



Datatilsynet



Forbrukertilsynet

KOMMUNAL- OG MODERNISERINGS-  
DEPARTEMENTET  
Postboks 8112 DEP  
0032 OSLO

Deres referanse

Vår referanse  
21/02527-3

Dato  
12.10.2021

## **Felles høringssvar fra Forbrukertilsynet og Datatilsynet - Forslag til ny ekomlov § 3-7 - samtykke til informasjonskapsler**

### **1. Innledning**

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

På side 33-37 i det vedlagte høringsnotatet redegjør departementet for forslaget til ny ekomlov § 3-7 angående informasjonskapsler. Departementet har særskilt bedt om høringsinstansenes syn på krav til samtykke, og hva som er den beste måten å gjennomføre samtykkekravet i praksis.

I lys av hvor viktig dette temaet er for å sikre alle brukere av digitale tjenester i Norge en trygg digital hverdag, har Datatilsynet og Forbrukertilsynet gått sammen for å inngi et felles høringssvar vedrørende forslaget til regulering av bruk av informasjonskapsler i den nye ekomloven. Tilsynene vil i tillegg levere hvert sitt høringssvar vedrørende andre temaer som er berørt av høringen.

Personopplysninger har blitt store penger i den digitale økonomien. Sosiale medier, apper, nettsider og andre digitale tjenester hvor forretningsmodellen er å tjene penger på forbrukeres data har blitt vanlig, og forbruker- og personvern glir over i hverandre.

Forbrukertilsynet og Datatilsynet har i flere år samarbeidet om hvordan forbrukervernregelverket og personvernregelverket kan brukes sammen og utfylle hverandre i møte med databaserte forretningsmodeller, med formål om å sikre trygghet for digitale forbrukere. Sammen har vi også frontet dette temaet i diskusjoner og samarbeid med andre europeiske og internasjonale myndigheter.

En betydelig andel av personopplysningene som samles inn om norske brukere, samles inn gjennom informasjonskapsler og andre sporingsteknologier som reguleres av dagens ekomlov § 2-7b. Rettstilstanden i Norge i dag vedrørende samtykke til informasjonskapsler er uklar, og dette har i praksis åpnet opp for bruk av forhåndsinnstillinger i nettleser eller andre løsninger hvor det er mye enklere å gi samtykke enn å la være å samtykke. Dette har i årevis medført en utstrakt innsamling av personopplysninger med svært begrenset kontroll og valgmulighet for forbrukerne.

Oppsummert har Datatilsynet og Forbrukertilsynet følgende innspill til forslaget til regulering av informasjonskapsler:

- Forslaget til ny ekomlov § 3-7 bør henvise til personvernforordningens definisjon av samtykke i stedet for å innta en definisjon i lovteksten. Se punkt 3.
- Departementet bør korrigere og tydeliggjøre uttalelsene knyttet til bruk av innstillinger i nettleser eller operativsystem som samtykke, da det med dagens løsninger ikke er mulig å oppfylle samtykkekravene i personvernforordningen på denne måten. Se punkt 4.
- Datatilsynet bør gis kompetanse til å føre tilsyn med bruk av informasjonskapsler dersom denne bruken innebærer behandling av personopplysninger – i tillegg til Nasjonal kommunikasjonsmyndighets tilsynskompetanse. Se punkt 5.

I det følgende vil vi utdype disse tre forslagene.

## **2. Om bestemmelsens virkeområde og formål**

Departementet beskriver virkeområdet til ekomloven § 2-7b, i overskriften til lovbestemmelsen og ellers i høringsnotatet, til å gjelde informasjonskapsler. Vi ønsker å poengtere at selv om bestemmelsen også gjelder informasjonskapsler, er det materielle virkeområdet langt bredere. Lovbestemmelsen regulerer en stor del av den digitale økonomien, alt fra innsamlingen av personopplysninger i overvåkingsøkonomien til uthenting av informasjon fra nyere kjøretøy, og er sentral også utenfor plasseringen av informasjonskapsler.

