Datatilsynet

Samferdselsdepartementet
Postboks 8010 Dep
0030 OSLO

Deres referanse	Vår referanse	Dato
17/482-	17/00293-2/EOL	28.03.2017

Datatilsynets høringsuttalelse - EU-kommisjonens forslag til kommunikasjonsvernforordning

Vi viser til brev av 2. mars 2017 hvor Samferdselsdepartementet sender på høring EU-kommisjonens forslag til kommunikasjonsvernforordning. Frist for høringsuttalelse er satt til 24. mars 2017. Datatilsynet har fått innvilget utsatt frist til 27. mars 2017.

I høringen ønsker Samferdselsdepartementet tilbakemelding på hva høringsinstansene ser som konsekvenser av å gjennomføre forslaget i norsk rett, og hvilke endringer det er ønskelig at norske myndigheter skal jobbe for i den videre prosessen.

I det følgende vil Datatilsynet først og fremst fremheve de positive konsekvensene av innføringen av ePrivacy forordningen. Delen som omhandler endringer norske myndigheter bør jobbe for tar for seg noen deler av forordningen som gir grunn til bekymring sett fra et personvernståsted. Vi har i våre kommentarer i stor grad støttet oss til en gjennomgang av forordningen fra EU-kommisjonens rådgivende organ i personvernspørsmål, Artikkel 29-gruppen.

Konsekvenser av å innføre ePrivacy forordningen i norsk rett

Harmonisert regelverk

EU-kommisjonens evaluering av dagens ePrivacydirektiv (2002/58/EC) viser at det er et behov for særregulering av tjenester som tilbyr elektronisk kommunikasjon, men at det regelverket som gjelder i dag ikke har virket etter hensikten. Dette gjelder blant annet på områder som angår borgernes krav på konfidensialitet rundt sin kommunikasjon som skjer online og rett til bestemme om de ønsker å dele personopplysninger for formål som ikke er nødvendige for å tilby en tjeneste. Evalueringen peker dessuten på at varslingsmekanismene hva gjelder sikkerhetsbrudd som har betydning for personvern heller ikke har fungert etter hensikten.

Kommisjonen peker på at mye av årsaken til at garantiene som ePrivacy-direktivet skulle ivareta ikke fungerer er at EU/EØS-landene har valgt ulike modeller for løsninger av oppgavene i regelverket, og dette har resultert i et fragmentert og lite oversiktlig regelverk. I

Postadresse:	Kontoradresse:	Telefon:	Telefaks:	Org.nr:	Hjemmeside:
Postboks 8177 Dep 0034 OSLO	Tollbugt 3	22 39 69 00	22 42 23 50	974 761 467	www.datatilsynet.no

tillegg er oppgavene, etter kommisjonen syn, spredd på for mange myndighetsorganer. Resultatet er et lite oversiktlig regelverk både for rettighetshavere og pliktsubjekter.

Datatilsynet er enig i at det er nødvendig med et oppdatert regelverk som verner alle borgeres kommunikasjon uavhengig av hvilke tekniske plattformer de måtte benytte seg av. Vi hilser derfor et regelverk som stiller krav til kommunikasjonsvern for OTT-tjenester og IoT-tjenester velkommen. Dagens regelverk har ikke vært tydelig nok med hensyn til regulering av teknologi som muliggjør sporing av borgernes adferd på nett, og Datatilsynet støtter en regelverksrevisjon som endrer dette. Vi erfarer dessuten en stor interesse for innhenting og bruk av metadata fra borgernes bruk av mobiltelefoner (trafikkdata og lokasjon). Dette er data som avslører mye om vårt privatliv, og som vi mener det er viktig å få på plass tydeligere regler for behandling av.

En konsekvens av å innføre ePrivacy forordningen i norsk rett er altså at regelverket knyttet til kommunikasjonsvern for EU/EØS-borgere blir harmonisert. Under forutsetning av at beskyttelsesnivået i det nye regelverket generelt sett blir hevet i forhold til i dag, støtter Datatilsynet dette underliggende målet. Dagens regulering har resultert i ulikt beskyttelsesnivå i de forskjellige europeiske statene, og et mer harmonisk regelverk vil derfor kunne øke borgernes rettssikkerhet.

Flytting av tilsynsmyndighet
En gjennomføring av ePrivacy forordningen vil også ha som konsekvens at tilsynsmyndighet blir flyttet fra NKOM og Forbrukerombudet til Datatilsynet.

Det følger av artikkel 18 i forslaget til ePrivacy forordning at det er det samme uavhengige tilsynsorgan som fører tilsyn med personvernforordningen som skal føre tilsyn med etterlevelsen av ePrivacy forordningen.

