Rada
Unii Europejskiej

Bruksela, 16 stycznia 2017 r.
(OR. en)

Międzyinstytucjonalny numer referencyjny:
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

PISMO PRZEWODNIE

Od:	Sekretarz Generalny Komisji Europejskiej, podpisał dyrektor Jordi AYET PUIGARNAU
Data otrzymania:	12 stycznia 2017 r.
Do:	Jeppe TRANHOLM-MIKKELSEN, Sekretarz Generalny Rady Unii Europejskiej
Nr dok. Kom.:	SWD(2017) 4 final
Dotyczy:	DOKUMENT ROBOCZY SŁUŻB KOMISJI STRESZCZENIE OCENY SKUTKÓW Towarzyszący dokumentowi: wniosek dotyczący rozporządzenia Parlamentu Europejskiego i Rady w sprawie poszanowania życia prywatnego oraz ochrony danych osobowych w łączności elektronicznej i uchylające dyrektywę 2002/58/WE (rozporządzenie w sprawie prywatności i łączności elektronicznej)

Delegacje otrzymują w załączeniu dokument SWD(2017) 4 final.

Zał.: SWD(2017) 4 final

KOMISJA
EUROPEJSKA

Bruksela, dnia 10.1.2017 r.
SWD(2017) 4 final

DOKUMENT ROBOCZY SŁUŻB KOMISJI

STRESZCZENIE OCENY SKUTKÓW

Towarzyszący dokumentowi:

Wniosek
ROZPORZĄDZENIE PARLAMENTU EUROPEJSKIEGO I RADY

w sprawie poszanowania życia prywatnego oraz ochrony danych osobowych w łączności elektronicznej i uchylające dyrektywę 2002/58/WE (rozporządzenie w sprawie prywatności i łączności elektronicznej)

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

A. Konieczność podjęcia działań

Na czym polega problem i dlaczego jest to problem?

Ocenę skutków przeprowadzono równolegle do oceny *ex post* dyrektywy o prywatności i łączności elektronicznej w ramach programu sprawności i wydajności regulacyjnej (REFIT).

Z ocen tych płynie ogólny wniosek, że cele dyrektywy o prywatności i łączności elektronicznej są nadal aktualne.

W wyniku oceny REFIT określono trzy główne grupy problemów:

- życie prywatne obywateli przy komunikowaniu się przez internet nie jest dostatecznie i skutecznie chronione;
- obywatele nie są skutecznie chronieni przed niezamawianymi materiałami marketingowymi;
- przedsiębiorstwa napotykają przeszkody spowodowane niejednolitymi przepisami oraz różnymi interpretacjami prawnymi w poszczególnych państwach członkowskich, jak również niejasnymi i przestarzałymi przepisami.

Na podstawie oceny REFIT uznano, że można byłoby uprościć przepisy, szczególnie w z uwagi na istnienie pewnych przestarzałych lub zbędnych przepisów oraz zasad egzekwowania.

Taki sam pogląd wyrażono również w opinii platformy REFIT, w której zalecono wzmocnienie ochrony życia prywatnego obywateli poprzez dostosowanie dyrektywy o prywatności i łączności elektronicznej do ogólnego rozporządzenia o ochronie danych, dodanie wyjątków do zasady wyrażania zgody na pliki cookie oraz ustosunkowanie się przez Komisję do problemów z wdrożeniem na szczeblu krajowym.

Co należy osiągnąć?

Cele szczegółowe przeglądu są następujące:

1. zapewnienie skutecznej poufności komunikacji elektronicznej;
2. zapewnienie skutecznej ochrony przez niezamawianymi informacjami handlowymi;
3. wzmocnienie harmonizacji i uproszczenie/aktualizacja ram prawnych.

Jaka jest wartość dodana działania na szczeblu UE?

Ponieważ łączność elektroniczna, szczególnie ta oparta ta protokołach internetowych, ma globalny zasięg, wymiary problemu wykraczają poza terytorium pojedynczego państwa członkowskiego. Krajowe przepisy dotyczące poufności komunikacji znacznie się różnią pod względem zakresu i treści. Chociaż państwa członkowskie mogą realizować politykę, która zapewni, aby prawo to nie było naruszane, celu tego nie osiągnięto by w sposób jednolity ze względu na brak wspólnych zasad unijnych i powodowałoby związane z korzystaniem z usług łączności elektronicznej ograniczenia w transgranicznym przepływie danych osobowych do innych państw członkowskich, które nie spełniają tych samych norm ochrony danych.

