

## **Erklæring fra Det Europæiske Databeskyttelsesråd om revisionen af e-databeskyttelsesforordningen og om dennes indvirkning på beskyttelse af enkeltpersoner med hensyn til den private og fortrolige karakter af deres kommunikation**

Databeskyttelsesmyndighederne i den Europæiske Union, der er samlet i Det Europæiske Databeskyttelsesråd, finder, at revisionen af det nuværende e-databeskyttelsesdirektiv (2002/58/EF, ændret ved 2009/136/EF) er et vigtigt og nødvendigt tiltag, som skal afsluttes hurtigt. IP-baserede kommunikationstjenester har været almindeligt udbredt siden 2009, og disse "over-the-top"-tjenester er i dag ikke omfattet af det nuværende direktiv. For at sikre at slutbrugernes kommunikationshemmelighed beskyttes, når disse nye tjenester anvendes, og for at skabe lige konkurrencevilkår for leverandører af elektronisk kommunikation og funktionelt tilsvarende tjenester, opfordrer vi Europa-Kommissionen, Parlamentet og Rådet til at arbejde sammen for at sikre en hurtig vedtagelse af den nye e-databeskyttelsesforordning. Denne forordning vil erstatte det nuværende direktiv snarest muligt, efter at den generelle forordning om databeskyttelse fik virkning fra maj i år.

I betragtning af at drøftelserne om forslaget skrider frem, og til gavn for medlovgiverne, har Databeskyttelsesrådet besluttet at tilbyde yderligere vejledning og præciseringer om nogle særlige forhold, der nævnes i de ændringer, som medlovgiveren har foreslået.

### **1. For at beskytte kommunikationshemmeligheden kræves der i forbindelse med elektronisk kommunikation særlig beskyttelse, der går ud over databeskyttelsesforordningen**

Kommunikationshemmeligheden (nutidens svar på brevhemmeligheden i forbindelse med postforsendelser) er en grundlæggende rettighed, der er beskyttet i henhold til artikel 7 i den Europæiske Unions Charter om Grundlæggende Rettigheder, og som allerede er gennemført ved e-databeskyttelsesdirektivet. Denne ret til fortrolighed skal anvendes i forbindelse med al elektronisk kommunikation, uanset hvilke midler der anvendes til at afsende kommunikationen, når den er i hvile eller i transit, fra afsenderen til modtageren, og rettigheden skal også beskytte integriteten af alle brugeres terminaludstyr.

Elektronisk kommunikation er fundamentet for mange væsentlige aktiviteter i vores moderne samfund, da kommunikationen understøtter udøvelsen af mange grundlæggende rettigheder, såsom retten til at tænke frit, samvittighedsfriheden, religionsfriheden, ytringsfriheden, informationsfriheden, forsamlingsfriheden, foreningsfriheden osv. Det er derfor nødvendigt at styrke kommunikationshemmeligheden og neutraliteten i de beskedtjenester, som formidler vores kommunikation.

I lyset af hvor vigtig og hvor udbredt anvendelsen af elektronisk kommunikation er i vores digitale tilværelse, er det meget sandsynligt, at denne kommunikation indeholder eller afslører særlige kategorier af personoplysninger, enten udtrykkeligt eller på grund af en simpel ophobning og blanding af indhold eller metadata fra elektronisk kommunikation. Herved gøres det muligt at drage meget nøjagtige konklusioner om personernes privatliv, som kan udgøre en høj risiko for deres rettigheder og deres frihedsrettigheder, og behandlingen af oplysningerne bør således tage højde herfor.

Derfor støtter vi fuldt ud tilgangen i den foreslåede forordning, der er baseret på brede forbud, snævre undtagelser og anvendelsen af samtykke. Følgelig bør der ikke være nogen mulighed ifølge e-databeskyttelsesforordningen for at behandle elektronisk kommunikationsindhold og elektroniske kommunikationsmetadata ved at angive uindskrænkede grunde, som f.eks. "legitime interesser", der går videre end, hvad der er nødvendigt for at levere elektroniske kommunikationstjenester. Herudover bør der ifølge e-databeskyttelsesforordningen ikke være mulighed for at behandle elektroniske kommunikationsmetadata med henblik på at opfylde en kontrakt. Dette betyder, at der ikke bør være en undtagelse baseret på det overordnede formål om opfyldelse af en kontrakt, da det fastlægges i forordningen, præcis hvilken databehandling, der er tilladt i denne henseende, som f.eks. behandling med henblik på at fakturere.

