

Uttalande av EDPB om översynen av e-integritetsförordningen och dess inverkan på skyddet för enskilda personer med avseende på integriteten och konfidentialiteten i deras kommunikation

Dataskyddsmyndigheterna i den Europeiska unionen, samlade i Europeiska dataskyddsstyrelsen, anser att en översyn av det nuvarande e-integritetsdirektivet (2002/58/EG, ändrat genom 2009/136/EG) är ett viktigt och nödvändigt steg som måste slutföras snabbt. Användandet av IP-baserade kommunikationstjänster har blivit utbrett sedan 2009 och dessa ”over-the-top”-tjänster omfattas för närvarande inte av det befintliga direktivet. För att säkerställa att användarnas konfidentialitet skyddas vid kommunikation då man utnyttjar dessa nya tjänster och för att skapa lika villkor för leverantörer av elektronisk kommunikation och funktionsmässigt likvärdiga tjänster uppmanar vi kommissionen, Europaparlamentet och rådet att arbeta tillsammans för att få till stånd ett snabbt antagande av e-integritetsförordningen, som ersätter det nuvarande direktivet så snart som möjligt efter ikraftträdandet av den allmänna dataskyddsförordningen i maj i år.

Med tanke på överläggningarna om förslaget, och till förmån för medlagstiftarna, har EDPB beslutat att ge ytterligare råd och förtydliganden angående vissa specifika frågor avseende de föreslagna ändringarna från medlagstiftaren.

1. Konfidentialitet vid elektronisk kommunikation kräver särskilt skydd utöver GDPR

Konfidentialitet vid kommunikation (den moderna motsvarigheten till den traditionella posthemligheten) är en grundläggande rättighet som skyddas enligt artikel 7 i stadgan om de grundläggande rättigheterna, och har redan införts genom e-integritetsdirektivet. Denna rätt till konfidentialitet måste tillämpas på all elektronisk kommunikation, oavsett på vilket sätt den sänds, vid vila och vid överföring, från avsändaren till mottagaren, och måste också skydda integriteten i alla användares terminalutrustning.

Elektronisk kommunikation är en hörnsten i många viktiga aktiviteter i våra moderna samhällen eftersom den stöder utövandet av många grundläggande rättigheter såsom tankefrihet, samvetsfrihet, religionsfrihet, yttrandefrihet, informationsfrihet, mötes- och föreningsfrihet osv. Det är därför nödvändigt att stärka konfidentialiteten och neutraliteten i de meddelandetjänster som tillhandahåller kommunikationen.

Med tanke på betydelsen och den utbredda användningen av elektronisk kommunikation i våra digitala liv är det mycket sannolikt att kommunikationen innehåller eller avslöjar särskilda kategorier av personuppgifter, antingen uttryckligen eller på grund av den blotta anhopningen och kombinationen av innehåll eller metadata, vilket gör det möjligt att dra mycket exakta slutsatser när det gäller människors privatliv, vilket innebär en hög risk för deras rättigheter och friheter, och därför bör behandlas därefter.

Därför stödjer vi fullt ut strategin i förslaget till förordning, som bygger på breda förbud, snäva undantag och tillämpning av samtycke. Det bör således inte ges någon möjlighet enligt e-integritetsförordningen att behandla innehåll från elektronisk kommunikation och metadata baserade på öppna grunder, såsom ”berättigade intressen”, som går utöver vad som är nödvändigt för tillhandahållandet av en elektronisk kommunikationstjänst. Det bör vidare inte ges möjlighet enligt e-integritetsförordningen att behandla metadata från elektronisk kommunikation för att fullgöra ett avtal, vilket innebär att det inte bör finnas undantag på grundval av det allmänna syftet med fullgörandet av avtalet, eftersom det i förordningen fastställs vilken exakt behandling som är tillåten för detta ändamål, exempelvis för faktureringsändamål.

EDPB vill betona att metadata från elektronisk kommunikation fortfarande kan behandlas utan samtycke efter att de verkligen har anonymiserats¹. EDPB uppmanar leverantörer av elektroniska kommunikationstjänster att utnyttja denna möjlighet för att skapa innovativa tjänster och samtidigt skydda integriteten.

2. e-integritetsdirektivet är redan i kraft

Skydd av konfidentialitet vid kommunikation är en rättighet som finns redan i dag. e-integritetsdirektivet från 2002, som ändrades 2009, innehåller redan ett allmänt förbud mot behandling av innehållet i elektronisk kommunikation och metadata. Sådana transaktioner är endast möjliga

- med samtycke från användaren, eller
- om de uppfyller ett av undantagen enligt e-integritetsdirektivet (överföring av elektronisk kommunikation, fakturering).

Överföringstjänster som används för tillhandahållande av maskin till maskin-tjänster omfattas också av det nuvarande direktivet. Dessa bestämmelser bibehålls i den föreslagna förordningen. På samma sätt är skyddet av terminalutrustning också redan en rättighet. Användningen av lagringskapaciteten i användarens terminalutrustning tillämpas på ett teknikneutralt sätt. Således är inte bara användningen av kakor, utan all spårningsteknik redan avhängigt av samtycke från användaren eller något av de undantag som anges i e-integritetsdirektivet.

Dessutom kan man i den föreslagna förordningen som ändrats av medlagstiftaren möjliggöra flera nya undantag som föreslogs av Artikel 29-gruppen², såsom säkerhetsuppdateringar och publikmätning. Dessa undantag avser särskilda typer av behandling med mycket begränsade integritetsrisker för användarna.

3. Den föreslagna förordningen syftar till att säkerställa en enhetlig tillämpning i alla medlemsstater och för alla typer av personuppgiftsansvariga

Det nuvarande e-integritetsdirektivet gäller inte elektroniska kommunikationstjänster som erbjuds av leverantörer som verkar över internet, trots att de erbjuder en tjänst som funktionellt sett är likvärdig.

