EVROPSKA
KOMISIJA

Bruselj, 10.1.2017
COM(2017) 10 final

2017/0003 (COD)

Predlog

UREDBA EVROPSKEGA PARLAMENTA IN SVETA

o spoštovanju zasebnega življenja in varstvu osebnih podatkov na področju elektronskih komunikacij ter razveljavitvi Direktive 2002/58/ES (uredba o zasebnosti in elektronskih komunikacijah)

(Besedilo velja za EGP)

{SWD(2017) 3 final}
{SWD(2017) 4 final}
{SWD(2017) 5 final}
{SWD(2017) 6 final}

OBRAZLOŽITVENI MEMORANDUM

1. OZADJE PREDLOGA

1.1 Razlogi za predlog in njegovi cilji

Cilj strategije za enotni digitalni trg[1] je povečati zaupanje v digitalne storitve in njihovo varnost. Ključni ukrep v ta namen je bila reforma okvira varstva podatkov in zlasti sprejetje Uredbe (EU) 2016/679, splošne uredbe o varstvu podatkov[2]. V strategiji za enotni digitalni trg je bil napovedan tudi pregled Direktive 2002/58/ES (v nadaljnjem besedilu: **direktiva o e-zasebnosti**)[3], da bi se zagotovili visoka raven varstva zasebnosti za uporabnike elektronskih komunikacijskih storitev in enaki pogoji za vse subjekte na trgu. Ta predlog je pregled direktive o e-zasebnosti, pri čemer predvideva cilje iz strategije za enotni digitalni trg in zagotavlja skladnost s splošno uredbo o varstvu podatkov.

Direktiva o e-zasebnosti zagotavlja varstvo temeljnih pravic in svoboščin, zlasti spoštovanje zasebnega življenja, zaupnost komunikacij in varstvo osebnih podatkov na področju elektronskih komunikacij. Zagotavlja tudi prosti pretok elektronskih komunikacijskih podatkov, opreme in storitev v Uniji. V sekundarnem pravu Unije izvaja temeljno pravico do spoštovanja zasebnega življenja v zvezi s komunikacijami v skladu s členom 7 Listine Evropske unije o temeljnih pravicah (v nadaljnjem besedilu: **Listina**).

Komisija je v skladu z zahtevami glede boljšega pravnega urejanja za direktivo o e-zasebnosti izvedla naknadni program uspešnosti in uspešnosti predpisov (v nadaljnjem besedilu: **ocena v okviru programa REFIT**). Iz zadevne ocene je razvidno, da cilji in načela sedanjega okvira še vedno veljajo. Vendar je od zadnjega pregleda direktive o e-zasebnosti leta 2009 na trgu prišlo do pomembnega tehnološkega in gospodarskega razvoja. Potrošniki in podjetja namesto tradicionalnih komunikacijskih storitev vse bolj uporabljajo nove internetne storitve, ki omogočajo medosebno komunikacijo, kot so govor po IO (VoIP), takojšnje sporočanje in spletna elektronska pošta. Za te povrhnje komunikacijske storitve se na splošno ne uporablja sedanji okvir Unije o elektronskih komunikacijah, vključno z direktivo o e-zasebnosti. Skladno s tem Direktiva ni prilagojena tehnološkemu razvoju, zaradi česar komunikacije, ki se opravljajo prek novih storitev, niso zaščitene.

1.2 Skladnost z veljavnimi predpisi s področja zadevne politike

Ta predlog je *lex specialis* glede na splošno uredbo o varstvu podatkov ter jo bo podrobno opredelil in dopolnil na področju elektronskih komunikacijskih podatkov, ki se štejejo za osebne podatke. Vse zadeve, ki se nanašajo na obdelavo osebnih podatkov in jih ta predlog ne obravnava posebej, so zajete v splošni uredbi o varstvu podatkov. Zaradi uskladitve s splošno uredbo o varstvu podatkov so bile razveljavljene nekatere določbe, kot so obveznosti glede varnosti iz člena 4 direktive o e-zasebnosti.

---

1 Sporočilo Komisije Evropskemu parlamentu, Svetu, Evropskemu ekonomsko-socialnemu odboru in Odboru regij, Strategija za enotni digitalni trg za Evropo (COM(2015) 192 final).

2 Uredba (EU) 2016/679 Evropskega parlamenta in Sveta z dne 27. aprila 2016 o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem pretoku takih podatkov ter o razveljavitvi Direktive 95/46/ES (Splošna uredba o varstvu podatkov) (UL L 119, 4.5.2016, str. 1–88).

3 Direktiva 2002/58/ES Evropskega parlamenta in Sveta z dne 12. julija 2002 o obdelavi osebnih podatkov in varstvu zasebnosti na področju elektronskih komunikacij (Direktiva o zasebnosti in elektronskih komunikacijah) (UL L 201, 31.7.2002, str. 37).

1.3 Skladnost z drugimi politikami Unije

Direktiva o e-zasebnosti je del regulativnega okvira za elektronske komunikacije. Komisija je leta 2016 sprejela predlog direktive o Evropskem zakoniku o elektronskih komunikacijah[4], ki spreminja okvir. Ta predlog ni sestavni del Evropskega zakonika o elektronskih komunikacijah, vendar se delno opira na opredelitve iz zadevnega zakonika, vključno z opredelitvijo „elektronskih komunikacijskih storitev“. Ta predlog tako kot Evropski zakonik o elektronskih komunikacijah v svoje področje uporabe vključuje ponudnike povrhnjih spletnih storitev, da odraža dejansko stanje na trgu. Poleg tega Evropski zakonik o elektronskih komunikacijah dopolnjuje ta predlog z zagotavljanjem varnosti elektronskih komunikacijskih storitev.

Direktiva o radijski opremi 2014/53/EU[5] zagotavlja enotni trg za radijsko opremo. Zlasti zahteva, da mora imeti radijska oprema, preden je dana na trg, vgrajeno zaščito za zagotavljanje varstva osebnih podatkov ter zasebnosti uporabnikov. Komisija je na podlagi direktive o radijski opremi in Uredbe (EU) št. 1025/2012[6] o evropski standardizaciji pooblaščena za sprejetje ukrepov. Ta predlog ne vpliva na direktivo o radijski opremi.

Predlog ne vključuje nobenih posebnih določb na področju hrambe podatkov. Ohranja vsebino člena 15 direktive o e-zasebnosti in jo usklajuje z besedilom člena 23 splošne uredbe o varstvu podatkov, ki državam članicam omogoča omejitev obsega pravic in obveznosti iz nekaterih členov direktive o e-zasebnosti. Države članice lahko zato ohranijo ali oblikujejo nacionalne okvire za hrambo podatkov, ki med drugim zagotavljajo usmerjene ukrepe za hrambo, če so taki okviri v skladu s pravom Unije ob upoštevanju sodne prakse Sodišča glede razlage direktive o e-zasebnosti in z Listino o temeljnih pravicah[7].

Nazadnje, predlog se ne uporablja za dejavnosti institucij, organov in agencij Unije. Vendar so njegova načela in zadevne obveznosti v zvezi s pravico do spoštovanja zasebnega življenja in komunikacij, ki se nanašajo na obdelavo elektronskih komunikacijskih podatkov, vključeni v predlog uredbe o razveljavitvi Uredbe (ES) št. 45/2001[8].

2. PRAVNA PODLAGA, SUBSIDIARNOST IN SORAZMERNOST

2.1 Pravna podlaga

Pravna podlaga predloga sta člena 16 in 114 Pogodbe o delovanju Evropske unije (v nadaljnjem besedilu: **PDEU**).

---

4 Predlog Komisije za Direktivo Evropskega parlamenta in Sveta o Evropskem zakoniku o elektronskih komunikacijah (Prenovitev) (COM/2016/0590 final – 2016/0288 (COD)).

5 Direktiva 2014/53/EU Evropskega parlamenta in Sveta z dne 16. aprila 2014 o harmonizaciji zakonodaj držav članic v zvezi z dostopnostjo radijske opreme na trgu in razveljavitvi Direktive 1999/5/ES (UL L 153, 22.5.2014, str. 62–106).

6 Uredba (EU) št. 1025/2012 Evropskega parlamenta in Sveta z dne 25. oktobra 2012 o evropski standardizaciji, spremembi direktiv 89/686/EGS in 93/15/EGS ter direktiv 94/9/ES, 94/25/ES, 95/16/ES, 97/23/ES, 98/34/ES, 2004/22/ES, 2007/23/ES, 2009/23/ES in 2009/105/ES Evropskega parlamenta in Sveta ter razveljavitvi Sklepa Sveta 87/95/EGS in Sklepa št. 1673/2006/ES Evropskega parlamenta in Sveta (UL L 316, 14.11.2012, str. 12–33).

7 Glej sodbo v združenih zadevah C-293/12 in C-594/12, Digital Rights Ireland in Seitlinger in drugi, ECLI:EU:C:2014:238 in sodbo v združenih zadevah C-203/15 in C-698/15, *Tele2 Sverige AB in Secretary of State for the Home Department*, ECLI:EU:C:2016:970.

8 Uredba (ES) št. 45/2001 Evropskega parlamenta in Sveta z dne 18. decembra 2000 o varstvu posameznikov pri obdelavi osebnih podatkov v institucijah in organih Skupnosti in o prostem pretoku takih podatkov (UL L 8, 12.1.2001, str. 1–22).

Člen 16 PDEU uvaja posebno pravno podlago za sprejetje predpisov v zvezi z varstvom posameznikov pri obdelavi osebnih podatkov v institucijah Unije in državah članicah v okviru dejavnosti s področja uporabe prava Unije ter v zvezi s prostim pretokom takih podatkov. Elektronska komunikacija posameznika se običajno šteje za osebne podatke, zato bi moralo varstvo posameznikov glede zasebnosti komunikacij in pri obdelavi takih podatkov temeljiti na členu 16.

Poleg tega je namen predloga zaščititi komunikacijo in povezane zakonite interese pravnih oseb. Pomen in obseg pravic na podlagi člena 7 Listine sta v skladu s členom 52(3) Listine enaka tistima iz člena 8(1) Evropske konvencije o varstvu človekovih pravic in temeljnih svoboščin (v nadaljnjem besedilu: **EKČP**). Kar zadeva področje uporabe člena 7 Listine, sodna praksa Sodišča Evropske unije (v nadaljnjem besedilu: **Sodišče**)[9] in EKČP[10] potrjujeta, da poklicnih dejavnosti pravnih oseb ni mogoče izključiti iz varstva pravice, ki jo zagotavljata člen 7 Listine in člen 8 EKČP.

Ker ima pobuda dvojni namen ter ker vidika, ki se nanaša na varstvo komunikacij pravnih oseb, in cilja, da se vzpostavi notranji trg za navedene elektronske komunikacije in zagotovi njegovo delovanje v zvezi s tem ni mogoče šteti za postranska, bi morala pobuda temeljiti tudi na členu 114 PDEU.

2.2 Subsidiarnost

Spoštovanje komunikacij je temeljna pravica, priznana z Listino. Vsebina elektronskih komunikacij lahko razkrije zelo občutljive informacije o končnih uporabnikih, ki sodelujejo v komunikaciji. Podobno lahko metapodatki iz elektronske komunikacije razkrijejo zelo občutljive in osebne podatke, kot je izrecno priznalo Sodišče[11]. Večina držav članic potrebo po zaščiti komunikacij priznava tudi kot posebno ustavno pravico. Države članice lahko sprejmejo politike, ki zagotavljajo, da se ta pravica ne krši, vendar tega brez predpisov Unije ne bi bilo mogoče enotno doseči in ustvarile bi se omejitve čezmejnih prenosov osebnih in neosebnih podatkov, ki so povezani z uporabo elektronskih komunikacijskih storitev. Da bi se ohranila skladnost s splošno uredbo o varstvu podatkov, je treba pregledati direktivo o e-zasebnosti in sprejeti ukrepe za uskladitev teh dveh instrumentov.

Zaradi tehnološkega razvoja in ambicij strategije za enotni digitalni trg se je povečala potreba po ukrepanju na ravni Unije. Uspešnost strategije EU za enotni digitalni trg je odvisna od tega, kako uspešno bo EU odpravila nacionalne omejitve in ovire ter izkoristila prednosti in ekonomije evropskega enotnega digitalnega trga. Poleg tega, ker internet in digitalne tehnologije ne poznajo meja, težava presega meje ozemlja posamezne države članice. Države članice same ne morejo učinkovito rešiti težav na tem področju. Da bi enotni digitalni trg deloval pravilno, so potrebni enaki pogoji za vse gospodarske subjekte, ki opravljajo nadomestljive storitve, in enakovredno varstvo končnih uporabnikov na ravni Unije.

2.3 Sorazmernost

Da se zagotovi učinkovito pravno varstvo spoštovanja zasebnosti in komunikacij, je treba razširiti področje uporabe, da bo zajemalo ponudnike povrhnjih spletnih storitev. Več priljubljenih ponudnikov povrhnjih spletnih storitev že spoštuje ali delno spoštuje načelo

---

9 Glej sodbo v zadevi C-450/06, Varec SA, ECLI:EU:C:2008:91, točka 48.

10 Glej med drugim sodbe ESČP v zadevi *Niemietz proti Nemčiji* z dne 16. decembra 1992, serija A št. 251-B, točka 29; *Société Colas Est in drugi proti Franciji*, št. 37971/97, točka 41, ESČP 2002-III; *Peck proti Združenemu kraljestvu*, št. 44647/98, ESČP 2003-I, točka 57 ter z dne 2. aprila 2015 v zadevi *Vinci Construction in GTM Génie Civil in Services proti Franciji*, št. 63629/10 in št. 60567/10, točka 63.

11 Glej opombo 7.

zaupnosti komunikacij, vendar industriji ni mogoče prepustiti samourejanja varstva temeljnih pravic. Prav tako je vse večji pomen učinkovitega varstva zasebnosti terminalske opreme, saj je ta v zasebnem in poklicnem življenju postala nepogrešljiva za shranjevanje občutljivih informacij. Vloga končnih uporabnikov se z izvajanjem direktive o e-zasebnosti ni dejansko povečala. Zato je za doseganje cilja treba izvajati načelo s centralizacijo privolitve v programski opremi in s spodbujanjem uporabnikov z informacijami o nastavitvah zasebnosti pri tej opremi. Kar zadeva izvrševanje te uredbe, je to odvisno od nadzornih organov in mehanizma za skladnost splošne uredbe o varstvu podatkov. Poleg tega predlog državam članicam omogoča, da za posebne zakonite namene sprejmejo nacionalne ukrepe odstopanja. Predlog zato ne presega tistega, kar je potrebno za doseganje zadevnih ciljev in je v skladu z načelom sorazmernosti iz člena 5 Pogodbe o Evropski uniji. Obveznosti, ki veljajo za zadevne storitve, se ohranjajo na čim manjši ravni in hkrati ne vplivajo na zadevne temeljne pravice.

