ikke føres noen kontroll med vilkårene for formidlingsplikten fra teleoperatørenes side.

Som et resultat av den manglende kunnskapen om og kontrollen av vilkårene for formidlingsplikten i gjeldende ekomlov § 2-10, er myndighetene som tar i bruk disse tjenestene ikke nødvendigvis en «statsmyndighet». Vi har blant annet sett mange eksempler på at kommuner tar i bruk disse lokasjonsbaserte SMS-varslings-tjenestene.

Videre er det forutsatt i forarbeidene at det er myndigheten som har ansvar for å vurdere hva som utgjør en «viktig melding».² Vi ser imidlertid at meldingene som sendes ut gjennom lokasjonsbasert SMS-varslings i dag har svært varierende innhold, og en del av dem vil etter vårt syn ikke oppfylle terskelen til å utgjøre en «viktig melding» slik departementet beskriver denne terskelen i høringsnotatet.

² Ot.prp. nr. 58 (2002-2003) s. 95

Ut ifra offentlig informasjon, fremstår det i tillegg som om anskaffelse av disse tjenestene innebærer ikke-ubetydelige kostnader for myndighetene.³

Vi ber derfor departementet om å klargjøre regelverket for formidling av viktig melding i forbindelse med revideringen av ekomloven og det kommende forslaget til ny forskriftsbestemmelse.

Befolkningsvarsling tjener svært viktige formål, og kan være med å verne om liv, helse og materielle verdier. Det kan imidlertid oppleves som inngripende å motta varsling fra myndighetene på mobiltelefonen, og særlig dersom varslingen er basert på hvor man oppholder seg. Slik varsling må derfor forbeholdes viktige meldinger hvor det er tidskritisk å nå ut til mange personer så raskt som mulig, og hvor det foreligger fare for liv og helse, eller betydelig skade på eller tap av verdier. Hjemmelen for formidling av viktig melding skal ikke kunne brukes for å dekke myndigheters alminnelige informasjonsbehov. Vi er enige i departementets vurderinger av hva som utgjør «viktig melding» på side 23 i høringsnotatet, men etter vårt syn bør denne terskelen tydeliggjøres i loven eller forskriften.

Både den gjeldende ekomlovens § 2-10 og den foreslåtte ekomlovens § 3-10, presiserer at formidlingsplikten for viktig melding gjelder fra «statsmyndighet». Etter vårt syn bør departementet ta stilling til og tydeliggjøre hvorvidt – og i så fall hvordan – formidling av viktig melding kan tas i bruk av kommuner eller andre ikke-statlige offentlige myndigheter. I denne forbindelse bruker rapporten om befolkningsvarsling fra DSB et eksempel hvor en kommune er den som kjenner faren best og derfor utformer meldingen, og politiet er den myndighet som treffer beslutningen om at varsling skal skje.⁴

Etter Datatilsynets syn bør også ansvarsforholdene mellom ekomtilbyderen og statsmyndigheten tydeliggjøres i loven, herunder at det er statsmyndighetens ansvar å vurdere at det gjelder en «viktig melding». Datatilsynet påpeker for ordens skyld at selv om statsmyndigheten ikke får tilgang til de taushetsbelagte personopplysningene om de som varsles, er ikke dette til hinder for at statsmyndigheten kan ha behandlingsansvar etter personvernforordningen i forbindelse med varslingen.⁵

Lovverket bør også tydelig angi hvilke former for mobilbaserte varslingsløsninger som må foreligge for at teletilbyderne skal ivareta formidlingsplikten i den foreslåtte ekomlovens § 3-10.

Når det gjelder hvilken løsning for mobilbasert varslingsystem som skal innføres i Norge, understreker Datatilsynet at det er viktig at personvernkonsekvensene for slike løsninger vurderes grundig.

³ <https://www.bergen.kommune.no/politikere-utvalg/api/fil/2870932/Framstilling-Direkteanskaffelse-Lokasjonsbasert-varslingsverktoy>.

⁴ DSB, *Befolkningsvarsling*, 2011 s. 11.