Formålet bak artikkel 5(3) i kommunikasjonsverndirektivet er å verne om brukernes kontroll over egne personopplysninger, og å sikre at de er informerte om hvordan personopplysningene deres blir benyttet.

Dette formålet er grunnmuren i personvernretten. Dessverre møter vi som tilsyn gjentatte eksempler på at dette ikke respekteres. En manglende respekt for personers selvbestemmelse over egne personopplysninger er en utfordring for norske brukeres menneskerettigheter som

ikke bare kan ha konsekvenser for den enkelte, men kan ha store konsekvenser for samfunnet som helhet, herunder nasjonale sikkerhetspolitiske utfordringer.<sup>1</sup>

Dette handler derfor om mer enn samtykkebokser som dukker opp når man besøker nettsiden til en nettavis eller en nettbutikk. Slik vi ser det handler det om helt grunnleggende rettigheter som den enkelte av oss har til å kunne kontrollere egne personopplysninger. Det er avgjørende at Datatilsynet og Nasjonal kommunikasjonsmyndighet kan føre effektivt tilsyn, men det er også avgjørende at bestemmelsen er gjennomført i norsk rett på en måte som verner om nettopp brukernes rettigheter og dermed ivaretar formålet med bestemmelsen.

### **3. Ekomloven § 3-7 bør henwise til personvernforordningens definisjon av samtykke**

Departementet foreslår å innta en presisering i ny ekomlov § 3-7 om at samtykket må være en frivillig, spesifikk, informert og utvetydig viljesytring gitt ved en erklæring eller en tydelig bekreftelse.

Vi er enige med departementet i at et samtykke etter kommunikasjonsverndirektivet må oppfylle kravene til et gyldig samtykke etter personvernforordningen. Forslaget til ny ordlyd speiler definisjonen av samtykke i personvernforordningen artikkel 4(11) og er en forbedring fra dagens rettstilstand, som skiller seg fra rettstilstanden i Europa for øvrig.

Det er imidlertid ikke bare artikkel 4(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.

Vi vurderer derfor at en direkte henvisning til personvernforordningen vil være en bedre lovteknisk løsning for å forhindre at det, som i dag, oppstår en ulik praktisering av regelverket mellom Norge og EØS-landene. Ved å innta en direkte henvisning til personvernforordningen vil det være klarere at hele forordningens regulering av samtykke gjelder. Dette vil videre sikre at samtykkekravene i ekomloven og personvernforordningen samsvarer. Det er gunstig at næringsdrivende og andre som behandler personopplysninger kun må forholde seg til én samtykkedefinisjon.

### **4. Samtykkekravet i ekomloven § 3-7 og bruk av tekniske innstillinger i nettleseren**

#### **4.1 Uklarhet rundt anvendelsen av tekniske innstillinger i nettleseren**

Vi forstår det slik at formålet med denne lovendringen er å harmonisere samtykkekravet i ekomloven og personvernforordningen. Dagens løsning er egnet til å gi inntrykk av at det i ekomloven er rom for å operere med et annet samtykkekrav enn det som fremgår av personvernforordningen.

---

<sup>1</sup> Se også Vivi Cahtrine Ringnes Wilhelmsen «*Naivt om datasikkerhet*» 11. januar 2021 i Dagbladet, tilgjengelig fra <https://www.dagbladet.no/meninger/naivt-om-datasikkerhet/73224346>

Datatilsynet advarte mot nåværende løsning i 2013, og vi er positive til at departementet benytter anledningen i dette lovarbeidet til å endre bestemmelsen.<sup>2</sup> Endringen er til gode for internettbrukere i Norge, og for virksomheter som må forholde seg til at reglene i Norge i dag er ulike fra andre EU og EØS-land.

I høringsnotatet skriver departementet at samtykke må være et aktivt valg fra brukerens side, og konkluderer med at:

«Kravet til samtykke vil etter departementets syn fremdeles være oppfylt ved at sluttbruker benytter en teknisk innstilling i nettleser eller tilsvarende i de tilfeller der dette er teknisk mulig.»

