EIROPAS
KOMISIJA

Briselē, 10.1.2017.
COM(2017) 10 final

2017/0003 (COD)

Priekšlikums

EIROPAS PARLAMENTA UN PADOMES REGULA

par privātās dzīves neaizskaramību un personas datu aizsardzību elektronisko sakaru jomā un ar ko atceļ Direktīvu 2002/58/EK (Privātuma un elektronisko sakaru regula)

(Dokuments attiecas uz EEZ)

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

PASKAIDROJUMA RAKSTS

1. PRIEKŠLIKUMA KONTEKSTS

1.1. Priekšlikuma pamatojums un mērķi

Digitālā vienotā tirgus stratēģijas ("**DVT stratēģija**")[1] mērķis ir palielināt uzticību digitālajiem pakalpojumiem un to drošību. Datu aizsardzības regulējuma reforma, jo īpaši Regulas (ES) 2016/679, Vispārīgās datu aizsardzības regulas ("**VDAR**")[2], pieņemšana, bija nozīmīgs solis šajā saistībā. DVT stratēģijas ietvaros arī tika paziņots par Direktīvas 2002/58/EK ("**E-privātuma direktīva**") [3]pārskatīšanu, lai nodrošinātu augsta līmeņa privātuma aizsardzību elektronisko sakaru pakalpojumu lietotājiem un vienlīdzīgus konkurences apstākļus visiem tirgus dalībniekiem. Šajā priekšlikumā tiek pārskatīta E-privātuma direktīva, paredzot DVT stratēģijas mērķus un nodrošinot konsekvenci ar VDAR.

E-privātuma direktīva nodrošina pamattiesību un pamatbrīvību aizsardzību, jo īpaši privātās dzīves neaizskaramību, sakaru konfidencialitāti un personas datu aizsardzību elektronisko sakaru nozarē. Tā arī garantē elektronisko sakaru datu, aprīkojuma un pakalpojumu brīvu apriti Savienībā. Ar to Savienības sekundārajos tiesību aktos ievieš pamattiesības uz privātās dzīves neaizskaramību attiecībā uz sakariem, kā noteikts Eiropas Savienības Pamattiesību hartas ("**Harta**") 7. pantā.

Saskaņā ar labāka regulējuma prasībām Komisija īstenoja E-privātuma direktīvas *ex post* Normatīvās atbilstības un izpildes programmu ("***REFIT* izvērtējums**"). No izvērtējuma izriet, ka spēkā esošā regulējuma mērķi un principi joprojām ir derīgi. Tomēr kopš pēdējās E-privātuma direktīvas pārskatīšanas 2009. gadā tirgū notikusi nozīmīga tehnoloģiskā un ekonomiskā attīstība. Patērētāji un uzņēmumi arvien vairāk paļaujas uz jauniem interneta pakalpojumiem, kas sniedz iespēju tradicionālo sakaru pakalpojumu vietā izmantot starppersonu sakaru pakalpojumus, piemēram, IP balss pārraidi, tūlītēju ziņapmaiņu un tīmekļa e-pasta pakalpojumus. Uz šiem "*Over-the-Top*" ("***OTT***") sakaru pakalpojumiem parasti neattiecas pašreizējais Savienības elektronisko sakaru regulējums, tai skaitā E-privātuma direktīva. Tādēļ direktīvā nav ņemta vērā tehnoloģiju attīstība, un attiecīgi ar jaunajiem pakalpojumiem nodrošinātie sakari nav aizsargāti.

1.2. Atbilstība pašreizējiem noteikumiem konkrētajā politikas jomā

Šis priekšlikums ir VDAR *lex specialis*, un tas konkretizēs un papildinās VDAR attiecībā uz elektronisko sakaru datiem, kuri kvalificējami kā personas dati. Visus jautājumus, kas attiecas uz personas datu apstrādi un nav konkrēti aplūkoti priekšlikumā, aptver VDAR. Veicot saskaņošanu ar VDAR, daži noteikumi tika atcelti, piemēram, E-privātuma direktīvas 4. panta drošības pienākumi.

---

1 Komisijas paziņojums Eiropas Parlamentam, Padomei, Eiropas Ekonomikas un sociālo lietu komitejai un Reģionu komitejai "Digitālā vienotā tirgus stratēģija Eiropai", COM(2015)192 *final*.

2 Eiropas Parlamenta un Padomes 2016. gada 27. aprīļa Regula (ES) 2016/679 par fizisku personu aizsardzību attiecībā uz personas datu apstrādi un šādu datu brīvu apriti un ar ko atceļ Direktīvu 95/46/EK (Vispārīgā datu aizsardzības regula), OV L 119, 4.5.2016., 1.–88. lpp.

3 Eiropas Parlamenta un Padomes 2002. gada 12. jūlija Direktīva 2002/58/EK par personas datu apstrādi un privātās dzīves aizsardzību elektronisko komunikāciju nozarē (direktīva par privāto dzīvi un elektronisko komunikāciju), OV L 201, 31.7.2002., 37. lpp.

1.3. Atbilstība pārējiem Savienības politikas virzieniem

E-privātuma direktīva ietilpst elektronisko sakaru tiesiskajā regulējumā. Komisija 2016. gadā pieņēma priekšlikumu direktīvai par Eiropas Elektronisko sakaru kodeksa izveidi ("**EESK**")[4], ar ko pārskata regulējumu. Lai gan šis priekšlikums nav EESK neatņemama daļa, tajā daļēji izmantotas EESK sniegtās definīcijas, tostarp "elektronisko sakaru pakalpojumu" definīcija. Tāpat kā EESK arī šī priekšlikuma piemērošanas jomā iekļauti *OTT* pakalpojumu sniedzēji, lai tādējādi atspoguļotu faktisko situāciju tirgū. Turklāt EESK papildina šo priekšlikumu, garantējot elektronisko sakaru pakalpojumu drošību.