⁵ *Wirtschaftsakademie*, C-210/16, avsnitt 38 og *Jehovan todistajat*, C-25/17, avsnitt 75.

Høringsnotatets punkt 4.1 – Plikt til å bevare taushet og slette eller anonymisere data – Forslagets ekomlov § 3-3 og ekomforskrift § 8-3

Forslaget til ny ekomlov viderefører i stor grad gjeldende ekomlov § 2-7 og 2-9, samt gjeldende ekomforskrift kapittel 7. Disse bestemmelsene gjennomfører kommunikasjonsverndirektivet artikkel 5, 6 og 9.

Datatilsynet påpeker at «kommunikasjonsformål» i gjeldende ekomlov § 2-7 og den foreslåtte ekomlov § 3-3, er et vidt og vagt begrep. Ekomloven bør i stedet bruke samme formulering som kommunikasjonsverndirektivet artikkel 6, og endre ordlyden til «formål om overføring av en kommunikasjon» eller tilsvarende.

Når det gjelder nødvendighetsvilkåret i den foreslåtte ekomloven § 3-3, viser Datatilsynet til kommunikasjonsverndirektivets fortalepunkt 30, hvor det følger at dette vilkåret må tolkes strengt:

Systems for the provision of electronic communications networks and services should be designed to limit the amount of personal data necessary to a strict minimum. Any activities related to the provision of the electronic communications service that go beyond the transmission of a communication and the billing thereof should be based on aggregated, traffic data that cannot be related to subscribers or users. Where such activities cannot be based on aggregated data, they should be considered as value added services for which the consent of the subscriber is required

Departementet har vurdert at det ikke er nødvendig å innføre en egen hjemmel i loven for lagring for av data for feilrettings- og informasjonssikkerhetsformål. I lys av nødvendighetsvilkåret som nevnt ovenfor, påpeker Datatilsynet at det ikke må lagres flere opplysninger enn strengt nødvendig for formålet. Lagring for sikkerhetstiltak eller feilretting må heller ikke utgjøre et uforholdsmessig personverninnngrep overfor sluttbrukerne, se PVN-2014-10. Vedrørende lagring av trafikkdata for feilrettingsformål, presiserer kommunikasjonsverndirektivets fortalepunkt 29:

*The service provider may process traffic data relating to subscribers and users **where necessary in individual cases** in order to detect technical failure or errors in the transmission of communications. (vår utheving).*

Vi ber om at departementet hensyntar dette i det videre lovarbeidet.

Forslaget til ekomforskrift § 8-3 omhandler samtykke, og viser til at det her «menes samtykke slik det er anvendt i personvernforordningen artikkel 4 nummer 11.» Vi er enig med departementet i at et samtykke etter kommunikasjonsverndirektivet må oppfylle kravene til et gyldig samtykke etter personvernforordningen. Det er imidlertid ikke bare artikkel 4 nr. 11 som regulerer kravene til samtykke i personvernforordningen. Artikkel 7 omhandler også kravene til et gyldig samtykke, og samtykkekravene må også tolkes i lys av personvernprinsippene i artikkel 5 og fortalepunkt 32, 33, 42 og 43. Forskriftsbestemmelsen

og merknaden bør presiseres i lys av dette, og vi anbefaler at departementet også tar inn en henvisning til personvernforordningen artikkel 7 i bestemmelsen.

Høringsnotatets punkt 4.1 - Hjemmel til å gi regler om unntak for behandling av personopplysninger som har som formål å bekjempe seksuelt misbruk av barn – Forslagets ekomlov § 3-2 og 3-3 og ekomforskrift § 8-5

Departementet foreslår at den midlertidige forordningen⁶ inkorporeres i forskrift til ekomloven, og at det tas inn spesifikke forskriftshjemler i bestemmelsen om taushetsplikt i § 3-2 og bestemmelsen om sletteplikt i § 3-3 som gir myndigheten hjemmel til å gi regler om unntak for behandling av personopplysninger og andre data i tilknytning til levering av nummeruavhengige person-til-person-kommunikasjonstjenester, som har som formål å bekjempe seksuelt misbruk av barn.