2.4 Izbira instrumenta

Komisija je pripravila predlog uredbe, da bi zagotovila skladnost s splošno uredbo o varstvu podatkov ter pravno varnost za uporabnike in podjetja z izogibanjem različnim razlagam v državah članicah. Uredba lahko zagotovi enakovredno raven varstva za uporabnike v vsej Uniji in nižje stroške izpolnjevanja obveznosti za podjetja, ki poslujejo čezmejno.

3. REZULTATI NAKNADNIH OCEN, POSVETOVANJ Z ZAINTERESIRANIMI STRANMI IN OCEN UČINKA

3.1 Naknadne ocene/preverjanja ustreznosti obstoječe zakonodaje

Z oceno v okviru programa REFIT se je proučilo, kako učinkovito je direktiva o e-zasebnosti prispevala k zadostnemu varstvu spoštovanja zasebnega življenja in zaupnosti komunikacij v EU. Prizadevalo se je tudi ugotoviti morebitne odvečne dele.

S to oceno se je ugotovilo, da so navedeni cilji Direktive še vedno **relevantni**. Splošna uredba o varstvu podatkov zagotavlja varstvo osebnih podatkov, direktiva o e-zasebnosti pa zagotavlja zaupnost komunikacij, ki lahko vključujejo tudi neosebne podatke in podatke o pravni osebi. Zato bi moral ločeni instrument zagotoviti učinkovito varstvo člena 7 Listine. Tudi za druge določbe, kot so predpisi o pošiljanju nepovabljenih sporočil za namene trženja, se je izkazalo, da so še vedno relevantne.

Kar zadeva **uspešnost in učinkovitost**, se je z oceno v okviru programa REFIT ugotovilo, da Direktiva ni v celoti izpolnila svojih ciljev. Zaradi nekaterih nejasno oblikovanih določb in dvoumnih pravnih terminov je ogroženo usklajevanje, kar ustvarja izzive za podjetja pri čezmejnem poslovanju. Nadalje se je v okviru ocene izkazalo, da so nekatere določbe po nepotrebnem obremenile podjetja in potrošnike. Pravilo privolitve zaradi zaščite zaupnosti terminalske opreme na primer ni izpolnilo svojih ciljev in končni uporabniki se morajo odzivati na zahteve glede sprejetja trajnih piškotkov, ne da bi jih razumeli, v nekaterih primerih pa se piškotki namestijo kar brez njihove privolitve. Pravilo privolitve je preveč vključujoče, saj zajema tudi vsiljive prakse, ki ne posegajo v zasebnost, in premalo vključujoče, saj ne zajema jasno nekaterih načinov sledenja (npr. sledenje spletnim uporabnikom z zajemom prstnega odtisa naprave), pri katerih se morda do naprave ne dostopa ali v njej shranjuje. Nazadnje, njegovo izvajanje lahko za podjetja pomeni strošek.

V okviru ocene se je ugotovilo, da imajo predpisi glede e-zasebnosti še vedno **dodano vrednost EU** za lažje doseganje cilja zagotavljati spletno zasebnost ob vse bolj nadnacionalnem trgu elektronskih komunikacij. Dokazalo se je tudi, da so na splošno predpisi

skladni z drugo zadevno zakonodajo, čeprav so bili glede na novo splošno uredbo o varstvu podatkov ugotovljeni nekateri odvečni deli (glej oddelek 1.2).

3.2 Posvetovanja z zainteresiranimi stranmi

Komisija je med 12. aprilom in 5. julijem 2016 organizirala javno posvetovanje ter prejela 421 odgovorov[12]. Ključne ugotovitve so[13]:

– **Potreba po posebnih predpisih o zaupnosti elektronskih komunikacij za področje elektronskih komunikacij**: Strinja se 83,4 % sodelujočih državljanov, potrošniških organizacij in organizacij civilne družbe ter 88,9 % javnih organov, ne strinja pa 63,4 % sodelujočih iz industrije.

– **Razširitev področja uporabe na nove komunikacijske storitve (povrhnje spletne storitve)**: Strinja se 76 % državljanov in civilne družbe ter 93,1 % javnih organov, tako razširitev pa podpira le 36,2 % sodelujočih iz industrije.

– **Sprememba izjem glede privolitve za obdelavo podatkov o prometu in lokaciji**: 49,1 % državljanov, organizacij civilne družbe in potrošniških organizacij ter 36 % javnih organov si ne želi razširitve izjem, medtem ko se 36 % industrije strinja z razširitvijo izjem, dve tretjini industrije pa se zavzemata le za razveljavitev zadevnih določb.

– **Podpora rešitvam, predlaganim v zvezi s vprašanjem privolitve za uporabo piškotkov**: 81,2 % državljanov in 63 % javnih organov podpira uvedbo obveznosti za proizvajalce terminalske opreme, da tržijo proizvode z aktiviranimi nastavitvami privzete zasebnosti, 58,3 % industrije pa je naklonjenih možnosti podpore samourejanja ali sourejanja.

Poleg tega je Komisija aprila 2016 organizirala dve delavnici, ena je bila odprta za vse zainteresirane strani, druga pa za nacionalne pristojne organe, na katerih so se obravnavala glavna vprašanja javnega posvetovanja. Mnenja, podana na delavnicah, so izražala rezultat javnega posvetovanja.

Da bi se pridobila mnenja državljanov, se je v vsej EU izvedla raziskava Eurobarometra o e-zasebnosti[14]. Ključne ugotovitve so[15]:

– Po mnenju 78 % sodelujočih je zelo pomembno, da je dostop do osebnih podatkov na njihovih računalnikih, pametnem telefonu ali tablici mogoč le z njihovim dovoljenjem.

– Po mnenju 72 % je zelo pomembno, da je zagotovljena zaupnost njihove elektronske pošte in takojšnjega sporočanja na spletu.

– 89 % se jih strinja s predlagano možnostjo, da bi se morala s privzetimi nastavitvami njihovega brskalnika preprečiti izmenjava informacij.

---

[12] 162 prispevkov državljanov, 33 iz organizacij civilne družbe in potrošniških organizacij, 186 iz industrije in 40 iz javnih organov, vključno s pristojnimi organi, ki izvršujejo direktivo o e-zasebnosti.

[13] Celotno poročilo je na voljo na naslednji spletni strani: https://ec.europa.eu/digital-single-market/news-redirect/37204.

[14] Raziskava Eurobarometra (EB) 443 o e-zasebnosti iz leta 2016 (SMART 2016/079).

[15] Celotno poročilo je na voljo na naslednji spletni strani: https://ec.europa.eu/digital-single-market/news-redirect/37205.

3.3 Zbiranje in uporaba strokovnih mnenj

Komisija je upoštevala naslednje nasvete zunanjih strokovnjakov:

– Usmerjena posvetovanja strokovnih skupin EU: Mnenje delovne skupine iz člena 29, mnenje Evropskega nadzornika za varstvo podatkov, mnenje skupine deležnikov platforme REFIT, mnenja Organa evropskih regulatorjev za elektronske komunikacije (BEREC), mnenja Agencije Evropske unije za varnost omrežij in informacij (ENISA) in mnenja članov mreže za sodelovanje na področju varstva potrošnikov.

– Zunanje strokovno znanje, zlasti naslednji študiji:

  – Študija „ePrivacy Directive: assessment of transposition, effectiveness and compatibility with proposed Data Protection Regulation“ (Direktiva o e-zasebnosti: ocena prenosa, učinkovitosti in skladnosti s predlagano uredbo o varstvu podatkov) (SMART 2013/007116).

  – Študija „Evaluation and review of Directive 2002/58 on privacy and the electronic communication sector“ (Ocena in pregled Direktive 2002/58 o zasebnosti in področju elektronskih komunikacij) (SMART 2016/0080).

3.4 Ocena učinka

Za ta predlog, glede katerega je Odbor za regulativni nadzor 28. septembra 2016 izdal pozitivno mnenje[16], se je izvedla ocena učinka. Da bi se upoštevala priporočila Odbora, so v oceni učinka bolje pojasnjeni področje uporabe pobude, njena skladnost z drugimi pravnimi instrumenti (s splošno uredbo o varstvu podatkov, Evropskim zakonikom o elektronskih komunikacijah in direktivo o radijski opremi) ter potreba po ločenem instrumentu. Osnovni scenarij je bolje razvit in pojasnjen. Analiza učinkov je okrepljena in bolj uravnotežena ter pojasnjuje in bolje opiše pričakovane stroške in koristi.

Glede na merila učinkovitosti, uspešnosti in skladnosti so se proučile naslednje možnosti politike:

– **možnost 1:** nezakonodajni ukrepi („mehkega prava“);

– **možnost 2:** manjša krepitev zasebnosti/zaupnosti in poenostavitev;

– **možnost 3:** zmerna krepitev zasebnosti/zaupnosti in poenostavitev;

– **možnost 4:** obsežna krepitev zasebnosti/zaupnosti in poenostavitev;

– **možnost 5:** razveljavitev direktive o e-zasebnosti.

Možnost 3 je bila ob upoštevanju njene učinkovitosti in skladnosti z večine vidikov izpostavljena kot **najprimernejša možnost** za doseganje zadevnih ciljev. Glavne koristi so:

– okrepljeno varstvo zaupnosti elektronskih komunikacij z razširitvijo področja uporabe pravnega instrumenta, da se tako vključijo nove elektronske komunikacijske storitve z enakovrednim delovanjem. Poleg tega Uredba končnemu uporabniku zagotavlja večji nadzor s pojasnilom, da se lahko privolitev izrazi prek ustreznih tehničnih nastavitev;

[16] http://ec.europa.eu/transparency/regdoc/?fuseaction=ia.

– večja zaščita pred nepovabljenimi sporočili z uvedbo obveznosti glede prikaza identifikacije klicne linije ali obvezne predpone pri klicih za namene trženja ter večje možnosti za onemogočanje klicev z neželenih številk;

– poenostavitev in pojasnitev regulativnega okolja z zmanjšanjem manevrskega prostora držav članic in razveljavitvijo zastarelih določb ter razširitev izjem od pravil privolitve.

Gospodarski učinek možnosti 3 naj bi bil na splošno sorazmeren s cilji predloga. Poslovne priložnosti, povezane z obdelavo elektronskih komunikacijskih podatkov, so odprte za tradicionalne elektronske komunikacijske storitve, za ponudnike povrhnjih spletnih storitev pa veljajo ista pravila. Ti gospodarski subjekti bodo imeli zato nekaj dodatnih stroškov zaradi izpolnjevanja obveznosti. Vendar ta sprememba ne bo bistveno vplivala na tiste ponudnike povrhnjih spletnih storitev, ki že poslujejo na podlagi privolitve. Nazadnje, učinek možnosti se ne bi zaznal v državah članicah, ki so te predpise že razširile na ponudnike povrhnjih spletnih storitev.

S centralizacijo privolitve v programski opremi, kot so internetni brskalniki, spodbujanjem uporabnikov, da izberejo svoje nastavitve zasebnosti, in razširitvijo izjem od pravila privolitve za uporabo piškotkov bi lahko precejšen del podjetij odstranil pasice in obvestila o piškotkih, kar bi lahko prineslo precejšen prihranek pri stroških in poenostavitev. Vendar bodo spletno usmerjeni oglaševalci morda težje pridobili privolitev, če se velik del uporabnikov odloči za nastavitev „zavrni piškotke tretjih oseb“. Hkrati operaterji spletnih strani zaradi centralizacije privolitve ne bodo prikrajšani za možnost, da pridobijo privolitev s posameznimi zahtevami, naslovljenimi na končne uporabnike, in tako ohranijo svoj sedanji poslovni model. Nekateri ponudniki brskalnikov ali podobne programske opreme bi imeli dodatne stroške, saj bi morali zagotoviti nastavitve, ki spoštujejo zasebnost.

V zunanji študiji so bili opredeljeni trije ločeni scenariji izvajanja možnosti 3 glede na subjekt, ki bo vzpostavil pogovorno okno med uporabnikom, ki je izbral nastavitev „zavrni piškotke tretjih oseb“ ali „ne sledi“, in obiskanimi spletnimi stranmi, ki uporabnika interneta spodbujajo, naj ponovno premisli o svoji odločitvi. Subjekti, ki bi lahko bili odgovorni za to tehnično nalogo, so: 1) programska oprema, kot so internetni brskalniki; 2) sledilnik tretje osebe; 3) posamezne spletne strani (tj. storitev informacijske družbe, ki jo zahteva uporabnik). Možnost 3 bi v primerjavi z osnovnim scenarijem prinesla skupne prihranke pri stroških zaradi izpolnjevanja obveznosti v višini 70 % (948,8 milijona EUR prihranka) v prvem scenariju (rešitev z brskalnikom). V drugih scenarijih bi bili prihranki pri stroških manjši. Ker skupni prihranki večinoma izhajajo iz izrazitega zmanjšanja števila podjetij, na katera bi to vplivalo, bi bil posamezni znesek stroškov zaradi izpolnjevanja obveznosti, ki naj bi jih imelo eno podjetje, v povprečju višji kot danes.

3.5 Ustreznost in poenostavitev ureditve

Ukrepi politike, predlagani v okviru najprimernejše možnosti, obravnavajo cilj poenostavitve in zmanjšanja upravnega bremena v skladu z ugotovitvami ocene v okviru programa REFIT in mnenjem skupine deležnikov platforme REFIT[17].

Skupina deležnikov platforme REFIT je Komisiji izdala tri sklope priporočil:

– varstvo zasebnega življenja državljana bi bilo treba okrepiti z uskladitvijo direktive o e-zasebnosti in splošne uredbe o varstvu podatkov;

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

– učinkovitost varstva državljanov pred nedovoljenim trženjem bi bilo treba okrepiti z dodajanjem izjem od pravila „privolitve“ za uporabo piškotkov;

– Komisija obravnava nacionalne težave pri izvajanju in spodbuja izmenjavo dobre prakse med državami članicami.

Predlog natančneje vsebuje:

– uporabo tehnološko nevtralnih opredelitev pojmov, da se vključijo nove storitve in tehnologije ter zagotovi, da bo Uredba ustrezna tudi v prihodnosti;

– razveljavitev varnostnih pravil za odpravo regulativnega podvajanja;

– pojasnjeno področje uporabe, kar bo pripomoglo k odpravi/zmanjšanju tveganja za različno izvajanje v državah članicah (točka 3 mnenja);

– pojasnjeno in poenostavljeno pravilo privolitve za uporabo piškotkov in drugih identifikatorjev, kot je pojasnjeno v oddelkih 3.1 in 3.4 (točka 2 mnenja);

– uskladitev nadzornih organov z organi, pristojnimi za izvrševanje splošne uredbe o varstvu podatkov in opiranje na mehanizem za skladnost splošne uredbe o varstvu podatkov.