Dessa leverantörer kommer dock att omfattas av den föreslagna förordningen. EDPB betonar att utökandet av förordningens tillämpningsområde till funktionsmässigt likvärdiga tjänster, inklusive så kallade ”over-the-top”-tjänster är ett viktigt inslag i reformen. Föreslagna ändringar i utkastet

¹ Enligt definitionen i [WP216](#), medan pseudonymiserade uppgifter förblir personuppgifter.

² Se [WP194](#) och [WP240](#)

till förordning som skulle kunna undergräva detta mål (t.ex. förslag att begränsa räckvidden av skyddet till kommunikationsdata som ”håller på att överföras”) bör undvikas, för att garantera lika villkor för alla leverantörer.

Den föreslagna förordningen gäller även så snart som uppgifter om användarnas beteende samlas in, oavsett om de har skapat ett konto för en tjänst eller inte. Detta kommer inte bara att erbjuda användarna av sådana tjänster det skydd de förtjänar, utan också möjliggöra en rättvis konkurrens mellan personuppgiftsansvariga. Det bör noteras att det medgivande som måste erhållas i enlighet med e-integritetsförordningen har samma innebörd som i GDPR. Framför allt kravet på att erhålla ett samtycke som har lämnats frivilligt kommer att hindra tjänsteleverantörer från att sätta upp kakväggar³ för sina användare, och skyldigheten att samtycket ska vara specifikt kommer att skapa lika konkurrensvillkor för leverantörer oavsett om användaren har loggat in eller inte.

Dessutom kommer inrättandet av särskilda påföljder för brott mot e-integritetsförordningen i kombination med ett utvidgat territoriellt tillämpningsområde, vilka båda speglar bestämmelserna i GDPR, att ge dataskyddsmyndigheterna verklig befogenhet, vilket kommer att ge dem möjlighet att verkställa tillämpningen av förordningen för alla elektroniska kommunikationsverktyg som används av användare inom EU.

4. Den nya förordningen måste tillämpa kravet på samtycke för kakor och liknande tekniker och erbjuda tjänsteleverantörer tekniska verktyg som gör det möjligt för dem att erhålla samtycke

På Europeiska kommissionens förslag är artikel 10 i den föreslagna förordningen utformad för att ge användare kontroll över användningen av deras terminalutrustnings lagringskapacitet. Europaparlamentet vidareutvecklade artikel 10 för att kräva integritetsskydd som standard för programvaruinställningar och tillhandahålla en teknisk lösning för att webbplatser ska kunna erhålla ett giltigt samtycke.

EDPB ger sitt fulla stöd till att stärka denna artikel, och anser att den uttryckligen bör gälla för operativsystem i smarta telefoner, surfplattor och alla andra ”användaragenter”, för att säkerställa att kommunikationsapplikationer kan beakta användarnas val, oavsett vilka tekniska medel som är inblandade.

Dessutom bör integritetsinställningar göra det lättare att ge och dra tillbaka samtycke på ett enkelt, bindande och genomförbart sätt gentemot alla parter, och användarna bör erbjudas ett tydligt val vid installationen, så att de kan ge sitt samtycke om de så önskar. Dessutom bör webbplatser och mobilapplikationer genom integritetsinställningarna kunna erhålla ett samtycke som överensstämmer med GDPR.

5. Slutsatser

Europeiska dataskyddsstyrelsen anser att:

- e-integritetsförordningen inte bör sänka den skyddsnivå som erbjuds genom det nuvarande direktivet om integritet och elektronisk kommunikation.
- e-integritetsförordningen bör ge skydd för alla typer av elektronisk kommunikation, inklusive de som utförs av ”over-the-top”-tjänster, på ett teknikneutralt sätt.
- Användarens samtycke bör inhämtas systematiskt på ett tekniskt genomförbart och verkställbart sätt innan data från elektronisk kommunikation behandlas eller innan kapacitet används för lagring eller behandling i en användares terminalutrustning. Det bör

³ En ”kakvägg” hindrar användare som inte samtycker från tillträde till en webbplats eller en tjänst.

inte finnas några undantag för att behandla dessa uppgifter på grundval av den personuppgiftsansvarigas "berättigade intresse", eller ett allmänt syfte att fullgöra ett avtal.

- Artikel 10 bör föreskriva ett effektivt sätt att erhålla samtycke för webbplatser och mobilapplikationer. Mer generellt bör inställningarna som standard skydda användarnas integritet, och dessa bör instrueras att välja en inställning efter att ha mottagit relevant och tydlig information. I detta avseende bör förordningen förbli teknikneutral för att säkerställa att dess tillämpning är konsekvent oavsett användningstyp.
- Den högsta nivån av granskning bör tillämpas på eventuella undantag i särskilda fall som lagstiftarna kan överväga att lägga till dem som redan ingår i kommissionens och Europaparlamentets förslag. I synnerhet bör allmänna typer av undantag i fall där en "offentlig myndighet" begär behandling av uppgifter granskas noga, och förslaget bör inte tillåta urskillningslös övervakning av var användarna befinner sig eller behandling av deras metadata.
- För att samtycket ska vara frivilligt i den mening som avses i GDPR får tillgången till tjänster och funktioner inte göras beroende av en användares samtycke till behandling av personuppgifter eller behandling av information som rör eller behandlas av slutanvändares terminalutrustning, vilket innebär att kakväggar uttryckligen bör förbjudas.
- Användningen av verkligt anonymiserade data från elektronisk kommunikation bör uppmuntras.
- Dessa förändringar kommer att skydda slutanvändarnas integritet i alla relevanta sammanhang och förhindra en snedvridning av konkurrensen.