Planowany przegląd dyrektywy o prywatności i łączności elektronicznej uważa się za zgodny z zasadą pomocniczości i proporcjonalności dzięki utrzymaniu podejścia harmonizacyjnego i mechanizmów współpracy, jednocześnie zaś umożliwia on państwom członkowskim przyjmowanie krajowych środków stanowiących odstępstwa motywowane konkretnymi prawnie uzasadnionymi celami.

B. Rozwiązania

Jakie są różne warianty działań służących osiągnięciu celów? Czy istnieje wariant preferowany? Jeżeli nie, dlaczego?

Warianty pogrupowano rosnąco według poziomu ambicji co do realizowania powyższych celów (jakimi są prywatność i uproszczenie) (wariant 1 jest najmniej ambitny, a wariant 4 jest najambitniejszy). W wariancie 5 rozważa się uchylenie dyrektywy o prywatności i łączności elektronicznej.

1. **Wariant 1: Środki nielegislacyjne („prawo miękkie”)**: obejmują wytyczne przedstawione przez Komisję, zachęcanie do inicjatyw na rzecz samoregulacji oraz inne środki prawa miękkiego.

2. **Wariant 2: Ograniczone wzmocnienie prywatności/poufności i ujednolicenie**: przewiduje się w nim minimalne wzmocnienie praw w zakresie prywatności/poufności (poprzez doprecyzowanie, że zakres instrumentu dotyczącego prywatności i łączności elektronicznej obejmuje usługi OTT, publicznie dostępne sieci WiFi oraz urządzenia internetu rzeczy) oraz ochronę przed niepożądanymi połączeniami (z doprecyzowaniem obecnych przepisów i wprowadzeniem wymogu stosowania znormalizowanego prefiksu), jak również uproszczenie (uchylenie przepisów o bezpieczeństwie, wzmocnienie współpracy w sprawach transgranicznych).

3. **Wariant 3: Wymierne wzmocnienie prywatności/poufności i ujednolicenie**: zawiera istotniejsze wzmocnienie praw w zakresie prywatności/poufności (rozszerzenie zakresu, poprawę przejrzystości ustawień prywatności, większą przejrzystość, wzmocnienie uprawnień w zakresie egzekwowania praw), ochronę przed niepożądanymi połączeniami (wprowadzenie możliwości rezygnacji z połączeń marketingowych) oraz uproszczenie (rozszerzenie wyjątków, dalsze uchylanie zbędnych przepisów i uporządkowanie egzekwowania przepisów przez powierzenie uprawnień organom odpowiedzialnym za egzekwowanie ogólnego rozporządzenia o ochronie danych oraz rozszerzenie mechanizmów spójności tego rozporządzenia).

4. **Wariant 4: Daleko idące wzmocnienie prywatności/poufności i ujednolicenie:** wprowadza się w nim idące jeszcze dalej środki poza opisanymi w wariancie 3, takie jak ogólny zakaz tak zwanych „ścian cookie”, uchylenie wyjątku uprzednich relacji biznesowych w odniesieniu do marketingu prowadzonego za pośrednictwem poczty elektronicznej i wiadomości tekstowych, dodatkowe uchylenia i uprawnienia wykonawcze Komisji.

5. **Wariant 5: Uchylenie dyrektywy o prywatności i łączności elektronicznej**: przewiduje się uchylenie dyrektywy o prywatności i łączności elektronicznej oraz stosowanie ogólnego rozporządzenia o ochronie danych, w tym systemu egzekwowania, na potrzeby ochrony poufności danych osobowych związanych z łącznością elektroniczną; uogólnione stosowanie systemu możliwości rezygnacji z niezamawianych materiałów i zastosowanie mechanizmu spójności przewidzianego w ogólnym rozporządzeniu o ochronie danych.

Kto należy do zainteresowanych stron? Które strony popierają poszczególne warianty?

- Na prawa **obywateli** wpływa poziom ochrony poufności ich komunikacji. Opowiadaliby się oni za wariantami wzmacniającymi ich prawa, takimi jak wariant 2, 3 i 4.
- **Organy krajowe i EIOD** poparłyby **warianty** prowadzące do większej i spójniejszej ochrony prywatności, takie jak wariant 2, 3 i 4.