3.6 Vpliv na temeljne pravice

Predlog naj bi povečal učinkovitost in raven varstva zasebnosti in osebnih podatkov, ki se obdelajo v zvezi z elektronskimi komunikacijami v skladu s členoma 7 in 8 Listine ter zagotovil večjo pravno varnost. Predlog dopolnjuje in podrobno opredeljuje splošno uredbo o varstvu podatkov. Učinkovito varstvo zaupnosti komunikacij je bistveno za izvajanje svobode izražanja in obveščanja ter drugih povezanih pravic, kot je pravica do varstva osebnih podatkov ali svobode misli, vesti in vere.

4. PRORAČUNSKE POSLEDICE

Predlog ne vpliva na proračun Unije.

5. DRUGI ELEMENTI

5.1 Načrti za izvedbo ter ureditev spremljanja, ocenjevanja in poročanja

Komisija bo spremljala uporabo Uredbe in Evropskemu parlamentu in Svetu ter Evropskemu ekonomsko-socialnemu odboru vsaka tri leta predložila poročilo o oceni te uredbe. Ta poročila bodo javna, v njih pa bosta podrobno pojasnjena učinkovita uporaba in izvrševanje te uredbe.

5.2 Natančnejša pojasnitev posameznih določb predloga

Poglavje I vsebuje splošne določbe: predmet urejanja (člen 1), področje uporabe (člena 2 in 3) in opredelitve pojmov, ki se uporabljajo v tej uredbi, vključno z navedbami zadevnih opredelitev iz drugih instrumentov EU, kot je splošna uredba o varstvu podatkov.

Poglavje II vsebuje ključne določbe, ki zagotavljajo zaupnost elektronskih komunikacij (člen 5), ter omejene dovoljene namene in pogoje obdelave podatkov v zvezi s takimi komunikacijami (člena 6 in 7). Obravnava tudi zaščito terminalske opreme z (i) zagotavljanjem celovitosti informacij, shranjenih na njej, in (ii) zaščito informacij, ki jih oddaja terminalska oprema, saj lahko omogočijo identifikacijo njenega končnega uporabnika (člen 8). Nazadnje, člen 9 podrobno pojasni privolitev končnih uporabnikov, ki je osrednja zakonska podlaga te uredbe, pri čemer izrecno navaja opredelitve in pogoje, kakor so določeni

v splošni uredbi o varstvu podatkov, člen 10 pa ponudnikom programske opreme, ki omogoča elektronsko komunikacijo, nalaga obveznost pomoči končnim uporabnikom pri sprejetju učinkovitih odločitev glede nastavitev zasebnosti. Člen 11 podrobno pojasni namene in pogoje, na podlagi katerih države članice omejijo navedene določbe.

Poglavje III obravnava pravice končnih uporabnikov glede nadzora pošiljanja in sprejemanja elektronskih komunikacij, da zaščitijo svojo zasebnost: (i) pravica končnih uporabnikov, da preprečijo prikaz identifikacije klicne linije in zagotovijo anonimnost (člen 12), z njenimi omejitvami (člen 13), ter (ii) obveznost ponudnikov javno razpoložljive medosebne komunikacije na podlagi številke, da se zagotovi možnost omejitve prejema neželenih klicev (člen 14). To poglavje ureja tudi pogoje, pod katerimi se lahko končni uporabniki vključijo v javno dostopne direktorije (člen 15), in pogoje, pod katerimi se lahko pošiljajo nepovabljena sporočila za namene neposrednega trženja (člen 17). Obravnava tudi varnostna tveganja in ponudnikom elektronskih komunikacijskih storitev nalaga obveznost, da končne uporabnike obvestijo v primeru posebnega tveganja, ki lahko ogrozi varnost omrežij in storitev. Obveznosti glede varnosti iz splošne uredbe o varstvu podatkov in Evropskega zakonika o elektronskih komunikacijah se bodo uporabljale za ponudnike elektronskih komunikacijskih storitev.

Poglavje IV določa nadzor in izvrševanje te uredbe, ki ju zaupa nadzornim organom, pristojnim za splošno uredbo o varstvu podatkov, ob upoštevanju močnih sinergij med vprašanji v zvezi s splošnim varstvom podatkov in zaupnostjo komunikacij (člen 18). Razširjena so pooblastila Evropskega odbora za varstvo podatkov (člen 19), mehanizem sodelovanja in skladnosti, predviden na podlagi splošne uredbe o varstvu podatkov, pa se bo uporabljal pri čezmejnih zadevah v zvezi s to uredbo (člen 20).

Poglavje V podrobno pojasnjuje različna pravna sredstva, ki so na voljo končnim uporabnikom (člena 21 in 22), in sankcije, ki se lahko uvedejo (člen 24), vključno s splošnimi pogoji za naložitev upravnih glob (člen 23).

Poglavje VI se nanaša na sprejetje delegiranih in izvedbenih aktov v skladu s členoma 290 in 291 Pogodbe.

Nazadnje, poglavje VII vsebuje končne določbe te uredbe: razveljavitev direktive o e-zasebnosti, spremljanje in pregled, začetek veljavnosti in uporabo. Kar zadeva pregled, namerava Komisija med drugim oceniti, ali je ločen pravni akt še vedno potreben ob upoštevanju pravnega, tehničnega ali gospodarskega razvoja in prve ocene Uredbe (EU) 2016/679, ki se bo izvedla do 25. maja 2020.

2017/0003 (COD)

Predlog

UREDBA EVROPSKEGA PARLAMENTA IN SVETA

o spoštovanju zasebnega življenja in varstvu osebnih podatkov na področju elektronskih komunikacij ter razveljavitvi Direktive 2002/58/ES (uredba o zasebnosti in elektronskih komunikacijah)

(Besedilo velja za EGP)

EVROPSKI PARLAMENT IN SVET EVROPSKE UNIJE STA –

ob upoštevanju Pogodbe o delovanju Evropske unije, zlasti člena 16 in člena 114 Pogodbe,

ob upoštevanju predloga Evropske komisije,

po posredovanju osnutka zakonodajnega akta nacionalnim parlamentom,

ob upoštevanju mnenja Evropskega ekonomsko-socialnega odbora[1],

ob upoštevanju mnenja Odbora regij[2],

ob upoštevanju mnenja Evropskega nadzornika za varstvo podatkov[3],

v skladu z rednim zakonodajnim postopkom,

ob upoštevanju naslednjega:

(1) Člen 7 Listine Evropske unije o temeljnih pravicah (v nadaljnjem besedilu: Listina) ščiti temeljno pravico vsakogar do spoštovanja svojega zasebnega in družinskega življenja, stanovanja ter komunikacij. Spoštovanje zasebnosti komunikacij je bistvena razsežnost te pravice. Zaupnost elektronskih komunikacij zagotavlja, da se informacije, ki se izmenjajo med udeleženci, in zunanji elementi take komunikacije, vključno s podatki o tem, kdaj so bile informacije poslane, od kod in komu, ne razkrijejo nikomur razen tistim, ki sodelujejo v komunikaciji. Načelo zaupnosti bi se moralo uporabljati za sedanja in prihodnja komunikacijska sredstva, vključno s klici, dostopom do interneta, aplikacijami za takojšnje sporočanje, elektronsko pošto, internetno telefonijo in osebnim sporočanjem prek družbenih medijev.

(2) Vsebina elektronskih komunikacij lahko razkrije zelo občutljive informacije o posameznikih, ki sodelujejo v komunikaciji, in sicer od osebnih izkušenj in čustev do zdravstvenega stanja, spolne usmerjenosti in političnih stališč, njihovo razkritje pa bi lahko povzročilo osebno in družbeno škodo, gospodarsko izgubo ali zadrego. Podobno lahko tudi metapodatki iz elektronske komunikacije razkrijejo zelo občutljive in osebne podatke. Ti metapodatki vključujejo klicane številke, obiskana spletišča, geografsko lokacijo, čas, datum in trajanje klica posameznika itd., kar omogoča natančne ugotovitve glede zasebnih življenj oseb, ki sodelujejo v elektronski

[1] UL C , , str. .
[2] UL C , , str. .
[3] UL C , , str. .

komunikaciji, kot so njihovi socialni odnosi, njihove vsakodnevne navade in dejavnosti, njihovi interesi, okusi itd.

(3) Elektronski komunikacijski podatki lahko razkrijejo tudi informacije o pravnih osebah, kot so poslovne skrivnosti ali druge občutljive informacije z gospodarsko vrednostjo. Zato bi se morale določbe te uredbe uporabljati za fizične in pravne osebe. Poleg tega bi morala ta uredba zagotoviti, da se določbe Uredbe (EU) 2016/679 Evropskega parlamenta in Sveta[4] uporabljajo tudi za končne uporabnike, ki so pravne osebe. To vključuje opredelitev pojma „privolitev“ na podlagi Uredbe (EU) 2016/679. Pri sklicevanju na privolitev končnega uporabnika, vključno s pravnimi osebami, bi se morala uporabljati ta opredelitev. Poleg tega bi morale imeti pravne osebe, kar zadeva nadzorne organe, enake pravice kot končni uporabniki, ki so fizične osebe, nadzorni organi pa bi morali biti na podlagi te uredbe odgovorni tudi za spremljanje njene uporabe, kar zadeva pravne osebe.

(4) V skladu s členom 8(1) Listine in členom 16(1) Pogodbe o delovanju Evropske unije ima vsakdo pravico do varstva osebnih podatkov, ki se nanašajo nanj. Uredba (EU) 2016/679 določa pravila o varstvu posameznikov pri obdelavi osebnih podatkov in pravila o prostem pretoku osebnih podatkov. Elektronski komunikacijski podatki lahko vključujejo osebne podatke, kot so opredeljeni v Uredbi (EU) 2016/679.

(5) Določbe te uredbe podrobno opredeljujejo in dopolnjujejo splošne predpise o varstvu osebnih podatkov iz Uredbe (EU) 2016/679, kar zadeva elektronske komunikacijske podatke, ki se štejejo za osebne podatke. Ta uredba torej ne zmanjšuje ravni varstva, ki jo na podlagi Uredbe (EU) 2016/679 uživajo posamezniki. Ponudnikom elektronskih komunikacijskih storitev bi morala biti obdelava elektronskih komunikacijskih podatkov dovoljena le v skladu s to uredbo.

(6) Načela in glavne določbe Direktive 2002/58/ES Evropskega parlamenta in Sveta[5] so na splošno trdne, vendar navedena direktiva ni popolnoma dohajala razvoja tehnološke in tržne resničnosti, zaradi česar zaščita zasebnosti in zaupnosti v zvezi z elektronskimi komunikacijami ni bila dosledna ali dovolj učinkovita. Te spremembe vključujejo vstop na trg elektronskih komunikacijskih storitev, ki z vidika potrošnika nadomestijo tradicionalne storitve, ni pa jim treba upoštevati istega sklopa predpisov. Druga sprememba se nanaša na nove tehnike, ki omogočajo sledenje spletnemu vedenju končnih uporabnikov in niso zajete v Direktivi 2002/58/ES. Direktivo 2002/58/ES bi zato bilo treba razveljaviti in jo nadomestiti s to uredbo.

(7) Države članice bi morale imeti možnost, da v okviru omejitev te uredbe ohranijo ali uvedejo nacionalne določbe, s katerimi nadalje podrobno opredelijo in pojasnijo uporabo predpisov iz te uredbe, da zagotovijo njihovo učinkovito uporabo in razlago. Zato bi moralo polje proste presoje, ki ga imajo države članice v zvezi s tem, ohraniti ravnovesje med varstvom osebnega življenja in osebnih podatkov ter prostim pretokom elektronskih komunikacijskih podatkov.

(8) Ta uredba bi se morala uporabljati za ponudnike elektronskih komunikacijskih storitev, ponudnike javno dostopnih direktorijev in ponudnike programske opreme, ki

---

[4] Uredba (EU) 2016/679 Evropskega parlamenta in Sveta z dne 27. aprila 2016 o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem pretoku takih podatkov ter o razveljavitvi Direktive 95/46/ES (Splošna uredba o varstvu podatkov) (UL L 119, 4.5.2016, str. 1–88).

[5] Direktiva 2002/58/ES Evropskega parlamenta in Sveta z dne 12. julija 2002 o obdelavi osebnih podatkov in varstvu zasebnosti na področju elektronskih komunikacij (Direktiva o zasebnosti in elektronskih komunikacijah) (UL L 201, 31.7.2002, str. 37).

omogoča elektronsko komunikacijo, vključno s pridobivanjem in navedbo informacij na internetu. Ta uredba bi se morala uporabljati tudi za fizične in pravne osebe, ki elektronske komunikacijske storitve uporabljajo za pošiljanje komercialnih sporočil za namene neposrednega trženja ali zbiranje informacij v zvezi s terminalsko opremo končnih uporabnikov oziroma informacij, ki so na njej shranjene.

(9) Ta uredba bi se morala uporabljati za elektronske komunikacijske podatke, ki se obdelajo v okviru zagotavljanja in uporabe elektronskih komunikacijskih storitev v Uniji, ne glede na to, ali obdelava poteka v Uniji ali zunaj nje. Poleg tega bi se morala ta uredba uporabljati tudi za elektronske komunikacijske podatke, ki se obdelajo v okviru zagotavljanja elektronskih komunikacijskih storitev iz držav zunaj Unije končnim uporabnikom v Uniji, s čimer bi se zagotovilo, da končni uporabniki ne bi bili prikrajšani za učinkovito varstvo.

(10) Radijska oprema in njena programska oprema, ki se da na notranji trg v Uniji, mora biti v skladu z Direktivo 2014/53/EU Evropskega parlamenta in Sveta[6]. Ta uredba ne bi smela vplivati na veljavnost katere koli zahteve iz Direktive 2014/53/EU ali na pooblastilo Komisije, da sprejme delegirane akte v skladu z Direktivo 2014/53/EU, s katerimi zahteva, da imajo posebne kategorije ali razredi radijske opreme vgrajeno zaščito za zagotavljanje varstva osebnih podatkov ter zasebnosti končnih uporabnikov.

(11) Storitve, ki se uporabljajo za komunikacijo, in tehnična sredstva za njihovo opravljanje so se precej razvili. Končni uporabniki tradicionalne storitve prenosa govorne telefonije, kratkih sporočil (SMS) in elektronske pošte vse bolj nadomeščajo s funkcionalno enakovrednimi spletnimi storitvami, kot so govor po IP (VoIP), neposredno sporočanje in spletna elektronska pošta. Da se zagotovi učinkovito in enakovredno varstvo končnih uporabnikov pri uporabi funkcionalno enakovrednih storitev, ta uredba uporablja opredelitev elektronskih komunikacijskih storitev iz [Direktive Evropskega parlamenta in Sveta o Evropskem zakoniku o elektronskih komunikacijah[7]]. Ta opredelitev ne zajema le storitev dostopa do interneta in storitev, ki v celoti ali delno obsegajo prenos signalov, ampak tudi medosebne komunikacijske storitve, ki so lahko na podlagi številke ali ne, kot so na primer govor po IP (VoIP), takojšnje sporočanje in spletna elektronska pošta. Varstvo zaupnosti komunikacij je bistveno tudi, kar zadeva medosebne komunikacijske storitve, ki so pomožne ob drugi storitvi; zato bi morale biti take vrste storitev, ki omogočajo tudi komunikacijo, zajete v tej uredbi.