Radioiekārtu direktīva 2014/53/ES ("**RID**")[5] nodrošina vienotu tirgu radioiekārtām. Konkrētāk, tajā paredz, ka pirms laišanas tirgū radioiekārtās jāietver drošības pasākumi, kas nodrošina lietotāja personas datu un privātuma aizsardzību. Saskaņā ar RID un Eiropas standartizācijas regulu (ES) Nr. 1025/2012[6] Komisijai ir pilnvaras pieņemt pasākumus. Šis priekšlikums neattiecas uz RID.

Priekšlikums neietver konkrētus noteikumus datu saglabāšanas jomā. Tajā saglabāta E-privātuma direktīvas 15. panta būtība, kura saskaņota ar VDAR 23. panta konkrēto formulējumu, kas dod pamatu dalībvalstīm ierobežot E-privātuma direktīvas konkrētos pantos minēto tiesību un pienākumu tvērumu. Tādējādi dalībvalstis drīkst saglabāt valsts regulējumu datu saglabāšanas jomā vai izveidot jaunu, kas cita starpā paredz mērķtiecīgus saglabāšanas pasākumus, ja vien šāds regulējums atbilst Savienības tiesību aktiem, ņemot vērā Tiesas judikatūru par E-privātuma direktīvas un Pamattiesību hartas interpretāciju[7].

Visbeidzot, priekšlikums neattiecas uz Savienības iestāžu, struktūru un aģentūru darbību. Tomēr tā principi un atbilstošie pienākumi attiecībā uz tiesībām uz privātās dzīves un sakaru neaizskaramību saistībā ar elektronisko sakaru datu apstrādi ir iekļauti priekšlikumā regulai, ar ko atceļ Regulu (EK) Nr. 45/2001[8].

2. JURIDISKAIS PAMATS, SUBSIDIARITĀTE UN PROPORCIONALITĀTE

2.1. Juridiskais pamats

Priekšlikuma atbilstošais juridiskais pamats ir Līguma par Eiropas Savienības darbību ("**LESD**") 16. pants un 114. pants.

LESD 16. pantā ir paredzēts īpašs juridiskais pamats, kas izmantojams, lai pieņemtu noteikumus par fizisko personu aizsardzību attiecībā uz Savienības iestāžu veikto personas datu apstrādi, kā arī personas datu apstrādi, ko veic dalībvalstis saistībā ar Savienības tiesību

---

4 Komisijas priekšlikums Eiropas Parlamenta un Padomes direktīvai par Eiropas Elektronisko sakaru kodeksa izveidi (pārstrādāta redakcija) (COM/2016/0590 *final* – 2016/0288 (COD)).

5 Eiropas Parlamenta un Padomes 2014. gada 16. aprīļa Direktīva 2014/53/ES par dalībvalstu tiesību aktu saskaņošanu attiecībā uz radioiekārtu pieejamību tirgū un ar ko atceļ Direktīvu 1999/5/EK (OV L 153, 22.5.2014., 62.–106. lpp.).

6 Eiropas Parlamenta un Padomes 2012. gada 25. oktobra Regula (ES) Nr. 1025/2012 par Eiropas standartizāciju, ar ko groza Padomes Direktīvas 89/686/EEK un 93/15/EEK un Eiropas Parlamenta un Padomes Direktīvas 94/9/EK, 94/25/EK, 95/16/EK, 97/23/EK, 98/34/EK, 2004/22/EK, 2007/23/EK, 2009/23/EK un 2009/105/EK, un ar ko atceļ Padomes Lēmumu 87/95/EEK un Eiropas Parlamenta un Padomes Lēmumu Nr. 1673/2006/EK (OV L 316, 14.11.2012., 12.–33. lpp.).

7 Sk. apvienotās lietas C-293/12 un C-594/12, *Digital Rights Ireland un Seitlinger u. c.*, ECLI:EU:C:2014:238; apvienotās lietas C-203/15 un C-698/15, *Tele2 Sverige AB un Secretary of State for the Home Department*, ECLI:EU:C:2016:970.

8 Eiropas Parlamenta un Padomes 2000. gada 18. decembra Regula (EK) Nr. 45/2001 par fizisku personu aizsardzību attiecībā uz personas datu apstrādi Kopienas iestādēs un struktūrās un par šādu datu brīvu apriti (OV L 8, 12.1.2001., 1.–22. lpp.).

aktu piemērošanas jomu, un noteikumus par šādu datu brīvu apriti. Tā kā elektroniskā saziņa, kurā iesaistīta fiziska persona, parasti tiek uzskatīta par saistītu ar personas datiem, fizisko personu aizsardzība attiecībā uz sakaru privātumu un šādu datu apstrādi jābalsta uz 16. pantu.

Turklāt priekšlikuma mērķis ir aizsargāt juridisko personu sakarus un saistītās likumīgās intereses. Hartas 7. pantā minēto tiesību nozīme un tvērums saskaņā ar Hartas 52. panta 3. punktu ir tāda pati kā Eiropas Cilvēktiesību un pamatbrīvību aizsardzības konvencijas ("**ECTK**") 8. panta 1. punktā paredzētā. Attiecībā uz Hartas 7. panta piemērošanas jomu Eiropas Savienības Tiesas ("**EST**")[9] un Eiropas Cilvēktiesību tiesas[10] judikatūra apstiprina, ka juridisko personu profesionālo darbību nedrīkst izslēgt no to tiesību aizsardzības, kas garantētas Hartas 7. pantā un ECTK 8. pantā.

