

Dataskydd.net Sverige  
Alsnögatan 18  
116 41 Stockholm

DFRI  
Box 3644  
103 59 Stockholm

MOTTAGARE: Post- och telestyrelsen, Näsäkerhetsavdelningen

## *Remissyttrande över Post- och telestyrelsens förslag till riktlinjer för LEK 6 kap 18 § – Dnr 17-9703*

Innehållsförteckning:

<i>Sammanfattning</i>	1
<i>Samtycke</i>	2
<i>Användning av webbkakor</i>	3
<i>Funktionellt eller inte, det är frågan</i>	4
<i>Teknisk standardisering och självreglering</i>	5

### *Sammanfattning*

- ✓ Riktlinjerna bör göra en uppdelning mellan funktionsbaserade webbkakor å ena sidan, och icke-funktionsbaserade webbkakor å andra sidan.
- ✓ Post- och telestyrelsen bör säkerställa att deras aktiviteter på andra områden inte i onödan orsakar eller påbjuder användning av icke-funktionsbaserade webbkakor.
- ✓ Riktlinjerna bör följa den av Post- och telestyrelsen redan etablerade definitionen av samtycke, i stället för att göra en ny och egen definition av samtycke med besvärande följdproblem.

Föreningen för digitala fri- och rättigheter (DFRI) är en ideell och partipolitiskt obunden förening som verkar för främjandet av digitala rättigheter. Föreningen har bland annat ansvarat för projektet PTS-knappen, som avser bestämmelserna i LEK 6 kap. 18 §, sedan 2012.<sup>1</sup>

Dataskydd.net är en svensk ideell, partipolitiskt obunden förening som verkar för bättre tekniskt och juridiskt dataskydd för privatpersoner i Sverige.

<sup>1</sup><https://dfri.se/pts-knappen>

## Samtycke

Post- och telestyrelsen (PTS) föreslår i dag att samtycke ska innebära följande:

1. ett översiktligt meddelande och fullständig information om användning av kakor lämnas och
2. användaren enkelt, till exempel genom inställningar i webbläsaren, kan
  - (a) förhindra att de kakor som används på webbplatsen lagras eller hämtas,
  - (b) granska vilka kakor som lagrats samt
  - (c) radera lagrade kakor.

2

men tidigare har PTS förslagit att ett samtycke ska utgöra

varje slag av frivillig, särskild och otvetydig viljeyttring genom vilken den registrerade, efter att ha fått information, godtar behandling av personuppgifter som rör honom eller henne /.../[och att] endast den vars uppgifter ska behandlas, /.../ med egen vilja kan godta behandlingen.<sup>3</sup> /.../ Även om samtyckesinhämtningen oftast sker i samband med avtalsingående får dock inhämtningen av samtycke inte framstå som ett avtalsvillkor. Ett avtal utgör en överenskommelse mellan flera parter medan ett samtycke utgörs av en ensidig viljeyttring från den som lämnar det.<sup>4</sup>

Det är inte uppenbart hur PTS skiljer mellan det samtycksgrundande *meddelandet* (som webbplatsansvarige själv får formulera, utan inflytande av den som samtycker) och det *avtal* som PTS menar inte i och av sig själv kan utgöra ett samtycke, och särskilt inte utgöra ett samtycke *innan* den som samtycker tagit del av det.

Inte heller är det uppenbart att inställningar i webbläsaren kan ersätta det individuella samtycket. Betyder det att privatpersoner på förhand, genom inställningspanelen, måste förutse hur de förhåller sig till avtal de ännu inte sett? Webbläsare är idag inte behäftade med sådana funktioner som PTS förutsätter i sitt andra samtyckeskriterium.

PTS har inte i sin Konsekvensbedömning eller i övrigt förklarat att det finns en strategi för att behäfta webbläsare med sådana funktionaliteter som låter den föreslagna definitionen av samtycke bli ett *individuellt samtycke* i svensk och europeisk juridisk mening. För att PTSs förslag alls ska kunna antas uppfylla något krav om samtycke krävs föreställningen att webbläsaren på något sätt kan *agera i konsumentens namn* och *avge samtycke åt konsumenten*.

Men om *webbläsaren* ska antas ha något i stil med en fullmakt att agera i konsumentens ställe, skapas en rad problem i andra sammanhang: vad händer om webbläsaren ”godkänner” installation av spyware, trojaner eller annan skadlig kod, kanske för att konsumenten låtit bli att instruera webbläsaren att inte köra javascript<sup>5</sup> eller för att konsumenten inte använder en reklamblockerare?<sup>6</sup>

PTS bryter mot sina egna tidigare föreskrifter på området, vilket knappast är önskvärt om målsättningen är att skapa tydligare klarhet. Dessutom bryter PTS

<sup>2</sup>Förslag till Post- och telestyrelsens allmänna råd om användande av kakor och andra jämförbara tekniker, s. 3.