(12) Povezane naprave in stroji vse bolj komunicirajo med sabo prek elektronskih komunikacijskih omrežij (internet stvari). Prenos komunikacij stroj-stroj vključuje prenos signalov prek omrežja in zato običajno pomeni storitev elektronskih komunikacij. Da se zagotovi popolno varstvo pravice do zasebnosti in do zaupnosti komunikacij ter spodbuja zanesljiv in varen internet stvari na enotnem digitalnem trgu, je treba pojasniti, da bi se morala ta uredba uporabljati za prenos komunikacij stroj-stroj. Načelo zaupnosti v tej uredbi bi se torej moralo uporabljati tudi za prenos komunikacij stroj-stroj. Posebni zaščitni ukrepi bi se lahko sprejeli tudi na podlagi sektorske zakonodaje, kot na primer Direktive 2014/53/EU.

---

6 Direktiva 2014/53/EU Evropskega parlamenta in Sveta z dne 16. aprila 2014 o harmonizaciji zakonodaj držav članic v zvezi z dostopnostjo radijske opreme na trgu in razveljavitvi Direktive 1999/5/ES (UL L 153, 22.5.2014, str. 62).

7 Predlog Komisije za Direktivo Evropskega parlamenta in Sveta o Evropskem zakoniku o elektronskih komunikacijah (Prenovitev) (COM/2016/0590 final – 2016/0288 (COD)).

(13) Razvoj hitrih in učinkovitih brezžičnih tehnologij je javnosti omogočil vse večjo razpoložljivost dostopa do interneta prek brezžičnih omrežij, dostopnih vsem v javnih in polzasebnih prostorih, kot so „dostopne točke“, nameščene na različnih krajih v mestu, veleblagovnicah, nakupovalnih središčih in bolnišnicah. Če se navedena komunikacijska omrežja zagotavljajo neopredeljeni skupini končnih uporabnikov, bi morala biti zaupnost komunikacij, ki se prenašajo prek takih omrežij, zaščitena. Dejstvo, da je lahko brezžična storitev elektronskih komunikacij pomožna ob drugih storitvah, ne bi smelo ovirati zagotavljanja varstva zaupnosti podatkov v zvezi s komunikacijami in uporabe te uredbe. Zato bi se morala ta uredba uporabljati za elektronske komunikacijske podatke, pri katerih se uporabljajo storitve elektronskih komunikacij in javna komunikacijska omrežja. Nasprotno se ta uredba ne bi smela uporabljati za zaprte skupine končnih uporabnikov, kot so korporacijska omrežja, dostop do katerih je omejen na člane korporacije.

(14) Elektronske komunikacijske podatke bi bilo treba opredeliti ustrezno široko in tehnološko nevtralno, da bi zajeli vse informacije, ki se nanašajo na preneseno ali izmenjano vsebino (vsebino elektronskih komunikacij) in informacije v zvezi s končnim uporabnikom storitev elektronskih komunikacij, ki se obdelajo za namene prenosa, razširjanja ali omogočanja izmenjave vsebine elektronskih komunikacij; vključno s podatki za sledenje in določitev vira in cilja komunikacije, geografske lokacije ter datuma, časa, trajanja in vrste komunikacije. Ne glede na to, ali se taki signali in povezani podatki prenašajo po žicah, z radijskimi valovi, z optičnimi ali drugimi elektromagnetnimi sredstvi, vključno s satelitskimi omrežji, kabelskimi omrežji, fiksnimi (vodovno in paketno komutiranimi, vključno z internetom) in mobilnimi prizemnimi omrežji, električnimi kabelskimi sistemi, bi bilo treba podatke, povezane s takimi signali, šteti za metapodatke v zvezi elektronskimi komunikacijami in bi zanje morale veljati določbe te uredbe. Elektronski komunikacijski metapodatki lahko vključujejo informacije, ki spadajo v naročnino na storitev, kadar se take informacije obdelujejo za namene prenašanja, razširjanja ali izmenjave vsebine elektronskih komunikacij.

(15) Elektronske komunikacijske podatke bi bilo treba obravnavati kot zaupne. To pomeni, da bi bilo treba prepovedati vsakršno poseganje v prenos elektronskih komunikacijskih podatkov brez privolitve vseh strani, udeleženih v komunikaciji, ne glede na to, ali se posega neposredno s človekovim posredovanjem ali posredno s samodejno obdelavo, ki jo izvajajo stroji. Prepoved prestrezanja podatkov v zvezi s komunikacijami bi se morala uporabljati med njihovim prenosom, tj. dokler naslovnik ne prejme vsebine elektronske komunikacije. Prestrezanje elektronskih komunikacijskih podatkov je mogoče, na primer, kadar nekdo, ki ni udeležen v komunikaciji, posluša klice, bere, skenira ali shrani vsebino elektronskih komunikacij ali povezanih metapodatkov za namene, ki niso izmenjava komunikacij. Prestrezanje je tudi, kadar tretje osebe spremljajo obiskana spletišča, čas obiskov, interakcijo z drugimi itd. brez privolitve zadevnega končnega uporabnika. Z razvojem tehnologije so se razvili tudi tehnični načini prestrezanja. Ti lahko vključujejo namestitev opreme, ki zbira podatke s terminalske opreme na ciljnih območjih, kot so t. i. lovilci IMSI (mednarodna identiteta mobilnega naročnika), ter programe in tehnike, ki na primer prikrito spremljajo spletne navade zaradi ustvarjanja profilov končnih uporabnikov. Drugi primeri prestrezanja vključujejo zajetje koristnih podatkov ali podatkov o vsebini na nešifriranih brezžičnih omrežjih in usmerjevalnikih, vključno s spletnimi navadami brez privolitve končnih uporabnikov.

(16) Prepoved shranjevanja komunikacij ni namenjena temu, da se prepove vsako samodejno, vmesno in prehodno shranjevanje teh informacij, če se tako shranjevanje izvaja le zaradi izvedbe prenosa na elektronskem komunikacijskem omrežju. Ne bi smela veljati za obdelavo elektronskih komunikacijskih podatkov zaradi zagotavljanja varnosti in neprekinjenosti elektronskih komunikacijskih storitev, vključno s preverjanjem varnostnih groženj, kot je prisotnost zlonamerne programske opreme, ali obdelavo metapodatkov zaradi zagotavljanja zahtev glede kakovosti storitev, kot sta prehodni čas, trepetanje itd.

(17) Obdelava elektronskih komunikacijskih podatkov je lahko koristna za podjetja, potrošnike in družbo kot celoto. Kar zadeva Direktivo 2002/58/ES, ta uredba razširja možnosti za ponudnike elektronskih komunikacijskih storitev, da na podlagi privolitve končnega uporabnika obdelajo elektronske komunikacijske metapodatke. Vendar končni uporabniki pripisujejo velik pomen zaupnosti svojih komunikacij, vključno z njihovimi dejavnostmi na spletu, in temu, da želijo nadzorovati uporabo elektronskih komunikacijskih podatkov za namene, ki niso prenos komunikacije. Zato bi morala ta uredba od ponudnikov elektronskih komunikacij zahtevati, da za obdelavo elektronskih komunikacijskih metapodatkov pridobijo privolitev končnih uporabnikov. Podatki o lokaciji, ki se generirajo drugače kot v okviru zagotavljanja elektronskih komunikacijskih storitev, se ne bi smeli šteti za metapodatke. Primeri, kako ponudniki elektronskih komunikacijskih storitev uporabljajo elektronske komunikacijske metapodatke, lahko vključujejo zagotavljanje toplotnih zemljevidov, tj. grafičnega prikaza podatkov s pomočjo barv, ki prikazuje prisotnost posameznikov. Da bi prikazali gibanje prometa v določene smeri v določenem obdobju, je potreben identifikator, ki poveže položaje posameznikov v določenih časovnih presledkih. Ta identifikator bi manjkal, če bi se uporabili anonimni podatki, in takega gibanja ne bi bilo mogoče prikazati. Javni organi in izvajalci javnega prometa na primer, ki bi elektronske komunikacijske metapodatke uporabili na tak način, bi lahko na podlagi uporabe obstoječe infrastrukture in pritiska nanjo opredelili, kje bi razvili novo infrastrukturo. Kadar bi lahko način obdelave elektronskih komunikacijskih metapodatkov, zlasti z uporabo novih tehnologij ter ob upoštevanju narave, obsega, okvira in namenov obdelave, verjetno precej ogrožal pravice in svoboščine fizičnih oseb, bi bilo treba pred obdelavo v skladu s členoma 35 in 36 Uredbe (EU) 2016/679 izvesti oceno učinka v zvezi z varstvom podatkov ali se po potrebi posvetovati z nadzornim organom.

(18) Končni uporabniki lahko privolijo v obdelavo svojih metapodatkov, da bi prejeli posebne storitve, kot so storitve zaščite pred goljufivimi ravnanji (z analizo podatkov o uporabi, lokaciji in računa stranke v realnem času). V digitalnem gospodarstvu so elektronske komunikacijske storitve namesto za plačilo pogosto na voljo v zameno za protistoritev, na primer za izpostavljenost končnih uporabnikov oglasom. Za namene te uredbe bi morala privolitev končnega uporabnika, ne glede na to, ali je ta fizična ali pravna oseba, imeti enak pomen kot privolitev posameznika, na katerega se nanašajo osebni podatki, na podlagi Uredbe (EU) 2016/679, zanjo pa bi morali veljati enaki pogoji. Osnovni širokopasovni dostop do interneta in govorne komunikacijske storitve se štejejo za osnovne storitve, ki posameznikom omogočajo komunikacijo in udeležbo v korist digitalnega gospodarstva. Privolitev v obdelavo podatkov, pridobljenih na podlagi uporabe interneta ali govorne komunikacije ne bo veljavna, če posameznik, na katerega se nanašajo osebni podatki, nima možnosti dejanske in prostovoljne izbire ali privolitve ne more zavrniti ali preklicati brez škode.

(19) Vsebina elektronskih komunikacij se nanaša na bistvo temeljne pravice do spoštovanja zasebnega in družinskega življenja, stanovanja in komunikacij, ki je varovana na podlagi člena 7 Listine. Vsako poseganje v vsebino elektronskih komunikacij bi moralo biti dovoljeno le na podlagi zelo jasno opredeljenih pogojev in za posebne namene, vzpostavljeni pa bi morali biti ustrezni zaščitni ukrepi pred zlorabo. Ta uredba ponudnikom elektronskih komunikacijskih storitev omogoča, da z informirano privolitvijo vseh zadevnih končnih uporabnikov obdelajo elektronske komunikacijske podatke v tranzitu. Ponudniki lahko na primer nudijo storitve, ki vključujejo skeniranje elektronske pošte, da se odstrani nekatero vnaprej določeno gradivo. Ta uredba zaradi občutljivosti vsebine komunikacij določa predpostavko, da bo obdelava takih podatkov o vsebini precej ogrožala pravice in svoboščine fizičnih oseb. Ponudnik elektronskih komunikacijskih storitev bi se moral pri obdelavi takih vrst podatkov pred obdelavo vedno posvetovati z nadzornim organom. Tako posvetovanje bi moralo biti v skladu s členom 36(2) in (3) Uredbe (EU) 2016/679. Navedena predpostavka ne zajema obdelave podatkov o vsebini zaradi opravljanja storitve, ki jo zahteva končni uporabnik, kadar je končni uporabnik privolil v tako obdelavo ter se ta izvaja za namene in trajanje, ki so nujno potrebni in sorazmerni za tako storitev. Ko končni uporabnik pošlje vsebino elektronske komunikacije in jo prejme končni uporabnik naslovnik ali končni uporabniki naslovniki, jo lahko končni uporabnik, končni uporabniki ali tretja oseba, ki je bila pooblaščena za beleženje ali shranjevanje takih podatkov, zabeleži ali shrani. Vsaka obdelava takih podatkov mora biti v skladu z Uredbo (EU) 2016/679.

(20) Terminalska oprema končnih uporabnikov elektronskih komunikacijskih omrežij in vsaka informacija, povezana z uporabo take terminalske opreme, ne glede na to, ali je zlasti shranjena na taki terminalski opremi ali jo ta oddaja, se od nje zahteva ali jo obdeluje, da se lahko poveže z drugo napravo ali omrežno opremo, sta del zasebnega področja končnih uporabnikov, ki zahteva varstvo na podlagi Listine Evropske unije o temeljnih pravicah in Evropske konvencije o varstvu človekovih pravic in temeljnih svoboščin. Ker taka oprema vsebuje ali obdeluje informacije, ki lahko razkrijejo podrobnosti o čustvenih, političnih in družbenih značilnostih posameznika, vključno z vsebino komunikacij, fotografijami, lokacijo posameznika z dostopanjem do GPS zmogljivosti naprave, seznami kontaktnih oseb in drugimi informacijami, ki so že shranjene na napravi, informacije v zvezi s tako opremo zahtevajo okrepljeno varstvo zasebnosti. Poleg tega lahko tako imenovana vohunska programska oprema, spletni hrošči, skriti identifikatorji, trajni piškotki in druge podobne sledilne naprave vdrejo v uporabnikov terminal brez njegove vednosti, da bi pridobili dostop do podatkov, shranili skrite podatke ali izsledili uporabnikove dejavnosti. Informacije, povezane z napravo končnega uporabnika, se lahko zbirajo tudi na daljavo za namene določitve in sledenja z uporabo „zajema prstnega odtisa naprave“, pogosto brez vednosti končnega uporabnika, in lahko resno posegajo v zasebnost teh končnih uporabnikov. Tehnike, ki prikrito spremljajo dejanja končnih uporabnikov, na primer s sledenjem njihovim spletnim dejavnostim ali lokaciji njihove terminalske opreme, ali uničujejo terminalsko opremo končnega uporabnika, resno ogrožajo zasebnost končnih uporabnikov. Zato bi moral biti vsak tak poseg v terminalsko opremo končnega uporabnika dovoljen le s privolitvijo končnega uporabnika ter za posebne in pregledne namene.