Uttalelsen følges derimot ikke opp av eksempler på hvordan kravet til et aktivt valg fra brukerens side og tekniske innstillinger i nettleseren kan utføres i praksis på en måte som oppfyller personvernforordningens krav. Vi er ikke kjent med at det per i dag finnes tekniske løsninger som gjør at et slikt samtykke kan gis og samtidig være i tråd med kravene til samtykke i personvernforordningen.

Slik vi leser det, bidrar denne uttalelsen dermed til å skape uklarhet om hvordan kravene i bestemmelsen skal leses og ikke minst gjennomføres i praksis. Dersom denne uttalelsen blir stående i lovproposisjonen, vil det kunne medføre at departementets ønske om et regelverk som er harmonisert med EØS-landene ikke oppfylles. Det er viktig at den foreslåtte endringen i ekomloven § 3-7 retter opp i dette. Vi vil redegjøre nærmere for dette i det følgende.

#### 4.2 Fortalepunkt 66 og EDPBs uttalelser

Departementet viser til at det i endringene i kommunikasjonsverndirektivet fra 2009 ble forutsatt i fortelepunkt 66 at samtykke kunne gis gjennom passende nettleserinnstillinger. Dette er en lesning av fortelepunkt 66 som vi mener det ikke er dekning for.

Fortalepunkt 66 lyder:

«Hvor det er teknisk muligt og **effektivt, i overensstemmelse med de relevante bestemmelser i direktiv 95/46/EF**, kan brugerens samtykke til databehandling udtrykkes gennem anvendelse af passende browserindstillinger eller andre applikationer» (vår uth.).

Fortalepunktet er ikke ment å være en endring eller et unntak fra samtykkekravet. Fortalepunkt 66 stadfester bare det åpenbare: Dersom det er mulig å avgi et samtykke som er lovlig i henhold til personvernforordningen, så er ikke teknologiske løsninger til hinder for dette. Det grunnleggende utgangspunktet om at samtykke etter personvernforordningen er teknologinøytralt, er imidlertid ikke et holdepunkt for å fravike forordningens krav til hva som utgjør et gyldig innhentet samtykke.

---

<sup>2</sup> <https://www.personvernbloggen.no/2013/03/05/cookies-regjeringen-har-valgt-en-darlig-losningen/>

Vi utdyper nærmere under punkt 4.3 hvorfor dagens tekniske løsninger ikke effektivt sikrer et samtykke som er i overensstemmelse med personvernforordningens krav.<sup>3</sup>

At det ikke foreligger tekniske løsninger som per dags dato sikrer en effektiv etterlevelse av personvernforordningens krav, i tråd med fortalepunktets forutsetninger, viser hvorfor det er viktig å fjerne referanser i forarbeidene til at samtykke kan innhentes gjennom tekniske innstillinger i nettleseren.

I høringsnotatet vises det også til uttalelser fra European Data Protection Board (EDPB) 9. mars 2021. Uttalelsen er et forslag til hvordan kommunikasjonsvern direktivets artikkel 5(3) kan videreføres og endres i den nye kommunikasjonsvernforordningen. Vi tolker det slik at uttalelsen er tatt med fordi departementet mener den støtter den forståelsen av fortalepunkt 66 som departementet gir uttrykk for på side 34 i høringsnotatet. Denne uttalelsen knytter seg til «samtykkesvinn», og kan ikke tas til inntekt for det synet som departementet forfekter på side 36-37 i notatet. Samtykkesvinn innebærer at brukere trykker på samtykkebokser for å få bort forstyrrende elementer på nettsiden, uten at de reelt sett ønsker å samtykke til behandlingen. Videre er det uttrykt at det er en fare for at det utvikles en kollektiv misnøye og utmattelse ved å stadig måtte ta disse valgene.

