



H R V A T S K I S A B O R
Odbor za europske poslove

Klasa: 022-03/17-03/50
Urbroj: 6521-31-17-01
Zagreb, 27. ožujka 2017.

ODBOR ZA PRAVOSUĐE
Predsjednik mr. sc. Orsat Miljenić

ODBOR ZA LJUDSKA PRAVA I PRAVA
NACIONALNIH MANJINA
Predsjednik dr. sc. Furio Radin

Poštovani predsjednici odbora,

Odbor za europske poslove na temelju članka 154. stavka 1. Poslovnika Hrvatskoga sabora prosljeđuje Odboru za pravosuđe i Odboru za ljudska prava i prava nacionalnih manjina stajalište o dokumentu Europske unije objavljenom u sklopu nove inicijative Europske komisije uključene u Radni program za razmatranje stajališta Republike Hrvatske za 2017. godinu:

Stajalište Republike Hrvatske o
Prijedlogu 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

koje je Koordinacija za vanjsku i europsku politiku i ljudska prava Vlade Republike Hrvatske usvojila Zaključkom: Klasa: 022-03/17-07/123, Urbroj: 50301-23/22-17-1 na sjednici održanoj 6. ožujka 2017. godine.

Predmetni Prijedlog uredbe Komisija je dostavila Hrvatskom saboru 14. veljače 2017., u sklopu nove inicijative iz Programa rada Europske komisije za 2017. „Paket o zaštiti podataka“.

U skladu s člankom 154. stavkom 2. Poslovnika Hrvatskoga sabora, molim vas da Odboru za europske poslove dostavite mišljenje o stajalištu Republike Hrvatske najkasnije do 14. travnja 2017. godine.

S poštovanjem,

PREDSJEDNIK ODBORA
Domagoj Milošević

U prilogu: - Stajalište Republike Hrvatske o COM (2017) 10
- COM (2017) 10
Na znanje: - INFODOK služba

PRIJEDLOG STAJALIŠTA RH

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)

Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications)

Brojčana oznaka dokumenta za raspravu na sastanku: 5358/17

Nadležno TDU za izradu prijedloga stajališta (nositelj izrade stajališta), ustrojstvena jedinica i službenik/ica:

Nadležno tijelo državne uprave:

Ministarstvo mora, prometa i infrastrukture
Hrvatska regulatorna agencija za mrežne djelatnosti

Ustrojstvena jedinica:

Uprava zračnog prometa, elektroničkih komunikacija i pošte
Sektor elektroničkih komunikacija i pošte (MMPI)

Nadležni službenik/ica:

Krešo Antonović, načelnik Sektora (MMPI)
kreso.antonovic@mmpi.hr

Zamjena:

Domagoj Maričić (HAKOM)
domagoj.maricic@hakom.hr

Nadležni službenik/ica u MVEP (Sek. za koord. eur. poslova):

Martina Jurić (martina.juric@mvep.hr), Ana Đukić (ana.dukic@mvep.hr)

Nadležna radna skupina Vijeća EU i nadležni službenik/ica u SP RH pri EU:

Radna skupina za telekomunikacije i informacijsko društvo
Viktor Šober, ministar savjetnik (Viktor.Sober@mvep.hr)

Osnovne sadržajne odredbe prijedloga EU:

EK ovim Prijedlogom uredbe želi osigurati konzistentnost s Općom uredbom o zaštiti podataka (GDPR) i pravnu sigurnost za građane i gospodarske subjekte, te smatra da će se upravo uredbom postići jednaka razina zaštite širom EU-a za korisnike usluga, kao i niži troškovi usklađivanja za gospodarske subjekte koji posluju na prekograničnim tržištima.

Poglavlje I. sadržava opće odredbe – predmet i područje primjene Uredbe te definicije pojmova, uključujući i upućivanje na odgovarajuće definicije iz drugih propisa EU-a, kao što je GDPR.

Poglavlje II. sadržava ključne odredbe kojima se osigurava povjerljivost elektroničkih komunikacija te ograničene dopuštene svrhe i uvjeti obrade komunikacijskih podataka. Također se uređuje zaštita terminalne opreme, na način da se jamči cjelovitost pohranjenih podataka te štite podaci koje odašilje terminalna oprema, budući da ta oprema omogućuje identifikaciju svojeg krajnjeg korisnika. Nadalje, propisuje se privola krajnjeg korisnika, kao temeljna pravna osnova ove Uredbe, pri čemu su njezina definicija i uvjeti uređeni u GDPR-u. Davatelje programske podrške koja dopušta elektroničke komunikacije obvezuje se na pomoć krajnjim korisnicima u učinkovitom odabiru postavki za zaštitu privatnosti. Zaključno, propisuje se u koje svrhe i uz koje uvjete DČ mogu ograničiti prava i obveze utvrđene u ovom poglavlju.

Poglavlje III. uređuje prava krajnjih korisnika na nadzor slanja i primanja elektroničkih komunikacija u cilju zaštite njihove privatnosti, i to pravo na sprječavanje prikaza pozivajućeg broja u svrhu zaštite anonimnosti, iznimke od ostvarivanja tog prava te obvezu davatelja javno dostupnih interpersonalnih komunikacijskih usluga temeljenih na brojevima da osiguraju mogućnost ograničenja prijma neželjenih poziva. Također, propisuju se uvjeti uz koje se krajnji korisnici mogu upisati u javno dostupne imenike te uvjeti uz koje se mogu obavljati neželjene komunikacije u svrhu izravne promidžbe. Nadalje, uređuje se obveza davatelja elektroničkih komunikacijskih usluga da upozore krajnje korisnike u slučaju nastanka sigurnosnog rizika koji može ugroziti sigurnost mreža i usluga.

Poglavlje IV. uređuje nadzor provedbe ove Uredbe koji se povjerava nadzornim tijelima nadležnima za GDPR, s obzirom na snažnu sinergiju između općih pitanja zaštite podataka i povjerljivosti komunikacija. Proširuju se ovlasti Europskog odbora za zaštitu podataka, a mehanizam suradnje i konzistentnosti, predviđen GDPR-om, primjenjivat će se i na prekogranična pitanja koja proizlaze iz ove Uredbe.

Poglavlje V. detaljno uređuje naknadu štete koju trpe krajnji korisnici zbog povrede odredaba ove Uredbe, te novčane kazne koje se mogu izreći, uključujući i opće uvjete za izricanje administrativnih kazna.

Poglavljem VI. propisuje se ovlast za donošenje delegiranih i provedbenih akata, u skladu s člancima 290. i 291. Ugovora o funkcioniranju Europske unije.

Poglavlje VII. sadržava završne odredbe koje se odnose na prestanak važenja Direktive 2002/58/EZ, praćenje učinkovitosti ove Uredbe, njezino periodično preispitivanje u cilju mogućih izmjena ili stavljanja izvan snage, a u svjetlu razvoja pravnog, tehničkog ili gospodarskog okvira, te stupanje na snagu i početak primjene ove Uredbe.

Razlozi za donošenje i pozadina dokumenta:

Prijedlog uredbe ima za cilj osnažiti i učiniti djelotvornijom zaštitu privatnosti i osobnih podataka koji se obrađuju u vezi s elektroničkim komunikacijama, u skladu s člancima 7. i 8. Povelje Europske unije o temeljnim pravima, te osigurati veću pravnu sigurnost. Prijedlogom uredbe nadopunjuje se i detaljnije razrađuje Opća uredba o zaštiti podataka (Uredba (EU) 2016/679), budući da je učinkovita zaštita povjerljivosti komunikacija od ključne važnosti za ostvarivanje slobode izražavanja i priopćavanja te drugih povezanih prava, kao što je pravo na zaštitu osobnih podataka ili pravo na slobodu mišljenja, savjesti i vjeroispovijedi.

Status dokumenta:

Prijedlog uredbe upućen je u zakonodavni postupak i o njemu je započela rasprava na Radnoj skupini Vijeća EU (WP TELE). Na sastanku zakazanom za 28. veljače 2017. raspravljat će se o dokumentu analize učinaka Prijedloga uredbe.

Stajalište RH:**Poglavlje I.**

U odnosu na područje primjene, člankom 2. stavkom 2.(c) određeno je kako se ova Uredba ne primjenjuje na elektroničke komunikacijske usluge koje nisu javno dostupne. U tom smislu **RH** izražava bojazan vezano uz eventualnu neovlaštenu obradu osobnih podataka u slučaju privatnih mreža na koje se privremeno prijavljuju korisnici kao "gosti".

Poglavlje II.

RH je rezervirana u pogledu tumačenja prava pojedinaca na izbor vezano uz korištenje pojedinih usluga. U uvodnoj odredbi 25. spominju se usluge kao što je slanje komercijalnih poruka krajnjim korisnicima s personaliziranim ponudama, primjerice kada ulaze u trgovine, te se pružatelji takvih usluga upozoravaju da bi na rubu područja pokrivenosti trebali istaknuti obavijesti kojima krajnje korisnike prije ulaska na definirano područje informiraju, uz ostalo, o upotrebi tehnologije unutar zadanog opsega. U odnosu na navedeno, kao i slične primjere, **RH** smatra kako je nužno razlučiti imaju li pojedinci pravo koristiti se uslugom (ulazak u trgovinu i/ili prolazak određenim područjem) bez davanja privole za obradu osobnih podataka, neovisno o postojanju upozorenja, te kako izraziti taj izbor. Izostankom prava na izbor pojedinac bi bio neizravno prisiljen na obradu svojih osobnih podataka.

Nadalje, u članku 10. stavku 2. Prijedloga uredbe navodi se da nakon instalacije softver obavješćuje krajnjeg korisnika o mogućnostima postavki privatnosti, pri čemu nije jasno što je uobičajena postavka ako korisnik isključivo odabere "prihvaćam", te je stoga potrebno propisati koja opcija treba biti zadana.

Poglavlje III.

RH nema primjedaba.

Poglavlje IV.

RH izražava rezervu na članak 18. Prijedloga uredbe te smatra kako bi pitanje određivanja nadzornih tijela ovom Uredbom trebalo ostaviti u nadležnosti državama članicama. Isključiva

nadzorna uloga tijela nadležnog za zaštitu osobnih podataka, za razliku od postojećeg iskustva RH, gdje su podijeljene odgovornosti između nacionalnog regulatornog tijela u području elektroničkih komunikacija (HAKOM) i nacionalnog tijela nadležnog za zaštitu osobnih podataka (AZOP), zahtijevat će značajno povećanje administrativnog kapaciteta, troškove stručnog osposobljavanja zaposlenika te moguća nova IT rješenja, a samim time i dodatne troškove za državni proračun.

Poglavlje V.

RH načelno podržava odredbe o novčanim kaznama. Međutim, imajući u vidu međusobnu povezanost ovoga Prijedloga uredbe s Uredbom (EU) 2016/679 (Opća uredba o zaštiti podataka) te Prijedlogom direktive Europskog parlamenta i Vijeća o Europskom zakoniku elektroničkih komunikacija, RH smatra kako bi trebalo dodatno objasniti je li nacionalno nadzorno tijelo nadležno za zaštitu osobnih podataka isključivo ovlašteno za izricanje sankcija predviđenih u ovom poglavlju, odnosno može li za izricanje ovih sankcija postojati podijeljena odgovornost između tog nadzornog tijela i nacionalnog regulatornog tijela u području elektroničkih komunikacija.

Poglavlje VI.

RH nema primjedaba.

Poglavlje VII.

RH nema primjedaba.

Stajališta DČ, EK i Predsjedništva EU:

U ovome trenutku još nije poznato.

Sporna/otvorena pitanja za DČ, EK i Predsjedništvo EU:

U ovome trenutku još nije poznato.

Stav RH o spornim/otvorenim pitanjima DČ, EK i Predsjedništva EU:

Zauzet će se kada navedena pitanja budu poznata.

Postojeće zakonodavstvo RH i potreba njegove izmjene slijedom usvajanja dokumenta:

Iako se radi o Prijedlogu uredbe koja se izravno primjenjuje u državama članicama, bit će potrebne izmjene zakonodavstva RH, i to Zakona o elektroničkim komunikacijama, u dijelu koji se odnosi na zaštitu podataka i sigurnost elektroničkih komunikacija, kako bi se izbjeglo preklapanje zakonskih odredaba s odredbama ove Uredbe koje će se neposredno primjenjivati. Također, bit će potrebno propisati nove novčane kazne za kršenje odredaba ove Uredbe.

Utjecaj provedbe dokumenta na proračun RH:

Donošenje ove Uredbe nema izravnog utjecaja na državni proračun, ali će imati neizravni utjecaj zbog novih ovlasti nadležnog tijela, slijedom čega će biti potrebno osigurati značajne dodatne administrativne kapacitete.



Bruxelles, 10.1.2017.
COM(2017) 10 final

2017/0003 (COD)

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)

(Tekst značajan za EGP)

{SWD(2017) 3 final}

{SWD(2017) 4 final}

{SWD(2017) 5 final}

{SWD(2017) 6 final}

OBRAZLOŽENJE

1. KONTEKST PRIJEDLOGA

1.1. Razlozi i ciljevi prijedloga

Cilj je strategije jedinstvenog digitalnog tržišta¹ povećati povjerenje u digitalne usluge i njihovu sigurnost. U tu je svrhu ključno djelovanje bila reforma okvira za zaštitu podataka, a posebno donošenje Uredbe (EU) 2016/679, Opće uredbe o zaštiti podataka („GDPR”)². U strategiji jedinstvenog digitalnog tržišta najavljeno je i preispitivanje Direktive 2002/58/EZ („Direktiva o e-privatnosti”)³ radi osiguranja visoke razine zaštite privatnosti korisnika elektroničkih komunikacijskih usluga i jednakih uvjeta za sve sudionike na tržištu. U ovom se prijedlogu preispituje Direktiva o e-privatnosti, kako je predviđena u ciljevima strategije digitalnog jedinstvenog tržišta, čime se osigurava usklađenost s GDPR-om.

Direktivom o e-privatnosti osigurava se zaštita temeljnih prava i sloboda, a posebno poštovanje privatnog života, povjerljivost komunikacija i zaštita osobnih podataka u području elektroničkih komunikacija. Njome se isto tako jamči slobodno kretanje elektroničkih komunikacijskih podataka te elektroničke komunikacijske opreme i usluga u Uniji. Njome se u sekundarno pravo Unije uvodi temeljno pravo na poštovanje privatnog života u pogledu komunikacija, kako je utvrđeno u članku 7. Povelje Europske unije o temeljnim pravima („Povelja”).

Komisija je u skladu sa zahtjevima bolje regulative provela *ex post* evaluaciju Direktive o e-privatnosti u okviru programa za prikladnost i učinkovitost propisa („**evaluacija u okviru programa REFIT**”). Iz te evaluacije proizlazi da su ciljevi i načela postojećeg okvira i dalje utemeljeni. Međutim, od posljednje revizije Direktive o e-privatnosti 2009. na tržištu je došlo do važnog tehnološkog i gospodarskog razvoja. Potrošači i poduzeća sve se više umjesto na tradicionalne komunikacijske usluge oslanjaju na nove internetske usluge za međuljudsku komunikaciju, kao što su govor putem IP-a, trenutačna razmjena poruka i usluge elektroničke pošte na internetu. Komunikacijske usluge OTT (eng. *over-the-top* – distribucija audiovizualnog i drugog sadržaja internetom) općenito ne podliježu postojećem okviru Unije za elektroničke komunikacije, uključujući Direktivu o e-privatnosti. Stoga Direktiva nije išla ukorak s tehnološkim razvojem, što je dovelo do nedovoljno učinkovite zaštite komunikacija koje se prenose novim uslugama.

1.2. Usklađenost s postojećim odredbama politike u tom području politike

Ovaj je prijedlog *lex specialis* u odnosu na GDPR te će se njime preciznije utvrditi i dopuniti GDPR u pogledu elektroničkih komunikacijskih podataka koji se smatraju osobnim podacima. Sva pitanja koja se odnose na obradu osobnih podataka koja nisu posebno riješena prijedlogom obuhvaćena su GDPR-om. Usklađivanje s GDPR-om dovelo je do stavljanja izvan snage određenih odredbi, kao što su sigurnosne obveze iz članka 4. Direktive o e-privatnosti.

¹ Komunikacija Komisije Europskom parlamentu, Vijeću, Europskom gospodarskom i socijalnom odboru i Odboru regija, Strategija jedinstvenog digitalnog tržišta za Europu, COM(2015) 192 final

² Uredba (EU) 2016/679 Europskog parlamenta i Vijeća od 27. travnja 2016. o zaštiti pojedinaca u vezi s obradom osobnih podataka i o slobodnom kretanju takvih podataka te o stavljanju izvan snage Direktive 95/46/EZ (Opća uredba o zaštiti podataka) (SL L 119, 4.5.2016., str. 1. – 88.)

