

Bruxelles, 16. siječnja 2017.
(OR. en)

Međuinstitucijski predmet:
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

POP RATNA BILJEŠKA

Od:	Glavni tajnik Europske komisije, potpisao g. Jordi AYET PUIGARNAU, direktor
Datum primitka:	12. veljače 2017.
Za:	g. Jeppe TRANHOLM-MIKKELSEN, glavni tajnik Vijeća Europske unije
Br. dok. Kom.:	SWD(2017) 4 final
Predmet:	RADNI DOKUMENT SLUŽBI KOMISIJE SAŽETAK PROCJENE UČINKA Priložen dokumentu Prijedlog Uredbe Europskog parlamenta i Vijeća o poštovanju privatnog života i zaštiti osobnih podataka u elektroničkim komunikacijama te stavljanju izvan snage Direktive 2002/58/EZ (Uredba o privatnosti i elektroničkim komunikacijama)

Za delegacije se u prilogu nalazi dokument SWD(2017) 4 final.

Priloženo: SWD(2017) 4 final



Bruxelles, 10.1.2017.
SWD(2017) 4 final

RADNI DOKUMENT SLUŽBI KOMISIJE

SAŽETAK PROCJENE UČINKA

Priložen dokumentu

Prijedlog Uredbe Europskog parlamenta i Vijeća

o poštovanju privatnog života i zaštiti osobnih podataka u elektroničkim komunikacijama te stavljanju izvan snage Direktive 2002/58/EZ (Uredba o privatnosti i elektroničkim komunikacijama)

{COM(2017) 10 final}

{SWD(2017) 3 final}

{SWD(2017) 5 final}

{SWD(2017) 6 final}

A. Potreba za djelovanjem

Što je problem i zašto?

Procjena učinka provedena je usporedno s *ex post* evaluacijom Direktive o privatnosti i elektroničkim komunikacijama (ePD) u okviru programa za prikladnost i učinkovitost propisa (REFIT).

Opći je zaključak da su ciljevi ePD-a i dalje relevantni.

U evaluaciji u okviru programa REFIT utvrđene su tri glavne skupine problema:

- tijekom komuniciranja na internetu privatni život građana nije dostatno i učinkovito zaštićen
- građani nisu učinkovito zaštićeni od neželjenog marketinga
- poduzeća se zbog rascjepkanog zakonodavstva, razlika u pravnim tumačenjima među državama članicama te nejasnih i zastarjelih odredbi suočavaju s preprekama

U evaluaciji u okviru programa REFIT zaključeno je i da postoji prostor za pojednostavnjenje, posebno određenih zastarjelih ili nepotrebnih odredbi i pravila o provedbi.

To je potvrđeno i u mišljenju platforme REFIT u kojem se preporučuje jačanje zaštite privatnog života građana usklađivanjem Direktive o privatnosti i elektroničkim komunikacijama s Općom uredbom o zaštiti podataka, i to dodavanjem izuzeća od pravila o suglasnosti za kolačiće te zahtjevom da Komisija rješava nacionalne provedbene probleme.

Što je potrebno postići?

Konkretni su ciljevi Direktive sljedeći:

1. osiguravanje učinkovite povjerljivosti elektroničkih komunikacija
2. osiguravanje učinkovite zaštite od neželjenih komercijalnih komunikacija
3. jačanje usklađivanja i pojednostavnjenja/ažuriranja pravnog okvira.

Koja je dodana vrijednost djelovanja na razini EU-a?

S obzirom na globalni doseg elektroničkih komunikacija, posebno onih koje se temelje na internetskim protokolima, riječ je o širem problemu koji ne obuhvaća samo državna područja pojedinačnih država članica. Nacionalna pravila o povjerljivosti komunikacija znatno se razlikuju u području primjene i sadržaju. Stoga, iako države članice mogu donijeti političke odluke za sprječavanje povrede tog prava, to se bez zajedničkih pravila na razini EU-a ne bi postiglo ujednačeno i stvorile bi se prepreke prekograničnom protoku osobnih podataka povezanih s uporabom elektroničkih komunikacijskih usluga prema drugim državama članicama koje nemaju jednake norme za zaštitu podataka.

Smatra se da je predstojeća revizija Direktive o privatnosti i elektroničkim komunikacijama u skladu s načelima supsidijarnosti i proporcionalnosti jer se njome zadržavaju pristup usklađivanja i mehanizmi suradnje, a državama članicama omogućuje se donošenje nacionalnih odstupajućih mjera u posebne legitimne svrhe.