<sup>3</sup>PTS-ER-2015:27, Inhämta samtycke enligt LEK – En vägledning, s. 7.

<sup>4</sup>Ibid., s. 8.

<sup>5</sup>Jfr. insticksprogrammet NoScript för webbläsaren Mozilla Firefox.

<sup>6</sup>Jfr. Adblock Plus eller µBlock Origin.

mot ambitionen att tolkningen av samtyckesbegreppet ska vara liknande i LEK som i PUL, enligt vad PTS tidigare anförde.

Genom att anspela på fantastiska tekniska funktionaliteter i användarutrustning som inte finns, framstår förslaget mer som ett försök från PTS att undvika att lagbestämmelsen alls tillämpas än som ett praktiskt sätt att tillämpa lagbestämmelsen.

### *Användning av webbkakor*

PTSs riktlinjer innehåller inga bestämmelser om *när* webbkakor bör användas. Av skäl 66 till direktiv 2009/136/EG framgår att lagstiftaren föreställt sig att vissa webbkakor är mer legitima än andra, så frågan är hur skillnaden mellan *legitima kakor* och *illegitima kakor* ska göras.

Av skäl 66 framgår lyckligtvis att denna distinktion kan göras när ”tekniska lagringen eller åtkomsten är strikt nödvändig av *det legitima skälet* att möjliggöra användning av en specifik tjänst som uttryckligen efterfrågas av abonnenten eller användaren.” Legitimitetskravet är alltså ett *funktionalitetskrav*, vilket uttrycks i den svenska lagstiftningen som att bestämmelserna om webbkakor ”[inte] hindrar sådan lagring eller åtkomst *som behövs för att överföra* ett elektroniskt meddelande via ett elektroniskt kommunikationsnät eller *som är nödvändig för att tillhandahålla* en tjänst som användaren eller abonnenten uttryckligen har begärt.” [våra kursiveringar i bägge lagcitaten]

PTS borde ha uppehållit sig på definitionen av *legitimt skäl, som behövs* eller *som är nödvändig*.

Många webbkakor används av reklamföretag som kontinuerligt vill utvärdera och mäta egenskaper och beteenden hos webbpubliker, för att kunna rikta reklam mot enskilda privatpersoner baserat på klassificeringar av deras egenskaper. Är dessa webbkakor *nödvändiga* i lagen om elektronisk kommunikationsbemärkelse, eftersom de krävs för att finansiera webbtjänsten i den utsträckning webbtjänsten företrädesvis försörjer sig genom reklamintäkter? Om så vore fallet, skulle ju bestämmelsen i LEK och ePrivacy-direktivet inte alls tillämpas mot dessa aktörer, och ingen ruta vore nödvändig. Det är denna sorts juridiska problem som PTS tråkigt nog undviker, men som behöver svar.

Dataskydd.net är skeptiska mot en sådan tolkning av lagstiftningen eftersom ordet *tillhandahållande* på andra ställen i den svenska lagtexten<sup>7</sup> används för att beskriva en teknisk funktionalitet, snarare än underliggande marknadsmekanism. För ordet *överföring* gäller analogt resonemang: lagstiftaren har avsett att ordet ska tolkas mot bakgrund av dess tekniska implementation, inte mot bakgrund av de affärsmodeller som överföraren avsett ska finansiera överföringen.

Frågan är alltså i stället vad som är *funktionsbaserade webbkakor* (webbkakor som möjliggör att spara information om vad konsumenten lagt i en köpkorg, komma ihåg att en användare är inloggad, eller som används för att komma ihåg inställningar konsumenten gjort på webbplatsen), och *icke-funktionsbaserade webbkakor* (webbkakor som relaterar till en bakomliggande affärsmodell eller finansieringsmodell för de tekniska funktionerna på webbplatsen).

<sup>7</sup>LEK 1 kap. 7 §, t. ex.

### *Funktionellt eller inte, det är frågan*

Vi menar att LEK 6 kap. 18 § ska i stället tolkas som att den etablerar en distinktion mellan *funktionsbaserade webbkakor* och *icke-funktionsbaserade webbkakor*, och att regeringens hänvisningar till integritetskränkningar samt EU-lagstiftarens resonemang i övrigt ger stöd för denna tolkning.

Samtycke krävs då inte för webbkakor som

- kommer ihåg att en användare är inloggad, eller
- kommer ihåg inställningar som användaren har gjort på webbplatsen, eller
- motsvarande tekniskt nödvändiga funktion.