Det er også fastslått at kapitlene VI og VII i personvernforordningen gjelder for ePrivacy forordningen. Disse kapitlene omhandler henholdsvis spesifikke krav til det uavhengige tilsynsorganet som skal ha myndighet etter personvernforordningen og beskrivelse av samarbeids- og konsistensmekanismene mellom de europeiske personvernmyndigheter som det er lagt opp til gjennom personvernforordningen.

I forslagets art. 19 er det videre fastslått at EDPB skal ha samme rolle etter ePrivacy forordningen som etter personvernforordningen art 70.

Fortalens punkt 38 begrunner valg av tilsynsmyndighet med at det er viktig å få harmonisert regelverket for kommunikasjonsvern med regelverket for personvern. Bakteppet er at EU-kommisjonen har gjort en revisjon av ePrivacy direktivet som konkluderer tydelig med at håndhevingen av disse reglene ikke har fungert etter gjeldende regelverk.

Evalueringen peker på at mye av årsaken til at garantiene som ePrivacy-direktivet skulle ivareta ikke fungerer er at EU/EØS-landene har valgt ulike modeller for løsninger av oppgavene i regelverket, og dette har resultert i et fragmentert og lite oversiktlig regelverk. I

tillegg er oppgavene, etter kommisjonen syn, spredd på for mange myndighetsorganer. Resultatet er et lite oversiktlig regelverk både for rettighetshavere og pliktsubjekter.

Hovedhensikten med forslaget som foreligger er dermed å sikre EU borgere et reelt kommunikasjonsvern ved å foreslå en modell som i større grad skal sørge for effektiv etterlevelse og håndhevelse av regelverket. Å fastholde løsningen med at nasjonalstatene har anledning til å spre tilsynskompetansen vil være i direkte motstrid med grunnpremissene for ePrivacy forordningen.

Datatilsynet mener dermed at det går klart frem av forslaget til ePrivacy forordning at det er Datatilsynet som er tillagt det hele og fulle tilsynskompetansen etter forordningen. Datatilsynet mener at en slik endring er positiv, og vi er beredt til å påta oss nye myndighetsområder. Vi stiller oss også positive til forpliktelsen til å samarbeide med relevante myndigheter som fastslått av artikkel 18 nr 2.

Utvidede myndighetsoppgaver
ePrivacyforordningen er å regne som lex specialis i forhold til personvernforordningen. Som konklusjonen over viser er det kompetente myndigheter etter personvernforordningen som også skal være kompetent myndighet etter ePrivacy forordningen. En konsekvens av dette er at også personvernmyndighetens oppgaver og myndighet etter ePrivacy forordningen følger av personvernforordningen. Forslagets art.18 viser til at tilsynsmyndighetens «tasks and powers» som relaterer seg til personvernforordningens kapittel VI, art. 57 og 58.

Personvernmyndighetenes oppgaver er dermed å kontrollere etterlevelsen av ePrivacy forordningen. Med den korte høringsfristen har vi ikke hatt tid til å gå grundig inn i de de enkelte materielle bestemmelsene for å forklare hva disse ville innebære av nye oppgaver for Datatilsynet. Kort oppsummert kan vi likevel si at det som er særskilt regulert i ePrivacy forordningen er:

Kommunikasjonsvern
- vern av innhold og metadata i kommunikasjon
- vern av utstyr brukt for kommunikasjon (cookie ++)

Vern mot eksponering av telefonnummer m.m
- ved oppringing, blokkering innkommende
- vern mot oppføring nummertjenester (fra opt-out til opt-in)
- vern mot direkte markedsføring

Dette er delvis nye oppgaver og delvis oppgaver som etter dagens regelverk håndheves av NKOM og Forbrukerombudet etter henholdsvis ePrivacy direktivet og markedsføringsloven.

Datatilsynet er beredt til å ta på seg disse nye oppgavene, og forutsetter at vi blir tilført de ekstra ressurser som er nødvendig for at vi skal kunne utføre oppgavene etter ePrivacy forordningen, jfr art 38. Dette nødvendiggjør en analyse av hvilke ressurser dette arbeidet legger beslag på hos de myndighetene som har det i dag. Vi mener en slik analyse må ta inn

over seg også et fremtidsperspektiv med hensyn til hvilket omfang ny teknologi som sporingsteknologi og OTT-tjenester vil bestå av.