(21) Izjeme glede obveznosti pridobitve privolitve za uporabo obdelovalnih in pomnilniških zmogljivosti terminalske opreme ali za dostop do informacij, shranjenih na terminalski opremi, bi morale biti omejene na primere, pri katerih se ne posega v zasebnost ali je to zelo omejeno. Privolitev se na primer ne bi smela zahtevati za

odobritev tehničnega shranjevanja ali dostopa, ki je nujno potreben za legitimni namen omogočanja uporabe posebne storitve, ki jo je izrecno zahteval končni uporabnik. To lahko vključuje shranjevanje piškotkov za trajanje ene same vzpostavljene seje na spletišču, da se sledi vnosom končnega uporabnika, ko izpolnjuje spletne obrazce na več straneh. Piškotki so lahko tudi legitimno in koristno orodje na primer pri merjenju spletnega prometa na spletni strani. Preverjanje konfiguracije, ki ga opravljajo ponudniki storitev informacijske družbe, da bi zagotovili storitev v skladu z nastavitvami končnega uporabnika, in zgolj evidentiranje dejstva, da naprava končnega uporabnika ne more prejeti vsebine, ki jo je zahteval končni uporabnik, ne bi smela pomeniti dostopa do take naprave ali uporabe obdelovalnih zmogljivosti naprave.

(22) Načini, ki se uporabijo za zagotavljanje informacij in pridobitev privolitve končnega uporabnika, bi morali biti čim bolj uporabniku prijazni. Zaradi vseprisotne uporabe trajnih piškotkov in drugih tehnik sledenja se končne uporabnike vse bolj poziva k privolitvi v shranjevanje takih trajnih piškotkov na njihovo terminalsko opremo. Zato so končni uporabniki prenasičeni s pozivi k privolitvi. Ta težava se lahko odpravi z uporabo tehničnih sredstev za pridobitev privolitve prek na primer preglednih in uporabniku prijaznih nastavitev. Zato bi morala ta uredba omogočiti izražanje privolitve z uporabo ustreznih nastavitev brskalnika ali druge aplikacije. Odločitve končnih uporabnikov glede določanja svojih splošnih nastavitev zasebnosti brskalnika ali druge aplikacije bi morale biti zavezujoče za vse tretje osebe in izvršljive proti njim. Spletni brskalniki so vrsta programske aplikacije, ki omogoča pridobivanje in navedbo informacij na internetu. Druge vrste aplikacij, kot so tiste, ki omogočajo klicanje in pošiljanje sporočil ali zagotavljajo usmerjanje poti, imajo prav tako take zmogljivosti. Spletni brskalniki posredujejo večino tega, kar se dogaja med končnim uporabnikom in spletiščem. S tega vidika so v prednostnem položaju, saj lahko igrajo dejavno vlogo ter končnemu uporabniku pomagajo pri nadzorovanju pretoka informacij na terminalsko opremo in z nje. Natančneje, spletni brskalniki se lahko uporabijo kot vratarji in pomagajo končnim uporabnikom, da preprečijo dostop do informacij na njihovi terminalski opremi (npr. pametnega telefona, tablice ali računalnika) ali njihovo shranjevanje.

(23) Načeli vgrajenega in privzetega varstva podatkov sta bili kodificirani na podlagi člena 25 Uredbe (EU) 2016/679. Trenutno so v večini spletnih brskalnikov privzete nastavitve za piškotke nastavljene na „sprejmi vse piškotke“. Za ponudnike programske opreme, ki omogoča pridobivanje in navedbo informacij na internetu, bi zato morala veljati obveznost konfiguracije programske opreme tako, da bo nudila možnost, da se tretjim osebam prepreči shranjevanje informacij na terminalski opremi; to je pogosto navedeno kot „zavrni piškotke tretjih oseb“. Končnim uporabnikom bi moral biti na voljo sklop možnosti za nastavitev zasebnosti, ki bi zajemal različne stopnje, od višje (npr. „nikoli ne sprejmi piškotkov“) do nižje (npr. „vedno sprejmi piškotke“) in srednje (npr. „zavrni piškotke tretjih oseb“ ali „sprejmi le piškotke ponudnika“). Take nastavitve zasebnosti bi morale biti predstavljene dobro vidno in razumljivo.

(24) Da bi lahko spletni brskalniki pridobili privolitev končnega uporabnika, kakor je opredeljena na podlagi Uredbe (EU) 2016/679, na primer v shranjevanje trajnih piškotkov tretjih oseb, bi med drugim morali zahtevati jasno pritrdilno dejanje končnega uporabnika terminalske opreme, ki bi pomenilo njegovo prostovoljno, izrecno, informirano in nedvoumno soglasje k shranjevanju takih piškotkov na terminalski opremi in dostopu z nje. Tako dejanje se lahko šteje za pritrdilno, če

morajo končni uporabniki dejavno izbrati „sprejmi piškotke tretjih oseb“, da bi potrdili svoje soglasje, in prejmejo potrebne informacije, na podlagi katerih se lahko odločijo. Zato je treba od ponudnikov programske opreme, ki omogočajo dostop do interneta, zahtevati, da končne uporabnike ob namestitvi obvestijo o možnostih glede izbire različnih nastavitev zasebnosti in od njih zahtevajo, da izberejo. Zagotovljene informacije končnih uporabnikov ne bi smele odvračati od tega, da izberejo višjo stopnjo nastavitev zasebnosti, ter bi morale vključevati ustrezne informacije o tveganjih, povezanih z omogočanjem shranjevanja piškotkov tretjih oseb na računalniku, vključno z zbiranjem dolgoročnih evidenc zgodovine brskanja posameznika in uporabo takih evidenc za pošiljanje usmerjenih oglasov. Spletne brskalnike se spodbuja, naj končnim uporabnikom zagotovijo preprosto spreminjanje nastavitev zasebnosti kadar koli med uporabo in uporabniku omogočijo, da naredi izjemo za nekatera spletišča ali jih da na beli seznam ali določi, za katera spletišča so piškotki (tretjih oseb) vedno ali nikoli dovoljeni.

(25) Za dostop do elektronskih komunikacijskih omrežij je potrebno redno oddajanje paketov podatkov, da se odkrije ali ohranja povezava z omrežjem ali drugimi napravami v omrežju. Poleg tega morajo imeti naprave dodeljen enotni naslov, da so lahko določljive na navedenem omrežju. Standardi za brezžične in mobilne telefone podobno vključujejo oddajanje dejavnih signalov z enotnimi identifikatorji, kot so naslov MAC, IMEI (mednarodna identiteta mobilne opreme), številka IMSI itd. Ena sama brezžična bazna postaja (tj. oddajnik in prejemnik), kot je brezžična dostopna točka, ima določen domet, v katerem se lahko take informacije zajamejo. Pojavili so se ponudniki storitev, ki na podlagi skeniranja informacij, povezanih z opremo, nudijo storitve sledenja z različnimi funkcionalnostmi, vključno s štetjem ljudi, zagotavljanjem podatkov o številu ljudi, ki čakajo v vrsti, določanjem števila ljudi na določenem območju itd. Te informacije se lahko uporabijo za bolj vsiljive namene, kot je pošiljanje komercialnih sporočil končnim uporabnikom, na primer pri vstopu v trgovine, s posamezniku prilagojenimi ponudbami. Nekatere od teh funkcionalnosti ne pomenijo velikih tveganj za zasebnost, druge pa, na primer tiste, ki zajemajo sledenje posameznikom v daljšem časovnem obdobju, vključno z večkratnimi obiski določenih lokacij. Ponudniki, ki izvajajo take prakse, bi morali na robu kritega območja postaviti vidna obvestila, ki končne uporabnike pred vstopom na določeno območje obveščajo, da je na določenem območju vzpostavljena tehnologija, o namenu sledenja, osebi, ki je zanj odgovorna, ter vseh ukrepih, ki jih lahko končni uporabnik terminalske opreme sprejme, da čim bolj zmanjša ali prepreči zbiranje informacij. Kadar se zbirajo osebni podatki, bi bilo treba zagotoviti dodatne informacije v skladu s členom 13 Uredbe (EU) 2016/679.

(26) Kadar obdelava elektronskih komunikacijskih podatkov, ki jo izvajajo ponudniki elektronskih komunikacijskih storitev, spada na področje te uredbe, bi morala ta uredba Uniji ali državam članicam omogočiti, da pod posebnimi pogoji z zakonom omejijo nekatere obveznosti in pravice, kadar taka omejitev pomeni potreben in sorazmeren ukrep v demokratični družbi za zaščito posebnih javnih interesov, tudi za nacionalno varnost, obrambo, javno varnost ter preprečevanje, preiskovanje, odkrivanje ali pregon kaznivih dejanj ali izvrševanje kazenskih sankcij, vključno z varovanjem pred grožnjami javni varnosti in preprečevanjem takih groženj, in drugih pomembnih ciljev v splošnem javnem interesu Unije ali države članice, zlasti pomembnega gospodarskega ali finančnega interesa Unije ali države članice ali spremljanja, pregledovanja ali urejanja, povezanega z izvajanjem javne oblasti zaradi takih interesov. Zato ta uredba ne bi smela vplivati na možnost držav članic, da zakonito prestrezajo elektronska sporočila ali da sprejmejo druge ukrepe, če so

potrebni in sorazmerni za zaščito navedenih javnih interesov, v skladu z Listino o temeljnih pravicah in Evropsko konvencijo o varstvu človekovih pravic in temeljnih svoboščin, kakor jo razlagata Sodišče Evropske unije in Evropsko sodišče za človekove pravice. Ponudniki elektronskih komunikacijskih storitev bi morali zagotoviti ustrezne postopke za olajšanje zakonitih zahtev pristojnih organov, po potrebi tudi ob upoštevanju vloge predstavnika, imenovanega v skladu s členom 3(3).

(27) Kar zadeva identifikacijo klicne linije, je treba zaščititi pravico klicatelja, da zavrne prikaz identitete priključka, s katerega kliče, in pravico poklicanega, da zavrne klice z neprepoznanih priključkov. Nekateri končni uporabniki, zlasti telefonski priključki za klice v sili in podobne organizacije, želijo zajamčiti anonimnost svojih klicateljev. Kar zadeva prikaz identitete priključka v zvezi, je treba zaščititi pravico in legitimne interese poklicanega, da zavrne prikaz identitete priključka, na katerega je klicatelj dejansko priključen.

(28) V posebnih primerih pa je prikrivanje prikaza identifikacije klicne linije upravičeno. Pravice končnih uporabnikov do zasebnosti v zvezi z identifikacijo klicne linije bi bilo treba omejiti, če je to potrebno zaradi izsledite nadležnih klicev, ter v zvezi s podatki o identiteti in lokaciji klicne linije, če je to potrebno za čim učinkovitejše opravljanje nalog služb za pomoč v sili, kot je e-klic.

(29) Obstaja tehnologija, ki ponudnikom elektronskih komunikacijskih storitev omogoča, da končnim uporabnikom na različne načine omejijo prejemanje neželenih klicev, vključno z onemogočanjem tihih klicev ter drugih goljufivih in nadležnih klicev. Ponudniki javno dostopne medosebne komunikacijske storitve na podlagi številke bi morali uporabljati to tehnologijo in končne uporabnike brezplačno zaščititi pred nadležnimi klici. Ponudniki bi morali zagotoviti, da so končni uporabniki seznanjeni z obstojem takih funkcij, na primer z objavo tega dejstva na svoji spletni strani.

(30) Javno dostopni direktoriji končnih uporabnikov elektronskih komunikacijskih storitev so široko razširjeni. Javno dostopni direktorij je vsak direktorij ali storitev, ki vsebuje informacije o končnem uporabniku, kot so telefonske številke (vključno z mobilnimi telefonskimi številkami) in podatki o elektronskih naslovih ter vključuje imeniške storitve. V skladu s pravico do zasebnosti in varstva osebnih podatkov fizičnih oseb je treba končne uporabnike, ki so fizične osebe, pred vključitvijo njihovih osebnih podatkov v direktorij vprašati za privolitev. V skladu z zakonitim interesom pravnih oseb imajo končni uporabniki, ki so pravne osebe, pravico, da nasprotujejo vključitvi z njimi povezanih podatkov v direktorij.

(31) Če končni uporabniki, ki so fizične osebe, privolijo v vključitev svojih podatkov v take direktorije, bi morali imeti možnost, da na podlagi privolitve določijo, katere kategorije osebnih podatkov se vključijo v direktorij (npr. ime, elektronski naslov, domači naslov, uporabniško ime, telefonska številka). Poleg tega bi morali ponudniki javno dostopnih direktorijev končne uporabnike pred njihovo vključitvijo v navedeni direktorij obvestiti o namenih direktorija in o njegovih iskalnih funkcijah. Končni uporabniki bi morali imeti možnost, da s privolitvijo določijo, na podlagi katerih kategorij osebnih podatkov se lahko iščejo njihovi kontaktni podatki. Kategorije osebnih podatkov, vključene v direktorij, in kategorije osebnih podatkov, na podlagi katerih se lahko iščejo kontaktni podatki končnega uporabnika, ne bi smele biti enake.

(32) V tej uredbi se pojem neposrednega trženja nanaša na vsako obliko oglaševanja, v okviru katere fizična ali pravna oseba pošlje sporočila za namene neposrednega trženja neposredno enemu ali več določenim ali določljivim končnim uporabnikom, ki uporabljajo elektronske komunikacijske storitve. To bi moralo poleg ponujanja

proizvodov in storitev v tržne namene vključevati tudi sporočila, ki jih pošljejo politične stranke, ki s fizičnimi osebami stopijo v stik prek elektronskih komunikacijskih storitev, da bi oglaševale svoje stranke. To bi moralo veljati tudi za sporočila, ki jih pošljejo druge neprofitne organizacije zaradi podpiranja namenov organizacije.

(33) Treba bi bilo zagotoviti zaščitne ukrepe za zaščito končnih uporabnikov pred nepovabljenimi sporočili za neposredno trženje, ki posegajo v zasebno življenje končnih uporabnikov. Stopnja poseganja v zasebnost in nadlegovanje se šteje za razmeroma podobno ne glede na številne tehnologije in kanale, ki se uporabljajo za pošiljanje teh elektronskih komunikacij, ne glede na to, ali se pri tem uporabijo avtomatizirani klicni in komunikacijski sistemi, aplikacije za takojšnje sporočanje, elektronska pošta, kratka sporočila SMS, večpredstavnostna sporočila MMS, Bluetooth itd. Zato je upravičeno zahtevati, da se pred pošiljanjem elektronskih komercialnih sporočil za neposredno trženje končnim uporabnikom pridobi privolitev končnega uporabnika, da se učinkovito zaščitijo posamezniki pred poseganjem v njihovo zasebno življenje in legitimni interesi pravnih oseb. Pravna varnost in potreba po zagotavljanju, da bodo predpisi, ki ščitijo pred nepovabljenimi elektronskimi sporočili, ustrezni tudi v prihodnosti, upravičujeta potrebo po opredelitvi enotnega sklopa predpisov, ki se ne spreminjajo glede na tehnologijo, uporabljeno za prenašanje teh nepovabljenih sporočil, in hkrati zagotavljajo enakovredno raven varstva za vse državljane v vsej Uniji. Vendar je razumno dovoliti, da se podatki o elektronskih naslovih uporabijo v okviru obstoječega razmerja med dobaviteljem in odjemalcem za ponujanje podobnih proizvodov ali storitev. Taka možnost bi se morala uporabljati le za tisto podjetje, ki je pridobilo podatke o elektronskih naslovih v skladu z Uredbo (EU) 2016/679.