Tā kā iniciatīvai ir divējāds mērķis, un tā juridisko personu sakaru aizsardzības aspekts un mērķis izveidot šo elektronisko sakaru iekšējo tirgu un nodrošināt tā darbību šajā saistībā nevar būt uzskatāmi par nejaušiem, iniciatīvai tādējādi arī jābūt balstītai uz LESD 114. pantu.

2.2. Subsidiaritāte

Sakaru neaizskaramība ir Hartā atzītas pamattiesības. Elektronisko sakaru saturs var atklāt ļoti sensitīvu informāciju par saziņā iesaistītajiem galalietotājiem. Tāpat arī elektronisko sakaru metadati var būt ļoti sensitīva un personiska informācija, kā to skaidri atzinusi EST[11]. Vairums dalībvalstu arī atzīst nepieciešamību aizsargāt sakarus, jo uzskata tās par atsevišķām konstitucionālajām tiesībām. Lai gan ir iespējams dalībvalstīs ieviest politiku, kas nodrošina šo tiesību ievērošanu, to nevarētu sasniegt saskaņotā veidā, jo nepastāv Savienības noteikumi, un tas radītu ar elektronisko sakaru pakalpojumu izmantošanu saistītu personas datu un datu, kas nav personas dati, pārrobežu plūsmu ierobežojumus. Visbeidzot, lai saglabātu konsekvenci ar VDAR, ir jāpārskata E-privātuma direktīva un jāpieņem pasākumi, ar ko varētu saskaņot abus instrumentus.

Tehnoloģiju attīstība un DVT stratēģijas vērienīgums ir stiprinājuši pamatu rīcībai Savienības līmenī. ES DVT panākumi ir atkarīgi no tā, cik efektīvi ES novērš neviendabīgumu valstu starpā un šķēršļus un izmanto Eiropas digitālā vienotā tirgus priekšrocības un ekonomikas. Turklāt, tā kā internetam un digitālajām tehnoloģijām nav robežu, nevar uzskatīt, ka problēma skar tikai vienas dalībvalsts teritoriju. Dalībvalstis nevar efektīvi atrisināt problēmas pašreizējā situācijā. DVT pienācīgas darbības nodrošināšanas prasības ir vienlīdzīgi konkurences apstākļi operatoriem, nodrošinot aizstājamus pakalpojumus un galalietotāju vienādu aizsardzību.

2.3. Proporcionalitāte

Lai nodrošinātu privātuma un sakaru neaizskaramības efektīvu juridisko aizsardzību, ir nepieciešams paplašināt piemērošanas jomu, lai aptvertu *OTT* pakalpojumu sniedzējus. Lai gan vairāki populāri *OTT* pakalpojumu sniedzēji jau atbilst vai daļēji atbilst sakaru konfidencialitātes principam, nozares pārstāvji nevar paši regulēt pamattiesību aizsardzību. Pieaug arī galiekārtu privātuma efektīvas aizsardzības nozīme, jo tās kļuvušas nepieciešamas privātajā dzīvē un profesionālajā jomā, lai uzglabātu sensitīvu informāciju. E-privātuma direktīvas īstenošana nav bijusi efektīva saistībā ar iespēju sniegšanu galalietotājiem. Tādēļ

---

9 Sk. C-450/06 *Varec SA*, ECLI:EU:C:2008:91, 48. punkts.

10 Sk. cita starpā ECT, spriedumi lietā *Niemietz pret Vāciju*, 1992. gada 16. decembra spriedums, A sērija Nr. 251-B, 29. punkts; *Société Colas Est u. c. pret Franciju*, Nr. 37971/97, 41. punkts; ECT 2002-III; *Peck pret Apvienoto Karalisti*, Nr. 44647/98, 57. punkts, ECT 2003-I; kā arī *Vinci Construction un GTM Génie Civil et Services pret Franciju*, Nr. 63629/10 un 60567/10, 63. punkts, 2015. gada 2. aprīlis.

11 Sk. 7. zemsvītras piezīmi.

mērķa sasniegšanai ir nepieciešama tāda principa ieviešana, saskaņā ar kuru centralizē piekrišanu programmatūras ietvaros un sniedz lietotājiem informāciju par tās privātuma iestatījumiem. Attiecībā uz šīs regulas īstenošanu priekšlikums balstās uz uzraudzības iestādēm un VDAR konsekvences mehānismu. Turklāt priekšlikums sniedz iespēju dalībvalstīm pieņemt valsts atkāpes pasākumus konkrētiem likumīgiem mērķiem. Tādējādi priekšlikums aptver tikai to, kas ir nepieciešams mērķu sasniegšanai, un atbilst samērīguma principam saskaņā ar Līguma par Eiropas Savienību 5. pantu. Attiecīgajiem pakalpojumiem piemērojamie pienākumi ir pēc iespējas minimālāki, vienlaikus neapdraudot attiecīgās pamattiesības.