Utvidet virkeområde
I motsetning til ePrivacy direktivet vil forordningen gjelde for såkalte Over-the-top tjenester (OTT). Dette er tjenester som tilbyr kommunikasjon, men som ikke har vært definert som «kjernetjenester» og dermed håndteres av leverandører som ikke vært forpliktet av krav til sikkerhet og kommunikasjonsvern på samme måte som de tradisjonelle teletilbyderne. Det betyr at tjenestetilbydere av applikasjoner for direktemeldinger som WhatsApp og Skype også må oppfylle kravene i ePrivacy forordningen. Stadig mer av vår kommunikasjon foregår på slike plattformer og det er dermed et stort fremskritt for personvernet at også disse må sørge for at vår kommunikasjon forblir et privat anliggende.

Anerkjennelse av sensitiviteten av kommunikasjonens innhold og metadata
Innføringen av ePrivacy forordningen vil på en helt annen måte enn foregående regelverk gjøre det tydelig at beskyttelse av både innholdet i vår kommunikasjon med andre og metadata knyttet til denne kommunikasjonen er grunnleggende for å ivareta personvernet.

Forordningen slår fast at analyse av innhold alltid skal regnes som «high risk»-behandling, jfr GDPR art. 35. Det slås også fast at metadata er egnet til å avsløre svært sensitive opplysninger om hver av oss.

Debatten omkring datalagringsdirektivet og digitalt grenseforsvar synliggjorde hvor viktig det er for oss at vi kan stole på at vår kommunikasjon med andre holdes konfidensiell. Det har imidlertid ikke vært like mye debatt omkring bruken av de metadata som akkumuleres ved vår bruk av ulike kommunikasjonskanaler. Datatilsynet mener det er svært positivt med en tydelig anerkjennelse av at metadata er dekket av kommunikasjonsvernet.

Hvilke endringer det er ønskelig at norske myndigheter skal jobbe for i den videre prosessen.

I fortalen til forslaget til ePrivacy forordning er det slått fast at behandlinger av personopplysninger etter ePrivacy forordningen skal nyte samme beskyttelsesnivå som etter personvernforordningen[1]. I det følgende peker vi på de deler av ePrivacy forordningen som kan resultere i at borgerne får et dårligere vern av sin kommunikasjon enn det som er tilfelle etter personvernforordningen. Dette er sider ved forordningen som vi ønsker at norske myndigheter skal jobbe for å endre.

Strengere vilkår for å tillate sporing av mobile enheter
Alle bærbare enheter har en MAC-adresse som kan knyttes til innehaveren av enheten – altså en personopplysning. En stadig mer utbredt teknologi som gjør bruk av MAC-adresser er Wifi-tracking eller Bluetooth-tracking som har som formål å analysere brukeradferd. Måten dette gjøres på er at en virksomhet fanger opp og lagrer MAC-adressene til de enhetene som

[1] Fortalens punkt 5

befinner seg i et område, kalkulerer lokasjon over tid for å se hvor vedkommende bruker beveger seg. Dette er maskin-til-maskin kommunikasjon som skjer uten at noen spesifikt setter i gang en innsamling av opplysninger der og da.

Med ePrivacy forordningen følger det en anerkjennelse av at kommunikasjon som skjer maskin-til-maskin også er personopplysninger som skal nyte godt av kommunikasjonsvern. Forutsatt at en slik anerkjennelse kommer til utrykk som materielle rettigheter for borgerne mener vi at dette er en presisering som bidrar sterkt til å styrke personvernet.

I det foreliggende forordningen er det imidlertid slik at den ansvarlige for denne type Wifi-tracking eller Bluetooth-tracking kun er forpliktet til å sørge for informasjon til den registrerte om at de blir sporet, og en mulighet til å reservere seg. Vi mener at denne type sporing ville utløse et krav om samtykke etter personvernforordningen, og at kun rett til informasjon og reservasjon betyr en lavere grad av beskyttelse enn etter personvernforordningen. Unntak fra et slikt samtykkekrav kan være aktuelt for løsninger som etableres i en lite inngripende form, for eksempel sporing i kort tid og hvor identifikatorer pseudonymiseres.

Vi mener også at innhenting av samtykke lar seg praktisk gjennomføre ved for eksempel bruk av en app som inviterer brukere til å tillate sporing i bestemte områder.

Datatilsynet ønsker at norske myndigheter skal jobbe for at det stilles krav om samtykke for å kunne spore enkeltpersoner ved hjelp av bærbare enheters MAC-adresser.

Analyse av kommunikasjonens innhold og metadata må ha samme beskyttelse
Som nevnt over mener Datatilsynet det er et stort fremskritt for personvernet at forordningen slår fast at metadata om kommunikasjon er egnet til å avsløre svært sensitive opplysninger om hver av oss.