Databeskyttelsesrådet vil gerne understrege, at elektroniske kommunikationsmetadata stadig kan behandles yderligere uden samtykke, efter at de er blevet helt anonymiserede<sup>1</sup>. Databeskyttelsesrådet opfordrer leverandører af elektroniske kommunikationstjenester til at benytte sig af denne mulighed for at skabe innovative tjenester og samtidigt sikre databeskyttelsen.

## **2. E-databeskyttelsesdirektivet er allerede i kraft**

Beskyttelse af kommunikationshemmeligheden er en rettighed, der allerede gælder i dag. Ved e-databeskyttelsesdirektivet fra 2002, som blev ændret i 2009, fastsattes der allerede et generelt forbud mod behandling af elektronisk kommunikationsindhold og elektroniske kommunikationsmetadata. Disse operationer er kun mulige:

- med forudgående samtykke fra brugeren, eller
- hvis de omfattes af en af undtagelserne i henhold til e-databeskyttelsesdirektivet (overføring af en elektronisk kommunikation eller debitering)

Transmissionstjenester, som anvendes til formidling af kommunikation mellem maskiner og maskintjenester, er også omfattet af det nuværende direktiv. Disse bestemmelser fastholdes i forslaget til forordningen.

Tilsvarende er beskyttelsen af terminaludstyr allerede en rettighed. Opbevaringskapaciteter i brugerens terminaludstyr anvendes på en teknologineutral måde. Det er således ikke kun cookies, men alle springsteknologier, der allerede kræver brugerens samtykke eller er omfattet af en af undtagelserne, som er fastlagt i e-databeskyttelsesdirektivet.

Herudover indføres der i den foreslåede forordning, som ændret af medlovgiveren, en række nye undtagelser, der var foreslået af Artikel 29-Gruppen<sup>2</sup>, som for eksempel sikkerhedsopdateringer og måling af antal besøgende. Disse undtagelser angår særlige typer behandling med meget begrænsede risici for brugernes privatliv.

---

<sup>1</sup> Som angivet i udtalelsen fra Artikel 29-Gruppen [WP216](#), hvorimod pseudonymiserede oplysninger forbliver personoplysninger.

<sup>2</sup> Se [WP194](#) og [WP240](#)

### **3. Forslaget til forordningen har til formål at sikre en ensartet anvendelse i alle medlemsstater og af alle typer dataansvarlige**

Det nuværende e-databeskyttelsesdirektiv anvendes ikke på elektroniske kommunikationstjenester, der tilbydes af leverandører, som opererer på internettet, på trods af at de leverer en tjeneste, der er funktionelt tilsvarende.

Disse leverandører er dog omfattet af den foreslåede forordning. Databeskyttelsesrådet understreger, at udvidelsen af forordningens anvendelsesområde til funktionelt tilsvarende tjenester, inkl. de såkaldte "over-the-top"-tjenester, er et vigtigt element af reformen. Forslag til ændringer af udkastet til forordning, som kan underminere dette mål (for eksempel forslag om at begrænse anvendelsesområdet for beskyttelse til kommunikationsdata "i transit"), bør undgås for at sikre lige konkurrencevilkår for alle leverandører.

Forslaget til forordning finder også anvendelse, så snart der indsamles oplysninger om brugerens adfærd, uanset om denne har oprettet en konto for en tjeneste eller ej. Denne tilgang vil ikke blot muliggøre den beskyttelse, som brugerne af disse tjenester fortjener, men den vil også skabe mulighed for fair konkurrence mellem de dataansvarlige. Det bør bemærkes, at det samtykke, som skal indhentes ifølge e-databeskyttelsesforordningen, har den samme betydning som i databeskyttelsesforordningen. Især vil kravet om at indhente et frivilligt samtykke forhindre tjenesteudbydere i at indføre "*cookie walls*"<sup>3</sup> over for brugerne, og kravet om, at samtykket skal være specifikt vil skabe lige konkurrencevilkår for leverandørerne, uanset om brugeren er logget på eller ej.

Herudover vil indførelsen af specifikke sanktioner for at overtræde e-databeskyttelsesforordningen i kombination med det udvidede territoriale anvendelsesområde, som begge afspejler bestemmelserne i databeskyttelsesforordningen, give reel beføjelse til databeskyttelsesmyndighederne, der får mulighed for at håndhæve forordningen for alle de elektroniske kommunikationsværktøjer, som brugerne i EU anvender.