2.4. Juridiskā instrumenta izvēle

Komisija izvirza priekšlikumu regulai, lai nodrošinātu konsekvenci ar VDAR un juridisko noteiktību lietotājiem un uzņēmumiem, novēršot atšķirīgu interpretāciju dalībvalstīs. Regula var nodrošināt lietotāju vienādu aizsardzības līmeni visā Savienībā un zemākas atbilstības izmaksas uzņēmumiem, kas darbojas ārvalstīs.

3. *EX POST* IZVĒRTĒJUMU, APSPRIEŠANĀS AR IEINTERESĒTAJĀM PERSONĀM UN IETEKMES NOVĒRTĒJUMU REZULTĀTI

3.1. *Ex post* izvērtējumi / spēkā esošo tiesību aktu atbilstības pārbaude

REFIT izvērtējumā tika aplūkots, cik efektīvi E-privātuma direktīva ir veicinājusi privātās dzīves neaizskaramības un sakaru konfidencialitātes pienācīgu aizsardzību ES. Tā mērķis bija arī noteikt iespējamo dublēšanos.

REFIT izvērtējumā secināts, ka direktīvas iepriekšējie mērķi joprojām ir **nozīmīgi.** Lai gan VDAR nodrošina personas datu aizsardzību, E-privātuma direktīva nodrošina tādu sakaru konfidencialitāti, kas var ietvert arī datus, kas nav personas dati, un ar juridisku personu saistītus datus. Tādēļ ar atsevišķu instrumentu būtu jānodrošina Hartas 7. panta efektīva aizsardzība. Citi noteikumi, piemēram, noteikumi par nepasūtītu tirgvedības paziņojumu sūtīšanu, arī joprojām ir nozīmīgi.

Efektivitātes un lietderības ziņā *REFIT* izvērtējumā atklāts, ka ar direktīvu nav pilnībā izpildīti tās mērķi. Konkrētu noteikumu neskaidra izstrāde un juridisko jēdzienu nenoteiktība ir apdraudējusi saskaņošanu, tādējādi radot problēmas uzņēmumiem saistībā ar darbību ārvalstīs. Izvērtējumā arī konstatēts, ka daži noteikumi ir radījuši nevajadzīgu slogu uzņēmumiem un patērētājiem. Piemēram, piekrišanas noteikums, kas paredzēja aizsargāt galiekārtu konfidencialitāti, neļāva sasniegt iecerētos mērķus, jo galalietotāji, nesaprotot to nozīmi, saskaras ar pieprasījumiem pieņemt pastāvīgās sīkdatnes, un dažos gadījumos sīkdatnes pat tiek izmantotas bez viņu piekrišanas. Piekrišanas noteikums ir pārāk iekļaujošs, jo tas aptver arī iejaukšanās praksi, kas neskar privātumu, taču tajā pašā laikā tas neiekļauj visu, jo skaidri neaptver dažas izsekošanas metodes (piem., "pirkstu nospiedumu lasītāju"), kas ne vienmēr ietver piekļuvi ierīcei vai datu glabāšanu tajā. Visbeidzot, tās ieviešana var būt dārga uzņēmumiem.

Izvērtējumā konstatēts, ka, ņemot vērā elektronisko sakaru tirgu, kas aizvien lielākā mērā kļūst pārnacionāls, e-privātuma noteikumiem joprojām ir **ES pievienotā vērtība**, jo tie ļauj labāk sasniegt mērķi nodrošināt privātumu tiešsaistē. Tajā arī apliecināts, ka kopumā noteikumi ir **saskaņoti** ar citiem atbilstošiem tiesību aktiem, lai gan tika konstatēti daži dublēšanās gadījumi ar jauno VDAR (sk. 1.2. apakšpunktu).

3.2. Apspriešanās ar ieinteresētajām personām

Komisija organizēja sabiedrisko apspriešanos no 2016. gada 12. aprīļa līdz 5. jūlijam un saņēma 421 atbildi[12]. Galvenie konstatējumi ir šādi[13].

– **Īpašu noteikumu nepieciešamība elektronisko sakaru nozarē par elektronisko sakaru konfidencialitāti**: 83,4 % atbildējušo iedzīvotāju, patērētāju un pilsoniskās sabiedrības organizāciju un 88,9 % publisko iestāžu piekrīt, bet 63,4 % atbildējušo nozares pārstāvju nepiekrīt.

– **Piemērošanas jomas paplašināšana, iekļaujot jaunus sakaru pakalpojumus (*OTT*)**: 76 % iedzīvotāju un pilsoniskās sabiedrības pārstāvju un 93,1 % publisko iestāžu piekrīt šādai paplašināšanai, bet tikai 36,2 % atbildējušo nozares pārstāvju to atbalsta.

– **Tādu atbrīvojumu maiņa, ko piešķir attiecībā uz informācijas plūsmas un atrašanās vietas datu apstrādi dotai piekrišanai**: 49,1 % iedzīvotāju, patērētāju un pilsoniskās sabiedrības organizāciju un 36 % publisko iestāžu dod priekšroku atbrīvojumu nepaplašināšanai, bet 36 % nozares pārstāvju atbalsta plašākus atbrīvojumus, kā arī 2/3 nozares pārstāvju atbalsta noteikumu vienkāršu atcelšanu.

– **Atbalsts risinājumiem, kas piedāvāti attiecībā uz piekrišanu sīkdatņu izmantošanai**: 81,2 % iedzīvotāju un 63 % publisko iestāžu atbalsta pienākumu noteikšanu galiekārtu ražotājiem attiecībā uz tādu produktu tirdzniecību, kuros aktivizēti iestatījumi par privātuma aizsardzību pēc noklusējuma, bet 58,3 % nozares pārstāvju dod priekšroku iespējai atbalstīt pašregulēšanu/kopregulēšanu.