³ Direktiva 2002/58/EZ Europskog parlamenta i Vijeća od 12. srpnja 2002. o obradi osobnih podataka i zaštiti privatnosti u području elektroničkih komunikacija (Direktiva o privatnosti i elektroničkim komunikacijama) (SL L 201, 31.7.2002., str. 37.)

1.3. Usklađenost s drugim politikama Unije

Direktiva o e-privatnosti dio je regulatornog okvira za elektroničke komunikacije. Komisija je 2016. donijela prijedlog Direktive o Europskom zakoniku elektroničkih komunikacija („EECC”)⁴, kojim se revidira okvir. Iako ovaj prijedlog nije sastavni dio EECC-a, on se djelomično temelji na definicijama predviđenima njime, uključujući definiciju „elektroničkih komunikacijskih usluga”. Ovim su prijedlogom, jednako kao i EECC-om, obuhvaćeni i pružatelji OTT usluga kao odraz tržišnih okolnosti. Osim toga, EECC-om se ovaj prijedlog dopunjuje tako što se osigurava sigurnost elektroničkih komunikacijskih usluga.

Direktivom o radijskoj opremi 2014/53/EU („RED”)⁵ osigurava se jedinstveno tržište radijske opreme. Njome se posebno zahtijeva da prije stavljanja na tržište radijska oprema mora obuhvaćati zaštitne mehanizme radi osiguranja zaštite osobnih podataka i privatnosti korisnika i pretplatnika. Komisija je na temelju RED-a i Uredbe o europskoj normizaciji (EU) 1025/2012⁶ ovlaštena donijeti mjere. Ovaj prijedlog nema utjecaja na RED.

Prijedlog ne uključuje nikakve posebne odredbe u području čuvanja podataka. U njemu je zadržana bit članka 15. Direktive o e-privatnosti te je usklađena s posebnim tekstom članka 23. GDPR-a kojim su propisani razlozi na temelju kojih države članice ograničavaju opseg prava i obveza iz posebnih članaka Direktive o e-privatnosti. Stoga države članice mogu zadržati ili stvoriti nacionalne okvire za čuvanje podataka kojima su propisane, među ostalim, ciljane mjere čuvanja pod uvjetom da su ti okviri usklađeni s pravom Unije, uzimajući u obzir sudsku praksu Suda u pogledu tumačenja Direktive o e-privatnosti i Povelje o temeljnim pravima⁷.

Naposljetku, prijedlog se ne primjenjuje na djelatnosti institucija, tijela i agencija Unije. Međutim, njegova načela i relevantne obveze koji se odnose na pravo na poštovanje privatnog života i komuniciranja u vezi s obradom elektroničkih komunikacijskih podataka uključeni su u prijedlog Uredbe o stavljanju izvan snage Uredbe (EZ) br. 45/2001⁸.

2. PRAVNA OSNOVA, SUPSIDIJARNOST I PROPORCIONALNOST

2.1. Pravna osnova

Članak 16. i članak 114. Ugovora o funkcioniranju Europske unije („UFEU”) čine relevantnu pravnu osnovu prijedloga.

Člankom 16. UFEU-a uvodi se posebna pravna osnova za donošenje pravila o zaštiti pojedinaca s obzirom na obradu osobnih podataka u institucijama Unije te u državama

⁴ Prijedlog Komisije za Direktivu Europskog parlamenta i Vijeća o Europskom zakoniku elektroničkih komunikacija (preinaka) (COM/2016/0590 final – 2016/0288 (COD))

⁵ Direktiva 2014/53/EU Europskog parlamenta i Vijeća od 16. travnja 2014. o usklađivanju zakonodavstava država članica o stavljanju na raspolaganje radijske opreme na tržištu i stavljanju izvan snage Direktive 1999/5/EZ (SL L 153, 22.5.2014., str. 62. – 106.)

⁶ Uredba (EZ) br. 1025/2012 Europskog parlamenta i Vijeća od 25. listopada 2012. o europskoj normizaciji, o izmjeni direktiva Vijeća 89/686/EEZ i 93/15/EEZ i direktiva 94/9/EZ, 94/25/EZ, 95/16/EZ, 97/23/EZ, 98/34/EZ, 2004/22/EZ, 2007/23/EZ, 2009/23/EZ i 2009/105/EZ Europskog parlamenta i Vijeća te o stavljanju izvan snage Odluke Vijeća 87/95/EEZ i Odluke br. 1673/2006/EZ Europskog parlamenta i Vijeća (SL L 316, 14.11.2012., str. 12. – 33.)

⁷ Vidjeti presude Digital Rights Ireland i Seitlinger i dr., spojeni predmeti C-293/12 i C-594/12, ECLI:EU:C:2014:238, te Tele2 Sverige AB i Secretary of State for the Home Department, spojeni predmeti C-203/15 i C-698/15, ECLI:EU:C:2016:970

⁸ Uredba (EZ) br. 45/2001 Europskog parlamenta i Vijeća od 18. prosinca 2000. o zaštiti pojedinaca u vezi s obradom osobnih podataka u institucijama i tijelima Zajednice i o slobodnom kretanju takvih podataka (SL L 8, 12.1.2001., str. 1. – 22.)

članicama kada obavljaju svoje aktivnosti u području primjene prava Unije i pravila o slobodnom kretanju takvih podataka. Budući da će se elektronička komunikacija koja uključuje fizičku osobu uobičajeno smatrati osobnim podacima, zaštitu fizičkih osoba u pogledu privatnosti komunikacija i obradu takvih podataka trebalo bi temeljiti na članku 16.

Osim toga, cilj je prijedloga zaštita komunikacija i s time povezanih legitimnih interesa pravnih osoba. U skladu s člankom 52. stavkom 3. Povelje, značenje i opseg prava na temelju članka 7. Povelje jednaki su onima utvrđenima u članku 8. stavku 1. Europske konvencije za zaštitu ljudskih prava i temeljnih sloboda („EKLJP”). U pogledu područja primjene članka 7. Povelje, sudskom praksom Suda Europske unije⁹ i Europskog suda za ljudska prava¹⁰ potvrđeno je da se poslovne djelatnosti pravnih osoba ne mogu isključiti iz zaštite prava zajamčenog člankom 7. Povelje i člankom 8. EKLJP-a.

Budući da se inicijativom nastoji postići dvostruki cilj te da se komponenta koja se odnosi na zaštitu komunikacija pravnih osoba i cilj ostvarenja unutarnjeg tržišta za te elektroničke komunikacije i osiguranja njegova funkcioniranja u tom pogledu ne mogu smatrati samo sporednima, inicijativu bi trebalo temeljiti i na članku 114. UFEU-a.

2.2. Supsidijarnost

Poštovanje komuniciranja temeljno je pravo priznato Poveljom. Na temelju sadržaja elektroničkih komunikacija mogu se otkriti vrlo osjetljive informacije o krajnjim korisnicima koji sudjeluju u komunikaciji. Slično tome, na temelju elektroničkih komunikacijskih metapodataka mogu se isto tako otkriti vrlo osjetljivi i osobni podaci, kako je izričito priznao Sud Europske unije.¹¹ Većina država članica isto tako priznaje potrebu za zaštitom komunikacija kao posebno ustavno pravo. Iako države članice mogu donijeti političke odluke u cilju sprječavanja povrede tog prava, to se bez pravila Unije ne bi postiglo ujednačeno te bi se stvorile prepreke prekograničnim protocima osobnih i neosobnih podataka povezanih s uporabom elektroničkih komunikacijskih usluga. Naposljetku, kako bi se zadržala usklađenost s GDPR-om, potrebno je preispitati Direktivu o e-privatnosti i donijeti mjere za usklađivanje tih dvaju instrumenata.

Tehnološkim razvojem i ciljevima koji se nastoje ostvariti strategijom jedinstvenog digitalnog tržišta ojačana je argumentacija za djelovanje na razini Unije. Uspjeh jedinstvenog digitalnog tržišta EU-a ovisi o učinkovitosti EU-a u ukidanju nacionalnih izoliranih sustava i uklanjanju prepreka te iskorištavanju prednosti i ekonomija europskog jedinstvenog digitalnog tržišta. Nadalje, budući da internet i digitalne tehnologije ne poznaju granice, razmjer problema prelazi granice državnog područja pojedinačne države članice. Države članice u trenutačnoj situaciji ne mogu učinkovito riješiti probleme. Jednaki uvjeti za gospodarske subjekte koji pružaju zamjenjive usluge i jednaka zaštita krajnjih korisnika na razini Unije zahtjevi su za pravilno funkcioniranje jedinstvenog digitalnog tržišta.

2.3. Proporcionalnost

Kako bi se osigurala učinkovita pravna zaštita poštovanja privatnosti i komuniciranja, potrebno je proširiti područje primjene i obuhvatiti pružatelje OTT usluga. Iako nekoliko popularnih pružatelja OTT usluga već poštuju ili djelomično poštuju načelo povjerljivosti

⁹ Vidi presudu Varec SA, C-450/06, ECLI:EU:C:2008:91, t. 48.

¹⁰ Vidi, među ostalim, presude EKLJP-a Niemietz/Njemačka, presuda od 16. prosinca 1992., serija A br.°251-B, t. 29., Soci  t   Colas Est i dr./Francuska, br. 37971/97, t. 41., EKLJP 2002-III, Peck/Ujedinjena Kraljevina, br. 44647/98, t. 57., EKLJP 2003-I, i Vinci Construction i GTM G  nie Civil et Services/Francuska, br.°63629/10 i 60567/10, t. 63., 2. travnja 2015.

¹¹ Vidi bilješku 7.

komunikacija, zaštita temeljnih prava ne može se prepustiti samoregulaciji industrije. Isto se tako povećava važnost učinkovite zaštite privatnosti terminalne opreme jer je ona u privatnom i profesionalnom životu postala nužna za pohranu osjetljivih informacija. Provedba Direktive o e-privatnosti nije učinkovita u pogledu omogućavanja većeg izbora za krajnje korisnike. Stoga je za ostvarenje cilja potrebno provesti to načelo centraliziranjem privole u softveru i davanjem informacija korisnicima o postavkama privatnosti softvera. Provedba se ove Uredbe oslanja na nadzorna tijela i mehanizam konzistentnosti GDPR-a. Nadalje, prijedlogom se državama članicama omogućuje poduzimanje nacionalnih odstupajućih mjera u posebne legitimne svrhe. Stoga prijedlog ne prelazi ono što je potrebno za ostvarenje ciljeva i u skladu je s načelom proporcionalnosti kako je utvrđeno u članku 5. Ugovora o Europskoj uniji. Obveze određene za obuhvaćene usluge zadržane su na najnižoj mogućoj razini te se njima ne zadire u predmetna temeljna prava.

2.4. Odabir instrumenta

Komisija iznosi prijedlog Uredbe kako bi izbjegavanjem različitih tumačenja u državama članicama osigurala usklađenost s GDPR-om i pravnu sigurnost za korisnike i poduzeća. Uredbom se može osigurati jednaka razina zaštite za korisnike u cijeloj Uniji i mogu se smanjiti troškovi usklađivanja za poduzeća koja posluju prekogranično.

3. REZULTATI *EX POST* EVALUACIJA, SAVJETOVANJA S DIONICIMA I PROCJENA UČINAKA

3.1. *Ex post* evaluacije / provjere prikladnosti postojećeg zakonodavstva

Evaluacijom u okviru programa REFIT ispitalo se koliko se Direktivom o e-privatnosti učinkovito pridonijelo primjerenom zaštitu poštovanja privatnog života i povjerljivosti komunikacija u EU-u. Njome su se isto tako nastojala utvrditi moguća nepotrebna ponavljanja.

U evaluaciji u okviru programa REFIT zaključeno je da su prethodno navedeni ciljevi Direktive i dalje **relevantni**. Dok se GDPR-om osigurava zaštita osobnih podataka, Direktivom o e-privatnosti osigurava se povjerljivost komunikacija, koje isto tako mogu sadržavati neosobne podatke i podatke povezane s pravnom osobom. Stoga bi zasebnim instrumentom trebalo osigurati učinkovitu zaštitu članka 7. Povelje. Pokazalo se da su ostale odredbe, kao što su pravila o slanju nezatraženih marketinških komunikacija, isto tako i dalje relevantne.

U evaluaciji u okviru programa REFIT utvrđeno je da s obzirom na **učinkovitost i djelotvornost** Direktivom nisu potpuno ispunjeni njezini ciljevi. Nejasnim sastavljanjem nekih odredbi i neodređenošću pravnih koncepata ugrožena je usklađenost te se poduzeća koja posluju prekogranično suočavaju s različitim izazovima. Iz evaluacije je nadalje vidljivo da je određenim odredbama stvoreno nepotrebno opterećenje za poduzeća i potrošače. Na primjer, pravilom o privoli u svrhu zaštite povjerljivosti terminalne opreme nisu ostvareni njegovi ciljevi jer krajnji korisnici primaju zahtjeve za prihvaćanje kolačića za praćenje, a da pritom ne razumiju njihovo značenje, a u nekim su slučajevima izloženi kolačićima čak i bez davanja svoje privole. Pravilo o privoli preširoko je jer su njime obuhvaćene i prakse kojima se ne narušava privatnost, ali i preusko jer njime nisu jasno obuhvaćene određene tehnike praćenja (npr. prikupljanje informacija o uređaju u svrhu njegove identifikacije i praćenja) koje možda ne uključuju pristup ili pohranu na uređaju. Naposljetku, njegova provedba može biti skupa za poduzeća.

U evaluaciji je zaključeno da pravila o e-privatnosti još uvijek imaju **dodanu vrijednost EU-a** za bolje ostvarenje cilja osiguranja privatnosti na internetu s obzirom na to da je tržište elektroničkih komunikacija u sve većoj mjeri transnacionalno. Njome se pokazalo i da su pravila općenito **usklađena** s ostalim relevantnim zakonodavstvom, iako je utvrđeno nekoliko nepotrebnih ponavljanja u odnosu na novi GDPR (vidi odjeljak 1.2.).

3.2. Savjetovanja s dionicima

Komisija je organizirala javno savjetovanje od 12. travnja do 5. srpnja 2016. i zaprimila 421 odgovor¹². Glavni su rezultati sljedeći¹³:

- **potreba za posebnim pravilima o povjerljivosti elektroničkih komunikacija u području elektroničkih komunikacija:** s tim se slaže 83,4 % građana i organizacija potrošača i civilnog društva koji su odgovorili te 88,9 % tijela javne vlasti, dok se 63,4 % ispitanika iz industrije ne slaže,
- **proširenje područja primjene na nove komunikacijske usluge (OTT-ovi):** s tim se slaže 76 % građana i organizacija civilnog društva te 93,1 % tijela javne vlasti, dok je samo 36,2 % ispitanika iz industrije za takvo proširenje,
- **izmjena izuzeća od privole za obradu podataka o prometu i lokaciji:** 49,1 % građana i organizacija potrošača i civilnog društva te 36 % tijela javne vlasti prednost daje neproširivanju izuzeća, dok je 36 % industrije za proširena izuzeća, a dvije trećine industrije zagovara potpuno stavljanje izvan snage odredbi,
- **potpora rješenjima predloženima u vezi s pitanjem privole za kolačiće:** 81,2 % građana i 63 % tijela javne vlasti podupiru propisivanje obveza proizvođačima terminalne opreme da na tržište stavljaju proizvode s aktiviranom privatnošću kao zadanim postavkama, dok je 58,3 % industrije za opciju davanja potpore samoregulaciji/koregulaciji.

Osim toga, u travnju 2016. Europska komisija organizirala je dvije radionice, jednu za sve dionike i jednu za nacionalna nadležna tijela, na kojima su se rješavala glavna pitanja iz javnog savjetovanja. Stajališta iznesena tijekom radionica bila su odraz rezultata javnog savjetovanja.

Za pribavljanje stajališta građana provedeno je istraživanje Eurobarometra o e-privatnosti¹⁴ u EU-u. Glavni su rezultati sljedeći¹⁵:

- 78 % građana navode da im je vrlo važno da se osobnim informacijama na njihovu računalu, pametnom telefonu ili tabletu može pristupiti samo uz njihovo dopuštenje,
- 72 % građana navode da im je vrlo važno da je zajamčena povjerljivost njihove elektroničke pošte i trenutačne razmjene poruka na internetu,
- 89 % građana slažu se s predloženom opcijom da bi zadanim postavkama pretraživača trebalo zaustaviti dijeljenje njihovih informacija.