B. Rješenja

Kojim se različitim mogućnostima mogu ostvariti ciljevi? Daje li se prednost određenoj mogućnosti? Ako ne, zašto?

Mogućnosti su grupirane u skladu s njihovom razinom ambicioznosti (tj. 1. mogućnost najmanje je

ambiciozna, a 4. je najambicioznija) u pogledu postizanja navedenih ciljeva (privatnost i pojednostavnjenje). U 5. mogućnosti razmatra se stavljanje ePD-a izvan snage.

1. mogućnost: nezakonodavne („pravno neobvezujuće”) mjere, obuhvaćene su smjernice koje je dala Komisija: poticanje samoregulatornih inicijativa i drugih neobvezujućih pravnih mjera

2. mogućnost: ograničeno jačanje privatnosti/povjerljivosti i usklađivanje: predviđeni su minimalno jačanje prava na privatnost/povjerljivost (zahvaljujući jasnom utvrđivanju područja primjene instrumenta iz Direktive o privatnosti i elektroničkim komunikacijama koji obuhvaća pružatelje OTT usluga, javno dostupne WiFi i IoT uređaje), zaštita od neželjenih poziva (zahvaljujući jasnom utvrđivanju postojećih pravila i uvođenju standardnog predbroja) te pojednostavnjenje (stavljanje izvan snage odredbi o zaštiti podataka, jačanje suradnje u prekograničnim predmetima)

3. mogućnost: odmjereno jačanje privatnosti/povjerljivosti i usklađivanje: predviđeni su znatno jačanje prava na privatnost/povjerljivost (proširenje područja primjene, pojačana transparentnost postavki privatnosti, povećanje transparentnosti, jačanje izvršnih ovlasti), zaštita od neželjenih komunikacija (zahvaljujući uvođenju te mogućnosti za marketinške pozive) te pojednostavnjenje (proširenje iznimaka, daljnje stavljanje izvan snage nepotrebnih odredbi i racionalizacija provedbe postojećih dodjelom ovlasti tijelima odgovornima za provedbu Opće uredbe o zaštiti podataka i proširenje mehanizma konzistentnosti iz Opće uredbe o zaštiti podataka).

4. mogućnost: dalekosežno jačanje privatnosti/povjerljivosti i usklađivanje: uz 3. mogućnost predviđene su i dalekosežne mjere kao što su opća zabrana obveznog prihvatanja kolačića (*cookie walls*) stavljanje izvan snage iznimke od korištenja prethodnog poslovnog odnosa za marketing e-poštom i SMS-om, dodatna stavljanja izvan snage te provedbene ovlasti Komisije.

5. mogućnost: stavljanje ePD-a izvan snage: predviđeno je stavljanje ePD-a izvan snage i osiguravanje primjenjivosti Opće uredbe o zaštiti podataka, uključujući sustav za provedbu zaštite povjerljivosti osobnih podataka koji se odnose na elektroničke komunikacije; opća primjena sustava izuzeća (*opt-out*) za neželjene komunikacije i primjena mehanizma konzistentnosti iz Opće uredbe o zaštiti podataka.

Tko su dionici? Tko podupire koju opciju?

- Na prava **građana** utječe razina zaštite povjerljivosti njihovih komunikacija. Građani bi dali prednost mogućnostima kojima se ta prava jačaju, primjerice 2., 3. i 4. mogućnosti.
- **Nacionalna tijela i Europski nadzornik za zaštitu podataka** dali bi prednost mogućnostima bolje i dosljednije zaštite privatnosti, primjerice 2., 3. i 4. mogućnosti.
- Obveze iz ePD-a prvenstveno se odnose na **pružatelje elektroničkih komunikacijskih usluga**. Oni bi se snažno zalagali za 5. mogućnost. Kao drugu opciju mogli bi prihvatiti 2. i 3. mogućnost koje bi zajamčile da konkurentni pružatelji OTT usluga podliježu istim pravilima.
- Pružatelji **Over-the-Top** usluga zalagali bi se i za 1. i 5. mogućnost jer općenito radije ne bi podliježali strožim regulatornim zahtjevima. Treća bi mogućnost bila najprihvatljivija nakon te dvije, s obzirom na stupanj fleksibilnosti koji se njome osigurava.
- **Internetski izdavači i operatori OBA** očito bi prednost dali 5. mogućnosti iz istih razloga kao i ECS-ovi i pružatelji OTT usluga.
- **Pružatelji usluga preglednika** podliježali bi posebnim odgovornostima u okviru 3. mogućnosti. Oni stoga ne bi poduprli 3. i 4. mogućnost.
- MSP-ovi bi uglavnom poduprli 1. i 5. mogućnost. Ako su ECS-ovi, odabrali bi 2. i 3. mogućnost kako bi se osigurali jednaki uvjeti na tržištu s pružateljima OTT usluga. Ako su pružatelji OTT usluga, prednost bi dali 1. i 5. mogućnosti, a nakon njih najprihvatljivija bi im bila 3. mogućnost.