Turklāt 2016. gada aprīlī Eiropas Komisija organizēja divus darbseminārus (vienā varēja piedalīties visas ieinteresētās personas, bet otrā – valstu kompetentās iestādes), kuros tika aplūkoti galvenie sabiedriskās apspriešanas jautājumi. Darbseminārос paustie viedokļi atspoguļoja sabiedriskās apspriešanas rezultātu.

Lai uzzinātu iedzīvotāju viedokli, visā ES veica Eirobarometra pētījumu par e-privātumu[14]. Galvenie konstatējumi ir šādi[15].

– 78 % respondentu uzskata, ka ir ļoti būtiski, lai privātā informācija viņu datorā, viedtālrunī vai planšetdatorā būtu pieejama tikai ar viņu atļauju.

– 72 % respondentu norāda, ka ir ļoti svarīgi garantēt e-pastu un tiešsaistes tūlītējās ziņapmaiņas konfidencialitāti.

– 89 % respondentu piekrīt ierosinātajai iespējai, ka viņu pārlūkprogrammas noklusējuma iestatījumiem būtu jāaptur viņu informācijas kopīgošana.

3.3. Ekspertu atzinumu pieprasīšana un izmantošana

Komisija izmantoja šādus ārējo ekspertu ieteikumus.

---

12 162 atbildes no iedzīvotājiem, 33 — no pilsoniskās sabiedrības un patērētāju organizācijām; 186 — no nozares pārstāvjiem, 40 — no publiskajām iestādēm, tostarp kompetentajām iestādēm, kas ievieš E-privātuma direktīvu.

13 Pilns ziņojums pieejams vietnē: https://ec.europa.eu/digital-single-market/news-redirect/37204.

14 2016. gada Eirobarometra pētījums (EB) 443 par e-privātumu (SMART 2016/079).

15 Pilns ziņojums pieejams vietnē: https://ec.europa.eu/digital-single-market/news-redirect/37205.

– Mērķtiecīgas konsultācijas ar ES ekspertu grupām: ar 29. pantu saistītās darba grupas atzinums; EDAU atzinums; *REFIT* platformas atzinums; *BEREC* viedokļi; *ENISA* viedokļi un Patērētāju aizsardzības un sadarbības tīkla dalībnieku viedokļi.

– Ārējo ekspertu atzinumi, jo īpaši divi turpmāk minētie pētījumi.

  – Pētījums "E-privātuma direktīva: novērtējums par transponēšanu, efektivitāti un saderību ar piedāvāto Datu aizsardzības regulu" (SMART 2013/007116).

  – Pētījums "Direktīvas 2002/58 par privāto dzīvi un elektronisko komunikāciju nozari izvērtēšana un pārskatīšana" (SMART 2016/0080).

3.4. Ietekmes novērtējums

Tika veikts šā priekšlikuma ietekmes novērtējums, un 2016. gada 28. septembrī Regulējuma kontroles padome sniedza pozitīvu atzinumu[16]. Lai īstenotu padomes ieteikumus, ietekmes novērtējumā labāk izskaidrota iniciatīvas piemērošanas joma, tās saskaņotība ar citiem juridiskajiem instrumentiem (VDAR, EESK, RID) un atsevišķa instrumenta nepieciešamība. Pamatscenārijs tika izvērsts plašāk un precizēts. Ietekmes analīze tika uzlabota un vairāk līdzsvarota, precizējot un uzlabojot paredzamo izmaksu un ieguvumu aprakstu.

Turpmāk minētie politikas varianti tika izpētīti saistībā ar efektivitātes, lietderības un saskaņotības kritērijiem:

– **1. variants:** neleģislatīvi (ieteikuma tiesību) pasākumi,

– **2. variants:** privātuma/konfidencialitātes ierobežota stiprināšana un vienkāršošana,

– **3. variants:** privātuma/konfidencialitātes samērīga stiprināšana un vienkāršošana,

– **4. variants:** privātuma/konfidencialitātes vērienīga stiprināšana un vienkāršošana,

– **5. variants:** E-privātuma direktīvas atcelšana.

Vairums aspektu apliecināja, ka **3. variants** ir **vēlamais variants** mērķu sasniegšanai, vienlaikus ņemot vērā tā efektivitāti un saskaņotību. Galvenie ieguvumi ir šādi.

– Elektronisko sakaru konfidencialitātes aizsardzības uzlabošana, paplašinot juridiskā instrumenta piemērošanas jomu, lai tajā iekļautu jaunus, funkcionāli līdzvērtīgus elektronisko sakaru pakalpojumus. Turklāt ar regulu tiek uzlabota galalietotāju kontrole, precizējot, ka piekrišanu var paust ar atbilstošiem tehniskajiem iestatījumiem.

– Aizsardzības uzlabošana pret nepasūtītiem paziņojumiem, ieviešot pienākumu nodrošināt izsaucošā numura noteikšanu vai obligātu prefiksu ar tirgvedību saistītiem zvaniem un uzlabojot iespējas bloķēt zvanus no nevēlamiem numuriem.

– Regulatīvās vides vienkāršošana un precizēšana, samazinot dalībvalstīm atvēlēto rīcības brīvību, atceļot novecojušus noteikumus un paplašinot izņēmumus attiecībā uz piekrišanas noteikumiem.