¹² 162 doprinosa građana, 33 doprinosa organizacija civilnog društva i potrošača, 186 doprinosa industrije i 40 doprinosa tijela javne vlasti, uključujući tijela nadležna za provedbu Direktive o e-privatnosti.

¹³ Potpuno izvješće dostupno je na poveznici: <https://ec.europa.eu/digital-single-market/news-redirect/37204>.

¹⁴ Istraživanje Eurobarometra (EB) 443 o e-privatnosti iz 2016. (SMART 2016/079)

¹⁵ Potpuno izvješće dostupno je na poveznici: <https://ec.europa.eu/digital-single-market/news-redirect/37205>.

3.3. Prikupljanje i primjena stručnog znanja

Komisija se oslanjala na sljedeće vanjske stručne savjete:

- ciljana savjetovanja sa stručnim skupinama EU-a: mišljenje Radne skupine iz članka 29., mišljenje Europskog nadzornika za zaštitu podataka, mišljenje platforme REFIT, stajališta Tijela europskih regulatora za elektroničke komunikacije („BEREC”), stajališta Europske agencije za mrežnu i informacijsku sigurnost („ENISA”) i stajališta članova Mreže za zaštitu i suradnju potrošača,
- vanjsko stručno znanje, posebno sljedeće dvije studije:
 - studiju „Direktiva o e-privatnosti: procjena prijenosa, učinkovitosti i usklađenosti s predloženom Uredbom o zaštiti podataka” (SMART 2013/007116),
 - studiju „Evaluacija i preispitivanje Direktive 2002/58 o privatnosti i području elektroničkih komunikacija” (SMART 2016/0080).

3.4. Procjena učinka

Provedena je procjena učinka za ovaj prijedlog za koji je Odbor za regulatorni nadzor 28. rujna 2016. izdao pozitivno mišljenje¹⁶. Kako bi se poduzele mjere u pogledu preporuka Odbora, u procjeni učinka bolje su objašnjeni područje primjene inicijative, njezina usklađenost s ostalim pravnim instrumentima (GDPR-om, EECC-om, RED-om) i potreba za zasebnim instrumentom. Dodatno je razvijen i pojašnjen osnovni scenarij. Analiza učinaka ojačana je i u većoj mjeri uravnotežena te je pojašnjen i učvršćen opis očekivanih troškova i koristi.

Ispitane su sljedeće opcije politike s obzirom na kriterije učinkovitosti, djelotvornosti i usklađenosti:

- **prva opcija:** nezakonodavne („pravno neobvezujuće”) mjere,
- **druga opcija:** ograničeno jačanje privatnosti/povjerljivosti i pojednostavnjenje,
- **treća opcija:** odmjereno jačanje privatnosti/povjerljivosti i pojednostavnjenje,
- **četvrta opcija:** dalekosežno jačanje privatnosti/povjerljivosti i pojednostavnjenje,
- **peta opcija:** stavljanje izvan snage Direktive o e-privatnosti.

S obzirom na većinu aspekata **treća opcija** izdvojena je kao **odabrana opcija** za ostvarenje ciljeva, uzimajući pritom u obzir njezinu učinkovitost i usklađenost. Glavne su koristi sljedeće:

- jačanje zaštite povjerljivosti elektroničkih komunikacija proširenjem područja primjene pravnog instrumenta radi uključivanja novih funkcionalno istovjetnih elektroničkih komunikacijskih usluga. Osim toga, Uredbom se jača kontrola krajnjeg korisnika pojašnjenjem da se privola može izraziti prikladnim tehničkim postavkama,
- jačanje zaštite od nezatraženih komunikacija uvođenjem obveze osiguranja prikaza broja pozivatelja ili obveznog predbroja za marketinške pozive te unaprijeđenih mogućnosti za blokiranje poziva upućenih s neželjenih brojeva,

¹⁶ <http://ec.europa.eu/transparency/regdoc/?fuseaction=ia>

- pojednostavnjenje i pojašnjenje regulatornog okruženja smanjenjem prostora za djelovanje ostavljenog državama članicama, stavljanjem izvan snage zastarjelih odredbi i proširenjem izuzeća od pravila o privoli.

Očekuje se da će gospodarski učinak treće opcije općenito biti proporcionalan ciljevima prijedloga. Za tradicionalne elektroničke komunikacijske usluge otvaraju se poslovne prilike povezane s obradom podataka iz komunikacija, dok pružatelji OTT usluga postaju podložni istim pravilima. Za te subjekte to podrazumijeva određene dodatne troškove usklađivanja. Međutim, ta promjena neće znatno utjecati na one OTT-ove koji već posluju na temelju privole. Naposljetku, učinak te opcije ne bi se osjetio u državama članicama koje su već proširile pravila na OTT-ove.

Centralizacijom privole u softveru, kao što su internetski preglednici, i traženjem od korisnika da odaberu svoje postavke privatnosti te proširenjem izuzeća na pravilo o privoli za kolačiće znatan dio poduzeća mogao bi prestati upotrebljavati natpise i obavijesti o kolačićima, što bi dovelo do znatnih ušteda troškova i pojednostavnjenja. Međutim, reklamnim oglašivačima na internetu može postati teže pribaviti privolu ako se veliki dio korisnika odluči za postavke „odbij kolačiće treće strane”. Istodobno se centralizacijom privole operatorima *web*-mjestima ne uskraćuje mogućnost da privolu pribave slanjem pojedinačnih zahtjeva krajnjim korisnicima i tako zadrže svoj postojeći poslovni model. Određeni pružatelji preglednika ili sličnog softvera imali bi dodatne troškove jer bi morali osigurati postavke kojima se pogoduje zaštititi privatnosti.

U vanjskoj su studiji utvrđena tri različita scenarija provedbe treće opcije ovisno o subjektu koji će uspostaviti okvir za dijalog između korisnika koji je odabrao postavke „Odbij kolačiće treće strane” ili „ne prati” i posjećenih *web*-mjestima koja žele da internetski korisnik ponovno razmotri svoj odabir. Subjekti koje bi se moglo zadužiti za tu tehničku zadaću jesu: 1. softver kao što su internetski preglednici; 2. treća strana koja prati aktivnosti; 3. pojedinačna *web*-mjestima (tj. usluga informacijskog društva koju je zatražio korisnik). Treća opcija dovela bi do ukupne uštede od 70 % u odnosu na troškove usklađivanja u odnosu na osnovni scenarij (ušteda od 948,8 milijuna EUR) u prvom scenariju (rješenje temeljeno na pregledniku) koji se provodi ovim prijedlogom. Uštede troškova bile bi manje u drugim scenarijima. Budući da ukupne uštede u velikoj mjeri proizlaze iz znatnog smanjenja broja obuhvaćenih poduzeća, očekuje se da bi pojedinačni iznos nastalih troškova usklađivanja za jedno poduzeće u prosjeku bio viši nego danas.

3.5. Prikladnost propisa i pojednostavnjenje

Političke mjere koje se predlažu u okviru odabrane opcije odnose se na cilj pojednostavnjenja i smanjenja administrativnog opterećenja u skladu s rezultatima evaluacije u okviru programa REFIT i mišljenja platforme REFIT¹⁷.

Platforma REFIT izdala je tri skupa preporuka Komisiji:

- zaštitu privatnog života građana trebalo bi ojačati usklađivanjem Direktive o e-privatnosti s Općom uredbom o zaštiti podataka,
- učinkovitost zaštite građana od nezatraženog marketinga trebalo bi ojačati dodavanjem izuzeća od pravila o privoli za kolačiće,
- Komisija rješava nacionalne provedbene probleme i olakšava razmjenu najbolje prakse među državama članicama.

¹⁷ http://ec.europa.eu/smart-regulation/refit/refit-platform/docs/recommendations/opinion_comm_net.pdf.

Preciznije, prijedlog obuhvaća sljedeće:

- uporabu tehnološki neutralnih definicija kako bi se obuhvatile nove usluge i tehnologije te time osigurala održivost Uredbe u budućnosti,
- stavljanje izvan snage pravila o sigurnosti kako bi se otklonilo regulatorno udvostručavanje,
- pojašnjenje područja primjene kako bi se pridonijelo uklanjanju/smanjenju rizika različite provedbe u državama članicama (točka 3. mišljenja),
- pojašnjenje i pojednostavnjenje pravila o privoli za uporabu kolačića i ostalih identifikatora kako je objašnjeno u odjeljcima 3.1. i 3.4. (točka 2. mišljenja),
- usklađivanje nadzornih tijela s tijelima nadležnima za provedbu GDPR-a i oslanjanje na mehanizam konzistentnosti GDPR-a.

3.6. Utjecaj na temeljna prava

Cilj je prijedloga povećati učinkovitost i razinu zaštite privatnosti i osobnih podataka koji se obrađuju u vezi s elektroničkim komunikacijama u skladu s člancima 7. i 8. Povelje i osigurati veću pravnu sigurnost. Prijedlogom se dopunjuje i preciznije utvrđuje GDPR. Učinkovita zaštita povjerljivosti komunikacija bitna je za ostvarenje slobode izražavanja i informiranja i ostalih povezanih prava, kao što su pravo na zaštitu osobnih podataka ili sloboda mišljenja, savjesti i vjeroispovijedi.

4. UTJECAJ NA PRORAČUN

Prijedlog nema nikakav utjecaj na proračun Unije.

5. OSTALI DIJELOVI

5.1. Planovi provedbe i mehanizmi praćenja, evaluacije i izvješćivanja

Komisija će pratiti primjenu Uredbe i svake tri godine podnijeti izvješće o njezinoj evaluaciji Europskom parlamentu te Vijeću i Europskom gospodarskom i socijalnom odboru. Izvješća će biti javna i u njima će se detaljno opisati učinkovita primjena i provedba ove Uredbe.

5.2. Detaljno objašnjenje posebnih odredbi prijedloga

Poglavlje I. sadržava opće odredbe: predmet (članak 1.), područje primjene (članci 2. i 3.) i definicije, uključujući upućivanja na relevantne definicije iz drugih instrumenata EU-a, kao što je GDPR.

Poglavlje II. sadržava ključne odredbe kojima se osigurava povjerljivost elektroničkih komunikacija (članak 5.) i ograničene dopuštene svrhe i uvjete obrade takvih podataka iz komunikacija (članci 6. i 7.). U njemu se rješava i pitanje zaštite terminalne opreme i. jamčenjem integriteta informacija pohranjenih na njoj i ii. zaštitom informacija koje odašilje terminalna oprema jer se na temelju njih može identificirati njezin krajnji korisnik (članak 8.). Naposljetku, u članku 9. detaljno se utvrđuje privola krajnjih korisnika, središnja zakonska osnova ove Uredbe, uz izričito upućivanje na njezinu definiciju i uvjeti predviđeni GDPR-om, dok se člankom 10. pružateljima softvera za elektroničke komunikacije propisuje obveza da krajnjim korisnicima pruže pomoć pri učinkovitom odabiru postavki privatnosti. U članku 11. detaljno se za države članice utvrđuju svrhe i uvjeti ograničavanja prethodno navedenih odredbi.

Poglavlje III. odnosi se na prava krajnjih korisnika na kontrolu slanja i primanja elektroničkih komunikacija radi zaštite privatnosti: i. pravo krajnjih korisnika da spriječe prikaz broja pozivatelja kako bi se zajamčila anonimnost (članak 12.), uključujući ograničenja (članak 13.), i ii. obvezu pružatelja javno dostupnih brojevnog utemeljenih interpersonalnih komunikacijskih usluga da osiguraju mogućnost ograničenja primanja neželjenih poziva (članak 14.). Tim se poglavljem isto tako uređuju uvjeti pod kojima se krajnje korisnike može uključiti u javno dostupne imenike (članak 15.) i uvjeti pod kojima se mogu provoditi nezatražene komunikacije u svrhu izravnog marketinga (članak 17.). Odnosi se i na sigurnosne rizike te je njime predviđena obveza za pružatelje elektroničkih komunikacijskih usluga da upozore krajnje korisnike u slučaju posebnog rizika kojim se može ugroziti sigurnost mreža i usluga. Sigurnosne obveze iz GDPR-a i EECC-a primjenjivat će se na pružatelje elektroničkih komunikacijskih usluga.

U poglavlju IV. utvrđuju se nadzor i provedba ove Uredbe te ih se povjerava nadzornim tijelima zaduženima za GDPR s obzirom na snažne sinergije između općih pitanja zaštite podataka i povjerljivosti komunikacija (članak 18.). Ovlasti Europskog odbora za zaštitu podataka proširuju se (članak 19.) te će se na prekogranična pitanja povezana s ovom Uredbom primjenjivati mehanizam suradnje i konzistentnosti predviđen GDPR-om (članak 20.).

U poglavlju V. detaljno se utvrđuju pravna sredstva dostupna krajnjim korisnicima (članci 21. i 22.) i sankcije koje se mogu propisati (članak 24.), uključujući opće uvjete propisivanja upravnih novčanih kazni (članak 23.).

Poglavlje VI. odnosi se na donošenje delegiranih i provedbenih akata u skladu s člancima 290. i 291. Ugovora.

Naposljetku, poglavlje VII. sadržava završne odredbe ove Uredbe: stavljanje izvan snage Direktive o e-privatnosti, praćenje i preispitivanje, stupanje na snagu i primjenu. U pogledu preispitivanja, Komisija namjerava ocijeniti, među ostalim, je li zaseban pravni akt i dalje potreban s obzirom na pravna, tehnička ili gospodarska kretanja te uzimajući u obzir prvu evaluaciju Uredbe (EU) 2016/679 koja se treba provesti do 25. svibnja 2020.

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)**

(Tekst značajan za EGP)

EUROPSKI PARLAMENT I VIJEĆE EUROPSKE UNIJE,

uzimajući u obzir Ugovor o funkcioniranju Europske unije, a posebno njegove članke 16. i 114.,

uzimajući u obzir prijedlog Europske komisije,

nakon prosljeđivanja nacрта zakonodavnog akta nacionalnim parlamentima,

uzimajući u obzir mišljenje Europskoga gospodarskog i socijalnog odbora¹,uzimajući u obzir mišljenje Odbora regija²,uzimajući u obzir mišljenje Europskog nadzornika za zaštitu podataka³,

u skladu s redovnim zakonodavnim postupkom,

budući da:

- (1) Člankom 7. Povelje Europske unije o temeljnim pravima („Povelja”) zaštićeno je temeljno pravo svakoga na poštovanje njegova privatnog i obiteljskog života, doma i komuniciranja. Poštovanje privatnosti komunikacija bitna je dimenzija tog prava. Povjerljivošću elektroničkih komunikacija osigurava se da se informacije koje razmjenjuju stranke i vanjski elementi takve komunikacije, uključujući podatke o tome kada su informacije poslane, odakle i kome, ne otkrivaju nikome osim strankama koje sudjeluju u komunikaciji. Načelo povjerljivosti trebalo bi se primjenjivati na sadašnja i buduća sredstva komunikacije, uključujući pozive, pristup internetu, aplikacije za trenutačnu razmjenu poruka, elektroničku poštu, telefonske pozive preko interneta i razmjenu osobnih poruka preko društvenih medija.
- (2) Sadržajem elektroničkih komunikacija mogu se otkriti vrlo osjetljivi podaci o fizičkim osobama koje sudjeluju u komunikaciji, od osobnih iskustava i osjećaja do zdravstvenih stanja, seksualnih sklonosti i političkih stavova, čije bi otkrivanje moglo za posljedicu imati osobnu ili društvenu štetu, ekonomski gubitak ili sramotu. Slično tome, elektroničkim komunikacijskim metapodacima mogu se isto tako otkriti vrlo osjetljive i osobne informacije. Ti metapodaci uključuju pozivane brojeve, posjećena web-mjesta, zemljopisnu lokaciju, vrijeme, datum i trajanje poziva koji je uputio

¹ SL C , , str. .

² SL C , , str. .

³ SL C , , str. .

pojedinaac itd., čime se omogućuje donošenje preciznih zaključaka o privatnim životima osoba koje sudjeluju u elektroničkoj komunikaciji, kao što su njihovi društveni odnosi, navike i svakodnevne aktivnosti, interesi, ukusi itd.