EDPBs uttalelse er knyttet til et ønske om at kommunikasjonsvernforordningen skal pålegge nettlesere og operativsystem å implementere en brukervennlig og effektiv mekanisme slik at de behandlingsansvarlige kan innhente et gyldig samtykke til behandlingen, og ikke minst sikre at brukerne som ikke ønsker sporing får sitt valg respektert uten at de stadig må trykke «nei» hver gang de besøker nettsiden. Selve forutsetningen for uttalelsen er imidlertid at det i dag ikke er mulig å innhente et gyldig samtykke i dag gjennom tekniske innstillinger i nettleseren. EDPB foreslår derfor at nettlesere og operativsystemer må ha en lovpålagt plikt for slik å sikre at en løsning utvikles.

I etterkant av Storbritannias fratreden fra EU har det også vært et uttalt ønske fra britisk hold om å fjerne samtykkebokser, blant annet for å motvirke utmattelsen brukere føler på og som er nevnt rett ovenfor. For å få til dette har Storbritannia, gjennom Information Commissioner's Office (ICO), tatt opp problemstillingen med G7-landene. Formålet er å finne frem til et alternativ til dagens praksis, og som benytter tekniske innstillinger og ivaretar brukernes personvern.

Også fra sivilsamfunnet er det fremmet alternative løsninger til dagens mange samtykkebokser. Blant annet har personvernorganisasjonen *noyb*, sammen med Universitetet i Wien, utviklet en tidlig prototype og et forslag til hvordan dette kan gjøres gjennom løsningen *Advanced Data Protection Control*. Det er for tidlig å si hvordan prosjektet kommer til å lykkes, men det illustrerer poenget om at de alminnelige innstillingene som finnes i en nettleser i dag ikke er tilstrekkelige.

---

<sup>3</sup> Referanser til direktiv 95/46/EF skal, slik departementet også fremhever, forstås som referanse til personvernforordningen jf. personvernforordningen artikkel 94(2).

Vi nevner disse trendene for å understreke at vi ikke er imot alternative løsninger til samtykke som unngår at brukere blir overveldet av samtykkebokser. En teknisk løsning må imidlertid sikre at brukere får en reell beskyttelse og valgmulighet over hvordan deres personopplysninger skal behandles, til hvilke formål og av hvem. Tekniske innstillinger i nettleseren for å hindre plasseringen av informasjonskapsler er ikke en slik løsning i dag, og fortalepunkt 66 og EDPBs uttalelser kan ikke brukes til å understøtte departementets uttalelser her.

### **4.3 Konkrete utfordringer ved å basere et samtykke på tekniske innstillinger i nettleseren**

#### **4.3.1 Generelt**

Å avgi et samtykke gjennom tekniske innstillinger i nettleseren utløser mange praktiske problemstillinger som gjør det vanskelig å forene med at samtykket er gyldig etter personvernforordningen. Som nevnt ovenfor følger det av fortalepunkt 66 at en teknisk løsning for å innhente samtykke gjennom nettleserinnstillinger må oppfylle kravene til et gyldig samtykke etter personvernforordningen.

Nettlesere og operativsystemer benytter i dag forhåndsinnstillinger, og selv om det skulle kreves en aktiv handling vil ikke samtykket være:

- Frivillig, ved at det ikke kan samtykkes for hvert formål;
- Spesifikt, ettersom samtykket ikke er knyttet til det spesifikke behandlingsformålet;
- Informert, fordi man ikke kan forstå hva man samtykker til i et slikt generelt samtykke;
- Utvetydig, ved at den behandlingsansvarlige ikke kan være sikker på at den registrerte har ment å samtykke til deres bruk av informasjonskapsler, og heller ikke kan bevise dette i henhold til personvernforordningen artikkel 7 nr. 1
- Samtykket kan ikke trekkes tilbake like lett som det er gitt

Vi utdyper disse punktene nedenfor. Våre innvendinger er ikke uttømmende, men forhåpentligvis illustrerende.