Paredzams, ka 3. varianta ekonomiskā ietekme kopumā būs samērīga ar priekšlikuma mērķiem. Darījumdarbības iespējas, kas saistītas ar sakaru datu apstrādi, ir izmantojamas saistībā ar tradicionālajiem elektronisko sakaru pakalpojumiem, taču uz *OTT* pakalpojumu sniedzējiem attiecina tos pašus noteikumus. Tas šiem operatoriem rada papildu atbilstības izmaksas. Tomēr šīs izmaiņas būtiski neietekmēs tos *OTT* pakalpojumu sniedzējus, kas jau

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

tagad savā darbībā ņem vērā piekrišanu. Visbeidzot, šī varianta ietekmi neizjutīs dalībvalstīs, kas jau ir paplašinājušas noteikumus, ietverot tajos *OTT* pakalpojumus.

Centralizējot piekrišanu programmatūras ietvaros, piemēram, interneta pārlūkprogrammās, un aicinot lietotājus izvēlēties privātuma iestatījumus, kā arī paplašinot izņēmumus attiecībā uz noteikumu par piekrišanu izmantot sīkdatnes, būtiska daļa uzņēmumu varētu likvidēt sīkdatņu reklāmkarogus un paziņojumus, tādējādi nodrošinot potenciāli ievērojamus izmaksu ietaupījumus un vienkāršošanu. Tomēr reklāmdevējiem, kas tiešsaistē izvieto mērķētu reklāmu, iespējams, būs sarežģītāk iegūt piekrišanu, ja liela daļa lietotāju izvēlēsies iestatījumus "noraidīt trešās personas sīkdatnes". Vienlaikus centralizēta piekrišana neliedz tīmekļa vietņu operatoriem iegūt piekrišanu ar individuāliem pieprasījumiem galalietotājiem, tādējādi saglabājot pašreizējo darījumdarbības modeli. Papildu izmaksas rastos dažiem pārlūkprogrammu vai līdzīgas programmatūras nodrošinātājiem, jo tiem būtu nepieciešams nodrošināt privātumu aizsargājošus iestatījumus.

Ārējā pētījumā tika noteikti trīs dažādi 3. varianta īstenošanas scenāriji saskaņā ar vienību, kas izveidos dialoglodziņu starp lietotāju, kurš izvēlējies iestatījumus "noraidīt trešās personas sīkdatnes" vai "neizsekot" un apmeklētajām tīmekļa vietnēm, kas vēlēsies, lai interneta lietotājs pārdomā. Par šo tehnisko uzdevumu var būt atbildīgas šādas vienības: 1) programmatūra, piemēram, interneta pārlūkprogrammas, 2) trešās personas izsekotājs, 3) atsevišķas tīmekļa vietnes (t. i., lietotāja pieprasītais informācijas sabiedrības pakalpojums). Salīdzinot ar pamatscenāriju, 3. variants kopumā ļautu ietaupīt līdzekļus attiecībā uz atbilstības izmaksām 70 % apmērā (EUR 948,8 miljonu lieli ietaupījumi) pirmajā scenārijā (pārlūkprogrammu risinājums), kas īstenots šajā priekšlikumā. Citos scenārijos izmaksu ietaupījumi būtu mazāki. Tā kā kopējie ietaupījumi lielā mērā ir saistīti ar skarto uzņēmumu skaita ļoti ievērojamu samazināšanos, paredzams, ka atbilstības izmaksu individuālais apjoms vienam uzņēmumam vidēji būtu augstāks nekā tagad.

3.5. Normatīvā atbilstība un vienkāršošana

Izvēlētā varianta ietvaros piedāvātie politikas pasākumi ir vērsti uz vienkāršošanas un administratīvā sloga samazināšanas mērķi saskaņā ar *REFIT* izvērtējumā un *REFIT* platformas atzinumā[17] izklāstītajiem konstatējumiem.

REFIT platforma Komisijai sniedza trīs ieteikumu kopumus.

– Saskaņojot E-privātuma direktīvu ar Vispārīgo datu aizsardzības regulu, efektīvā jāaizsargā iedzīvotāju privātā dzīve.

– Pievienojot izņēmumus noteikumam par piekrišanu sīkdatņu izmantošanai, efektīvāk jāaizsargā iedzīvotāji pret nepasūtītiem tirgvedības paziņojumiem.

– Komisija risina valstu īstenošanas problēmas un veicina paraugprakses apmaiņu dalībvalstu starpā.

Priekšlikumā īpaši paredzēti šādi aspekti.

– Tehnoloģiski neitrālu definīciju izmantošana ar mērķi saprast jaunos pakalpojumus un tehnoloģijas, lai nodrošinātu regulas atbilstību nākotnes prasībām.

– Drošības noteikumu atcelšana ar mērķi novērst regulatīvo dublēšanos.

– Piemērošanas jomas precizēšana ar mērķi palīdzēt novērst/samazināt risku, ka īstenošana var noritēt atšķirīgi katrā dalībvalstī (atzinuma 3. punkts).

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

– Tā piekrišanas noteikuma precizēšana un vienkāršošana, kas attiecas uz sīkdatņu un citu identifikatoru izmantošanu, kā skaidrots 3.1. un 3.4. apakšpunktā (atzinuma 2. punkts).

– Uzraudzības iestāžu darbības saskaņošana ar iestādēm, kas ir kompetentas ieviest VDAR, un paļaušanās uz VDAR konsekvences mehānismu.