- (3) Elektroničkim komunikacijskim podacima mogu se otkriti i informacije o pravnim subjektima, kao što su poslovne tajne ili druge osjetljive informacije koje imaju ekonomsku vrijednost. Stoga bi odredbe ove Uredbe trebalo primjenjivati na fizičke i pravne osobe. Nadalje, ovom bi Uredbom trebalo osigurati primjenu odredbi Uredbe (EU) 2016/679 Europskog parlamenta i Vijeća⁴ i na krajnje korisnike koji su pravne osobe. To uključuje definiciju privole u skladu s Uredbom (EU) 2016/679. Pri upućivanju na privolu krajnjeg korisnika, uključujući pravne osobe, trebalo bi primjenjivati tu definiciju. Osim toga, pravne osobe trebale bi imati jednaka prava kao i krajnji korisnici koji su fizičke osobe u pogledu nadzornih tijela; nadalje, nadzorna tijela iz ove Uredbe trebala bi biti odgovorna i za praćenje primjene ove Uredbe u pogledu pravnih osoba.
- (4) U skladu s člankom 8. stavkom 1. Povelje i člankom 16. stavkom 1. Ugovora o funkcioniranju Europske unije svatko ima pravo na zaštitu svojih osobnih podataka. Uredbom (EU) 2016/679 utvrđuju se pravila koja se odnose na zaštitu fizičkih osoba u pogledu obrade osobnih podataka i pravila koja se odnose na slobodno kretanje osobnih podataka. Elektronički komunikacijski podaci mogu uključivati osobne podatke kako su definirani Uredbom (EU) 2016/679.
- (5) Odredbama ove Uredbe preciznije se utvrđuju i dopunjuju opća pravila o zaštiti osobnih podataka utvrđena Uredbom (EU) 2016/679 u pogledu elektroničkih komunikacijskih podataka koji se smatraju osobnim podacima. Stoga se ovom Uredbom ne smanjuje razina zaštite koju fizičke osobe uživaju na temelju Uredbe (EU) 2016/679. Obradu elektroničkih komunikacijskih podataka koju provode pružatelji elektroničkih komunikacijskih usluga trebalo bi dopustiti samo u skladu s ovom Uredbom.
- (6) Iako su načela i glavne odredbe Direktive 2002/58/EZ Europskog parlamenta i Vijeća⁵ i dalje općenito utemeljeni, ta Direktiva nije u potpunosti išla ukorak s razvojem tehnoloških i tržišnih okolnosti, što je dovelo do nedosljedne ili nedovoljno učinkovite zaštite privatnosti i povjerljivosti u odnosu na elektroničke komunikacije. Taj razvoj uključuje ulazak na tržište elektroničkih komunikacijskih usluga kojima se iz perspektive potrošača mogu zamijeniti tradicionalne usluge, ali one ne moraju biti u skladu s istim skupom pravila. Drugi se razvoj odnosi na nove tehnike kojima se omogućuje praćenje ponašanja krajnjih korisnika na internetu i koje nisu obuhvaćene Direktivom 2002/58/EZ. Stoga bi Direktivu 2002/58/EZ trebalo staviti izvan snage i zamijeniti ovom Uredbom.
- (7) Državama članicama trebalo bi omogućiti da u okvirima ove Uredbe zadrže ili uvedu nacionalne odredbe kojima dodatno utvrđuju i pojašnjavaju primjenu pravila ove Uredbe radi osiguranja učinkovite primjene i tumačenja tih pravila. Stoga bi diskrecijskim pravom koje države članice imaju u tom pogledu trebalo očuvati

⁴ Uredba (EU) 2016/679 Europskog parlamenta i Vijeća od 27. travnja 2016. o zaštiti pojedinaca u vezi s obradom osobnih podataka i o slobodnom kretanju takvih podataka te o stavljanju izvan snage Direktive 95/46/EZ (Opća uredba o zaštiti podataka) (SL L 119, 4.5.2016., str. 1. – 88.)

⁵ Direktiva 2002/58/EZ Europskog parlamenta i Vijeća od 12. srpnja 2002. o obradi osobnih podataka i zaštiti privatnosti u području elektroničkih komunikacija (Direktiva o privatnosti i elektroničkim komunikacijama) (SL L 201, 31.7.2002., str. 37.)

ravnotežu između zaštite privatnog života i osobnih podataka i slobodnog kretanja elektroničkih komunikacijskih podataka.

- (8) Ova bi se Uredba trebala primjenjivati na pružatelje elektroničkih komunikacijskih usluga, pružatelje javno dostupnih imenika i pružatelje softvera za elektroničke komunikacije, uključujući pronalaženje i prikaz informacija na internetu. Ova bi se Uredba isto tako trebala primjenjivati na fizičke i pravne osobe koje se služe elektroničkim komunikacijskim uslugama za slanje izravnih marketinških komercijalnih komunikacija ili prikupljanje informacija povezanih s terminalnom opremom krajnjih korisnika ili informacija pohranjenih na njoj.
- (9) Ova bi se Uredba trebala primjenjivati na elektroničke komunikacijske podatke koji se obrađuju u vezi s pružanjem i uporabom elektroničkih komunikacijskih usluga u Uniji, bez obzira na to odvija li se obrada u Uniji. Štoviše, kako se krajnjim korisnicima u Uniji ne bi onemogućila učinkovita zaštita, ovu bi Uredbu isto tako trebalo primjenjivati na elektroničke komunikacijske podatke koji se obrađuju u vezi s elektroničkim komunikacijskim uslugama koje se pružaju izvan Unije krajnjim korisnicima u Uniji.
- (10) Radijska oprema i pripadajući softver koji se stavljaju na unutarnje tržište u Uniji moraju biti usklađeni s Direktivom 2014/53/EU Europskog parlamenta i Vijeća⁶. Ova Uredba ne bi trebala utjecati na primjenu bilo kojih zahtjeva iz Direktive 2014/53/EU ni na ovlast Komisije za donošenje delegiranih akata na temelju Direktive 2014/53/EU kojom se zahtijeva da određene kategorije ili razredi radijske opreme obuhvaćaju zaštitne mjere radi osiguranja zaštite osobnih podataka i privatnosti krajnjih korisnika.
- (11) Usluge koje se upotrebljavaju u komunikacijske svrhe i tehnička sredstva za njihovu isporuku razvili su se u znatnoj mjeri. Krajnji korisnici tradicionalnu govornu telefoniju, tekstualne poruke (SMS) i usluge elektroničke pošte sve više zamjenjuju funkcionalno istovjetnim internetskim uslugama kao što su govor putem IP-a, usluge razmjene poruka i usluge elektroničke pošte na internetu. Kako bi se osigurala učinkovita i jednaka zaštita krajnjih korisnika kada se služe funkcionalno istovjetnim uslugama, u ovoj se Uredbi upotrebljava definicija elektroničkih komunikacijskih usluga utvrđena [Direktivom Europskog parlamenta i Vijeća o Europskom zakoniku elektroničkih komunikacija⁷]. Ta definicija uključuje ne samo usluge pristupa internetu i usluge koje se u cijelosti ili djelomično sastoje od prijenosa signala, već i interpersonalne komunikacijske usluge koje mogu i ne moraju biti brojevno utemeljene, kao što su, na primjer, govor putem IP-a, usluge razmjene poruka i usluge elektroničke pošte na internetu. Zaštita povjerljivosti komunikacija ključna je i u pogledu interpersonalnih komunikacijskih usluga koje su pomoćne uz drugu uslugu; stoga bi takvu vrstu usluga koje isto tako imaju komunikacijsku funkcionalnost trebalo obuhvatiti ovom Uredbom.
- (12) Povezani uređaji i strojevi sve više međusobno komuniciraju služeći se elektroničkim komunikacijskim mrežama (internet stvari). Prijenos komunikacija između strojeva uključuje prijenos signala mrežom i stoga uobičajeno predstavlja elektroničku komunikacijsku uslugu. Kako bi se osigurala potpuna zaštita prava na privatnost i

⁶ Direktiva 2014/53/EU Europskog parlamenta i Vijeća od 16. travnja 2014. o usklađivanju zakonodavstava država članica o stavljanju na raspolaganje radijske opreme na tržištu i stavljanju izvan snage Direktive 1999/5/EZ (SL L 153, 22.5.2014., str. 62.)

⁷ Prijedlog Komisije za Direktivu Europskog parlamenta i Vijeća o Europskom zakoniku elektroničkih komunikacija (preinaka) (COM/2016/0590 final – 2016/0288 (COD))

povjerljivost komunikacija te promicao pouzdan i siguran internet stvari na jedinstvenom digitalnom tržištu, potrebno je pojasniti da bi se ova Uredba trebala primjenjivati na prijenos komunikacija među strojevima. Stoga bi se načelo povjerljivosti sadržano u ovoj Uredbi trebalo primjenjivati i na prijenos komunikacija između strojeva. Posebne zaštitne mjere mogle bi se isto tako donijeti u skladu sa sektorskim zakonodavstvom, kao što je, na primjer, Direktiva 2014/53/EU.

- (13) Razvojem brzih i učinkovitih bežičnih tehnologija potiče se sve veća dostupnost pristupa internetu za javnost putem bežičnih mreža kojima može pristupiti svatko u javnom i polujavnom prostoru, kao što su pristupne točke smještene na različitim mjestima u gradu, u robnim kućama, trgovačkim centrima i bolnicama. Povjerljivost komunikacija koje se prenose takvim mrežama trebalo bi zaštititi ako se usluge te komunikacijske mreže pružaju nedefiniranoj skupini krajnjih korisnika. Činjenicom da bežične elektroničke komunikacijske usluge mogu biti pomoćne uz druge usluge ne bi trebalo spriječiti osiguranje zaštite povjerljivosti podataka iz komunikacija i primjenu ove Uredbe. Stoga bi se ova Uredba trebala primjenjivati na elektroničke komunikacijske podatke u okviru kojih se upotrebljavaju elektroničke komunikacijske usluge i javne komunikacijske mreže. Suprotno tome, ova se Uredba ne bi trebala primjenjivati na zatvorene skupine krajnjih korisnika kao što su korporativne mreže za koje je pristup ograničen na članove korporacije.
- (14) Elektroničke komunikacijske podatke trebalo bi definirati dovoljno široko i tehnološki neutralno kako bi se obuhvatile sve informacije o sadržaju koji se prenosi ili razmjenjuje (sadržaj elektroničkih komunikacija) i informacije o krajnjem korisniku elektroničkih komunikacijskih usluga koje se obrađuju u svrhu prijenosa, distribucije ili omogućavanja razmjene sadržaja elektroničkih komunikacija, uključujući podatke za praćenje i identifikaciju izvora i odredišta komunikacije, zemljopisnu lokaciju te datum, vrijeme, trajanje i vrstu komunikacije. Prenose li se takvi signali i povezani podaci žičanim, radijskim, svjetlosnim ili drugim elektromagnetskim sredstvom, uključujući satelitske mreže, kabelske mreže, nepokretne (s prespajanjem kanala i prespajanjem paketa podataka, uključujući internet) i pokretne zemaljske mreže te elektroenergetske kabelske sustave, podatke povezane s takvim signalima trebalo bi smatrati elektroničkim komunikacijskim metapodacima i stoga bi oni trebali podlijegati ovoj Uredbi. Elektronički komunikacijski metapodaci mogu uključivati informacije koje su dio pretplate na uslugu kada se takve informacije obrađuju u svrhe prijenosa, distribucije ili razmjene sadržaja elektroničkih komunikacija.
- (15) Elektroničke komunikacijske podatke trebalo bi tretirati kao povjerljive. To znači da bi trebalo zabraniti svako zadiranje u prijenos elektroničkih komunikacijskih podataka, bez obzira je li to ljudskom intervencijom ili automatiziranom obradom koju provode strojevi, bez privole svih stranaka u komunikaciji. Zabranu presretanja podataka o komunikacijama trebalo bi primjenjivati tijekom njihova prijenosa, odnosno dok predviđeni primatelj ne primi sadržaj elektroničke komunikacije. Do presretanja elektroničkih komunikacijskih podataka može doći, na primjer, kada netko tko nije stranka u komunikaciji sluša pozive, čita, pregledava ili pohranjuje sadržaj elektroničkih komunikacija ili povezane metapodatke u svrhe koje nisu razmjena komunikacija. Do presretanja dolazi i ako treće strane bez privole dotičnog krajnjeg korisnika prate posjećena web-mjesta, vrijeme posjeta, interakciju s drugima itd. S razvojem tehnologije povećava se i broj tehničkih načina za uključivanje u presretanje. Takvi načini mogu se kretati od instalacije opreme za prikupljanje podataka iz terminalne opreme na ciljanim područjima, kao što su uređaji za presretanje međunarodne oznake pokretnog pretplatnika (IMSI) (IMSI catcher), do programa i

tehnika kojima se, na primjer, prikriveno prate navike pregledavanja u svrhu stvaranja profila krajnjeg korisnika. Drugi primjeri presretanja uključuju prikupljanje podataka o stvarnoj poruci ili podataka o sadržaju iz nešifriranih bežičnih mreža i usmjernika, uključujući navike pregledavanja bez privole krajnjih korisnika.

- (16) Cilj zabrane pohrane komunikacija nije zabrana svake automatske, privremene ili prijelazne pohrane tih informacija ako je to samo u svrhu provedbe prijenosa u elektroničkoj komunikacijskoj mreži. Ne bi trebalo zabraniti ni obradu elektroničkih komunikacijskih podataka kako bi se osigurali sigurnost i kontinuitet elektroničkih komunikacijskih usluga, uključujući provjeru sigurnosnih prijetnji kao što su prisutnost zlonamjernog softvera ili obradu metapodataka radi osiguravanja potrebnih zahtjeva za kvalitetu usluge, kao što su latencija, varijacije kašnjenja itd.
- (17) Obrada elektroničkih komunikacijskih podataka može biti korisna za poduzeća, potrošače i društvo u cjelini. U odnosu na Direktivu 2002/58/EZ ovom se Uredbom za pružatelje elektroničkih komunikacijskih usluga proširuju mogućnosti obrade elektroničkih komunikacijskih metapodataka na temelju privole krajnjih korisnika. Međutim, krajnji korisnici pridaju veliku važnost povjerljivosti svojih komunikacija, uključujući aktivnosti na internetu, i tome da žele kontrolirati uporabu elektroničkih komunikacijskih podataka u svrhe koje nisu prijenos komunikacije. Stoga bi ovom Uredbom od pružatelja elektroničkih komunikacijskih usluga trebalo zahtijevati da pribave privolu krajnjih korisnika za obradu elektroničkih komunikacijskih metapodataka, koji bi trebali uključivati podatke o mjestu na kojem se nalazi uređaj, a nastali su za potrebe odobravanja i održavanja pristupa uslugama i povezanosti s njima. Podatke o lokaciji koji nisu generirani u kontekstu pružanja usluga elektroničkih komunikacija ne bi trebalo smatrati metapodacima. Primjeri komercijalne uporabe elektroničkih komunikacijskih metapodataka od strane pružatelja elektroničkih komunikacijskih usluga mogu uključivati toplinske mape, grafičke prikaze podataka uz primjenu boja kojima se označava prisutnost pojedinaca (heatmap). Za prikaz kretanja prometa u određenim smjerovima tijekom određenog razdoblja potreban je identifikator za povezivanje položaja pojedinaca u određenim vremenskim intervalima. Taj bi identifikator nedostajao ako bi se upotrebljavali anonimni podaci i ne bi bilo moguće prikazati takvo kretanje. Od takve bi uporabe elektroničkih komunikacijskih metapodataka korist mogli imati, na primjer, tijela javne vlasti i javni prijevoznici kako bi utvrdili gdje razviti novu infrastrukturu na temelju uporabe postojeće infrastrukture i pritiska na nju. Ako je vjerojatno da će se određenom vrstom obrade elektroničkih komunikacijskih metapodataka, posebno uz primjenu novih tehnologija te uzimajući u obzir prirodu, opseg, kontekst i svrhe obrade, prouzročiti visoki rizik za prava i slobode fizičkih osoba, trebalo bi prije obrade provesti procjenu učinka na zaštitu podataka i, ovisno o slučaju, savjetovanje s nadzornim tijelom u skladu s člancima 35. i 36. Uredbe (EU) 2016/679.
- (18) Krajnji korisnici mogu dati privolu za obradu svojih metapodataka kako bi primili posebne usluge kao što su usluge zaštite od prijevanih aktivnosti (analizom podataka u uporabi, lokacije i korisničkog računa u stvarnom vremenu). U digitalnom gospodarstvu usluge se često isporučuju u zamjenu za nenovčanu protuuslugu, na primjer izlaganje krajnjih korisnika oglasima. Za potrebe ove Uredbe privola krajnjeg korisnika, neovisno o tome je li on fizička ili pravna osoba, trebala bi imati isto značenje i podlijegati istim uvjetima kao i privola ispitanika na temelju Uredbe (EU) 2016/679. Osnovne usluge širokopojsnog pristupa internetu i govorne komunikacijske usluge trebaju se smatrati bitnim uslugama za pojedince kojima im se omogućuje komunikacija i sudjelovanje u koristima digitalnog gospodarstva. Privola

za obradu podataka iz uporabe internetske ili govorne komunikacije neće biti valjana ako ispitanik nema istinski ili slobodan izbor ili ako nije u mogućnosti odbiti ili povući privolu bez posljedica.

