Europeiska unionens råd

Bryssel den 16 januari 2017
(OR. en)

Interinstitutionellt ärende:
2017/0003 (COD)

5358/17
ADD 4

TELECOM 12
COMPET 32
MI 45
DATAPROTECT 4
CONSOM 19
JAI 40
DIGIT 10
FREMP 3
CYBER 10
IA 12
CODEC 52

FÖLJENOT

från:	Jordi AYET PUIGARNAU, direktör, för Europeiska kommissionens generalsekreterare
inkom den:	12 januari 2017
till:	Jeppe TRANHOLM-MIKKELSEN, generalsekreterare för Europeiska unionens råd
Komm. dok. nr:	SWD(2017) 4 final
Ärende:	ARBETSDOKUMENT FRÅN KOMMISSIONENS AVDELNINGAR SAMMANFATTNING AV KONSEKVENSBEDÖMNINGEN Följedokument till Förslag till Europaparlamentets och rådets förordning om respekt för privatlivet och skydd av personuppgifter i samband med elektronisk kommunikation och om upphävande av direktiv 2002/58/EG (förordning om integritet och elektronisk kommunikation)

För delegationerna bifogas dokument – SWD(2017) 4 final.

Bilaga: SWD(2017) 4 final

EUROPEISKA
KOMMISSIONEN

Bryssel den 10.1.2017
SWD(2017) 4 final

ARBETSDOKUMENT FRÅN KOMMISSIONENS AVDELNINGAR

SAMMANFATTNING AV KONSEKVENSBEDÖMNINGEN

Följedokument till

Förslag till Europaparlamentets och rådets förordning

om respekt för privatlivet och skydd av personuppgifter i samband med elektronisk kommunikation och om upphävande av direktiv 2002/58/EG (förordning om integritet och elektronisk kommunikation)

{COM(2017) 10 final}
{SWD(2017) 3 final}
{SWD(2017) 5 final}
{SWD(2017) 6 final}

A. Behov av åtgärder

Vad är problemet och varför är det ett problem?

Konsekvensbedömningen har genomförts parallellt med efterhandsutvärderingen av direktivet om integritet och elektronisk kommunikation (*direktivet*) inom ramen för programmet om lagstiftningens ändamålsenlighet och resultat (*Refit-programmet*).

Den allmänna slutsatsen är att direktivets syften fortfarande är relevanta.

Refit-utvärderingen identifierade tre huvudproblem:

- Skyddet av medborgarnas privatliv är otillräckligt i samband med onlinekommunikation.
- Medborgarna har inte något effektivt skydd mot icke begärd marknadsföring.
- Företagen möter hinder i form av fragmenterad lagstiftning, olika rättsliga tolkningar i olika medlemsstater och otydliga och föråldrade bestämmelser.

Refit-utvärderingen visade också att det finns utrymme för förenkling, särskilt när det gäller en del föråldrade eller onödiga bestämmelser och bestämmelserna om kontroll av efterlevnaden.

Detta stöds också av Refit-plattformens yttrande, där det rekommenderas att skyddet av medborgarnas privatliv stärks genom en anpassning av direktivet om integritet och elektronisk kommunikation till den allmänna dataskyddsförordningen, genom att det införs undantag från samtyckesbestämmelsen för kakor och genom att kommissionen åtgärdar nationella genomförandeproblem.

Vad vill man uppnå?

De särskilda målen med översynen är att

1. säkerställa effektiv konfidentialitet vid elektronisk kommunikation,
2. säkerställa ett effektivt skydd mott icke begärd kommersiell kommunikation, och
3. öka harmoniseringen och förenkla/uppdatera den rättsliga ramen.

Vad är mervärdet med åtgärder på EU-nivå?

Eftersom elektronisk kommunikation, särskilt sådan som är baserad på internetprotokoll, har en global räckvidd är problemet inte begränsat till enskilda medlemsstaters territorium. De nationella bestämmelserna om konfidentialitet vid kommunikation skiljer sig mycket från varandra i fråga om tillämpningsområde och innehåll. Medlemsstaterna skulle visserligen kunna genomföra politiska åtgärder som säkerställer att denna rättighet inte överträds, men det skulle inte kunna uppnås på ett enhetligt sätt utan gemensamma EU-bestämmelser. Det skulle också medföra begränsningar för de gränsöverskridande flödena av personuppgifter i samband med användningen av elektroniska kommunikationstjänster till andra medlemsstater som inte uppfyller samma datskyddskrav.