- **Dostawcy łączności elektronicznej** są głównymi adresatami obowiązków przewidzianych dyrektywą o prywatności i łączności elektronicznej. Zdecydowanie opowiadaliby się za wariantem 5. W drugiej kolejności byliby skłonni zaakceptować wariant 2 i 3, w których przewiduje się, że konkurujący z nimi dostawcy usług OTT podlegaliby tym samym przepisom.
- Również dostawcy **usług OTT** skłanialiby się ku wariantowi 1 i 5, ponieważ woleliby nie być objęci bardziej rygorystycznymi wymogami regulacyjnymi. Poza wspomnianymi dwoma najszerzej akceptowalnym wariantem byłby wariant 3 z uwagi na stopień elastyczności, jaki zapewnia.
- **Właściciele stron internetowych i podmioty zajmujące się internetową reklamą behawioralną,** z tych samych względów co dostawcy łączności elektronicznej i dostawcy OTT, zdecydowanie preferowaliby wariant 5.
- **Dostawcy przeglądarek internetowych** w wariancie 3 mieliby szczególne obowiązki. Z tego względu nie poparliby wariantu 3 ani 4.
- **MŚP** zasadniczo opowiedziałyby się za wariantem 1 i 5. Jeżeli są dostawcami usług łączności elektronicznej, poparłyby wariant 2 i 3 z równymi warunkami działania względem dostawców usług OTT. Jeżeli są dostawcami usług OTT, preferowały wariant 1 i 5, a wariant 3 byłby na trzecim miejscu.

C. Skutki wariantu preferowanego

Jakie są korzyści wariantu preferowanego (jeżeli nie określono takiego wariantu – głównych wariantów)?

Preferowany jest wariant 3. Główne korzyści są następujące:

- wzmocnienie ochrony poufności poprzez definiowanie neutralne pod względem technologicznym, zwiększona kontrola użytkownika i wymogi w zakresie przejrzystości, a także skuteczniejsze egzekwowanie przepisów;
- wzmocnienie ochrony przeciwko niezamawianym materiałom dzięki wprowadzeniu możliwości rezygnacji z połączeń marketingowych, wprowadzeniu prefiksu oraz wynikającemu z tego zakazowi wykonywania anonimowych połączeń marketingowych, jak również większe możliwości w zakresie blokowania połączeń z niepożądanych numerów;
- uproszczenie poprzez ujednolicenie i doprecyzowanie otoczenia regulacyjnego dzięki ograniczeniu pola manewru państw członkowskich, uchylenie przestarzałych przepisów i rozszerzenie wyjątków od zasad wyrażenia zgody.

Jakie koszty pociągnie za sobą wariant preferowany (jeżeli nie określono takiego wariantu – główne warianty)?

Oczekuje się, że wariant preferowany przyniesie oszczędności ze względu na dodatkowe ujednolicenie i uproszczenie. Przykładowo obliczono, że oszczędność kosztów związanych z prywatnością i łącznością elektroniczną osiągnięta poprzez scentralizowane zarządzanie ustawieniami prywatności dla wszystkich stron internetowych i aplikacji to oszczędność w wysokości do 70 %.

Na poziomie poszczególnych kategorii zainteresowanych stron pewne koszty związane z przeglądem modeli biznesowych pod kątem zgodności z prawem będą musieli ponieść dostawcy **usług OTT**. Niemniej jednak nie przewiduje się, aby były to znaczne koszty. **Właściciele stron internetowych** mogą ponieść pewne niewielkie koszty związane z dostosowaniem. **Dostawcy przeglądarek i podobnych aplikacji umożliwiających dostęp do internetu** musieliby ponieść znaczne koszty, aby zapewnić użytkownikom odpowiednie opcje wyboru w ustawieniach prywatności. **Telemarketerzy** ponieśliby pewne koszty w następstwie wprowadzenia możliwości rezygnacji z połączeń marketingowych.

Czy skutki dla krajowych budżetów i administracji będą znaczące?
Główne skutki dla krajowych budżetów i administracji będą wynikać z wdrożenia mechanizmów spójności oraz ewentualnej potrzeby przesunięcia uprawnień w zakresie egzekwowania przepisów wyłącznie na organy odpowiedzialne za ochronę danych. Skutek nie będzie dotkliwy, ponieważ można wykorzystać synergię z istniejącymi już unijnymi organami koordynacyjnymi (np. w obszarze ochrony danych).
Czy wystąpią inne znaczące skutki?
Nie.
Proporcjonalność?
Wariant preferowany obejmuje wyważone środki, z których wszystkie zdają się konieczne do realizacji wyznaczonych celów bez nakładania nadmiernego obciążenia na stosowne zainteresowane strony. Ponadto środki zaprojektowano jako elastyczne, aby umożliwić konieczne wyjątki, a także aby były one neutralne pod względem technologicznym, co ma ograniczyć do minimum zakłócenia konkurencji i zapewnić równe warunki działania.
D. Działania następcze
Kiedy nastąpi przegląd przyjętej polityki?
Ciągłe monitorowanie zostanie zapewnione między innymi dzięki sprawozdaniom przedkładanym Komisji przez państwa członkowskie oraz Parlamentowi Europejskiemu, Radzie i Komitetowi Ekonomiczno-Społecznemu przez Komisję.