- (19) Sadržaj elektroničkih komunikacija odnosi se na bit temeljnog prava na poštovanje privatnog i obiteljskog života, doma i komuniciranja koje je zaštićeno člankom 7. Povelje. Svako zadiranje u sadržaj elektroničkih komunikacija trebalo bi dopustiti samo pod vrlo jasno definiranim uvjetima, u posebne svrhe i podložno odgovarajućim zaštitnim mjerama za sprječavanje zlouporabe. Ovom se Uredbom predviđa mogućnost za pružatelje elektroničkih komunikacijskih usluga da obrađuju elektroničke komunikacijske podatke u tranzitu na temelju informirane privole svih dotičnih krajnjih korisnika. Na primjer, pružatelji mogu ponuditi usluge koje uključuju pregledavanje elektroničke pošte kako bi se uklonio određeni unaprijed definirani materijal. S obzirom na osjetljivost sadržaja komunikacija, u ovoj se Uredbi pretpostavlja da će se obradom takvih podataka o sadržaju prouzročiti visoki rizici za prava i slobode fizičkih osoba. Pri obradi takve vrste podataka pružatelj elektroničke komunikacijske usluge trebao bi se prije obrade uvijek savjetovati s nadzornim tijelom. Takvo bi se savjetovanje trebalo provesti u skladu s člankom 36. stavcima 2. i 3. Uredbe (EU) 2016/679. Pretpostavkom nije obuhvaćena obrada podataka o sadržaju radi pružanja usluge koju je zatražio krajnji korisnik ako je krajnji korisnik dao privolu za takvu obradu i ako se ona provodi u svrhe i u trajanju koji su nužno potrebni i proporcionalni za takvu uslugu. Nakon što krajnji korisnik pošalje i nakon što predviđeni krajnji korisnik ili krajnji korisnici prime sadržaj elektroničkih komunikacija, mogu ga zabilježiti ili pohraniti krajnji korisnik, krajnji korisnici ili treća strana kojoj je povjereno bilježenje ili pohrana takvih podataka. Svaka obrada takvih podataka mora biti u skladu s Uredbom (EU) 2016/679.
- (20) Terminalna oprema krajnjih korisnika elektroničkih komunikacijskih mreža i sve informacije o uporabi takve terminalne opreme, neovisno o tome jesu li pohranjene na takvoj opremi ili ih ona odašilje, jesu li zatražene ili obrađene kako bi se omogućilo njezino povezivanje s drugim uređajem ili mrežnom opremom, dio su privatnog područja krajnjih korisnika koje zahtijeva zaštitu u skladu s Poveljom Europske unije o temeljnim pravima i Europskom konvencijom za zaštitu ljudskih prava i temeljnih sloboda. S obzirom na to da takva oprema sadržava ili obrađuje informacije kojima se mogu otkriti pojedinosti o emocionalnom, političkom i društvenom životu pojedinca, uključujući sadržaj komunikacija, slike, lokaciju pojedinca pristupom postavkama GPS-a na uređaju, popise kontakata i ostale informacije koje su već pohranjene na uređaju, informacije povezane s takvom opremom zahtijevaju jaču zaštitu privatnosti. Nadalje, takozvani špijunski softver, web-prisluškivači, skriveni identifikatori, kolačići za praćenje i ostali slični alati za neželjeno praćenje mogu ući u terminalnu opremu krajnjeg korisnika bez njegova znanja u cilju dobivanja pristupa informacijama, pohranjivanja skrivenih informacija ili ulaženja u trag aktivnostima. Informacije povezane s uređajem krajnjeg korisnika mogu se prikupljati i daljinski u svrhu identifikacije i praćenja primjenom tehnika kao što je „device fingerprinting” (prikupljanje informacija o uređaju u svrhu njegove identifikacije i praćenja), često bez znanja krajnjeg korisnika, čime se može ozbiljno zadrijeti u privatnost tih krajnjih korisnika. Tehnike za prikriveno praćenje postupaka krajnjih korisnika, na primjer praćenjem njihovih aktivnosti na internetu ili lokacije njihove terminalne opreme, ili za narušavanje rada terminalne opreme krajnjih korisnika ozbiljna su prijetnja privatnosti krajnjih korisnika. Stoga bi svako takvo zadiranje u terminalnu opremu krajnjeg korisnika trebalo dopustiti samo uz privolu krajnjeg korisnika te u posebne i transparentne svrhe.

- (21) Izuzeća od obveze pribavljanja privole za uporabu kapaciteta terminalne opreme za obradu ili pohranu ili za pristup informacijama pohranjenima na terminalnoj opremi trebalo bi ograničiti na situacije koje ne uključuju nikakvo ili uključuju samo vrlo ograničeno narušavanje privatnosti. Na primjer, privolu ne bi trebalo tražiti za odobrenje tehničke pohrane ili nužno potrebnog ili proporcionalnog pristupa u legitimnu svrhu omogućavanja uporabe posebne usluge koju je izričito zatražio krajnji korisnik. To može uključivati pohranu kolačića u trajanju pojedinačne uspostavljene sesije na web-mjestu radi praćenja ulaznih informacija krajnjeg korisnika kada popunjava internetske obrasce od više stranica. Kolačići mogu biti legitiman i koristan alat, na primjer, za mjerenje internetskog prometa prema web-mjestu. Ako pružatelji usluga informacijskog društva poduzmu provjeru konfiguracije kako bi pružili uslugu u skladu s postavkama krajnjeg korisnika i samo zabilježe činjenicu da uređaj krajnjeg korisnika ne može primiti sadržaj koji je zatražio krajnji korisnik, to ne bi trebalo predstavljati pristup takvom uređaju ili uporabu kapaciteta uređaja za obradu.
- (22) Metode koje se primjenjuju za pružanje informacija i pribavljanje privole krajnjeg korisnika trebale bi biti što pristupačnije. S obzirom na sveprisutnu uporabu kolačića za praćenje i ostalih tehnika praćenja, od krajnjih se korisnika sve češće traži da daju privolu za pohranu takvih kolačića za praćenje na svoju terminalnu opremu. Stoga su krajnji korisnici prezasićeni zahtjevima za davanje privole. Taj se problem može riješiti uporabom tehničkih sredstava za davanje privole, na primjer transparentnim i pristupačnim postavkama. Stoga bi se ovom Uredbom trebala predvidjeti mogućnost izražavanja privole odabirom odgovarajućih postavki preglednika ili druge aplikacije. Odluke krajnjih korisnika u pogledu prilagodbe općih postavki privatnosti preglednika ili druge aplikacije trebale bi biti obvezujuće za sve treće strane i izvršive u pogledu svih trećih strana. *Web*-preglednici vrsta su softverske aplikacije za pronalaženje i prikaz informacija na internetu. Druge vrste aplikacija, kao što su one kojima se omogućuju pozivi i razmjena poruka ili pružaju informacije o smjeru puta, imaju iste mogućnosti. *Web*-preglednici u velikoj mjeri posreduju u onome što se događa između krajnjeg korisnika i *web*-mjesta. Iz te su perspektive oni u povlaštenom položaju u kojem imaju aktivnu ulogu pomažući krajnjem korisniku u kontroli protoka informacija prema terminalnoj opremi i od nje. *Web*-preglednici mogu se posebno upotrebljavati kao filtri mreže s pomoću kojih se krajnjim korisnicima pomaže da spriječe pristup informacijama iz svoje terminalne opreme (na primjer pametnog telefona, tablet računala ili računala) ili pohranu takvih informacija.
- (23) Načela tehničke i integrirane zaštite podataka kodificirana su na temelju članka 25. Uredbe (EU) 2016/679. Trenutačno je u većini preglednika prema zadanim postavkama odabrana opcija „Prihvati sve kolačiće”. Stoga bi pružatelji softvera za pronalaženje i prikaz informacija na internetu trebali biti obvezni konfigurirati softver tako da nudi mogućnost da se trećim stranama onemogući pohranjivanje informacija na terminalnoj opremi; to se često prikazuje kao postavka „Odbij kolačiće treće strane”. Krajnjim bi korisnicima trebalo ponuditi skup opcija za postavke privatnosti u rasponu od viših (na primjer „Nikada ne prihvaćaj kolačiće”) do nižih (na primjer „Uvijek prihvati kolačiće”) i srednjih (na primjer „Odbij kolačiće treće strane” ili „Prihvati samo kolačiće prve strane”). Takve bi postavke privatnosti trebalo prikazati na lako vidljiv i razumljiv način.
- (24) Kako bi *web*-preglednici mogli pribaviti privolu krajnjih korisnika u skladu s Uredbom (EU) 2016/679, na primjer za pohranu kolačića treće strane za praćenje, oni bi, među ostalim, od krajnjeg korisnika terminalne opreme trebali zatražiti da jasnom potvrdnom radnjom da dobrovoljan, poseban, informiran i nedvosmislen pristanak za

pohranu takvih kolačića na terminalnu opremu i pristup tim kolačićima iz terminalne opreme. Radnja se može smatrati potvrdnom ako se, na primjer, od krajnjih korisnika zahtijeva da aktivno odaberu postavku „Prihvati kolačiće treće strane” kako bi potvrdili svoj pristanak i ako su im dane informacije potrebne za odabir. U tu je svrhu potrebno od pružatelja softvera za pristup internetu zahtijevati da u trenutku instalacije obavijeste krajnje korisnike o različitim mogućnostima odabira postavki privatnosti i da od njih zatraže da odaberu postavke. Pruženim informacijama krajnje korisnike ne bi trebalo odvratiti od odabira viših postavki privatnosti te bi one trebale uključivati relevantne informacije o rizicima povezanim s omogućivanjem pohrane kolačića treće strane na računalu, uključujući izradu dugoročne evidencije o povijesti pregledavanja pojedinaca i uporabu te evidencije za slanje ciljanog oglašavanja. Potiče se da se na *web*-preglednicima krajnjim korisnicima osiguraju jednostavni načini promjene postavki privatnosti u bilo kojem trenutku tijekom uporabe i omogući korisniku da stvori izuzeća za određena *web*-mjesta ili popis dopuštenih *web*-mjesta ili da utvrdi za koja su *web*-mjesta uvijek odnosno za koja *web*-mjesta nikad nisu dopušteni kolačići (trećih) strana.

- (25) Za pristup elektroničkim komunikacijskim mrežama potrebna je redovita emisija određenih podatkovnih paketa kako bi se otkrila ili zadržala veza s mrežom ili drugim uređajima u mreži. Nadalje, uređaji moraju imati jedinstvenu adresu koja im je dodijeljena za utvrđivanje njihova identiteta u toj mreži. Slično tome, standardni bežični telefoni i mobiteli emitiraju aktivne signale koji sadržavaju jedinstvene identifikatore, kao što su adresa MAC, međunarodni identifikator mobilnog uređaja („IMEI”), međunarodni identifikator mobilnoga pretplatnika („IMSI”) itd. Pojedinačna bežična bazna stanica (odnosno odašiljač i prijamnik), kao što je bežična pristupna točka, ima određeni raspon unutar kojeg se mogu prikupljati takve informacije. Pojavili su se pružatelji usluga koji nude usluge praćenja na temelju pregledavanja informacija povezanih s opremom s različitim funkcionalnostima, uključujući brojanje ljudi, pružanje podataka o broju ljudi koji čekaju u redu, provjeru broja ljudi na određenom području itd. Te se informacije mogu upotrebljavati u još intruzivnije svrhe, kao što je slanje komercijalnih poruka krajnjim korisnicima s personaliziranim ponudama, primjerice kada ulaze u trgovine. Iako neke od tih funkcionalnosti ne podrazumijevaju visoke rizike za privatnost, druge podrazumijevaju, na primjer one koje uključuju praćenje pojedinaca tijekom vremena, uključujući višestruke posjete određenim lokacijama. Pružatelji koji provode takve prakse trebali bi na rubu područja pokrivenosti istaknuti obavijesti kojima krajnje korisnike prije ulaska na definirano područje informiraju o upotrebi tehnologije unutar zadanog opsega, o svrsi praćenja, osobi odgovornoj za praćenje i postojanju bilo koje mjere koju krajnji korisnik terminalne opreme može poduzeti kako bi smanjio ili zaustavio prikupljanje. Ako se prikupljaju osobni podaci, trebalo bi osigurati dodatne informacije u skladu s člankom 13. Uredbe (EU) 2016/679.
- (26) Ako je obrada podataka elektroničkih komunikacija koju provode pružatelji elektroničkih komunikacijskih usluga obuhvaćena područjem primjene ove Uredbe, njome bi se trebala predvidjeti mogućnost da Unija ili države članice pod posebnim uvjetima zakonom ograniče određene obveze i prava ako je takvo ograničenje nužna i proporcionalna mjera u demokratskom društvu za zaštitu posebnih javnih interesa, uključujući nacionalnu sigurnost, obranu i javnu sigurnost te prevenciju, istrage, otkrivanje ili progon kaznenih djela ili izvršavanje kaznenih sankcija, među ostalim i prevenciju i zaštitu od prijetnji javnoj sigurnosti, ili drugih važnih ciljeva od općeg javnog interesa Unije ili države članice, posebno važnoga gospodarskog ili financijskog interesa Unije ili države članice, ili funkcije praćenja, inspekcije ili

regulativne funkcije koja je povezana s izvršavanjem službene ovlasti za takve interese. Stoga ova Uredba ne bi trebala utjecati na sposobnost država članica da provode zakonito presretanje elektroničkih komunikacija ili poduzimaju druge mjere ako je to nužno i proporcionalno za zaštitu prethodno navedenih javnih interesa, u skladu s Poveljom Europske unije o temeljnim pravima i Europskom konvencijom za zaštitu ljudskih prava i temeljnih sloboda kako ih tumače Sud Europske unije i Europski sud za ljudska prava. Pružatelji elektroničkih komunikacijskih usluga trebali bi osigurati odgovarajuće postupke za olakšavanje legitimnih zahtjeva nadležnih tijela, uzimajući u obzir, ako je to relevantno, ulogu predstavnika imenovanog u skladu s člankom 3. stavkom 3.

- (27) Kad je riječ o prikazu broja pozivatelja, potrebno je zaštititi pravo pozivatelja da onemogući prikaz broja s kojeg se poziv upućuje i pravo primatelja da odbije pozive s neidentificiranih brojeva. Određeni krajnji korisnici, posebno službe za korisnike i slične organizacije, zainteresirani su za jamčenje anonimnosti svojih pozivatelja. Kad je riječ o prikazu broja pozvane linije, potrebno je zaštititi pravo i legitimni interes primatelja da onemogući prikaz broja linije s kojom je pozivatelj doista povezan.
- (28) U posebnim je slučajevima opravdano poništiti uklanjanje prikaza broja pozivatelja. Prava krajnjih korisnika na privatnost u pogledu prikaza broja pozivatelja trebalo bi ograničiti ako je to potrebno kako bi se ušlo u trag uznemirujućim pozivima te u pogledu prikaza broja pozivatelja i podataka o lokaciji ako je to potrebno kako bi se hitnim službama, kao što je sustav eCall, omogućila što učinkovitija provedba njihovih zadaća.
- (29) Postoji tehnologija kojom se pružateljima elektroničkih komunikacijskih usluga omogućuje da za krajnje korisnike na različite načine ograniče primanje neželjenih poziva, među ostalim i blokiranjem tih poziva i ostalih prijevarnih te uznemirujućih poziva. Pružatelji javno dostupnih brojevnog utemeljenih interpersonalnih komunikacijskih usluga trebali bi uvesti tu tehnologiju i besplatno zaštititi krajnje korisnike od uznemirujućih poziva. Pružatelji bi trebali osigurati da krajnji korisnici budu upoznati s postojanjem tih funkcionalnosti, na primjer, tako da te činjenice objave na svojem *web*-mjestu.
- (30) Javno dostupni imenici krajnjih korisnika elektroničkih komunikacijskih usluga distribuiraju se posvuda. Javno dostupan imenik znači svaki imenik ili usluga koji sadržavaju informacije o krajnjim korisnicima, kao što su telefonski brojevi (uključujući brojeve mobitela), i adresa elektroničke pošte, te uključuje imeničke usluge. U skladu s pravom na privatnost i zaštitu osobnih podataka fizičke osobe, od krajnjih korisnika koji su fizičke osobe mora se zatražiti privola prije uključivanja njihovih osobnih podataka u imenik. U skladu s legitimnim interesom pravnih subjekata, krajnji korisnici koji su pravni subjekti imaju pravo na prigovor u pogledu uključivanja svojih podataka u imenik.
- (31) Ako krajnji korisnici koji su fizičke osobe daju privolu za uvrštavanje svojih podataka u takve imenike, trebali bi imati mogućnost da na temelju privole odrede koje se kategorije osobnih podataka uvrštavaju u imenik (na primjer ime, adresa elektroničke pošte, kućna adresa, korisničko ime, telefonski broj). Osim toga, pružatelji javno dostupnih imenika trebali bi obavijestiti krajnje korisnike o svrhama imenika i funkcijama pretraživanja imenika prije uvrštavanja njihovih podataka u taj imenik. Krajnji korisnici trebali bi imati mogućnost da na temelju privole odrede prema kojim se kategorijama njihovih osobnih podataka mogu pretraživati njihovi kontaktni podaci. Kategorije osobnih podataka uvrštenih u imenik i kategorije osobnih podataka prema

kojima se mogu pretraživati kontaktni podaci krajnjeg korisnika ne bi nužno trebale biti iste.