Datatilsynet påpeker for ordens skyld at de behandlingene av personopplysninger som forordningen åpner for, krever et rettslig grunnlag etter personvernforordningen artikkel 6.

I tillegg vurderer vi at behandling av personopplysninger med formål om å oppdage og rapportere seksuelt misbruk av barn på nett til politimyndigheter, vil kunne innebære behandling av opplysninger om «lovovertrедelser», jf. personvernforordningen artikkel 10. Behandling av personopplysninger som omfattes av artikkel 10, og som ikke utføres under offentlige myndigheters kontroll, krever enten at behandlingen er tillatt i henhold til medlemsstatenes nasjonale rett som sikrer nødvendige garantier for de registreres rettigheter og friheter, eller at et av vilkårene i artikkel 9 nr. 2 bokstav a, c, d, e, f være oppfylt, jf. personopplysningsloven § 11. Uten at det innføres en egen hjemmel i nasjonal rett i tråd med kravene i artikkel 10, vil dermed en slik behandling av personopplysninger kunne være i strid med personvernforordningen. Dersom det på et senere tidspunkt vurderes å innføre en slik hjemmel i nasjonal rett, er det viktig at personvernkonsekvensene vurderes, og at den underlegges en ny høring og demokratisk kontroll.

Særlig om lagring og utlevering av IP-adresser – Forslagets ekomlov § 3-3, 3-4 og 3-5.

Datatilsynet avga som nevnt 18. januar 2021 høringsuttalelse til forslaget om endringer i ekomloven, (lagring av IP-adresser mv.), og vi viser til dette høringssvaret. Departements referanse er 20/3645-1.

I høringsuttalelsen uttalte Datatilsynet at lagring av IP-adresser over tid og muligheten for politiet til å be om alle IP-adresser knyttet til en person over et gitt tidsrom innebærer at personens bevegelser kan spores. I realiteten vil dette medføre en skjult overvåking av store deler av den norske befolkning ved at politiet faktisk vil ha denne muligheten. Dette er et sentralt dilemma i et samfunn hvor private aktører samler inn store mengder data og politiet

⁶ Regulation of the European Parliament and of the Council on a temporary derogation from certain provisions of Directive 2002/58/EC of the European Parliament and of the Council as regards the use of technologies by number-independent interpersonal communications service providers for the processing of personal and other data for the purpose of combatting child sexual abuse online.

gis tilgang i ettertid. Det er derfor viktig å se helheten i innsamling, lagring, utlevering og kontroll konkret for å vurdere hvilken innvirkning forslaget har for personvernet.

Datatilsynet er av den oppfatning av en slik skjult overvåkning vil være i strid med Grl. § 102 og EMK art. 8, som oppstiller strenge vilkår for når skjult overvåking kan tillates. De såkalte Weber-kriteriene stiller blant annet krav til uavhengig forhåndskontroll for å iverksette skjult overvåking.⁷

Forslaget slik det foreligger, er etter vårt syn i strid med kommunikasjonsvernet og siste praksis fra EU-domstolen, spesielt i La Quadrature du Net (sak C-511/18 og sak C-512/18), som bygger på Tele2/Watson hvor domstolen i premiss 120 krever en uavhengig forhåndskontroll av om vilkårene er oppfylt:

Med henblik på i praksis at sikre fuld iagttagelse af disse betingelser er det afgørende, at de kompetente nationale myndigheders adgang til de lagrede data i princippet, undtagen i behørigt begrundede hastende tilfælde, er undergivet en forudgående kontrol, der foretages af enten en domstol eller en uafhængig administrativ enhed, og at denne domstols eller denne enheds afgørelse træffes på grundlag af en begrundet anmodning, som navnlig fremsættes af disse myndigheder inden for rammerne af procedurer med henblik på forebyggelse, afsløring eller strafferetlig forfølgning.

Dette ble ikke tatt hensyn til når det endelige lovforslaget ble utformet.

I forslagens § 3-4 om plikt til lagring av IP-adresser fremgår det:

Det skal ikke lagres destinasjonsinformasjon.