(34) Kadar končni uporabniki privolijo v prejemanje nepovabljenih sporočil za neposredno trženje, bi še vedno morali imeti možnost, da kadar koli enostavno prekličejo svojo privolitev. Da bi olajšali učinkovito izvajanje pravil Unije v zvezi z nepovabljenimi sporočili za neposredno trženje, je treba prepovedati zakrivanje identitete in uporabo lažnih identitet, lažnih povratnih naslovov ali številk pri pošiljanju nepovabljenih komercialnih sporočil za neposredno trženje. Nepovabljena sporočila za namene trženja bi zato morala biti kot taka jasno prepoznavna, v njih pa bi morala biti navedena identiteta pravne ali fizične osebe, ki prenaša sporočilo ali v katere imenu se sporočilo prenaša, in zagotovljene informacije, ki jih prejemniki potrebujejo za uveljavljanje svoje pravice do nasprotovanja prejemanju nadaljnjih pisnih in/ali ustnih sporočil za trženje.

(35) Da se zagotovi enostaven preklic privolitve, bi morale pravne ali fizične osebe, ki sporočila za neposredno trženje prenašajo prek elektronske pošte, navesti povezavo ali veljavni naslov elektronske pošte, ki ga lahko končni uporabniki enostavno uporabijo za preklic svoje privolitve. Pravne ali fizične osebe, ki sporočila za neposredno trženje prenašajo prek govorno-govornih klicev in klicev z avtomatičnimi klicnimi in komunikacijskimi sistemi, bi morale razkriti identiteto priključka, na katerega se lahko pokliče podjetje, ali navesti posebno kodo, iz katere bi bilo razvidno, da je klic tržne narave.

(36) Govorno-govorni klici za namene neposrednega trženja, pri katerih se ne uporabljajo avtomatizirani klicni in komunikacijski sistemi, so dražji za pošiljatelja in končnim uporabnikom ne nalagajo nobenih finančnih stroškov. Države članice bi zato morale imeti možnost, da vzpostavijo ali ohranijo nacionalne sisteme, ki dovoljujejo, da se taki klici opravijo le končnim uporabnikom, ki temu niso nasprotovali.

(37) Ponudniki storitev, ki ponujajo javno dostopne elektronske komunikacijske storitve, bi morali obvestiti končne uporabnike o ukrepih, ki jih lahko sprejmejo za zagotovitev varnosti sporočil, na primer z uporabo posebnih vrst programske opreme ali tehnologij šifriranja. Zahteva po obveščanju končnih uporabnikov o posebnih varnostnih tveganjih ne razrešuje ponudnika storitve njegove obveznosti, da na svoje stroške sprejme ustrezne in takojšnje ukrepe za odpravo vsakih novih, nepredvidenih varnostnih tveganj ter da spet vzpostavi običajno raven varnosti storitve. Zagotavljanje informacij o varnostnih tveganjih naročniku bi moralo biti brezplačno. Varnost se ocenjuje z vidika člena 32 Uredbe (EU) 2016/679.

(38) Da se zagotovi popolna skladnost z Uredbo (EU) 2016/679, bi bilo treba za izvrševanje določb te uredbe pooblastiti organe, ki so že odgovorni za izvrševanje določb Uredbe (EU) 2016/679, saj ta uredba temelji na mehanizmu za skladnost iz Uredbe (EU) 2016/679. Zaradi umestitve v njihovo ustavno, organizacijsko in upravno strukturo bi države članice morale imeti možnost, da imajo več kot en nadzorni organ. Nadzorni organi bi morali biti odgovorni tudi za spremljanje uporabe te uredbe glede elektronskih komunikacijskih podatkov za pravne osebe. Take dodatne naloge ne bi smele ogroziti zmožnosti nadzornega organa, da opravlja svoje naloge glede varstva osebnih podatkov na podlagi Uredbe (EU) 2016/679 in te uredbe. Vsakemu nadzornemu organu bi bilo treba zagotoviti dodatne finančne in človeške vire, prostore in infrastrukturo, potrebne za učinkovito opravljanje nalog na podlagi te uredbe.

(39) Vsak nadzorni organ bi moral biti na ozemlju svoje države članice pristojen za izvajanje pooblastil in opravljanje nalog, določenih v tej uredbi. Za zagotovitev doslednega spremljanja in izvrševanja te uredbe v vsej Uniji bi morali biti naloge in učinkovita pooblastila nadzornih organov v vseh državah članicah enaki, hkrati pa ne bi smeli vplivati na pooblastila organov, pristojnih za pregon v skladu s pravom držav članic, da sodne organe opozorijo na kršitve te uredbe in sodelujejo v sodnih postopkih. Države članice in njihove nadzorne organe se spodbuja, da pri uporabi te uredbe upoštevajo posebne potrebe mikro, malih in srednjih podjetij.

(40) Da bi okrepili izvrševanje predpisov iz te uredbe, bi moral imeti vsak nadzorni organ pooblastila, da poleg ustreznih ukrepov v skladu s to uredbo ali namesto njih naloži kazni, vključno z upravnimi globami. Ta uredba bi morala navajati kršitve, zgornjo mejo in merila za določanje s tem povezanih upravnih glob, ki bi jih moral v vsakem posameznem primeru določiti pristojni nadzorni organ ob upoštevanju vseh zadevnih okoliščin v določeni situaciji ter zlasti narave, teže in trajanja kršitve ter njenih posledic in sprejetih ukrepov za zagotavljanje skladnosti z obveznostmi iz te uredbe in za preprečitev ali ublažitev posledic kršitve. Za namene določanja globe na podlagi te uredbe bi bilo treba pojem „podjetje“ razumeti kot podjetje v skladu s členoma 101 in 102 Pogodbe.

(41) Da se dosežejo cilji te uredbe, in sicer da se zaščitijo temeljne pravice in svoboščine posameznikov in zlasti njihova pravica do varstva osebnih podatkov ter da se zagotovi prosti pretok osebnih podatkov v Uniji, bi bilo treba na Komisijo prenesti pooblastilo, da v skladu s členom 290 Pogodbe sprejme akte za dopolnitev te uredbe. Zlasti bi bilo treba sprejeti delegirane akte, kar zadeva informacije, ki se navedejo, tudi v standardiziranih ikonah, da se v jasno razvidni in razumljivi obliki posredujejo pregled nad zbiranjem informacij, ki jih oddaja terminalska oprema, njegov namen, informacije o osebi, ki je zanj odgovorna, ter vsak ukrep, ki ga lahko končni uporabnik terminalske opreme sprejme, da zbiranje čim bolj omeji. Delegirani akti so potrebni tudi za določitev kode za identifikacijo neposrednih klicev za namene trženja, vključno s tistimi, ki se izvedejo prek avtomatiziranih klicnih in komunikacijskih

sistemov. Zlasti je pomembno, da se Komisija ustrezno posvetuje in da se ta posvetovanja izvedejo v skladu z načeli, določenimi v Medinstitucionalnem sporazumu o boljši pripravi zakonodaje z dne 13. aprila 2016[8]. Za zagotovitev enakopravnega sodelovanja pri pripravi delegiranih aktov Evropski parlament in Svet zlasti prejmeta vse dokumente sočasno kot strokovnjaki iz držav članic, njuni strokovnjaki pa se sistematično lahko udeležujejo sestankov strokovnih skupin Komisije, ki zadevajo pripravo delegiranih aktov. Poleg tega bi bilo treba za zagotovitev enotnih pogojev izvajanja te uredbe na Komisijo prenesti izvedbena pooblastila, kadar je tako določeno v tej uredbi. Ta pooblastila bi bilo treba izvajati v skladu z Uredbo (EU) št. 182/2011.

(42) Ker cilja te uredbe, in sicer zagotovitve enakovredne ravni varstva fizičnih in pravnih oseb ter prostega pretoka elektronskih komunikacijskih podatkov v vsej Uniji, države članice ne morejo zadovoljivo doseči, temveč se zaradi obsega ali učinkov ukrepov lažje doseže na ravni Unije, lahko Unija sprejme ukrepe v skladu z načelom subsidiarnosti iz člena 5 Pogodbe o Evropski uniji. V skladu z načelom sorazmernosti iz navedenega člena ta uredba ne presega tistega, kar je potrebno za doseganje navedenega cilja.

(43) Direktivo 2002/58/ES bi bilo treba razveljaviti –

SPREJELA NASLEDNJO UREDBO:

[8] Medinstitucionalni sporazum med Evropskim parlamentom, Svetom Evropske unije in Evropsko komisijo o boljši pripravi zakonodaje z dne 13. aprila 2016 (UL L 123, 12.5.2016, str. 1–14).

POGLAVJE I
SPLOŠNE DOLOČBE

Člen 1
Predmet urejanja

1. Ta uredba določa predpise glede varstva temeljnih pravic in svoboščin fizičnih in pravnih oseb pri zagotavljanju in uporabi elektronskih komunikacijskih storitev in zlasti pravic do spoštovanja zasebnega življenja in komunikacij ter varstva posameznikov pri obdelavi osebnih podatkov.

2. Ta uredba zagotavlja prosti pretok elektronskih komunikacijskih podatkov in elektronskih komunikacijskih storitev v Uniji, ki ne sme biti omejen ali prepovedan iz razlogov, povezanih s spoštovanjem zasebnega življenja in komunikacij fizičnih in pravnih oseb in varstvom posameznikov pri obdelavi osebnih podatkov.

3. Določbe te uredbe podrobno opredeljujejo in dopolnjujejo Uredbo (EU) 2016/679 z določitvijo posebnih predpisov za namene iz odstavkov 1 in 2.

Člen 2
Področje uporabe

1. Ta uredba se uporablja za obdelavo elektronskih komunikacijskih podatkov, ki se izvaja v povezavi z zagotavljanjem in uporabo elektronskih komunikacijskih storitev, in za informacije, povezane s terminalsko opremo končnih uporabnikov.

2. Ta uredba se ne uporablja za:

(a) dejavnosti zunaj področja uporabe prava Unije;

(b) dejavnosti držav članic, ki spadajo na področje uporabe poglavja 2 naslova V Pogodbe o Evropski uniji;

(c) storitve elektronskih komunikacij, ki niso javno dostopne;

(d) dejavnosti pristojnih organov za namene preprečevanja, preiskovanja, odkrivanja ali pregona kaznivih dejanj ali izvrševanja kazenskih sankcij, vključno z varovanjem pred grožnjami javni varnosti in njihovim preprečevanjem;

3. Obdelavo elektronskih komunikacijskih podatkov v institucijah, organih, uradih in agencijah Unije ureja Uredba (EU) 00/0000 [nova uredba, ki bo nadomestila Uredbo (ES) št. 45/2001].

4. Ta uredba ne posega v uporabo Direktive 2000/31/ES[9], zlasti v uporabo pravil o odgovornosti posrednih ponudnikov storitev iz členov 12 do 15 navedene direktive.

5. Ta uredba ne posega v določbe Direktive 2014/53/ES.

Člen 3
Ozemeljska veljavnost in predstavnik

1. Ta uredba se uporablja za:

[9] Direktiva 2000/31/ES Evropskega parlamenta in Sveta z dne 8. junija 2000 o nekaterih pravnih vidikih storitev informacijske družbe, zlasti elektronskega poslovanja na notranjem trgu (Direktiva o elektronskem poslovanju) (UL L 178, 17.7.2000, str. 1–16).

(a) zagotavljanje elektronskih komunikacijskih storitev končnim uporabnikom v Uniji, ne glede na to, ali mora končni uporabnik zanje plačati;

(b) uporabo takih storitev;

(c) varstvo informacij, povezanih s terminalsko opremo končnih uporabnikov, ki se nahajajo v Uniji.

2. Kadar ponudnik elektronske komunikacijske storitve nima sedeža v Uniji, pisno imenuje predstavnika v Uniji.

3. Predstavnik ima sedež v eni od držav članic, v kateri so končni uporabniki takih elektronskih komunikacijskih storitev.

4. Predstavnik je pooblaščen za odgovarjanje na vprašanja in zagotavljanje informacij poleg ali namesto ponudnika, ki ga predstavlja, zlasti nadzornim organom in končnim uporabnikom glede vseh vprašanj, povezanih z obdelavo elektronskih komunikacijskih podatkov za namene zagotavljanja skladnosti s to uredbo.

5. Imenovanje predstavnika v skladu z odstavkom 2 ne posega v pravne ukrepe, ki bi se lahko uvedli zoper fizično ali pravno osebo, ki obdeluje elektronske komunikacijske podatke v povezavi z zagotavljanjem elektronskih komunikacijskih storitev v državah zunaj Unije končnim uporabnikom v Uniji.

Člen 4
Opredelitev pojmov

1. V tej uredbi se uporabljajo naslednje opredelitve pojmov:

(a) opredelitve pojmov iz Uredbe (EU) 2016/679;

(b) opredelitve pojmov „elektronsko komunikacijsko omrežje“, „elektronska komunikacijska storitev“, „medosebna komunikacijska storitev“, „medosebna komunikacijska storitev na podlagi številke“, „številčno neodvisna medosebna komunikacijska storitev“, „končni uporabnik“ in „klic“ iz točke (1), (4), (5), (6), (7), (14) oziroma (21) člena 2 [Direktive o Evropskem zakoniku o elektronskih komunikacijah];

(c) opredelitev pojma „terminalska oprema“ iz člena 1(1) Direktive Komisije 2008/63/ES[10].

2. Za namene točke (b) odstavka 1 opredelitev pojma „medosebna komunikacijska storitev“ vključuje storitve, ki omogočajo medosebno in interaktivno komunikacijo le kot manjši pomožni del storitve, ki je dejansko povezan z drugo storitvijo.