- (32) U ovoj Uredbi izravni marketing podrazumijeva svaki oblik oglašavanja kojim fizička ili pravna osoba izravno šalje, služeći se elektroničkim komunikacijskim uslugama, izravne marketinške komunikacije jednom ili više krajnjih korisnika čiji je identitet utvrđen ili se može utvrditi. Uz ponudu proizvoda i usluga u komercijalne svrhe, to bi trebalo uključivati i poruke koje šalju političke stranke koje elektroničkim komunikacijskim uslugama stupaju u kontakt s fizičkim osobama kako bi promicale svoje stranke. Isto bi trebalo vrijediti i za poruke koje šalju neprofitne organizacije u potporu ciljevima organizacije.
- (33) Trebalo bi osigurati mjere za zaštitu krajnjih korisnika od nezatraženih komunikacija u svrhe izravnog marketinga kojima se zadire u privatni život krajnjih korisnika. Stupanj narušavanja privatnosti i uznemiravanja smatra se relativno sličnim neovisno o širokom rasponu tehnologija i kanala koji se upotrebljavaju za provedbu tih elektroničkih komunikacija, neovisno o tome upotrebljavaju li se automatizirani sustavi pozivanja i komunikacijski sustavi, aplikacije za trenutačnu razmjenu poruka, elektronička pošta, SMS, MMS, Bluetooth itd. Stoga je opravdano zahtijevati da se privola krajnjeg korisnika pribavi prije nego što se krajnjim korisnicima pošalju komercijalne elektroničke komunikacije u svrhe izravnog marketinga kako bi se pojedinci učinkovito zaštitili od narušavanja njihova privatnog života, kao i legitiman interes pravnih osoba. Pravna sigurnost i potreba da pravila o zaštiti od nezatraženih elektroničkih komunikacija budu održiva u budućnosti opravdavaju potrebu za utvrđivanjem jedinstvenog skupa pravila koja se ne razlikuju ovisno o tehnologiji korištenoj za slanje tih nezatraženih komunikacija, pri čemu bi se svim građanima u Uniji trebala zajamčiti istovjetna razina zaštite. Međutim, razumno je dopustiti da se podaci o elektroničkoj pošti upotrebljavaju u kontekstu postojećeg odnosa s potrošačima za ponudu sličnih proizvoda ili usluga. Tu bi mogućnost trebalo primjenjivati samo na isto poduzeće koje je elektroničke kontaktne podatke pribavilo u skladu s Uredbom (EU) 2016/679.
- (34) Ako su krajnji korisnici dali privolu za primanje nezatraženih komunikacija u svrhu izravnog marketinga, i dalje bi trebali imati mogućnost da na jednostavan način u bilo kojem trenutku povuku privolu. Kako bi se olakšalo učinkovito izvršenje pravila Unije o nezatraženim porukama u svrhu izravnog marketinga, potrebno je zabraniti maskiranje identiteta i uporabu lažnih identiteta, lažnih povratnih adresa ili brojeva pri slanju nezatraženih komercijalnih komunikacija u svrhe izravnog marketinga. Nezatražene marketinške komunikacije trebale bi stoga biti jasno prepoznatljive kao takve i u njima bi trebalo navesti identitet pravne ili fizičke osobe koja prenosi komunikaciju ili u čije se ime komunikacija prenosi i pružiti potrebne informacije na temelju kojih primatelji mogu ostvariti svoje pravo na prigovor u pogledu primanja daljnjih pismenih i/ili usmenih marketinških poruka.
- (35) Kako bi se omogućilo jednostavno povlačenje privole, pravne ili fizičke osobe koje provode izravne marketinške komunikacije elektroničkom poštom trebale bi navesti poveznicu ili valjanu adresu elektroničke pošte koju krajnji korisnici mogu jednostavno upotrijebiti za povlačenje svoje privole. Pravne ili fizičke osobe koje provode izravne marketinške komunikacije govornim pozivima i pozivima preko automatiziranih sustava pozivanja i komunikacijskih sustava trebale bi prikazati svoj broj na koji je moguće nazvati poduzeće ili navesti poseban kôd na temelju kojeg se može utvrditi da je poziv marketinške prirode.

- (36) Govorni izravni marketinški pozivi koji ne uključuju uporabu automatiziranih sustava pozivanja ili komunikacijskih sustava skuplji su za pošiljatelja i ne uključuju nikakve financijske troškove za krajnje korisnike. Stoga bi države članice trebale imati mogućnost uspostave i/ili održavanja nacionalnih sustava kojima se dopuštaju takvi pozivi samo krajnjim korisnicima koji nisu uložili prigovor.
- (37) Pružatelji usluga koji nude elektroničke komunikacijske usluge trebali bi obavijestiti krajnje korisnike o mjerama koje mogu poduzeti kako bi zaštitili sigurnost svojih komunikacija, na primjer uporabom posebnih vrsta softvera ili tehnologija šifriranja. Zahtjev za obavješćivanje krajnjih korisnika o posebnim sigurnosnim rizicima ne podrazumijeva oslobađanje pružatelja usluga od obveze da o vlastitom trošku poduzme odgovarajuće i hitne mjere kako bi otklonio sve nove, nepredviđene sigurnosne rizike i ponovno uspostavio normalnu sigurnosnu razinu usluge. Pružanje informacije o sigurnosnim rizicima za pretplatnika bi trebalo biti besplatno. Sigurnost se procjenjuje na temelju članka 32. Uredbe (EU) 2016/679.
- (38) Kako bi se osigurala potpuna usklađenost s Uredbom (EU) 2016/679, izvršenje odredaba ove Uredbe trebalo bi povjeriti istim tijelima koja su odgovorna za izvršenje odredaba Uredbe (EU) 2016/679 te se ova Uredba oslanja na mehanizam konzistentnosti iz Uredbe (EU) 2016/679. Države članice trebale bi imati mogućnost da uspostave više od jednog nadzornog tijela radi usklađivanja sa svojom ustavnom, organizacijskom i upravnom strukturom. Nadzorna tijela trebala bi biti odgovorna i za praćenje primjene ove Uredbe u pogledu elektroničkih komunikacijskih podataka za pravne subjekte. Takvim dodatnim zadaćama ne bi se trebala ugroziti sposobnost nadzornog tijela za provedbu zadaća povezanih sa zaštitom osobnih podataka na temelju Uredbe (EU) 2016/679 i ove Uredbe. Svakom nadzornom tijelu trebalo bi osigurati dodatne financijske i ljudske resurse, prostorije i infrastrukturu koji su potrebni za učinkovitu provedbu zadaća na temelju ove Uredbe.
- (39) Svako nadzorno tijelo trebalo bi biti nadležno na državnom području svoje države članice kako bi izvršavalo ovlasti i obavljalo zadaće utvrđene ovom Uredbom. Kako bi se osiguralo dosljedno praćenje i izvršenje ove Uredbe u cijeloj Uniji, nadzorna tijela trebala bi u svakoj državi članici imati iste zadaće i stvarne ovlasti, ne dovodeći u pitanje ovlasti tijela kaznenog progona u skladu s pravom države članice da pravosudna tijela upozore na povrede ove Uredbe i da sudjeluju u pravnim postupcima. Države članice i nadzorna tijela potiče se da pri primjeni ove Uredbe uzmu u obzir posebne potrebe mikropoduzeća te malih i srednjih poduzeća.
- (40) Kako bi se ojačalo izvršenje pravila ove Uredbe, svako nadzorno tijelo trebalo bi imati ovlast da za svaku povredu ove Uredbe uz druge odgovarajuće mjere u skladu s ovom Uredbom ili umjesto njih uvede sankcije, uključujući upravne novčane kazne. U ovoj Uredbi trebalo bi navesti povrede te gornju granicu i kriterije za određivanje povezanih upravnih novčanih kazni, što bi za svaki pojedinačni slučaj trebalo odrediti nadležno nadzorno tijelo, uzimajući u obzir sve bitne okolnosti konkretne situacije, vodeći računa posebno o prirodi, težini i trajanju povrede i njezinim posljedicama te mjerama poduzetima kako bi se osiguralo poštovanje obveza na temelju ove Uredbe te spriječile ili ublažile posljedice povrede. Za potrebe određivanja novčane kazne na temelju ove Uredbe poduzetnik bi se trebao smatrati poduzetnikom u skladu s člancima 101. i 102. Ugovora.
- (41) Kako bi se ostvarili ciljevi ove Uredbe, odnosno zaštita temeljnih prava i sloboda fizičkih osoba, a posebno njihovo pravo na zaštitu osobnih podataka, i osiguravanje slobodnog kretanja osobnih podataka unutar Unije, Komisiji bi trebalo delegirati

ovlast za donošenje akata u skladu s člankom 290. Ugovora radi dopune ove Uredbe. Konkretno, trebalo bi donijeti delegirane akte u pogledu informacija koje se trebaju pružiti, uključujući i s pomoću standardiziranih ikona, kako bi se osigurao lako vidljiv i razumljiv pregled nad prikupljanjem informacija koje emitira terminalna oprema, svrhe prikupljanja, osoba odgovorna za prikupljanje i svih mjera koje krajnji korisnik terminalne opreme može poduzeti kako bi smanjio prikupljanje. Delegirani akti potrebni su i za utvrđivanje koda za identifikaciju izravnih marketinških poziva, uključujući pozive preko automatiziranih sustava pozivanja i komunikacijskih sustava. Posebno je važno da Komisija provede odgovarajuća savjetovanja u skladu s načelima utvrđenima u Međuinstitucijskom sporazumu o boljoj izradi zakonodavstva od 13. travnja 2016.⁸ Konkretno, kako bi se osiguralo ravnopravno sudjelovanje u izradi delegiranih akata, Europski parlament i Vijeće primaju sve dokumente u isto vrijeme kada i stručnjaci iz država članica te njihovi stručnjaci sustavno imaju pristup sastancima stručnih skupina Komisije koje se bave izradom delegiranih akata. Nadalje, radi osiguranja jedinstvenih uvjeta za provedbu ove Uredbe, provedbene ovlasti trebalo bi dodijeliti Komisija kada je to predviđeno ovom Uredbom. Te bi se ovlasti trebale izvršavati u skladu s Uredbom (EU) br. 182/2011.

(42) S obzirom na to da cilj ove Uredbe, odnosno osiguravanje istovjetne razine zaštite fizičkih i pravnih osoba te slobodnog protoka elektroničkih komunikacijskih podataka u cijeloj Uniji, ne mogu dostatno ostvariti države članice, nego se zbog opsega ili učinaka djelovanja on na bolji način može ostvariti na razini Unije, Unija može donijeti mjere u skladu s načelom supsidijarnosti utvrđenim u članku 5. Ugovora o Europskoj uniji. U skladu s načelom proporcionalnosti utvrđenim u tom članku ova Uredba ne prelazi ono što je potrebno za ostvarivanje tog cilja.

(43) Direktivu 2002/58/EZ trebalo bi staviti izvan snage,

DONIJELI SU OVU UREDBU:

⁸ Međuinstitucijski sporazum Europskog parlamenta, Vijeća Europske unije i Europske komisije o boljoj izradi zakonodavstva od 13. travnja 2016. (SL L 123, 12.5.2016., str. 1– 14.)

POGLAVLJE I.

OPĆE ODREDBE

Članak 1.

Predmet

1. Ovom se Uredbom utvrđuju pravila u pogledu zaštite temeljnih prava i sloboda fizičkih i pravnih osoba pri pružanju i uporabi elektroničkih komunikacijskih usluga, posebno prava na poštovanje privatnog života i komuniciranja i zaštita fizičkih osoba u pogledu obrade osobnih podataka.
2. Ovom se Uredbom osigurava slobodno kretanje elektroničkih komunikacijskih podataka i elektroničkih komunikacijskih usluga unutar Unije, koje se ne smije ograničiti niti zabraniti zbog razloga povezanih s poštovanjem privatnog života i komuniciranja fizičkih i pravnih osoba te zaštitom fizičkih osoba u pogledu obrade osobnih podataka
3. Odredbama ove Uredbe preciznije se utvrđuje i dopunjuje Uredba (EU) 2016/679 utvrđivanjem posebnih pravila u svrhe navedene u stavcima 1. i 2.

Članak 2.

Glavno područje primjene

1. Ova se Uredba primjenjuje na obradu elektroničkih komunikacijskih podataka koja se provodi u vezi s pružanjem i uporabom elektroničkih komunikacijskih usluga i na informacije povezane s terminalnom opremom krajnjih korisnika.
2. Ova se Uredba ne primjenjuje na:
 - (a) aktivnosti koje nisu obuhvaćene područjem primjene prava Unije;
 - (b) aktivnosti država članica koje su obuhvaćene područjem primjene glave V. poglavlja 2. Ugovora o Europskoj uniji;
 - (c) elektroničke komunikacijske usluge koje nisu javno dostupne;
 - (d) aktivnosti koje nadležna tijela provode u svrhu prevencije, istrage, otkrivanja ili progona kaznenih djela ili izvršavanja kaznenih sankcija, uključujući prevenciju i zaštitu od prijetnji javnoj sigurnosti;
3. Obrada elektroničkih komunikacijskih podataka koju provode institucije, tijela, uredi i agencije Unije uređena je Uredbom (EU) 00/0000 [nova Uredba kojom se zamjenjuje Uredba 45/2001].
4. Ovom se Uredbom ne dovodi u pitanje primjena Direktive 2000/31/EZ⁹, posebno pravila o odgovornosti posrednih pružatelja usluga iz članka 12. do 15. te Direktive.
5. Ovom se Uredbom ne dovode u pitanje odredbe Direktive 2014/53/EU.

⁹ Direktiva 2000/31/EZ Europskog parlamenta i Vijeća od 8. lipnja 2000. o određenim pravnim aspektima usluga informacijskog društva na unutarnjem tržištu, posebno elektroničke trgovine (Direktiva o elektroničkoj trgovini) (SL L 178, 17.7.2000., str. 1–16.)

Članak 3.
Teritorijalno područje primjene i predstavnik

1. Ova se Uredba primjenjuje na:
 - (a) pružanje elektroničkih komunikacijskih usluga krajnjim korisnicima u Uniji, bez obzira na to plaćaju li ih krajnji korisnici ili ne;
 - (b) uporabu takvih usluga;
 - (c) zaštitu informacija povezanih s terminalnom opremom krajnjih korisnika koji se nalaze u Uniji.
2. Ako nema poslovni nastan u Uniji, pružatelj elektroničkih komunikacijskih usluga pisanim putem imenuje predstavnika u Uniji.
3. Predstavnik ima poslovni nastan u jednoj od država članica u kojima se nalaze krajnji korisnici takvih elektroničkih komunikacijskih usluga.
4. Predstavnik ima ovlast da uz ili umjesto pružatelja kojeg predstavlja odgovara na pitanja i pruža informacije, posebno nadzornim tijelima i krajnjim korisnicima, o svim pitanjima povezanim s obradom elektroničkih komunikacijskih podataka radi osiguranja usklađenosti s ovom Uredbom.
5. Imenovanjem predstavnika u skladu sa stavkom 2. ne dovode se u pitanje pravni postupci koji bi se mogli pokrenuti protiv fizičke ili pravne osobe koja obrađuje elektroničke komunikacijske podatke u vezi s elektroničkim komunikacijskim uslugama koje se iz država koje nisu članice Unije pružaju krajnjim korisnicima u Uniji.