I forslaget til merknader til § 3-2 står det imidlertid:

En IP-adresse kan ikke lengre uten videre sammenliknes med abonnementsopplysninger til en fasttelefon. Bruken av IP-adresse har vokst i takt med digitaliseringen av samfunnet. Vi omgir oss med utstyr – pc, smartklokker, mobiler, biler etc. som tildeles forskjellige IP-adresser basert på hvilket nettverk og hvordan en er koplet til internett. Tildelt IP-adresse, navn og tidspunkt kan derfor i noen grad også gi opplysninger om bevegelser når de settes i sammenheng over et gitt tidsrom. Denne informasjonen er derfor mer sensitiv i dag enn den var i 2003 når ekomloven ble vedtatt. Dette kommer også til uttrykk i de nylige avsatte EU-dommene Digital Rights/Quadrature.

Datatilsynet vil påpeke at det er umulig å ikke lagre opplysninger om bevegelser når IP-adresser lagres over tid, noe departementet selv anerkjenner. Det blir derfor selvmotsigende at man i forslagens § 3-4 inntar at «Det skal ikke lagres destinasjonsinformasjon».

⁷ Weber-kriteriene ble først omtalt i Weber and Saravia v. Germany.

Dersom ordningen opprettholdes, må enten politiets mulighet til å hente ut IP-adresser tilknyttet en person over et gitt tidspunkt begrenses i lovverket, eller det må underlegges domstolskontroll.

Datatilsynet er tilsynsmyndighet og skal kontrollere lovligheten av politiets behandling av opplysninger.

I forslaget § 3-5 fremgår det:

«Politiet og påtalemyndigheten skal oversende en årlig rapport om uthenting av IP-adresser til myndigheten.»

Datatilsynet antar «myndigheten» her referer til Nkom. For å gjøre tilsynsarbeidet vårt mer effektivt, ber vi om at departementet presiserer i ordlyden at Datatilsynet er blant de myndighetene som skal motta den årlige rapporten.

Til høringsnotatets punkt 13.4 – Informasjon til nummeropplysningstjenester – Forslagets ekomloven § 12-5 og ekomforskrift 7-3.

Departementet har forslått enkelte endringer fra dagens regelverk knyttet til utlevering til nummeropplysningstjenester, herunder at det ikke lenger utleveres opplysninger om fødselsdato. I tillegg er inntatt et forslag til ny ekomforskrift § 7-3 fjerde ledd, som fastsetter at opplysninger om barn ikke skal overføres med mindre det er gitt samtykke til det.

Datatilsynet har jobbet mye med nummeropplysningsmarkedet, og har også jevnlig saksbehandlermøter med Nkom vedrørende dette feltet.

Markedet for nummeropplysningsvirksomhet har etter Datatilsynets oppfatning endret seg vesentlig siden nåværende regelverk ble innført. Tradisjonell nummeropplysning var telefonkataloger, og etter hvert også nummeropplysningsoppslag via SMS eller på nett. Dagens marked for nummeropplysning er i langt større grad databasert, og nummeropplysningsinformasjonen som utleveres fra ekomtilbyderne sammenstilles med andre kilder. I dag leveres nummeropplysningstjenester i stor utstrekning til virksomheter via API-er. Tjenestene som tilbys er blant vask av personopplysninger i virksomheters kundelister, eller auto-utfyllingstjenester som automatisk fyller ut resterende felter dersom en kunde taster inn f.eks. telefonnummeret sitt i et registreringsskjema. Datatilsynet stiller spørsmål ved om denne typen tjenester i det hele tatt utgjør nummeropplysningsvirksomhet, eller om det i stedet må anses som annen verdiøkende virksomhet. I dagens marked er risikoen for ulovlig viderebruk eller spredning av nummeropplysningsinformasjon betydelig større enn tidligere.

Datatilsynets standpunkt er at utlevering av nummeropplysningsinformasjon til nummeropplysningsvirksomhet bør være basert på sluttbrukerens samtykke, i stedet for dagens reservasjonsrett. Kommunikasjonsverndirektivet artikkel 12 åpner for en slik løsning.