Den kommande översynen av direktivet bedöms uppfylla både subsidiaritetsprincipen och proportionalitetsprincipen i och med harmoniseringsinriktningen och samarbetsmekanismen bevaras, samtidigt som medlemsstaterna kan vidta nationella undantagsåtgärder för särskilda legitima ändamål.

B. Lösningar

Vilka olika alternativ finns för att nå målen? Finns det ett rekommenderat alternativ? Om inte, varför?

Alternativen behandlas efter ambitionsnivå i förhållande till ovannämnda mål (personlig integritet och förenkling). Alternativ 1 har lägst ambitionsnivå och alternativ 4 högst. Under alternativ 5 analyseras ett upphävande av direktivet.

1. **Alternativ 1: Andra åtgärder än lagstiftning (icke-bindande instrument)**: Alternativet omfattar riktlinjer från kommissionen samt uppmuntran till självregleringsinitiativ och andra icke-bindande åtgärder.

2. **Alternativ 2: Begränsad förstärkning av den personliga integriteten/konfidentialiteten samt harmonisering**: Alternativet omfattar den lägsta graden av förstärkning av rätten till personlig integritet och konfidentialitet (genom ett klargörande av att instrumentet för integritet och elektronisk kommunikation omfattar OTT-leverantörer, allmänt tillgänglig wifi och sakernas internet) och skydd mot icke begärda samtal (klargörande av de nuvarande bestämmelserna och införande av ett standardprefix) samt förenkling (upphävande av säkerhetsbestämmelser, stärkande av samarbetet i gränsöverskridande ärenden).

3. **Alternativ 3: Måttlig förstärkning av den personliga integriteten/konfidentialiteten samt harmonisering**: Alternativet omfattar en mer omfattande förstärkning av rättigheterna avseende integritet och konfidentialitet (utvidgat tillämpningsområde, öppnare redovisning av sekretessinställningar, ökad öppenhet och insyn, stärkta verkställandebefogenheter), skydd mot icke begärd kommunikation (marknadsföringssamtal endast till dem som godkänt det (*opt-in*)) och förenkling (utökade undantag, upphävande av ytterligare onödiga bestämmelser och rationaliserad kontroll av efterlevnaden genom att befogenheter ges till de myndigheter som ansvarar för den allmänna dataskyddsförordningen och mekanismen för enkelhet enligt den förordningen utvidgas).

4. **Alternativ 4: Långtgående förstärkning av den personliga integriteten/konfidentialiteten samt harmonisering.** Alternativet omfattar mer långtgående åtgärder utöver alternativ 3, t.ex. ett allmänt förbud mot väggar mot kakor (*cookie walls*), upphävande av undantaget för tidigare affärsförhållanden när det gäller marknadsföring via e-post och sms, ytterligare upphävanden och kommissionens genomförandebefogenheter.

5. **Alternativ 5: Upphävande av direktivet**: Alternativet föreskriver att direktivet upphävs och att den allmänna dataskyddsförordningen sedan tillämpas, inbegripet systemet för kontroll av efterlevnad, för att skydda konfidentialiteten för personuppgifter i samband med elektronisk kommunikation. Det omfattar en allmän tillämpning av ett system som innebär att den som inte vill ha icke-begärd kommunikation anmäler det (*opt-out system*) och att mekanismen för enkelhet enligt den allmänna dataskyddsförordningen används.

Vilka är de olika aktörerna? Vem stöder vilka alternativ?

- **Medborgarnas** rättigheter påverkas av skyddsnivån för konfidentialiteten vid kommunikation. De skulle förespråka alternativ som stärker deras rättigheter, som alternativen 2, 3 och 4.
- **Nationella myndigheter och Europeiska datatillsynsmannen** skulle stödja alternativ som stärker skyddet av den personliga integriteten och gör det mer konsekvent, som alternativen 2, 3 och 4.
- **Leverantörer av elektronisk kommunikation** är den viktigaste målgruppen för direktivets skyldigheter. De skulle starkt förespråka alternativ 5. Som nödlösning skulle de kanske kunna godta alternativen 2 och 3, som säkerställer att konkurrerande OTT-leverantörer omfattas av

samma bestämmelser.