#### **4.3.2 Frivillig**

Det mest umiddelbare problemet ved å basere et samtykke på innstillinger i nettleseren er den manglende graden av valgfrihet for brukerne. Det følger av fortalepunkt 43 til personvernforordningen at «Samtykket antas å ikke være gitt frivillig dersom det ikke er mulig å gi separat samtykke for forskjellige behandlingsaktiviteter, selv om det er hensiktsmessig i det enkelte tilfellet [...]». En forutsetning for å kunne avgi et gyldig samtykke er at man ikke blir presentert med en «alt-eller-ingenting»-løsning. Brukeren skal selv ha mulighet til å si nei til enkelte formål og behandlinger.

Nettleserinnstillinger som er begrenset til å tillate plasseringen av informasjonskapsler fra alle, ingen eller enkelte bestemte nettsider gir ikke tilstrekkelig mulighet for brukeren til å samtykke til (eller avslå) behandlingsaktiviteter for ulike formål. Dette har også klare koblinger til kravet om at samtykket må være spesifikt.

#### **4.3.3 Informert**

I C-61/19 (Orange Romania) avsnitt 40 fremhever domstolen at informasjonen må «enable the data subject to be able to determine easily the consequences of any consent» og «ensure that the consent is well informed».

Departementet drøfter ikke tidspunktet informasjonen må fremlegges. Det er imidlertid ikke tilstrekkelig at informasjonen er tilgjengelig etter at informasjonskapslene har blitt plassert hos brukeren. Også dette utfordrer departementets standpunkt.

Personvernforordningen fremhever i fortalepunkt 58 at et informert samtykke er særlig vanskelig ved markedsføring på nett. Etter at fortalepunktet gjengir prinsippet om åpenhet rettes det særlig fokus mot utfordringene for nettbasert sporing:

«Dette er særlig relevant i situasjoner der det økende antallet aktører samt de komplekse teknologiene som brukes, gjør det vanskelig for den registrerte å vite og forstå om, av hvem og for hvilket formål vedkommendes personopplysninger samles inn, f.eks. i forbindelse med nettreklame».

Mangfoldet av aktører som mottar de innsamlede personopplysninger og informasjon til brukeren er en utfordring uavhengig av hvordan samtykket innhentes, men aktualiseres i særlig grad med samtykke gjennom tekniske innstillinger gjennom nettleseren. En forutsetning for at tekniske innstillinger kan benyttes vil være at aktørene standardiserer sporingen de gjennomfører, slik at brukeren er sikker på hva deres samtykke omfatter på tvers av ulike aktører og brukervilkår. I tillegg må brukeren kunne velge til hvilke formål personopplysningene skal benyttes, og av hvilke aktører.

#### **4.3.4 Aktiv handling**

I høringsnotatet skriver departementet at:

«Etter departementets syn, tar ikke dommen tydelig stilling til spørsmålet om sluttbruker kan samtykke generelt til bruk av informasjonskapsler gjennom selv å krysse av for dette i innstillingene til nettleserne.»

Problemet er ikke bare om det er rettslig adgang til å samtykke generelt og udifferensiert til sporing av store annonsenettverk som operer i bakgrunnen og uten at brukeren har kjennskap til hvordan, av hvem og til hvilke formål personopplysningene om vedkommende behandles. Problemet er at det ikke kan oppstilles en presumsjon om at brukeren aktivt har samtykket til slik sporing ved at brukerens nettleser tillater at informasjonskapsler plasseres.

I fortalepunkt 32 i personvernforordningen står det at «Samtykke bør gis i form av en tydelig bekreftelse [...]» og videre at «Taushet, forhåndsavkryssede bokser eller inaktivitet bør derfor ikke utgjøre et samtykke». Departementet er også innom problemstillingen når dere skriver at:

«Uavhengig av hvordan samtykket innhentes, kreves det imidlertid at dette gis gjennom et aktivt valg av brukeren. Dersom samtykke skal gis gjennom nettleseren må sluttbrukeren selv gi et aktivt samtykke.»