Reservasjonsretten er etter Datatilsynets oppfatning blitt mindre effektiv på grunnlag av den ovennevnte utviklingen av nummeropplysningsmarkedet, samt den økte risikoen for spredning av informasjonen. Behandlingen av nummeropplysningsinformasjon fra nummeropplysningsvirksomheter fremstår i tillegg som mer omfattende og inngripende for sluttbrukerne enn før, noe vi mener også taler for at det bør innføres en samtykkeløsning. Datatilsynet har videre sett eksempler på useriøse nummeropplysningsaktører som ikke oppdaterer nummeropplysningsinformasjonen sin, og reservasjonsretten blir i slike tilfeller illusorisk.

Videre påpeker Datatilsynet at det er svært uklart hva som ligger i begrepet «nummeropplysningsvirksomhet», og hvor grensene går i lys av markedsutviklingen. Grensene som presiseres i dagens regelverk og den forslåtte ekomloven § 12-5, er ikke tydelige nok. Mangelen på en klar definisjon av nummeropplysningsvirksomhet medfører uklarheter for ekomtilbyderne i forbindelse med rekkevidden av utleveringsplikten deres, samt uklarhet for nummeropplysningsaktørene vedrørende hva nummeropplysningene lovlig kan brukes til. Uklarheten medfører også utfordringer for tilsynsmyndighetene når det skal føres tilsyn med dette markedet. Vi ber derfor departementet klargjøre hva som ligger i nummeropplysningsvirksomhet, særlig i lys av dagens marked og hvilke typer tjenester som tilbys.

Datatilsynet vurderer videre at det bør innføres en eksplisitt formålsbegrensning i den nye ekomloven eller ekomforskriften, som fastsetter at nummeropplysningstjenester ikke kan behandle utlevert nummeropplysningsinformasjon til andre formål enn nummeropplysningsvirksomhet. Etter Datatilsynets syn vil en slik viderebehandling for andre formål som hovedregel være i strid med personvernforordningen artikkel 5 nr. bokstav b og artikkel 6 nr. 4, men vi mener det er gode grunner som taler for å fastsette en eksplisitt formålsbegrensning i ekomregelverket. Viderebehandling for andre formål vil bidra til å utvanne effekten av en reservasjon eller eventuell rett til å trekke tilbake samtykke. En formålsbegrensning, sammen med en klar definisjon av «nummeropplysningsvirksomhet» som nevnt ovenfor, vil gjøre de rettslige rammene langt klarere for de involverte aktørene, samt gjøre tilsyn med denne bransjen betydelig mer effektivt.

Vi ber også departementet klargjøre hvorvidt nummeropplysningsinformasjon er omfattet av taushetsplikten i den foreslåtte ekomloven § 3-2.

Når det gjelder hvilke opplysninger som ekomtilbyderen skal overføre til nummeropplysningsvirksomheter, følger det av dataminimeringsprinsippet i personvernforordningen artikkel 5 nr. 1 bokstav c at det ikke skal utleveres flere opplysninger enn det som er nødvendig for formålet. Vi er derfor enig med departementet i at fødselsdato ikke er nødvendig for formålet om nummeropplysning, og at denne informasjonen ikke skal utleveres.

Som nevnt ovenfor vurderer Datatilsynet at all utlevering av nummeropplysningsinformasjon bør være basert på samtykke, i stedet for en reservasjonsløsning. Subsidiært er vi enig i departementets forslag om at nummeropplysningsinformasjon hvor et barn er registrert som bruker, ikke skal utleveres med mindre det foreligger samtykke. Det bør klargjøres i

bestemmelsen at nummeropplysningsinformasjonen ikke skal overføres når barnet fyller 18 år dersom barnet tidligere har trukket tilbake et samtykke gitt av sluttbruker. Når det gjelder definisjonen av samtykke, bør det henvises til personvernforordningen.