3.6. Ietekme uz pamattiesībām

Priekšlikuma mērķis paredz nodrošināt saistībā ar elektroniskajiem sakariem apstrādāto personas datu un privātuma aizsardzības lielāku efektivitāti un augstāku līmeni atbilstīgi Hartas 7. un 8. pantam, kā arī lielāku juridisko noteiktību. Priekšlikums papildina un konkretizē VDAR. Sakaru konfidencialitātes efektīva aizsardzība ir būtiska vārda un informācijas brīvības un citu saistīto tiesību īstenošanā, piemēram, tiesību uz personas datu aizsardzību vai domas, apziņas un reliģijas brīvību īstenošanā.

4. IETEKME UZ BUDŽETU

Priekšlikums neietekmē Savienības budžetu.

5. CITI ELEMENTI

5.1. Īstenošanas plāni un uzraudzības, izvērtēšanas un ziņošanas kārtība

Komisija uzraudzīs regulas piemērošanu un iesniegs ziņojumu par tās izvērtēšanu Eiropas Parlamentam, Padomei un Eiropas Ekonomikas un sociālo lietu komitejai ik pēc trim gadiem. Šie ziņojumi būs publiski pieejami, un tajos būs detalizēti izklāstīta šīs regulas efektīvā piemērošana un izpilde.

5.2. Konkrētu priekšlikuma noteikumu sīkāks skaidrojums

Priekšlikuma I nodaļa ietver vispārējos noteikumus: priekšmets (1. pants), piemērošanas joma (2. un 3. pants) un definīcijas, ietverot atsauces uz attiecīgām definīcijām no citiem ES instrumentiem, piemēram, VDAR.

Priekšlikuma II nodaļa ietver galvenos noteikumus, ar ko nodrošina elektronisko sakaru konfidencialitāti (5. pants) un šādu sakaru datu apstrādes ierobežotos atļautos nolūkus un nosacījumus (6. un 7. pants). Tajā aplūkota arī galiekārtu aizsardzība, ko nodrošina, i) garantējot tajās saglabātās informācijas integritāti un ii) aizsargājot galiekārtu emitēto informāciju, jo tā var ļaut identificēt galalietotāju (8. pants). Visbeidzot, 9. pantā detalizēti aprakstīta galalietotāju piekrišana, šīs regulas galvenais likumīgais pamats, skaidri atsaucoties uz VDAR sniegto definīciju un nosacījumiem, bet 10. pantā paredzēts pienākums tādas programmatūras nodrošinātājiem, kas nodrošina elektroniskos sakarus, palīdzēt galalietotājiem pieņemt efektīvu izvēli par privātuma iestatījumiem. Priekšlikuma 11. pantā detalizēti aprakstīti nolūki un nosacījumi, kas attiecas uz dalībvalstīm iepriekš minēto noteikumu ierobežošanas gadījumā.

Priekšlikuma III nodaļa attiecas uz galalietotāju tiesībām kontrolēt elektronisko paziņojumu sūtīšanu un saņemšanu, lai aizsargātu to privātumu: i) galalietotāju tiesības liegt izsaucošā numura uzrādīšanu ar mērķi garantēt anonimitāti (12. pants) un šādas uzrādīšanas ierobežojumus (13. pants); ii) numuratkarīgu starppersonu sakaru pakalpojumu sniedzēju pienākums garantēt iespēju ierobežot nevēlamu zvanu saņemšanu (14. pants). Ar šo nodaļu arī regulē nosacījumus, saskaņā ar kuriem galalietotājus var iekļaut publiski pieejamos abonentu sarakstos (15. pants), un nosacījumus, saskaņā ar kuriem var sūtīt nepasūtītus paziņojumus attiecībā uz tiešo tirgvedību (17. pants). Tā arī attiecas uz drošības riskiem un paredz

elektronisko sakaru pakalpojumu sniedzēju pienākumu brīdināt galalietotājus tāda konkrēta riska gadījumā, kas var apdraudēt tīklu un pakalpojumu drošību. VDAR un EESK minētie drošības pienākumi attieksies uz elektronisko sakaru pakalpojumu sniedzējiem.

Priekšlikuma IV nodaļā ir paredzēta šīs regulas uzraudzība un izpilde, uzticot to uzraudzības iestādēm, kas ir atbildīgas par VDAR, un šajā saistībā ir ņemta vērā spēcīgā sinerģija starp vispārējiem datu aizsardzības jautājumiem un sakaru konfidencialitāti (18. pants). Eiropas Datu aizsardzības kolēģijas pilnvaras tiek paplašinātas (19. pants), un VDAR paredzētais sadarbības un konsekvences mehānisms tiks piemērots ar šo regulu saistītajos pārrobežu jautājumos (20. pants).

Priekšlikuma V nodaļā detalizēti izklāstīti galalietotājiem pieejamie dažādie tiesiskās aizsardzības līdzekļi (21. un 22. pants) un piemērojamās sankcijas (24. pants), ietverot administratīvo naudas sodu piemērošanas vispārējos nosacījumus (23. pants).

Priekšlikuma VI nodaļa ir saistīta ar deleģēto un īstenošanas aktu pieņemšanu saskaņā ar Līguma 290. un 291. pantu.

Visbeidzot, VII nodaļa ietverti šīs regulas nobeiguma noteikumi: E-privātuma direktīvas atcelšana, uzraudzība un pārskatīšana, stāšanās spēkā un piemērošana. Attiecībā uz pārskatīšanu Komisija plāno cita starpā izvērtēt, vai joprojām nepieciešams atsevišķs tiesību akts, ņemot vērā juridisko, tehnisko vai ekonomisko attīstību un ņemot vērā Regulas (ES) 2016/679 pirmo izvērtējumu, kas jāsniedz līdz 2020. gada 25. maijam.