Domstolen behandlet spørsmålet i relasjon til forhåndsavkryssede bokser i Planet49-dommen. Avsnitt 55 begrunner hvorfor forhåndsavkryssede bokser *ikke* kan utgjøre et gyldig samtykke. For tekniske innstillinger i nettleseren er det samme utfordring ved at det er tilnærmet umulig å stadfeste hvorvidt en bruker har tatt et aktivt valg om å samtykke til behandlingen av vedkommendes personopplysninger, bare ved at brukeren besøker nettsiden. I tillegg kommer problemstillingen knyttet til hvor informert dette samtykket er, som nevnt ovenfor og i dommen.

Selv om nettleseren tillater plasseringen av informasjonskapsler er det ikke tilstrekkelig for å stadfeste at det foreligger et aktivt valg fra brukerens side til omfattende sporing blant et utall tredjeparter. Departementet tar ikke stilling til hvordan kravet om et aktivt samtykke kan oppfylles gjennom tekniske innstillinger i nettleseren.

#### **4.3.5 Trekke tilbake**

Departementet skriver at «et samtykke skal også kunne trekkes tilbake like lett som det er gitt». I praksis vil det med dagens løsninger innebære at brukeren selv sletter de lagrede informasjonskapslene fra nettleseren. Forutsetningen for dette er at man kjenner til hvordan man sletter informasjonskapslene. Dersom informasjonskapslene blir plassert ved å besøke nettsiden er det vanskelig å se at samtykket kan trekkes tilbake like lett som det er gitt.

### **5 Datatilsynet bør ha tilsynskompetanse etter ekomloven § 3-7**

Hele tiden blir det samlet inn personopplysninger gjennom teknikker som faller innenfor virkeområdet til kommunikasjonsverndirektivet artikkel 5(3), og dermed nåværende ekomloven § 2-7b og fremtidige § 3-7. Selve innhenting av personopplysninger vil dermed være regulert av kommunikasjonsverndirektivet og ekomloven som *lex specialis*, mens den etterfølgende behandlingen av personopplysninger (for eksempel lagring, analyse, sammenstilling eller deling) blir regulert av personvernforordningen. Den etterfølgende behandlingen vil bare være lovlig dersom den har et gyldig rettslig grunnlag i personvernforordningen artikkel 6. Slik dette er lagt opp i dag er det derfor to tilsynsmyndigheter som har ansvaret for å føre tilsyn med hver sin del av dette økosystemet.

For en vanlig person som ønsker å rette en klage mot hvordan personopplysninger om dem samles inn, fremstår den fragmenterte tilsynskompetansen mellom Nkom og Datatilsynet som forvirrende og byråkratisk. Dagens løsning harmonerer dårlig med vanlige folks forventninger til myndighetenes tilsyn over bruken og innsamlingen av deres personopplysninger på internett. Det store antallet henvendelser til Datatilsynet som knytter seg til behandlingen av personopplysninger som faller innenfor virkeområdet til artikkel 5(3) i



kommunikasjonsverndirektivet gjenspeiler også at ansvarsfordelingen fremstår som uklar og vilkårlig.

Vi foreslår derfor at departementet åpner for at også Datatilsynet kan håndheve den nye § 3-7.

Det vil gjøre det enklere å følge opp hele behandlingsløpet under ett, og vurdere lovligheten av den opprinnelige innsamlingen, og dermed også lovligheten av den etterfølgende bruken og behandlingen av de innsamlede personopplysningene. Å unnta store deler av innsamlingen av personopplysninger på internett fra Datatilsynets tilsynsmyndighet, gjør det svært vanskelig for Datatilsynets å løse sitt samfunnsoppdrag.

Forbudet mot dobbeltstraff underbygger også det vil være mer effektivt og hensiktsmessig om Datatilsynet kan føre tilsyn med alle aspekter av behandlingen av personopplysninger i saker som blir klaget inn til Datatilsynet.<sup>4</sup> I dag har verken Datatilsynet eller Nkom kompetanse til å sanksjonere både innsamlingen etter ekomloven § 2-7b og den videre bruken av personopplysningene som ble innsamlet.