For at ordninger knyttet til reservasjoner, tilbaketrekninger av samtykker og hemmelige numre skal være effektive, bør nummeropplysningstjenestene pålegges å oppdatere nummeropplysningsinformasjonen som så ofte som mulig. Vi stiller derfor spørsmål ved adgangen til å avtale seg bort fra at oppdatert nummeropplysningsinformasjon utleveres en gang per virkedag i forslaget til ny ekomforskrift § 7-3 syvende ledd.

Særlig om entydig identifisering – Forslagets ekomlov § 2-8 og ekomforskrift § 1-7

Det følger av forslaget ekomlov § 2-8 og ekomforskrift § 1-7 at tilbyder skal kunne dokumentere hvilken type identitetsbevis som er benyttet ved identifikasjonskontroll, og skal kunne dokumentere hvordan kravet til entydig identifisering er oppfylt.

I forslaget til merknader til ekomforskriften § 1-7, fremgår det at registrering kan eksempelvis skje ved at tilbyder eller underleverandør i bestillingsdokumentet markerer hvilken type identitetsbevis og referansenummer/kontrollnummer mv. som er benyttet ved bestillingen.

I forbindelse med dokumentasjonsplikten, presiserer Datatilsynet at det er viktig at det ikke lagres kopier av ID-dokumenter for dette formålet. Å fremlegge legitimasjonsdokument for kontroll av identitet kan være relevant dersom slik kontroll er nødvendig. Det kan imidlertid ikke senere bevises at rett person har avgitt legitimasjonsdokument bare ved å inneha en kopi av dokumentet. At tilbyder har kopi av et legitimasjonsdokument vil ikke bevise annet enn at det er tatt kopi av et legitimasjonsdokument. Dette har dermed ikke mer verdi enn om et legitimasjonsdokument fremlegges kun for kontroll. Det vil innbefatte risiko å etablere flere arkiver for legitimasjonsdokumenter hos de ulike tilbydere og eventuelt hos alle underleverandører/butikker. Å kopiere et legitimasjonsdokument tilfredsstiller ikke formålet som et bevis, og er ikke nødvendig å lagre for formålet om å kunne dokumentere hvordan kravet til entydig identifisering er oppfylt. Vi ber departementet tydeliggjøre dette, for eksempel i merknaden til forskriftsbestemmelsen.

Vi viser for øvrig til Datatilsynets høringssvar av 3. desember 2019 vedrørende endringer i ekomloven og ekomforskriften med forslag om lovhjemmel for leveringsplikt for bredbånd og tydeligere krav til entydig identifisering av sluttbrukere. Departementets referanse er 19/2447-4.

Til høringsnotats punkt 15.2 – Overtredelsesgebyr – Forslagets ekomlov § 15-12 og ekomforskrift § 11-5.

Forslaget til ekomlov § 15-12 og ekomforskrift § 11-5 regulerer ileggelse og utmåling av overtredelsesgebyr. Forslaget legger opp til at de fleste overtredelser av pliktene i loven skal kunne sanksjoneres med overtredelsesgebyr, og at maksgrensen for overtredelsesgebyr er fem prosent av foretakets omsetning.

En rekke av pliktene i ekomregelverket henger tett sammen med pliktene i personvernregelverket, og samme handling kan innebære brudd på begge regelverkene. Datatilsynet vurderer derfor at det er viktig at bøtenivåene etter de to regelverkene ikke er vesentlig forskjellige der bruddene omhandler behandling av personopplysninger. Det vil fremstå som vilkårlig og potensiell forskjellsbehandling dersom en ekomtilbyder behandler personopplysninger på en måte som bryter med begge regelverk, men får et vesentlig lavere gebyr for det tilfelle hvor gebyret gis av Nkom etter ekomlovens regler.

Vi ber derfor departementet presisere i merknadene at gebyr gitt etter personvernregelverket kan være relevant for utmålingen av gebyr etter ekomregelverket.

Avsluttende merknad

Datatilsynet er tilgjengelig for å diskutere innspillene våre nærmere dersom det er ønskelig.

Med vennlig hilsen

Jørgen Skorstad
avdelingsdirektør, jus

Anders Sæve Obrestad
juridisk seniorrådgiver

Dokumentet er elektronisk godkjent og har derfor ingen håndskrevne signaturer