Informationskraven kan för dessa webbkakor utformas på enkla och intuitiva sätt för konsumenten: till exempel kan ett meddelande om användningen av webbkakor placeras i anslutning till den funktionalitet som kräver webbkakor (i närheten av knappen som anger ”lägg i varukorg”, eller ”logga in”).

Samtycke och därmed även utförligare information krävs i stället för webbkakor som

- motiveras av ett behov att kartlägga användningen av webbplatsen, eller
- motiveras av ett behov att få bättre kännedom om webbplatsens besökare, eller
- motsvarande till webbplatsen ekonomiskt betingade funktion.

För dessa fall kan krävas en pop-up-ruta, ett PUL-avtal (framtida GDPR-avtal) och en möjlighet för konsumenten att ta ställning till om webbkakan alls får lagras i konsumentens webbläsares kakregister.

PTS bör, utöver att förtydliga uppdelningen mellan funktionsbaserade och icke-funktionsbaserade webbkakor, dessutom se över riktlinjer som PTS utfärdar i andra sammanhang. Det PTS-finansierade projektet [webbriktlinjer.se](https://webbriktlinjer.se) innehåller till exempel tre rekommendationer som borde ses över utifrån risken att de förleder verksamheter som förlitar sig på riktlinjerna att ägna sig åt olovlig användning av webbkakor enligt LEK:

1. Riktlinje 107 (Prio 2). Analysera hur webbplatsen kommer att användas, och av vem.<sup>8</sup>
2. Riktlinje 37 (Prio 3). Följ upp hur webbplatsen används.<sup>9</sup>
3. Riktlinje 36 (Prio 4). Kontrollera besöksstatistiken och sökbeteendet regelbundet.<sup>10</sup>

Samtliga rekommendationer lånar sig idag till intrycket att webbutvecklaren måste utforma webbplatsen på ett sådant sätt att icke-funktionsbaserade webbkakor placeras på konsumentens dator. Riktlinjerna bör i stället uppmuntra webbutvecklare att använda utvecklingstekniker som inte kräver icke-funktionsbaserade webbkakor.

Dataskydd.net har i sina projekt [Webbkoll](https://webbkoll.dataskydd.net)<sup>11</sup> och [Kommunundersökning](https://kommuner.dataskydd.net)<sup>12</sup> precis arbetat med att hitta sätt att komma ifrån den sortens icke-funktionella användning av webbkakor som man lätt förleds att implementera av riktlinjerna. Även om våra projekt är dataskyddsbetonade, det vill säga orienterade kring

<sup>8</sup><https://webbriktlinjer.se/riktlinjer/107-utfor-anvandningsanalys/>

<sup>9</sup><https://webbriktlinjer.se/riktlinjer/37-folj-upp-hur-webbplatsen-anvands/>

<sup>10</sup><https://webbriktlinjer.se/riktlinjer/36-kontrollera-regelbundet-besoksstatistik-och-sokbeteende/>

<sup>11</sup><https://webbkoll.dataskydd.net>

<sup>12</sup><https://dataskydd.net/kommuner>

privatpersoners möjlighet att förutse och förstå hur deras personuppgifter används i digitala miljöer, tror vi att våra resultat och rekommendationer går att använda även för att uppfylla lagen om elektronisk kommunikation.

### *Teknisk standardisering och självreglering*

Det är klandervärt att PTS har väntat så länge med att utfärda riktlinjer. Medan PTS har rullat tummarna har möjligheterna till teknisk standardisering på det sätt som föreslås i direktivet 2009/136/EC, skäl 66, i princip passerat.

Trots initiala försök i organet för webbläsarstandardisering, W3C, att komma till bukt med den situation som EU:s lagstiftare 2009 försökte åtgärda, lyckades starka ekonomiska intresser avvärja projektet genom att göra det ohållbart. Helt industridrivna standardiseringsorgan, som bygger på frivilligt deltagande från aktörer i näringslivet och ideell sektor, kan nämligen bara uppnå sådana målsättningar som inte ligger i konflikt med några särskilt starka näringslivsaktörers egenupplevda ekonomiska intresse.

Det slår undan benen på premisserna för både konkurrensupprätthållande lagstiftning och konsumentskyddande lagstiftning, om tillsynsmyndigheter väljer att strunta i en viss lagstiftning bara för att de som ska tillämpa den inte vill bli reglerade.

Men ytterligare klander bör naturligtvis riktas mot PTS i det att de inte bara undlåtit att skapa riktlinjer för LEK 6 kap. 18 §, utan dessutom skapat webbriktlinjer som aktivt motarbetar lagbestämmelsens syfte.