Det vil være mer effektivt og hensiktsmessig om Datatilsynet kan føre tilsyn med alle aspekter av behandlingen av personopplysninger i saker som blir klaget inn til Datatilsynet.

Slik vi ser det er det ingen skranker i EØS-retten mot en slik fordeling av tilsynskompetansen. Personvernrådet (EDPB) har i sin veileder om samspillet mellom kommunikasjonsverndirektivet og personvernforordningen drøftet hvorvidt det er adgang til en slik ansvarsfordeling. Personvernrådet konkluderte med at det eksisterer en slik adgang.

Dessuten følger det direkte av artikkel 15a i direktiv 2009/136/EF at håndhevelseskompetanse for bestemmelsene i kommunikasjonsverndirektivet kan deles mellom ulike tilsynsmyndigheter.

I EU har medlemslandene valgt ulike løsninger for å håndheve nasjonale regler med opphav i kommunikasjonsverndirektivet. Blant annet har datatilsynene i Spania (AEPD) og Frankrike (CNIL) kompetanse til å håndheve kommunikasjonsverndirektivet artikkel 5(3).

For å sikre at Datatilsynet har tilstrekkelig kompetanse til å føre effektive tilsyn, ber vi departementet om at Datatilsynet får kompetanse til å føre kontroll med ekomloven § 3-7. Vi foreslår at en slik adgang legges til personopplysningsloven.

For ordens skyld presiserer vi at dette forslaget ikke skal ha noen innvirkning på Nkom sin tilsynskompetanse med bestemmelsen.

## **6 Avslutning**

Vi er positive til at departementet foreslår å endre nåværende ekomlov § 2-7b. Endringen er på overtid og helt nødvendig for å sikre innbyggernes personvern. Endringen er også et gode

---

<sup>4</sup> Forbudet mot dobbeltstraff innebærer at to tilsynsmyndigheter ikke hver for seg kan ilegge overtredelsesgebyr for samme forhold.

for virksomheter som ikke lenger trenger å forholde seg til ulike samtykkekrav i Norge og resten av EØS.

Oppsummert mener vi at departementet ikke har begrunnet hvordan det mener et samtykke gjennom tekniske innstillinger kan gjennomføres. I dagens marked finnes det ikke løsninger som ivaretar personvernforordningens samtykkekrav, og det vil trolig først bli en realitet ved gjennomføringen av kommunikasjonsvernforordningen dersom det blir pålagt å utvikle slike løsninger – noe EDPB blant annet støtter i uttalelsen som er sitert i høringsnotatet.

I realiteten vil det være opp til virksomheter å påvise at det innhentede samtykket er innhentet på lovlig vis. Kunnskapen om personvernforordningens krav til hva som utgjør et lovlig innhentet samtykke varierer fra virksomhet til virksomhet. Departementets uttalelser om at samtykke også kan innhentes gjennom tekniske innstillinger i nettleseren kan bidra til at virksomheter ulovlig innhenter og behandler personopplysninger, med henvisning til departementets uttalelser. Brukere som forventer at samtykke skal være i tråd med forordningens krav og som føler en maktesløshet ved å bli fratatt eget valg vil antakeligvis fortsette å klage inn fraværende samtykkeløsninger.

Dersom departementet tar hensyn til våre innvendinger anser vi at samtykkekravet i Norge vil være på linje med resten av EØS, slik at lovgivers uttalte intensjon i forarbeidene fra 2012-2013 om et harmonisert regelverk endelig oppfylles.

Både Forbrukertilsynet og Datatilsynet er tilgjengelig for å diskutere dette nærmere dersom det er ønskelig.

Med vennlig hilsen

Trond Rønningen  
direktør, Forbrukertilsynet

Bjørn Erik Thon  
direktør, Datatilsynet

*Dokumentet er elektronisk godkjent og har derfor ingen håndskrevne signaturer*