### **4. I den nye forordning skal samtykkekravet om cookies og lignende teknologier håndhæves, og tjenesteudbydere skal tilbydes at anvende de tekniske værktøjer, som muliggør, at de kan indhente dette samtykke**

Som foreslået af Kommissionen er artikel 10 i forslaget til forordning udarbejdet med henblik på at give brugerne mulighed for at kontrollere brugen af lagringsfunktionerne i deres terminaludstyr. Artikel 10 blev videreudviklet af Parlamentet til at indeholde krav om privatlivsbeskyttelse som standard med hensyn til softwareindstillingerne og for at give websteder en teknisk løsning til indhentelse af gyldigt samtykke.

Databeskyttelsesrådet støtter fuldt ud forbedringen af denne artikel og finder, at den udtrykkeligt bør anvendes på operativsystemer til smartphones, tablets og alle andre "brugeragenter" for at sikre, at kommunikationsapplikationerne kan tage hensyn til de valg, som brugerne træffer, uanset hvilke tekniske midler der benyttes.

Herudover bør privatlivsindstillingerne fremme, at der kan gives og trækkes samtykke tilbage på en enkel måde, der er bindende og kan gøres gældende over for alle parter, og brugerne bør ved installationen gives et entydigt valg, der giver dem mulighed for at give samtykke, hvis de ønsker at give det. Desuden bør applikationer til websteder og mobiltelefoner gennem privatlivsindstillingerne kunne indhente et samtykke i overensstemmelse med databeskyttelsesforordningen.

---

<sup>3</sup> En "*cookie wall*" forhindrer brugere, som ikke har givet deres samtykke, i at få adgang til et websted eller en tjeneste.

## 5. Konklusioner

Databeskyttelsesrådet finder:

- E-databeskyttelsesforordningen bør ikke føre til et lavere beskyttelsesniveau end det, der følger af det nuværende e-databeskyttelsesdirektiv.
- E-databeskyttelsesforordningen bør beskytte alle typer elektronisk kommunikation, inkl. de typer som udføres ved hjælp af "over-the-top"-tjenester, på en teknologineutral måde.
- Der bør systematisk indhentes samtykke fra brugerne på en teknisk gennemførlig måde, som kan håndhæves, før der sker behandling af elektroniske kommunikationsdata og før anvendelse af lagrings- eller behandlingsfunktionerne i en brugers terminaludstyr. Der bør ikke være nogen undtagelser for at behandle disse data baseret på den dataansvarliges "legitime interesser" eller det almene formål om opfyldelse af en kontrakt.
- I artikel 10 bør der fastsættes en effektiv måde, hvorpå applikationer til websteder og mobiltelefoner kan indhente samtykke. Mere overordnet bør indstillingerne sikre brugernes privatlivsbeskyttelse som standard, og brugerne bør vejledes om valget af en indstilling gennem relevante og gennemsigtige oplysninger. I denne henseende bør forordningen forblive teknologineutral for at sikre, at den til stadighed anvendes på en ensartet måde, uanset i hvilke tilfælde den benyttes.
- Der bør anvendes en særdeles nøje kontrol med alle konkrete undtagelser, som lovgiverne eventuelt ønsker at føje til de undtagelser, der allerede er medtaget i udkastene fra Kommissionen og Parlamentet. Især bør alle bredt formulerede undtagelser i tilfælde, hvor "en offentlig myndighed" anmoder om behandling af data, nøje kontrolleres, og forslaget bør ikke give mulighed for vilkårlig overvågning af brugernes placering eller for behandling af deres metadata.
- For at give et frivilligt samtykke, jf. kravet i databeskyttelsesforordningen, må adgangen til tjenester og funktioner ikke gøres betinget af, at en bruger giver samtykke til behandling af personoplysninger eller til behandling af oplysninger, der vedrører eller er behandlet af slutbrugernes terminaludstyr, hvilket indebærer, at "cookie walls" udtrykkeligt bør forbydes.
- Der bør opfordres til at anvende helt anonymiserede elektroniske kommunikationsdata.
- Ovennævnte tiltag vil beskytte slutbrugernes privatliv i enhver relevant sammenhæng og forhindre eventuelle konkurrenceforvridninger.