- **OTT-leverantörer** skulle också förespråka alternativen 1 och 5, eftersom de normalt föredrar att inte omfattas av striktare regleringskrav. Efter dessa alternativ skulle alternativ 3 vara det mest godtagbara, eftersom det ger ett visst manöverutrymme.
- **Utgivare av webbplatser och leverantörer av beteendebaserad reklam (OBA)**skulle helt klart föredra alternativ 5 av samma skäl som leverantörer av elektroniska kommunikationstjänster och OTT-leverantörer.
- **Leverantörer av webbläsare** skulle omfattas av särskilda skyldigheter enligt alternativ 3. De skulle därför inte stödja alternativ 3 och 4.
- **Små och medelstora företag** skulle generellt stödja alternativ 1 och 5. Leverantörer av elektroniska kommunikationstjänster skulle stödja alternativ 2 och 3 i och med att OTT-leverantörer får samma konkurrensvillkor. OTT-leverantörer skulle dock föredra alternativ 1 och 5, och därefter skulle alternativ 3 vara mest godtagbart för dem.

C. Det rekommenderade alternativets konsekvenser

Vad är nyttan med det rekommenderade alternativet (om sådana alternativ finns, annars anges för huvudsakliga alternativ)?

Det rekommenderande alternativet är alternativ 3. De viktigaste fördelarna är följande:

- Ökat skydd av konfidentialiteten genom en teknikneutral definition, förbättrad kontroll för användarna, stärkta krav på öppenhet och effektivare kontroll av efterlevnaden.
- Förbättrat skydd mot icke begärd kommunikation i och med att ”opt-in” införs för marknadsföringssamtal och att man inför ett prefix, förbjuder anonyma marknadsföringssamtal och ökar möjligheterna att blockera samtal från oönskade nummer.
- Förenkling genom harmonisering och ett förtydligade regleringsvillkoren. i och med att man minskar det manöverutrymme som lämnats åt medlemsstaterna, upphäver föråldrade bestämmelser och breddar undantagen från samtyckesbestämmelserna.

Vad är kostnaderna för de rekommenderade alternativen (om sådana alternativ finns, annars anges för huvudsakliga alternativ)?

Det rekommenderade alternativet förväntas ge besparingar till följd av ytterligare harmonisering och förenkling. Man beräknas t.ex. kunna göra besparingar på upp till 70 % av kostnaderna för integritet och elektronisk kommunikation genom en centraliserad förvaltning av sekretessval som görs en enda gång för alla webbplatser och tillämpningar.

Om man tittar på enskilda kategorier av aktörer skulle **OTT-aktörer** få en del kostnader kopplade ändrad rättslig status för affärsmodellerna. Dessa kostnader väntas dock inte bli betydande. **Utgivare av webbplatser** kan få vissa mindre anpassningskostnader. **Leverantörer av webbläsare och liknande tillämpningar som möjliggör internettillgång** skulle få betydande kostnader för att säkerställa att användarna får rätt valmöjligheter när det gäller sekretessinställningar. **Marknadsförare** skulle få vissa kostnader genom införandet av ”opt-in” för marknadsföringssamtal.

Påverkas medlemsstaternas budgetar och förvaltningar i betydande grad?

Den viktigaste påverkan på nationella budgetar och förvaltningar kommer från genomförandet av mekanismen för enhetlighet och det eventuella behovet av att flytta alla befogenheter till dataskyddsmyndigheterna när det gäller kontroll av efterlevnaden. Påverkan anses dock inte vara betydande eftersom samverkan med befintliga EU-samordningsorgan (t.ex. på dataskyddsområdet) skulle kunna utnyttjas.

Uppstår andra betydande konsekvenser?
Nej.
Proportionalitet?
Det rekommenderade alternativet omfattar väl avvägda åtgärder som samtliga anses nödvändiga för att målet ska kunna uppnås utan att det medför några orimliga bördor för berörda aktörer. Åtgärderna är också flexibelt utformade, så att nödvändiga undantag tillåts, och teknikneutrala för att minska snedvridningen av konkurrensen och säkra lika konkurrensvillkor.
D. Uppföljning
När kommer åtgärderna att ses över?
Kontinuerlig övervakning kommer att säkerställas genom bl.a. medlemsstaternas rapporter till kommissionen och kommissionens rapporter till Europaparlamentet, rådet och Europeiska ekonomiska och sociala kommittén.