Samtidig registrerer vi at forordningen opererer med to ulike beskyttelsesnivå for innholdsdata og metadata. For å analysere innholdsdata kreves det at sluttbrukerne samtykker til dette, mens for metadata er det tilstrekkelig å oppfylle et skjønnsmessig nødvendighetskrav knyttet til blant annet fakturering. Gitt presumsjonen at begge typer data avslører svært sensitive opplysninger om hver av oss, og at analyse av slike data representerer et betydelig inngrep i vår private sfære, bør de nyte samme beskyttelsesnivå.

Vi mener hovedregelen for analyse av både innholdsdata og metadata må være samtykke fra sluttbrukerne, og at eventuelle unntak kan spesifiseres nærmere.

Datatilsynet ønsker at norske myndigheter skal jobbe for at hovedregelen for å kunne analysere metadata om enkeltpersoners kommunikasjon blir samtykke på lik linje med kravene som stilles for å analysere innholdsdata.

Krav om innebygd personvern på datamaskiner og programvare
Vi lever i en tid hvor antallet kommunikasjonsplattformer øker og med dem tredjeparter som ønsker å høste personopplysninger fra disse plattformene. Det er derfor viktig at ePrivacy forordningen gjelder for all programvare som legger til rette for kommunikasjon, inkludert søkemotorer, operasjonssystem, apper og brukergrensesnitt for Internet of Things. Behovet for sluttbrukerne til å ha kontroll med hvem som gis tilgang til deres personopplysninger øker proporsjonalt med kompleksiteten i utstyr, programvare og aktører som ønsker å «koble seg på».

På denne bakgrunn mener vi at det er særskilt viktig å fremheve personvernforordningens krav til innebygd personvern.

ePrivacy forordningens krav til leverandører av programvare om å gi sluttbruker muligheten til å hindre en begrenset form for inngripen i datamaskinen vil ikke tilfredsstille det som kreves for å ha innebygd personvern. Innebygd personvern ville være at maskinvare og programvare hadde standardinnstillinger som gjorde at urettmessig inngripen automatisk ble forhindret.

Datatilsynet ønsker at norske myndigheter skal jobbe for at det stilles krav om at maskinvare og programvare skal ha standardinnstillinger som gjør at urettmessig inngripen automatisk blir forhindret.

Forbud mot tracking walls
Mange nettsider opererer i dag med en praksis hvor sluttbrukere for å få tilgang til innholdet på nettsiden må «samtykke» til å la seg spore over tid og ved bruk av andre nettsider. Dette kalles «tracking walls» og er en type praksis vi mener er svært invaderende med hensyn til personvern.

Datatilsynet ønsker at norske myndigheter skal jobbe for et forbud mot «tracking walls».

Mulighet for spesialregulering
Vi er kjent med at NKOM bruker en del ressurser på saksbehandling av søknader om dispensasjon fra taushetsplikt. Vi mener at dagens regler om dispensasjon fra taushetsplikt, og saksbehandling av slike søknader ikke nødvendigvis er en oppgave som vil følge med ePrivacy forordningen. Dette fordi det i forslaget til ePrivacy forordning art. 11 er åpnet for et nasjonalt handlingsrom for å ha unntaksregler fra kommunikasjonvern. Ordninger som legger til rette for søknad om dispensasjon fra kommunikasjonsvern kan følgelig spesialreguleres utenfor ePrivacy forordningen. Datatilsynet bør for øvrig ikke ha noen rolle i denne type rutinemessig godkjenning da slik forvaltning bør følge sektorprinsippet.

Datatilsynet anmoder Samferdselsdepartementet om å jobbe for å utnytte det mulighetsrommet som ligger i forordningens art. 11 for spesialregulering.

Sammendrag

- Datatilsynet ønsker et nytt, harmonisert regelverk hva gjelder kommunikasjonsvern velkommen.

- Datatilsynet er positive til å påta seg et nytt myndighetsområde og nye tilsynsoppgaver.

- Datatilsynet mener at forordningens anerkjennelse av sensitiviteten av kommunikasjonens innhold og metadata er viktig.

- Endringer som norske myndigheter bør jobber for å få med er:

  -Strengere vilkår for å tillate sporing av mobile enheter
  -Analyse av kommunikasjonens innhold og metadata må ha samme beskyttelse
  -Krav om innebygd personvern på datamaskiner og programvare
  -Forbud mot «tracking walls»

Med vennlig hilsen

Bjørn Erik Thon
direktør

Eirin Oda Lauvset
seniorrådgiver

Kopi: Kommunal- og moderniseringsdepartementet
v/Statsforvaltningsavdelingen
Postboks 8112 Dep, 0032 OSLO