3. Za namene te uredbe se prav tako uporabljajo naslednje opredelitve:

(a) „elektronski komunikacijski podatki“ pomenijo vsebino elektronskih komunikacij in elektronske komunikacijske metapodatke;

(b) „vsebina elektronske komunikacije“ pomeni vsebino, ki se izmenja s storitvami elektronskih komunikacij, kot so besedilo, govor, videi, slike in zvok;

(c) „elektronski komunikacijski metapodatki“ pomenijo podatke, ki se obdelajo v elektronskem komunikacijskem omrežju za namene prenašanja, razširjanja ali

[10] Direktiva Komisije 2008/63/ES z dne 20. junija 2008 o konkurenci na trgih za telekomunikacijsko terminalsko opremo (UL L 162, 21.6.2008, str. 20–26).

izmenjave vsebine elektronskih komunikacij; vključno s podatki, ki se uporabljajo za sledenje in določitev vira in cilja komunikacije, lokacije naprave v okviru komunikacije ter datuma, časa, trajanja in vrste komunikacije;

(d) „javno dostopni direktorij“ pomeni direktorij končnih uporabnikov elektronskih komunikacijskih storitev v natisnjeni ali elektronski obliki, ki se objavi ali da na voljo javnosti ali delu javnosti, vključno prek imeniške storitve;

(e) „elektronska pošta“ pomeni vsako elektronsko sporočilo, ki vsebuje informacije, kot so besedilo, govor, video, zvok ali slika, poslano prek elektronskega komunikacijskega omrežja, ki se lahko shrani v omrežju ali povezanih računalniških zmogljivostih ali na terminalski opremi njegovega prejemnika;

(f) „sporočila za namene neposrednega trženja“ pomenijo vsako obliko oglaševanja v pisni ali govorni obliki, ki je bilo poslano enemu ali več določenim ali določljivim končnim uporabnikom elektronskih komunikacijskih storitev, vključno z uporabo avtomatiziranih klicnih in komunikacijskih sistemov z ali brez človekovega posega, elektronske pošte, kratkih sporočil SMS itd.;

(g) „govorno-govorni klici za namene neposrednega trženja“ pomenijo klice v živo, pri katerih se ne uporabljajo avtomatizirani klicni sistemi in komunikacijski sistemi;

(h) „avtomatizirani klicni in komunikacijski sistemi“ pomenijo sisteme, ki lahko avtomatično pokličejo enega ali več prejemnikov v skladu z navodili, določenimi za navedeni sistem, in prenašajo zvoke, ki niso govor v živo, vključno s klici, pri katerih se z uporabo avtomatiziranih klicnih in komunikacijskih sistemov klicano osebo poveže s posameznikom.

POGLAVJE II
VARSTVO ELEKTRONSKIH KOMUNIKACIJ FIZIČNIH IN PRAVNIH OSEB TER INFORMACIJ, SHRANJENIH NA NJIHOVI TERMINALSKI OPREMI

Člen 5
Zaupnost elektronskih komunikacijskih podatkov

Elektronski komunikacijski podatki so zaupni. Vsem osebam razen končnim uporabnikom je prepovedano vsako poseganje v elektronske komunikacijske podatke, kot je poslušanje, prisluškovanje, shranjevanje, spremljanje, skeniranje ali kakšen drug način prestrezanja, nadzorovanja ali obdelave elektronskih komunikacijskih podatkov, razen kadar je to dovoljeno v skladu s to uredbo.

Člen 6
Dovoljena obdelava elektronskih komunikacijskih podatkov

1. Ponudniki elektronskih komunikacijskih omrežij in storitev lahko elektronske komunikacijske podatke obdelujejo, če:

(a) je to potrebno zaradi prenosa sporočila, in sicer za trajanje, potrebno za ta namen, ali

(b) je to potrebno zaradi ohranjanja ali obnovitve elektronskih komunikacijskih omrežij in storitev ali odkrivanje tehničnih okvar in/ali napak pri prenosu elektronskih komunikacij, za trajanje, potrebno za ta namen.

2. Ponudniki elektronskih komunikacijskih omrežij in storitev lahko elektronske komunikacijske metapodatke obdelujejo, če:

(a) je to potrebno zaradi izpolnjevanja zahtev v zvezi s kakovostjo storitve v skladu z [Direktivo o Evropskem zakoniku o elektronskih komunikacijah] ali Uredbo (EU) 2015/2120[11], za trajanje, potrebno za ta namen, ali

(b) je to potrebno zaradi zaračunavanja, izračuna plačila medsebojnih povezav, odkrivanja ali preprečevanja goljufive uporabe ali zlorabe elektronskih komunikacijskih storitev ali naročnine nanje, ali

(c) je zadevni končni uporabnik privolil v obdelavo svojih metapodatkov v zvezi s komunikacijami za enega ali več določenih namenov, vključno z zagotavljanjem posebnih storitev takim končnim uporabnikom, če zadevnega namena ali namenov ne bi bilo mogoče izpolniti z obdelavo anonimiziranih informacij.

3. Ponudniki elektronskih komunikacijskih storitev lahko vsebino elektronskih komunikacij obdelujejo le:

(a) zaradi zagotavljanja posebne storitve končnemu uporabniku, če so zadevni končni uporabniki privolili v obdelavo vsebine svojih elektronskih komunikacij in navedene storitve ni mogoče opraviti brez obdelave take vsebine, ali

(b) če so vsi zadevni končni uporabniki privolili v obdelavo vsebine svojih elektronskih komunikacij za enega ali več določenih namenov, ki jih ni mogoče izpolniti z obdelavo anonimiziranih informacij, in se je ponudnik posvetoval z nadzornim organom. Za posvetovanje z nadzornim organom se uporablja člen 36(2) in (3) Uredbe(EU) 2016/679.

Člen 7
Shranjevanje in izbris elektronskih komunikacijskih podatkov

1. Ko naslovnik ali naslovniki prejmejo vsebino elektronske komunikacije, ponudnik elektronske komunikacijske storitve brez poseganja v člen 6(1)(b) ter člen 6(3)(a) in (b) izbriše vsebino elektronske komunikacije ali navedene podatke anonimizira. Take podatke lahko zabeležijo ali shranijo končni uporabniki ali tretja oseba, ki so jo končni uporabniki pooblastili za beleženje, shranjevanje ali kakšno drugo obdelavo takih podatkov, v skladu z Uredbo (EU) 2016/679.

2. Ponudnik elektronske komunikacijske storitve brez poseganja v člen 6(1)(b) ter člen 6(2)(a) in (c) izbriše elektronske komunikacijske metapodatke ali navedene podatke anonimizira, ko ti podatki več niso potrebni zaradi prenosa sporočila.

3. Kadar se elektronski komunikacijski metapodatki obdelujejo zaradi zaračunavanja v skladu s členom 6(2)(b), se lahko zadevni metapodatki shranijo do konca obdobja, med katerim se lahko obračun zakonito izpodbija ali sprožijo postopki za pridobitev plačila v skladu z nacionalno zakonodajo.

[11] Uredba (EU) 2015/2120 Evropskega parlamenta in Sveta z dne 25. novembra 2015 o določitvi ukrepov v zvezi z dostopom do odprtega interneta in spremembi Direktive 2002/22/ES o univerzalni storitvi in pravicah uporabnikov v zvezi z elektronskimi komunikacijskimi omrežji in storitvami ter Uredbe (EU) št. 531/2012 o gostovanju v javnih mobilnih komunikacijskih omrežjih v Uniji (UL L 310, 26.11.2015, str. 1–18).

Člen 8

Varstvo informacij v zvezi s terminalsko opremo končnih uporabnikov oziroma informacij, ki so na njej shranjene

1. Uporaba obdelovalnih in pomnilniških zmogljivosti terminalske opreme in zbiranje informacij s terminalske opreme končnih uporabnikov, tudi o programski in strojni opremi, razen če navedeno izvaja zadevni končni uporabnik, sta prepovedana, razen če:

(a) je to potrebno le zaradi izvedbe prenosa elektronske komunikacije prek elektronskega komunikacijskega omrežja, ali

(b) je končni uporabnik v to privolil, ali

(c) je to potrebno zaradi opravljanja storitve informacijske družbe, ki jo je zahteval končni uporabnik, ali

(d) je to potrebno zaradi merjenja spletnega občinstva, če tako merjenje izvaja ponudnik storitve informacijske družbe, ki jo je zahteval končni uporabnik.

2. Zbiranje informacij, ki jih oddaja terminalska oprema, da se lahko poveže z drugo napravo in/ali omrežno opremo, je prepovedano, razen če:

(a) se izvaja izključno zaradi tega, za čas, ki je za to potreben, in za namene vzpostavitve povezave, ali

(b) je objavljeno jasno in vidno obvestilo, ki obvešča vsaj o načinih zbiranja, njegovem namenu, osebi, ki je zanj odgovorna, in drugih informacijah, ki se zahtevajo na podlagi člena 13 Uredbe (EU) 2016/679, kadar se zbirajo osebni podatki, ter o vseh ukrepih, ki jih lahko končni uporabnik terminalske opreme sprejme, da zbiranje prepreči ali čim bolj omeji.

Zbiranje takih informacij se lahko izvaja le, če so bili uporabljeni ustrezni tehnični in organizacijski ukrepi za zagotavljanje ravni varnosti glede na tveganje, kakor je določeno v členu 32 Uredbe (EU) 2016/679.

3. Informacije, ki se zagotovijo v skladu s točko (b) odstavka 2, se lahko navedejo skupaj z uporabo standardiziranih ikon, da se v jasno razvidni, razumljivi in berljivi obliki zagotovi smiseln pregled načrtovanega zbiranja.

4. Komisija je v skladu s členom 27 pooblaščena za sprejemanje delegiranih aktov za določitev informacij, ki se navedejo v standardiziranih ikonah, in postopkov za določitev standardiziranih ikon.

Člen 9

Privolitev

1. Uporabljajo se opredelitev pojma in pogoji za privolitev iz člena 4(11) in člena 7 Uredbe (EU) 2016/679.

2. Brez poseganja v odstavek 1 se lahko privolitev, kadar je tehnično mogoče in izvedljivo za namene člena 8(1)(b), izrazi z uporabo ustreznih tehničnih nastavitev programske aplikacije, ki omogoča dostop do interneta.

3. Končni uporabniki, ki so privolili v obdelavo elektronskih komunikacijskih podatkov, kakor je določeno v členu 6(2)(c) in členu 6(3)(a) in (b), imajo možnost, da kadar koli prekličejo svojo privolitev v skladu s členom 7(3)

Uredbe (EU) 2016/679, o tej možnosti pa se jih opominja v rednih 6-mesečnih intervalih, dokler traja obdelava.

Člen 10
Informacije in možnosti nastavitve zasebnosti, ki se bodo zagotovile

1. Programska oprema, dana na trg, ki omogoča elektronske komunikacije, vključno s pridobivanjem in navedbo informacij na internetu, ponuja možnost, da se tretjim osebam prepreči shranjevanje informacij na terminalski opremi končnega uporabnika ali obdelava informacij, že shranjenih na navedeni opremi.

2. Programska oprema ob namestitvi končnega uporabnika obvesti o možnostih nastavitve zasebnosti in za nadaljevanje namestitve od njega zahteva, naj privoli v nastavitev.

3. Programska oprema, ki je že nameščena 25. maja 2018, mora zahteve na podlagi odstavkov 1 in 2 izpolniti pri prvi posodobitvi programske opreme, vendar najpozneje do 25. avgusta 2018.

Člen 11
Omejitve

1. Pravo unije ali pravo države članice lahko z zakonodajnim ukrepom omeji obseg obveznosti in pravic iz členov od 5 do 8, če taka omejitev spoštuje bistvo temeljnih pravic in svoboščin ter je potreben in sorazmeren ukrep v demokratični družbi za zagotavljanje enega ali več splošnih javnih interesov iz člena 23(1)(a) do (e) Uredbe (EU) 2016/679 ali spremljanja, pregledovanja ali urejanja, povezanega z izvajanjem javne oblasti zaradi takih interesov.

2. Ponudniki elektronskih komunikacijskih storitev vzpostavijo notranje postopke za odzivanje na zahteve po dostopu do elektronskih komunikacijskih podatkov končnega uporabnika na podlagi zakonodajnega ukrepa, sprejetega v skladu z odstavkom 1. Pristojnim nadzornim organom morajo, na njihovo zahtevo, predložiti informacije o teh postopkih, število prejetih zahtevkov, sklicevanje na pravno utemeljitev in njihov odgovor.

POGLAVJE III
PRAVICE FIZIČNIH IN PRAVNIH OSEB DO NADZORA ELEKTRONSKIH KOMUNIKACIJ

Člen 12
Prikaz in omejitev prikaza identitete kličočega in priključka v zvezi

1. Kadar je na voljo prikaz identitete kličočega in priključka v zvezi v skladu s členom [107] [Direktive o Evropskem zakoniku o elektronskih komunikacijah], ponudniki javno dostopnih medosebnih komunikacijskih storitev na podlagi številke:

(a) kličočemu končnemu uporabniku zagotovijo možnost, da prepreči prikaz identifikacije klicne linije pri vsakem klicu, pri vsaki povezavi ali stalno;

(b) klicanemu končnemu uporabniku zagotovijo možnost, da pri dohodnih klicih prepreči prikaz identifikacije klicne linije;

(c) klicanemu končnemu uporabniku zagotovijo možnost, da zavrne dohodne klice, če je kličoči končni uporabnik preprečil prikaz identifikacije klicne linije;

(d) klicanemu končnemu uporabniku zagotovijo možnost, da kličočemu končnemu uporabniku prepreči prikaz identitete priključka v zvezi.

2. Možnosti iz točk (a), (b), (c) in (d) odstavka 1 se končnemu uporabniku zagotovijo na preprost in brezplačen način.

3. Točka (a) odstavka 1 se uporabi tudi v zvezi s klici v tretje države, če ti klici prihajajo iz Unije. Točke (b), (c) in (d) odstavka 1 se uporabijo tudi za dohodne klice, če prihajajo iz tretjih držav.

4. Kadar je na voljo prikaz identitete kličočega ali priključka v zvezi, ponudniki javno dostopnih medosebnih komunikacijskih storitev na podlagi številke javnosti zagotovijo informacije o možnostih iz točk (a), (b), (c) in (d) odstavka 1.

Člen 13

Izjeme glede prikaza in omejitve prikaza identifikacije klicne linije in priključka v zvezi

1. Ne glede na to, ali je kličoči končni uporabnik preprečil prikaz identifikacije klicne linije, ponudniki javno dostopnih medosebnih komunikacijskih storitev na podlagi številke, kadar se klic izvede službam za pomoč v sili, prekličejo odpravo prikaza identifikacije klicne linije in zavrnitev ali odsotnost privolitve končnega uporabnika v zvezi z obdelavo metapodatkov, za vsak priključek pri organizacijah, ki obravnavajo nujne komunikacije, vključno s telefonsko centralo za javno varnost, in sicer za namen odzivanja na takšne klice.

2. Države članice uvedejo več posebnih določb v zvezi z vzpostavitvijo postopkov in okoliščinami, v katerih ponudniki javno dostopnih medosebnih komunikacijskih storitev na podlagi številke začasno prekličejo odpravo prikaza identifikacije klicne linije, če končni uporabniki zahtevajo izsledite zlonamernih ali nadležnih klicev.

Člen 14

Onemogočanje dohodnih klicev

Ponudniki javno dostopnih medosebnih komunikacijskih storitev na podlagi številke uporabljajo najsodobnejše ukrepe, s katerimi končnim uporabnikom omejijo prejemanje neželenih klicev, klicanemu končnemu uporabniku pa tudi brezplačno zagotovijo:

(a) onemogočanje dohodnih klicev z določenih številk ali iz anonimnih virov;

(b) onemogočanje avtomatičnega posredovanja klica na terminal končnega uporabnika, ki ga izvaja tretja oseba.