C. Učinci one mogućnosti kojoj se daje prednost

Koje su koristi od mogućnosti kojoj se daje prednost (a ako je nema, od glavnih mogućnosti)?

Mogućnost kojoj se daje prednost jest 3. mogućnost. Njezine su glavne prednosti sljedeće:

- poboljšanje zaštite povjerljivosti tehnološki neutralnom definicijom, pojačanom kontrolom korisnika i pojačanim zahtjevima u pogledu transparentnosti te učinkovitijom provedbom
- poboljšanje zaštite od neželjenih komunikacija (zahvaljujući uvođenju te mogućnosti za marketinške pozive), uvođenje predbroja, a time i zabrana anonimnih marketinških poziva te poboljšane mogućnosti blokiranja poziva upućenih s neželjenih brojeva
- pojednostavnjenje zahvaljujući usklađivanju i pojašnjenju regulatornog okruženja smanjenjem prostora za djelovanje ostavljenog državama članicama, stavljanjem izvan snage zastarjelih odredbi i proširenjem izuzeća od pravila o suglasnosti.

Koliki su troškovi mogućnosti kojoj se daje prednost (a ako je nema, glavnih mogućnosti)?

Očekuje se da će se mogućnošću kojoj se daje prednost ostvariti ušteda zahvaljujući dodatnom usklađivanju i pojednostavnjenju. Na primjer, ušteda do 70 % troškova povezanih s e-privatnošću izračunana je na temelju centraliziranog upravljanja opcijama privatnosti, koje se unose jednom za sva *web*-mjesto i aplikacije.

Na razini pojedinih kategorija dionika, **OTT dionici** morali bi snositi neke troškove preispitivanja zakonitosti svojih poslovnih modela. Međutim očekuje se da takvi troškovi neće biti znatni. **Internetski izdavači** mogli bi snositi određene male troškove prilagodbe. **Pružatelji usluga preglednika i pružatelji usluga sličnih aplikacija koje omogućuju pristup internetu** snosili bi znatne troškove da bi korisnicima omogućili odgovarajuće opcije u postavkama privatnosti. **Subjekti koji stavljaju proizvode na tržište** snosili bi određene troškove nakon uvođenja zaštite od neželjenih komunikacija za marketinške pozive (*opt-in*).

Hoće li to bitno utjecati na nacionalne proračune i administraciju?

Na nacionalne proračune i administraciju utjecala bi primjena mehanizma konzistentnosti i moguća potreba za preraspodjelom ovlasti samo tijelima za zaštitu podataka. No taj se utjecaj ne smatra znatnim jer bi se mogla iskoristiti sinergija s već postojećim koordinacijskim tijelima EU-a (npr. u području zaštite podataka).

Hoće li znatno utjecati na nešto drugo?

Neće

Proporcionalnost?

Mogućnost kojoj se daje prednost uključuje uravnotežene mjere, koje se smatraju potrebnima za postizanje predmetnog cilja, a pritom ne uzrokuju prekomjerno opterećenje za relevantne dionike. Osim toga, mjere su osmišljene da bi se omogućili fleksibilnost i potrebna izuzeća, a tehnološki su neutralne kako bi se minimaliziralo narušavanje tržišnog natjecanja i osigurali ravnopravni uvjeti.

D. Daljnje mjere

Kad će se ta politika preispitati?

Osigurat će se kontinuirano praćenje, između ostalog, izvješćivanjem država članica Komisiji te Komisije Europskom parlamentu, Vijeću i Europskom gospodarskom i socijalnom odboru.