Članak 4.
Definicije

1. Za potrebe ove Uredbe primjenjuju se sljedeće definicije:
 - (a) definicije iz Uredbe (EU) 2016/679;
 - (b) definicije „elektroničke komunikacijske mreže”, „elektroničke komunikacijske usluge”, „interpersonalne komunikacijske usluge”, „brojevno utemeljene interpersonalne komunikacijske usluge”, „brojevno neovisne interpersonalne komunikacijske usluge”, „krajnjeg korisnika” i „poziva” iz članka 2. točaka 1., 4., 5., 6., 7., 14. i 21. [Direktive o Europskom zakoniku elektroničkih komunikacija];
 - (c) definicija „terminalne opreme” iz članka 1. točke 1. Direktive Komisije 2008/63/EZ¹⁰.
2. Za potrebe stavka 1. točke (b) definicija „interpersonalne komunikacijske usluge” uključuje usluge kojima se omogućuje interpersonalna i interaktivna komunikacija samo kao manja pomoćna funkcija koja je neraskidivo povezana s drugom uslugom.
3. Osim toga, za potrebe ove Uredbe primjenjuju se sljedeće definicije:
 - (a) „elektronički komunikacijski podaci ” znači sadržaj elektroničkih komunikacija i elektronički komunikacijski metapodaci;

¹⁰ Direktiva Komisije 2008/63/EZ od 20. lipnja 2008. o tržišnom natjecanju na tržištima telekomunikacijske terminalne opreme (SL L 162, 21.6.2008., str. 20– 26.)

- (b) „sadržaj elektroničkih komunikacija” znači sadržaj koji se razmjenjuje elektroničkim komunikacijskim uslugama, primjerice tekst, govor, video, slike i zvuk;
- (c) „elektronički komunikacijski metapodaci ” znači podaci koji su obrađeni u elektroničkoj komunikacijskom mreži u svrhe prijenosa, distribucije ili razmjene sadržaja elektroničkih komunikacija, uključujući podatke koji se upotrebljavaju za slijeđenje i identifikaciju izvora i odredišta komunikacije, podatke o lokaciji uređaja generirane u kontekstu pružanja elektroničkih komunikacijskih usluga te datum, vrijeme, trajanje i vrstu komunikacije;
- (d) „javno dostupan imenik” znači imenik krajnjih korisnika elektroničkih komunikacijskih usluga, neovisno o tome je li u tiskanom ili elektroničkom obliku, koji se objavljuje ili stavlja na raspolaganje javnosti ili dijelu javnosti, među ostalim i putem imeničke službe;
- (e) „elektronička pošta” znači svaka elektronička poruka koja sadržava informacije kao što su tekst, govor, video, zvuk ili slika i koja je poslana elektroničkom komunikacijskom mrežom te koja se može pohraniti u mreži ili na povezanoj računalnoj opremi ili na terminalnoj opremi njezinih primatelja;
- (f) „izravne marketinške komunikacije” znači svaki oblik oglašavanja, neovisno o tome je li u pisanom ili usmenom obliku, koji se šalje jednom ili više krajnjih korisnika elektroničkih komunikacijskih usluga čiji je identitet utvrđen ili se može utvrditi, među ostalim i uporabom automatiziranih sustava pozivanja i komunikacijskih sustava uz sudjelovanje ljudi ili bez njega, elektroničke pošte, SMS-a itd.;
- (g) „izravni marketinški govorni pozivi” znači pozivi uživo koji ne podrazumijevaju uporabu automatiziranih sustava pozivanja i komunikacijskih sustava;
- (h) „automatizirani sustavi pozivanja i komunikacijski sustavi” znači sustavi koji mogu automatski započinjati pozive prema jednom ili više primatelja u skladu s uputama postavljenima za taj sustav i prenositi zvukove koji nisu govor uživo, uključujući pozive uz uporabu automatiziranih sustava pozivanja i komunikacijskih sustava koji povezuju primatelja s pojedincem.

POGLAVLJE II.

ZAŠTITA ELEKTRONIČKIH KOMUNIKACIJA FIZIČKIH I PRAVNIH OSOBA TE INFORMACIJA POHRANJENIH NA NJIHOVOJ TERMINALNOJ OPREMI

Članak 5.

Povjerljivost elektroničkih komunikacijskih podataka

Elektronički komunikacijski podaci povjerljivi su. Zabranjuje se svako zadiranje u elektroničke komunikacijske podatke, kao što su slušanje, prisluškivanje, pohranjivanje, praćenje, pregledavanje ili drugi oblici presretanja, nadzora ili obrade elektroničkih komunikacijskih podataka koje provode osobe koje nisu krajnji korisnici, osim ako je to dopušteno ovom Uredbom.

Članak 6.

Dopuštena obrada elektroničkih komunikacijskih podataka

1. Pružatelji elektroničkih komunikacijskih mreža i usluga mogu obrađivati elektroničke komunikacijske podatke :

- (a) ako je to nužno za prijenos komunikacije u trajanju nužnom u tu svrhu ili
 - (b) ako je to nužno za održavanje ili ponovnu uspostavu sigurnosti elektroničkih komunikacijskih mreža i usluga ili za otkrivanje tehničkih kvarova i/ili pogrešaka u prijenosu elektroničkih komunikacija u trajanju nužnom u tu svrhu.
2. Pružatelji elektroničkih komunikacijskih usluga mogu obrađivati elektroničke komunikacijske metapodatke:
- (a) ako je to nužno za ispunjavanje obveznih zahtjeva za kvalitetu uslugu u skladu s [Direktivom o Europskom zakoniku elektroničkih komunikacija] ili Uredbom (EU) 2015/2120¹¹ u trajanju nužnom u tu svrhu ili
 - (b) ako je to nužno za naplatu, izračun plaćanja međusobnog povezivanja, otkrivanje ili zaustavljanje prijevera ili zloruporaba povezanih s uporabom elektroničkih komunikacijskih usluga ili pretplatom na njih ili
 - (c) ako je dotični krajnji korisnik dao privolu za obradu svojih komunikacijskih metapodataka u jednu posebnu svrhu ili više njih, uključujući za pružanje posebnih usluga takvim krajnjim korisnicima, pod uvjetom da se dotična svrha ili dotične svrhe ne mogu ispuniti obradom informacija koje su anonimizirane.
3. Pružatelji elektroničkih komunikacijskih usluga mogu obrađivati sadržaj elektroničkih komunikacija samo:
- (a) u svrhu pružanja posebne usluge krajnjem korisniku ako su dotični krajnji korisnik ili krajnji korisnici dali privolu za obradu sadržaja svojih elektroničkih komunikacija i ako se ta usluga ne može pružiti bez obrade takvog sadržaja ili
 - (b) ako su svi dotični krajnji korisnici dali privolu za obradu sadržaja svojih elektroničkih komunikacija u jednu ili više utvrđenih svrha koje se ne mogu ispuniti obradom informacija koje su anonimizirane i ako se pružatelj savjetovao s nadzornim tijelom. Članak 36. stavci 2. i 3. Uredbe (EU) 2016/679 primjenjuju se na savjetovanje s nadzornim tijelom.

Članak 7.

Pohrana i brisanje elektroničkih komunikacijskih podataka

1. Ne dovodeći u pitanje članak 6. stavak 1. točku (b) i članak 6. stavak 3. točke (a) i (b), pružatelj elektroničkih komunikacijskih usluga briše sadržaj elektroničkih komunikacija ili anonimizira te podatke nakon što predviđeni primatelj ili primatelji prime sadržaj elektroničkih komunikacija. Te podatke mogu bilježiti ili pohranjivati krajnji korisnici ili treća strana kojoj je povjereno njihovo bilježenje, pohrana ili drugi oblik obrade takvih podataka u skladu s Uredbom (EU) 2016/679.
2. Ne dovodeći u pitanje članak 6. stavak 1. točku (b) i članak 6. stavak 2. točke (a) i (c), pružatelj elektroničkih komunikacijskih usluga briše elektroničke komunikacijske metapodatke ili anonimizira te podatke kada oni više nisu potrebni za prijenos komunikacije.

¹¹ Uredba (EU) 2015/2120 Europskog parlamenta i Vijeća od 25. studenoga 2015. o utvrđivanju mjera u vezi s pristupom otvorenom internetu te o izmjeni Direktive 2002/22/EZ o univerzalnoj usluzi i pravima korisnika u vezi s elektroničkim komunikacijskim mrežama i uslugama i Uredbe (EU) br. 531/2012 o *roamingu* u javnim pokretnim komunikacijskim mrežama u Uniji (SL L 310, 26.11.2015., str. 1– 18.)

3. Ako se elektronički komunikacijski metapodaci obrađuju radi naplaćivanja u skladu s člankom 6. stavkom 2. točkom (b), relevantni metapodaci mogu se čuvati do kraja razdoblja u kojem se može zakonito osporiti račun ili izvršiti plaćanje u skladu s nacionalnim pravom.

Članak 8.

Zaštita informacija pohranjenih na terminalnoj opremi krajnjih korisnika i informacija povezanih s tom opremom

1. Zabranjuju se uporaba kapaciteta terminalne opreme za obradu i pohranu i prikupljanje informacija iz terminalne opreme krajnjih korisnika, uključujući informacije o njezinu softveru i hardveru, koje ne provodi dotični krajnji korisnik, osim zbog sljedećih razloga:
 - (a) to je nužno samo u svrhu provedbe prijenosa elektroničke komunikacije elektroničkom komunikacijskom mrežom ili
 - (b) krajnji korisnik dao je privolu ili
 - (c) to je nužno za pružanje usluge informacijskog društva koju je zatražio krajnji korisnik ili
 - (d) ako je to nužno za mjerenje broja posjetitelja *web*-mjestu, pod uvjetom da takvo mjerenje izvršava pružatelj usluge informacijskog društva koju je zatražio krajnji korisnik.
2. Zabranjuje se prikupljanje informacija koje emitira terminalna oprema kako bi se omogućilo njezino povezivanje s drugim uređajem i/ili s mrežnom opremom, osim:
 - (a) ako se ono provodi isključivo i u trajanju nužnom u svrhu uspostave veze ili
 - (b) ako je istaknuta jasna obavijest u kojoj se navode barem načini prikupljanja, njegova svrha, osoba odgovorna za prikupljanje i ostale informacije koje se zahtijevaju na temelju članka 13. Uredbe (EU) 2016/679 u slučaju prikupljanja osobnih podataka te sve mjere koje krajnji korisnik terminalne opreme može poduzeti kako bi zaustavio ili smanjio prikupljanje.

Prikupljanje takvih informacija uvjetovano je primjenom odgovarajućih tehničkih i organizacijskih mjera kako bi se osigurala odgovarajuća razina sigurnosti s obzirom na rizike kako je utvrđeno u članku 32. Uredbe (EU) 2016/679.
3. Informacije koje treba pružiti u skladu sa stavkom 2. točkom (b) mogu se pružiti u kombinaciji sa standardiziranim ikonama kako bi se na lako vidljiv, razumljiv i jasno čitljiv način dao smislen pregled prikupljanja.
4. Komisija je ovlaštena donijeti delegirane akte u skladu s člankom 27. kojima se određuju informacije koje se moraju prikazati standardiziranom ikonom te postupci za utvrđivanje standardiziranih ikona.

Članak 9.

Privola

1. Primjenjuju se definicija i uvjeti privole predviđeni člankom 4. stavkom 11. i člankom 7. Uredbe (EU) 2016/679.

2. Ne dovodeći u pitanje stavak 1., ako je to tehnički moguće i izvedivo, privola se za potrebe članka 8. stavka 1. točke (b) može izraziti uporabom odgovarajućih tehničkih postavki softverske aplikacije za pristup internetu.
3. Krajnji korisnici koji su dali privolu za obradu elektroničkih komunikacijskih podataka kako je utvrđeno u članku 6. stavku 2. točki (c) i članku 6. stavku 3. točkama (a) i (b) imaju mogućnost u svakom trenutku povući svoju privolu kako je utvrđeno u članku 7. stavku 3. Uredbe (EU) 2016/679 te ih se na tu mogućnost podsjeća u periodičnim intervalima od šest mjeseci tijekom cijelog trajanja obrade.

Članak 10.

Informacije i mogućnosti koje treba osigurati u vezi s postavkama privatnosti

1. Softverom za elektroničke komunikacije, uključujući pronalaženje i prikaz informacija na internetu, koji je stavljen na tržište nudi se mogućnost sprječavanja trećih strana da pohrane informacije na terminalnoj opremi krajnjeg korisnika ili obrađuju informacije koje su već pohranjene na toj opremi.
2. Nakon instalacije softver obavještuje krajnjeg korisnika o mogućnostima postavki privatnosti i za nastavak instalacije od krajnjeg korisnika zahtijeva privolu za postavke.
3. U slučaju softvera koji je na datum 25. svibnja 2018. već instaliran zahtjevi iz stavaka 1. i 2. ispunjuju se u trenutku prvog ažuriranja softvera, a najkasnije 25. kolovoza 2018.

Članak 11.

Ograničenja

1. Pravom Unije ili države članice može se zakonodavnom mjerom ograničiti opseg obveza i prava predviđenih člancima 5. do 8. ako se tim ograničenjem poštuje bit temeljnih prava i sloboda te ako je ono nužna, prikladna i proporcionalna mjera u demokratskom društvu za zaštitu jednog ili više općih javnih interesa iz članka 23. stavka 1. točaka (a) do (e) Uredbe (EU) 2016/679 ili funkcije praćenja, inspekcije ili regulatorne funkcije koja je povezana s izvršavanjem službene ovlasti za takve interese.
2. Pružatelji elektroničkih komunikacijskih usluga uspostavljaju unutarnje postupke za odgovaranje na zahtjeve za pristup elektroničkim komunikacijskim podacima krajnjih korisnika na temelju zakonodavne mjere donesene u skladu sa stavkom 1. Nadležnim nadzornim tijelima na njihov zahtjev dostavljaju informacije o tim postupcima, broju zaprimljenih zahtjeva, pozivanju na pravnu utemeljenost i svojem odgovoru.

POGLAVLJE III.

PRAVA FIZIČKIH I PRAVNIH OSOBA NA KONTROLU ELEKTRONIČKIH KOMUNIKACIJA

Članak 12.

Prikaz i ograničenje prikaza broja pozivatelja i broja pozvane linije

1. Ako se nudi prikaz broja pozivatelja i broja pozvane linije u skladu s člankom [107.] [Direktive o Europskom zakoniku elektroničkih komunikacija], pružatelji javno

dostupnih brojevno utemeljenih interpersonalnih komunikacijskih usluga osiguravaju sljedeće:

- (a) krajnjem korisniku pozivatelju mogućnost da spriječi prikaz broja pozivatelja po pozivu, po vezi ili trajno;
 - (b) krajnjem korisniku primatelju mogućnost da spriječi prikaz broja pozivatelja za dolazne pozive;
 - (c) krajnjem korisniku primatelju mogućnost da odbije dolazne pozive za koje je krajnji korisnik pozivatelj spriječio prikaz broja pozivatelja;
 - (d) krajnjem korisniku primatelju mogućnost da krajnjem korisniku pozivatelju spriječi prikaz broja pozvane linije.
2. Mogućnosti iz stavka 1. točaka (a), (b), (c) i (d) osiguravaju se krajnjim korisnicima jednostavnim sredstvima i besplatno.
 3. Stavak 1. točka (a) primjenjuje se i u pogledu poziva u treće zemlje koji potječu iz Unije. Stavak 1. točke (b), (c) i (d) primjenjuju se i na dolazne pozive koji potječu iz trećih zemalja.
 4. Ako se nudi prikaz broja pozivatelja ili broja pozvane linije, pružatelji javno dostupnih brojevno utemeljenih interpersonalnih komunikacijskih usluga pružaju javnosti informacije o mogućnostima utvrđenima u stavku 1. točkama (a), (b), (c) i (d).

Članak 13.