Člen 15

Javno dostopni direktoriji

1. Ponudniki javno dostopnih direktorijev pridobijo privolitev končnih uporabnikov, ki so fizične osebe, za vključitev njihovih osebnih podatkov v direktorij in nato privolitev teh končnih uporabnikov za vključitev podatkov glede na kategorijo osebnih podatkov, če so taki podatki pomembni za namen direktorija, kot ga določi ponudnik direktorija. Ponudniki končnim uporabnikom, ki so fizične osebe, zagotovijo načine za preverjanje, popravek ali izbris takih podatkov.

2. Ponudniki javno dostopnega direktorija končne uporabnike, ki so fizične osebe in katerih podatki so v direktoriju, obvestijo o razpoložljivih iskalnih funkcijah direktorija in pridobijo privolitev končnih uporabnikov, preden omogočijo take iskalne funkcije v zvezi z njihovimi podatki.

3. Ponudniki javno dostopnih direktorijev omogočijo končnim uporabnikom, ki so pravne osebe, da nasprotujejo vključitvi z njimi povezanih podatkov v direktorij. Ponudniki takim končnim uporabnikom, ki so pravne osebe, zagotovijo načine za preverjanje, popravek ali izbris takih podatkov.

4. Možnost, da končni uporabniki niso vključeni v javno dostopni direktorij ali da preverijo, popravijo in izbrišejo katere koli podatke, ki se nanašajo nanje, se zagotovi brezplačno.

Člen 16
Nepovabljena sporočila

1. Fizične ali pravne osebe lahko uporabljajo elektronske komunikacijske storitve za namene pošiljanja sporočil za neposredno trženje končnim uporabnikom, ki so fizične osebe in ki so v to privolili.

2. Kadar fizična ali pravna oseba pridobi podatke o elektronskem naslovu za elektronsko pošto svoje stranke v okviru prodaje proizvoda ali storitve v skladu z Uredbo (EU) 2016/679, lahko navedena fizična ali pravna oseba te podatke o elektronskem naslovu uporabi za neposredno trženje podobnih lastnih proizvodov ali storitev le, če je strankam dana jasna in izrecna možnost, da na brezplačen in enostaven način nasprotujejo takšni uporabi. Pravica do nasprotovanja se zagotovi pri zbiranju in ko se pošlje sporočilo.

3. Brez poseganja v odstavka 1 in 2 fizične ali pravne osebe, ki uporabljajo elektronske komunikacijske storitve za namene opravljanja klicev za namene neposrednega trženja:

(a) prikažejo identiteto priključka, na katerem so dosegljive, ali

(b) prikažejo posebno kodo/predpono, iz katere je razvidno, da je klic tržne narave.

4. Ne glede na odstavek 1 lahko države članice z zakonom zagotovijo, da se lahko govorno-govorni klici za namene neposrednega trženja končnim uporabnikom, ki so fizične osebe, opravijo le pri končnih uporabnikih, ki so fizične osebe in niso nasprotovali prejemanju navedenih sporočil.

5. Države članice v okviru zakonodaje Unije in veljavne nacionalne zakonodaje zagotovijo, da so legitimni interesi končnih uporabnikov, ki so pravne osebe, glede nepovabljenih sporočil, poslanih na načine iz odstavka 1, ustrezno zaščiteni.

6. Vsaka fizična ali pravna oseba, ki za prenos sporočil za namene neposrednega trženja uporablja elektronske komunikacijske storitve, končne uporabnike obvesti o tržni naravi sporočila in identiteti pravne ali fizične osebe, v katere imenu se sporočilo prenaša, ter zagotovi informacije, ki jih prejemniki potrebujejo za enostavno uveljavljanje svoje pravice do preklica privolitve k sprejemanju nadaljnjih sporočil za namene trženja.

7. Komisija je pooblaščena za sprejetje izvedbenih ukrepov v skladu s členom 26(2), s katerimi določi kodo ali predpono za identifikacijo klicev za namene trženja v skladu s točko (b) odstavka 3.

Člen 17
Informacije o odkritih varnostnih tveganjih

V primeru posebnega tveganja, ki bi lahko ogrozilo varnost omrežij in elektronskih komunikacijskih storitev, mora ponudnik elektronske komunikacijske storitve zadevne končne uporabnike obvestiti o takem tveganju in, če tveganje presega obseg ukrepov, ki jih ponudnik storitve lahko sprejme, o vseh možnih sredstvih za odpravo tveganja, vključno z navedbo verjetnih stroškov.

POGLAVJE IV
NEODVISNI NADZORNI ORGANI IN IZVRŠEVANJE

Člen 18
Neodvisni nadzorni organi

1. Neodvisni nadzorni organ ali organi, ki so odgovorni za spremljanje uporabe Uredbe (EU) 2016/679, so odgovorni tudi za spremljanje uporabe te uredbe. Pri tem se smiselno uporabljata poglavji VI in VII Uredbe (EU) 2016/679. Naloge in pooblastila nadzornih organov se izvajajo v zvezi s končnimi uporabniki.
2. Kadar je primerno, nadzorni organ ali organi iz odstavka 1 sodelujejo z nacionalnimi regulativnimi organi, ustanovljenimi v skladu z [Direktivo o Evropskem zakoniku o elektronskih komunikacijah].

Člen 19
Evropski odbor za varstvo podatkov

Evropski odbor za varstvo podatkov, ustanovljen na podlagi člena 68 Uredbe (EU) 2016/679, je pristojen za zagotavljanje dosledne uporabe te uredbe. Evropski odbor za varstvo podatkov v ta namen opravlja naloge iz člena 70 Uredbe (EU) 2016/679. Odbor izvaja tudi naslednje naloge:

(a) svetuje Komisiji o vseh predlaganih spremembah te uredbe;

(b) na lastno pobudo oziroma na zahtevo katerega od svojih članov ali Komisije preuči vsako vprašanje v zvezi z uporabo te uredbe ter izda smernice, priporočila in najboljše prakse, da spodbudi njeno dosledno uporabo.

Člen 20
Postopek sodelovanja in usklajevalni postopek

Vsak nadzorni organ prispeva k dosledni uporabi te uredbe v vsej Uniji. V ta namen nadzorni organi sodelujejo med seboj in s Komisijo v skladu s poglavjem VII Uredbe (EU) 2016/679 v zvezi z zadevami iz te uredbe.

POGLAVJE V
PRAVNA SREDSTVA, ODGOVORNOST IN KAZNI

Člen 21
Pravna sredstva

1. Brez poseganja v katero koli drugo upravno ali pravno sredstvo ima vsak končni uporabnik elektronskih komunikacijskih storitev na voljo enaka pravna sredstva, določena v členih 77, 78 in 79 Uredbe (EU) 2016/679.

2. Vsaka fizična ali pravna oseba, ki ni končni uporabnik, na katero so negativno vplivale kršitve te uredbe in ima zakoniti interes za prenehanje ali prepoved domnevnih kršitev, vključno s ponudnikom elektronskih komunikacijskih storitev, ki ščiti svoje zakonite poslovne interese, ima pravico, da v zvezi s takimi kršitvami vloži pravno sredstvo pri sodišču.

Člen 22
Pravica do odškodnine in odgovornost

Vsak končni uporabnik elektronskih komunikacijskih storitev, ki je zaradi kršitve te uredbe utrpel premoženjsko ali nepremoženjsko škodo, ima pravico, da od kršitelja dobi odškodnino za nastalo škodo, razen če kršitelj dokaže, da nikakor ni odgovoren za dogodek, ki povzroči škodo v skladu s členom 82 Uredbe (EU) 2016/679.

Člen 23
Splošni pogoji za naložitev upravnih glob

1. Za namene tega člena se za kršitve te uredbe uporablja poglavje VII Uredbe (EU) 2016/679.

2. V skladu z odstavkom 1 se za kršitve naslednjih določb te uredbe uporabljajo upravne globe v znesku do 10 000 000 EUR ali v primeru družbe v znesku do 2 % skupnega svetovnega letnega prometa v preteklem proračunskem letu, odvisno od tega, kateri znesek je višji:

(a) obveznosti vsake pravne ali fizične osebe, ki obdeluje elektronske komunikacijske podatke v skladu s členom 8;

(b) obveznosti ponudnika programske opreme, ki omogoča elektronske komunikacije v skladu s členom 10;

(c) obveznosti ponudnika javno dostopnih direktorijev v skladu s členom 15;

(d) obveznosti vsake pravne ali fizične osebe, ki uporablja elektronske komunikacijske storitve v skladu s členom 16.

3. V skladu z odstavkom 1 tega člena se za kršitve načela zaupnosti komunikacij, dovoljene obdelave elektronskih komunikacijskih podatkov, rokov za izbris iz členov 5, 6 in 7 uporabljajo upravne globe v znesku do 20 000 000 EUR ali v primeru družbe v znesku do 4 % skupnega svetovnega letnega prometa v preteklem proračunskem letu, odvisno od tega, kateri znesek je višji.

4. Države članice določijo predpise o kaznih za kršitve členov 12, 13, 14 in 17.

5. Za neupoštevanje odredbe, ki jo izda nadzorni organ, iz člena 18 se uporabljajo upravne globe v znesku do 20 000 000 EUR ali v primeru družbe v znesku do 4 %

skupnega svetovnega letnega prometa v preteklem proračunskem letu, odvisno od tega, kateri znesek je višji.

6. Brez poseganja v popravljalna pooblastila nadzornih organov na podlagi člena 18 lahko vsaka država članica določi pravila o tem, ali in v kolikšni meri se lahko javnim organom in telesom s sedežem v zadevni državi članici naložijo upravne globe.

7. Nadzorni organ izvaja pooblastila iz tega člena na podlagi ustreznih postopkovnih zaščitnih ukrepov v skladu s pravom Unije in pravom države članice, vključno z učinkovitim pravnim sredstvom in ustreznim pravnim postopkom.

8. Kadar pravni sistem države članice ne določa upravnih glob, se lahko ta člen uporablja tako, da pristojni nadzorni organ sproži postopek za naložitev globe, pristojna nacionalna sodišča pa jo izrečejo, pri čemer mora biti zagotovljeno, da so ta pravna sredstva učinkovita in imajo enak učinek, kot ga imajo upravne globe, ki jih naložijo nadzorni organi. V vsakem primeru pa so globe učinkovite, sorazmerne in odvračilne. Te države članice Komisijo uradno obvestijo o določbah svojih zakonov, ki jih sprejmejo na podlagi tega odstavka do [xxx], brez odlašanja pa tudi o vseh nadaljnjih spremembah teh predpisov ali spremembah, ki vplivajo nanje.

Člen 24
Kazni

1. Države članice določijo pravila o drugih kaznih, ki se uporabljajo za kršitve te uredbe, zlasti za kršitve, za katere se ne uporabljajo upravne globe v skladu s členom 23, in sprejmejo vse potrebne ukrepe za zagotovitev, da se te kazni izvajajo. Te kazni morajo biti učinkovite, sorazmerne in odvračilne.

2. Vsaka država članica Komisijo uradno obvesti o določbah svojih zakonov, ki jih sprejme na podlagi odstavka 1, najpozneje 18 mesecev po datumu, določenem v členu 29(2), in brez odlašanja tudi o vsakršni naknadni spremembi, ki nanje vpliva.

POGLAVJE VI
DELEGIRANI IN IZVEDBENI AKTI

Člen 25
Izvajanje pooblastila

1. Pooblastilo za sprejetje delegiranih aktov se Komisiji podeli pod pogoji, določenimi v tem členu.

2. Pooblastilo za sprejemanje delegiranih aktov iz člena 8(4) se prenese na Komisijo za nedoločen čas od [datuma začetka veljavnosti te uredbe].

3. Prenos pooblastila iz člena 8(4) lahko kadar koli prekliče Evropski parlament ali Svet. S sklepom o preklicu preneha veljati podelitev pooblastila iz navedenega sklepa. Sklep začne učinkovati dan po njegovi objavi v *Uradnem listu Evropske unije* ali na poznejši dan, ki je določen v navedenem sklepu. Sklep ne vpliva na veljavnost že veljavnih delegiranih aktov.

4. Komisija se pred sprejetjem delegiranega akta posvetuje s strokovnjaki, ki jih imenujejo vse države članice, v skladu z načeli, določenimi v Medinstitucionalnem sporazumu o boljši pripravi zakonodaje z dne 13. aprila 2016.

5. Komisija takoj po sprejetju delegiranega akta o njem sočasno uradno obvesti Evropski parlament in Svet.

6. Delegirani akt, sprejet na podlagi člena 8(4), začne veljati le, če mu niti Evropski parlament niti Svet ne nasprotujeta v roku dveh mesecev od uradnega obvestila Evropskemu parlamentu in Svetu o tem aktu ali če pred iztekom tega roka tako Evropski parlament kot Svet obvestita Komisijo, da mu ne bosta nasprotovala. Ta rok se na pobudo Evropskega parlamenta ali Sveta podaljša za dva meseca.

Člen 26
Odbor

1. Komisiji pomaga Odbor za komunikacije, ustanovljen na podlagi člena 110 [Direktive o Evropskem zakoniku o elektronskih komunikacijah]. Ta odbor je odbor v smislu Uredbe (EU) št. 182/2011[12].

2. Pri sklicevanju na ta odstavek se uporablja člen 5 Uredbe (EU) št. 182/2011.

POGLAVJE VII
KONČNE DOLOČBE

Člen 27
Razveljavitev

1. Direktiva 2002/58/ES se razveljavi z učinkom od 25. maja 2018.

2. Sklicevanja na razveljavljeno direktivo se štejejo kot sklicevanja na to uredbo.

Člen 28
Klavzula o spremljanju in oceni

Komisija najpozneje do 1. januarja 2018 določi podroben program za spremljanje učinkovitosti te uredbe.

Komisija najpozneje tri leta po začetku uporabe te uredbe in nato vsaka tri leta oceni to uredbo in glavne ugotovitve predloži Evropskemu parlamentu in Svetu ter Evropskemu ekonomsko-socialnemu odboru. Na podlagi zadevne ocene se po potrebi pripravi predlog spremembe ali razveljavitve te uredbe ob upoštevanju pravnega, tehničnega ali gospodarskega razvoja.

Člen 29
Začetek veljavnosti in uporaba

1. Ta uredba začne veljati dvajseti dan po objavi v *Uradnem listu Evropske unije*.

2. Uporablja se od 25. maja 2018.

[12] Uredba (EU) št. 182/2011 Evropskega parlamenta in Sveta z dne 16. februarja 2011 o določitvi splošnih pravil in načel, na podlagi katerih države članice nadzirajo izvajanje izvedbenih pooblastil Komisije (UL L 55, 28.2.2011, str. 13–18).

Ta uredba je v celoti zavezujoča in se neposredno uporablja v vseh državah članicah.

V Bruslju,

Za Evropski parlament	*Za Svet*
Predsednik	*Predsednik*