Izuzeca od prikaza i ograničenja prikaza broja pozivatelja i broja pozvane linije

1. Neovisno o tome je li krajnji korisnik pozivatelj spriječio prikaz broja pozivatelja, ako je poziv upućen hitnim službama, pružatelji javno dostupnih brojevno utemeljenih interpersonalnih komunikacijskih usluga poništavaju uklanjanje prikaza broja pozivatelja i uskraćivanje ili nedostatak privole krajnjeg korisnika za obradu metapodataka, za svaku liniju posebno u slučaju organizacija koje se bave hitnim komunikacijama, uključujući pristupne točke sigurnosnog poziva, radi odgovaranja na takve komunikacije.
2. Države članice uspostavljaju detaljnije odredbe o uspostavi postupaka i o okolnostima u kojima pružatelji javno dostupnih brojevno utemeljenih interpersonalnih komunikacijskih usluga privremeno poništavaju uklanjanje prikaza broja pozivatelja ako krajnji korisnici zatraže ulaženje u trag zlonamjernih ili uznemirujućim pozivima.

Članak 14.

Blokiranje dolaznih poziva

Pružatelji javno dostupnih brojevno utemeljenih interpersonalnih komunikacijskih usluga uvode najsuvremenije mjere za ograničenje neželjenih poziva koje primaju krajnji korisnici i krajnjem korisniku primatelju poziva besplatno osiguravaju sljedeće mogućnosti:

- (a) blokiranje dolaznih poziva s određenih brojeva ili iz anonimnih izvora;
- (b) zaustavljanje automatskog prosljeđivanja poziva treće strane na terminalnu opremu krajnjeg korisnika.

Članak 15.
Javno dostupni imenici

1. Pružatelji javno dostupnih imenika pribavljaju privolu krajnjih korisnika koji su fizičke osobe za uvrštavanje njihovih osobnih podataka u imenik i, posljedično, pribavljaju privolu tih krajnjih korisnika za uvrštavanje podataka prema kategoriji osobnih podataka u mjeri u kojoj su takvi podaci relevantni za svrhu imenika koju je odredio pružatelj imenika. Krajnjim korisnicima koji su fizičke osobe pružatelji osiguravaju sredstvo za provjeru, ispravak i brisanje tih podataka.
2. Pružatelji javno dostupnog imenika obavješćuju krajnje korisnike koji su fizičke osobe i čiji su osobni podaci u imeniku o dostupnim funkcijama pretraživanja imenika i pribavljaju privolu krajnjih korisnika prije no što omoguće takve funkcije pretraživanja u vezi s njihovim podacima.
3. Pružatelji javno dostupnih imenika osiguravaju krajnjim korisnicima koji su pravne osobe mogućnost da ulože prigovor na uključivanje njihovih podataka u imenik. Pružatelji osiguravaju krajnjim korisnicima koji su pravne osobe sredstvo za provjeru, ispravak i brisanje takvih podataka.
4. Mogućnost za krajnje korisnike da ne budu uključeni u javno dostupni imenik ili da provjere, isprave i izbrišu bilo koje svoje podatke osigurava se besplatno.

Članak 16.
Nezatražene komunikacije

1. Fizičke ili pravne osobe mogu se služiti elektroničkim komunikacijskim uslugama za slanje izravnih marketinških komunikacija krajnjim korisnicima koji su fizičke osobe i koji su dali svoju privolu.
2. Ako fizička ili pravna osoba u kontekstu prodaje proizvoda ili usluge od svojeg potrošača pribavi elektroničke kontaktne podatke za elektroničku poštu u skladu s Uredbom (EU) 2016/679, ta fizička ili pravna osoba može se služiti tim elektroničkim kontaktnim podacima za izravni marketing svojih sličnih proizvoda ili usluga samo ako je potrošačima jasno i izričito dana mogućnost besplatnog i jednostavnog prigovora na takvu uporabu. Pravo na prigovor daje se u trenutku prikupljanja i pri svakom slanju poruke.
3. Ne dovodeći u pitanje stavke 1. i 2., fizičke ili pravne osobe koje se služe elektroničkim komunikacijskim uslugama za upućivanja izravnih marketinških poziva:
 - (a) navode broj na koji ih se može kontaktirati ili
 - (b) navode poseban kod ili predbroj na temelju kojeg se može utvrditi da je poziv marketinške prirode.
4. Neovisno o stavku 1., države članice mogu zakonom urediti da je upućivanje izravnih marketinških govornih poziva krajnjim korisnicima koji su fizičke osobe dopušteno samo u pogledu krajnjih korisnika koji su fizičke osobe i koji nisu izrazili prigovor na primanje takvih komunikacija.
5. Države članice u okviru prava Unije i primjenjivog nacionalnog prava osiguravaju dovoljnu zaštitu legitimnog interesa krajnjih korisnika koji su pravne osobe u pogledu nezatraženih komunikacija koje se šalju sredstvima iz stavka 1.

6. Svaka fizička ili pravna osoba koja se služi elektroničkim komunikacijskim uslugama za prijenos izravnih marketinških komunikacija obavješćuje krajnje korisnike o marketinškoj prirodi komunikacije i identitetu pravne ili fizičke osobe u čije ime se komunikacija prenosi te primateljima pruža informacije potrebne kako bi ostvarili svoje pravo na jednostavno povlačenje privole za primanje daljnjih marketinških komunikacija.
7. Komisija je ovlaštena za donošenje provedbenih mjera u skladu s člankom 26. stavkom 2. za utvrđivanje koda ili predbroja za identifikaciju marketinških poziva u skladu sa stavkom 3. točkom (b).

Članak 17.

Informacije o otkrivenim sigurnosnim rizicima

U slučaju određenog rizika kojim se može ugroziti sigurnost mreža i elektroničkih komunikacijskih usluga pružatelj elektroničke komunikacijske usluge obavješćuje krajnje korisnike o takvom riziku i, ako rizik nije obuhvaćen područjem primjene mjera koje pružatelj usluga treba poduzeti, obavješćuje krajnje korisnike o svim mogućim pravnim sredstvima, uključujući naznaku mogućih povezanih troškova.

POGLAVLJE IV. NEOVISNA NADZORNA TIJELA I IZVRŠENJE

Članak 18.

Neovisna nadzorna tijela

1. Neovisno nadzorno tijelo ili tijela odgovorna za praćenje primjene Uredbe (EU) 2016/679 odgovorna su i za praćenje primjene ove Uredbe. Poglavlja VI. i VII. Uredbe (EU) 2016/679 primjenjuju se *mutatis mutandis*. Nadzorna tijela svoje zadaće i ovlasti izvršavaju u pogledu krajnjih korisnika.
2. Nadzorno tijelo ili tijela iz stavka 1., kada god je to prikladno, surađuju s nacionalnim regulatornim tijelima osnovanima u skladu s [Direktivom o Europskom zakoniku elektroničkih komunikacija].

Članak 19.

Europski odbor za zaštitu podataka

Europski odbor za zaštitu podataka, osnovan na temelju članka 68. Uredbe (EU) 2016/679, nadležan je za osiguravanje dosljedne primjene ove Uredbe. U tu svrhu Europski odbor za zaštitu podataka obavlja zadaće utvrđene u članku 70. Uredbe (EU) 2016/679. Odbor ima i sljedeće zadaće:

- (a) savjetovati Komisiju o svim predloženim izmjenama ove Uredbe;
- (b) ispitati, na vlastitu inicijativu, na zahtjev jednog od svojih članova ili na zahtjev Komisije, sva pitanja koja se odnose na primjenu ove Uredbe te izdati smjernice, preporuke i primjere najbolje prakse kako bi poticao dosljednu primjenu ove Uredbe.

Članak 20.

Postupci suradnje i konzistentnosti

Svako nadzorno tijelo doprinosi dosljednoj primjeni ove Uredbe u cijeloj Uniji. U tu svrhu nadzorna tijela surađuju međusobno i s Komisijom u skladu s poglavljem VII. Uredbe (EU) 2016/679 na pitanjima obuhvaćenima ovom Uredbom.

POGLAVLJE V. PRAVNA SREDSTVA, ODGOVORNOST I SANKCIJE

Članak 21.

Pravna sredstva

1. Ne dovodeći u pitanje druga upravna ili pravosudna sredstva, svaki krajnji korisnik elektroničkih komunikacijskih usluga ima na raspolaganju ista pravna sredstva koja su predviđena člancima 77., 78. i 79. Uredbe (EU) 2016/679.
2. Svaka fizička ili pravna osoba koja nije krajnji korisnik i na koju negativno utječu povrede ove Uredbe te koja ima legitiman interes za prestanak ili zabranu navodnih povreda, uključujući pružatelja elektroničkih komunikacijskih usluga koji štiti svoje legitimne poslovne interese, ima pravo pokrenuti pravni postupak u pogledu takvih povreda.

Članak 22.

Pravo na naknadu štete i odgovornost

Svaki krajnji korisnik elektroničkih komunikacijskih usluga koji je pretrpio materijalnu ili nematerijalnu štetu zbog povrede ove Uredbe ima pravo na naknadu od počinitelja povrede za pretrpljenu štetu, osim ako počinitelj povrede dokaže da ni na koji način nije odgovoran za događaj koji je prouzročio štetu u skladu s člankom 82. Uredbe (EU) 2016/679.

Članak 23.

Opći uvjeti za izricanje upravnih novčanih kazni

1. Za potrebe ovog članka na povrede ove Uredbe primjenjuje se poglavlje VII. Uredbe (EU) 2016/679.
2. Za povrede sljedećih odredaba ove Uredbe u skladu sa stavkom 1. izriču se upravne novčane kazne u iznosu do 10 000 000 EUR ili, u slučaju poduzetnika, do 2 % ukupnog godišnjeg prometa na svjetskoj razini za prethodnu financijsku godinu ako je taj iznos veći:
 - (a) obveze svake pravne ili fizičke osobe koja obrađuje elektroničke komunikacijske podatke u skladu s člankom 8.;
 - (b) obveze pružatelja softvera za elektroničke komunikacije u skladu s člankom 10.;
 - (c) obveze pružatelja javno dostupnih imenika u skladu s člankom 15.;
 - (d) obveze svake pravne ili fizičke osobe koja se služi elektroničkim komunikacijskim uslugama u skladu s člankom 16.
3. Za povrede načela povjerljivosti komunikacija, dopuštene obrade elektroničkih komunikacijskih podataka i rokova za brisanje u skladu s člancima 5., 6. i 7. izriču se u skladu sa stavkom 1. ovog članka upravne novčane kazne u iznosu do

20 000 000 EUR ili, u slučaju poduzetnika, do 4 % ukupnog godišnjeg prometa na svjetskoj razini za prethodnu financijsku godinu ako je taj iznos veći.

4. Države članice utvrđuju pravila o sankcijama za povrede članaka 12., 13., 14. i 17.
5. Za nepoštovanje odluke nadzornog tijela iz članka 18. izriču se upravne novčane kazne u iznosu do 20 000 000 EUR ili, u slučaju poduzetnika, do 4 % ukupnog godišnjeg prometa na svjetskoj razini za prethodnu financijsku godinu ako je taj iznos veći.
6. Ne dovodeći u pitanje korektivne ovlasti nadzornih tijela na temelju članka 18., svaka država članica može utvrditi pravila o tome mogu li se i u kojoj mjeri tijelima javne vlasti i tijelima s poslovnim nastanom u toj državi članici izreći upravne novčane kazne.
7. Na izvršavanje ovlasti nadzornog tijela na temelju ovog članka primjenjuju se odgovarajuće postupovne zaštitne mjere u skladu s pravom Unije i pravom države članice, uključujući učinkoviti pravni lijek i odgovarajući postupak.
8. Ako pravnim sustavom države članice nisu predviđene upravne novčane kazne, ovaj se članak može primjenjivati tako da novčanu kaznu pokreće nadležno nadzorno tijelo, a izriču je nadležni nacionalni sudovi, pri čemu osiguravaju da su ta pravna sredstva učinkovita i imaju jednak učinak kao i upravne novčane kazne koje izriču nadzorna tijela. U svakom slučaju novčane kazne koje se izriču moraju biti učinkovite, proporcionalne i odvraćajuće. Te države članice do [xxx] obavješćuju Komisiju o svojim zakonodavnim odredbama koje donesu u skladu s ovim stavkom te, bez odgode, o svim daljnjim izmjenama zakona ili izmjeni koje na njih utječu.

Članak 24. Sankcije

1. Države članice utvrđuju pravila o ostalim sankcijama koje se primjenjuju na povrede ove Uredbe, posebno povrede koje ne podliježu upravnim novčanim kaznama u skladu s člankom 23., te poduzimaju sve potrebne mjere kako bi se osigurala njihova provedba. Te sankcije moraju biti učinkovite, proporcionalne i odvraćajuće.
2. Svaka država članica najkasnije 18 mjeseci nakon datuma utvrđenog u članku 29. stavku 2. obavješćuju Komisiju o svojim zakonodavnim odredbama koje donese u skladu sa stavkom 1. te, bez odgode, o svim daljnjim izmjenama koje na njih utječu.

POGLAVLJE VI. DELEGIRANI AKTI I PROVEDBENI AKTI

Članak 25. Izvršavanje delegiranja ovlasti

1. Ovlast za donošenje delegiranih akata dodjeljuje se Komisiji pod uvjetima utvrđenima u ovom članku.
2. Ovlast za donošenje delegiranih akata iz članka 8. stavka 4. dodjeljuje se Komisiji na neodređeno vrijeme počevši od [datuma stupanja na snagu ove Uredbe].
3. Europski parlament ili Vijeće u svakom trenutku mogu opozvati delegiranje ovlasti iz članka 8. stavka 4. Odlukom o opozivu prekida se delegiranje ovlasti koje je u njoj navedeno. Opoziv počinje proizvoditi učinke sljedećeg dana od dana objave te

odluke u *Službenom listu Europske unije* ili na kasniji dan naveden u toj odluci. On ne utječe na valjanost delegiranih akata koji su već na snazi.

4. Prije donošenja delegiranog akta Komisija se savjetuje sa stručnjacima koje je imenovala svaka država članica u skladu s načelima utvrđenima u Međuinstitucijskom sporazumu o boljoj izradi zakonodavstva od 13. travnja 2016.
5. Čim donese delegirani akt, Komisija o tome istovremeno obavještuje Europski parlament i Vijeće.
6. Delegirani akt donesen na temelju članka 8. stavka 4. stupa na snagu samo ako Europski parlament ili Vijeće u roku od dva mjeseca od primitka obavijesti o tom aktu na njega ne ulože nikakav prigovor ili ako su prije isteka tog roka i Europski parlament i Vijeće obavijestili Komisiju da neće uložiti prigovore. Taj se rok produljuje za dva mjeseca na inicijativu Europskog parlamenta ili Vijeća.

Članak 26.

Odbor

1. Komisiji pomaže Odbor za komunikacije osnovan na temelju članka 110. [Direktive o Europskom zakoniku elektroničkih komunikacija]. Navedeni odbor smatra se odborom u smislu Uredbe (EU) br. 182/2011¹².
2. Pri upućivanju na ovaj stavak primjenjuje se članak 5. Uredbe (EU) br. 182/2011.

POGLAVLJE VII. ZAVRŠNE ODREDBE

Članak 27.

Stavljanje izvan snage

1. Direktiva 2002/58/EZ stavlja se izvan snage s učinkom od 25. svibnja 2018.
2. Upućivanja na direktivu stavljenju izvan snage smatraju se upućivanjima na ovu Uredbu.

Članak 28.

Klauzula o praćenju i evaluaciji

Komisija najkasnije do 1. siječnja 2018. uspostavlja detaljan program za praćenje učinkovitosti ove Uredbe.

Komisija najkasnije tri godine nakon datuma primjene ove Uredbe i svake tri godine nakon toga provodi evaluaciju ove Uredbe te glavne rezultate predstavlja Europskom parlamentu, Vijeću i Europskom gospodarskom i socijalnom odboru. Evaluacija prema potrebi uključuje prijedlog izmjene ili stavljanja izvan snage ove Uredbe s obzirom na pravna, tehnička ili gospodarska kretanja.

¹² Uredba (EU) br. 182/2011 Europskog parlamenta i Vijeća od 16. veljače 2011. o utvrđivanju pravila i općih načela u vezi s mehanizmima nadzora država članica nad izvršavanjem provedbenih ovlasti Komisije (SL L 55, 28.2.2011., str. 13– 18.)

Članak 29.
Stupanje na snagu i primjena

1. Ova Uredba stupa na snagu dvadesetog dana od dana objave u *Službenom listu Europske unije*.
2. Primjenjuje se od 25. svibnja 2018.

Ova je Uredba u cijelosti obvezujuća i izravno se primjenjuje u svim državama članicama.
Sastavljeno u Bruxellesu

Za Europski parlament
Predsjednik

Za Vijeće
Predsjednik