2017/0003 (COD)

Priekšlikums

EIROPAS PARLAMENTA UN PADOMES REGULA

par privātās dzīves neaizskaramību un personas datu aizsardzību elektronisko sakaru jomā un ar ko atceļ Direktīvu 2002/58/EK (Privātuma un elektronisko sakaru regula)

(Dokuments attiecas uz EEZ)

EIROPAS PARLAMENTS UN EIROPAS SAVIENĪBAS PADOME,

ņemot vērā Līgumu par Eiropas Savienības darbību un jo īpaši tā 16. un 114. pantu,

ņemot vērā Eiropas Komisijas priekšlikumu,

pēc leģislatīvā akta projekta nosūtīšanas valstu parlamentiem,

ņemot vērā Eiropas Ekonomikas un sociālo lietu komitejas atzinumu[1],

ņemot vērā Reģionu komitejas atzinumu[2],

ņemot vērā Eiropas Datu aizsardzības uzraudzītāja atzinumu[3],

saskaņā ar parasto likumdošanas procedūru,

tā kā:

(1) Eiropas Savienības Pamattiesību hartas (turpmāk "Harta") 7. pants aizsargā ikvienas personas pamattiesības uz viņa/viņas privātās un ģimenes dzīves, mājokļa un saziņas neaizskaramību. Šo tiesību būtisks aspekts ir personas sakaru privātuma neaizskaramība. Elektronisko sakaru konfidencialitāte nodrošina, ka informācija, ar kuru puses apmainās, un šādas saziņas ārējie elementi (piemēram, kad, no kurienes un kam informācija nosūtīta) nav atklājami nevienam citam kā vien šajā saziņā iesaistītajām pusēm. Konfidencialitātes princips būtu jāpiemēro gan tagad izmantotajiem saziņas līdzekļiem, gan tiem, kas tiks izmantoti nākotnē, tostarp izsaukumiem, saziņai internetā, tūlītējās ziņapmaiņas lietotnēm, e-pastiem, zvaniem internetā un privātajai ziņapmaiņai sociālajos medijos.

(2) Elektronisko sakaru saturs par saziņā iesaistītajām fiziskām personām var atklāt īpaši sensitīvu informāciju – no personīgās pieredzes un emocijām līdz medicīniskajām problēmām, seksuālajai orientācijai un politiskajiem uzskatiem –, kuras izpaušana var radīt personisku un sociālu kaitējumu, ekonomisku zaudējumu vai apkaunojumu. Līdzīgā veidā ļoti sensitīvu un personisku informāciju var atklāt arī elektronisko sakaru metadati. Šie metadati ietver izsauktos numurus, apmeklētās tīmekļa vietnes, ģeogrāfisko atrašanās vietu, personas veiktā izsaukuma laiku, datumu un ilgumu, kā arī citu informāciju, kas ļauj izdarīt precīzus secinājumus par elektroniskajā saziņā

[1] OV C [...], [...], [...]. lpp.
[2] OV C [...], [...], [...]. lpp.
[3] OV C [...], [...], [...]. lpp.

iesaistīto personu privāto dzīvi, piemēram, par viņu sociālajām attiecībām, ikdienas paradumiem un nodarbēm, interesēm, gaumi utt.

(3) Elektronisko sakaru dati var arī atklāt informāciju par tiesību subjektiem, piemēram, komercnoslēpumus vai cita veida sensitīvu informāciju, kurai ir ekonomiska vērtība. Tādēļ šīs regulas noteikumi būtu jāpiemēro gan fiziskām, gan juridiskām personām. Turklāt ar šo regulu būtu jānodrošina Eiropas Parlamenta un Padomes Regulas (ES) 2016/679[4] noteikumu piemērošana galalietotājiem, kuri ir juridiskas personas. Tas attiecas arī uz Regulā (ES) 2016/679 definēto piekrišanu. Ja tiek izmantota atsauce uz piekrišanu, ko dod galalietotājs, ieskaitot juridiskas personas, būtu jāpiemēro šī definīcija. Juridiskām personām arī vajadzētu būt tādām pašām tiesībām attiecībā uz uzraudzības iestādēm kā galalietotājiem, kas ir fiziskas personas; turklāt šajā regulā uzraudzības iestādēm vajadzētu būt atbildīgām arī par šīs regulas piemērošanas uzraudzību attiecībā uz juridiskām personām.

(4) Saskaņā ar Hartas 8. panta 1. punktu un Līguma par Eiropas Savienības darbību 16. panta 1. punktu ikvienai personai ir tiesības uz savu personas datu aizsardzību. Regulā (ES) 2016/679 izklāstīti noteikumi par fizisku personu aizsardzību personas datu apstrādē un par personas datu brīvu apriti. Elektronisko sakaru datu vidū var būt personas dati, kas definēti Regulā (ES) 2016/679.

(5) Šīs regulas noteikumi konkretizē un papildina vispārīgos noteikumus par personas datu aizsardzību, kuri izklāstīti Regulā (ES) 2016/679 attiecībā uz elektronisko sakaru datiem, kas kvalificējami kā personas dati. Tāpēc šajā regulā netiek vājināta aizsardzība, kas fiziskām personām noteikta saskaņā ar Regulu (ES) 2016/679. Elektronisko sakaru datu apstrāde, ko veic elektronisko sakaru pakalpojumu sniedzēji, būtu jāatļauj tikai saskaņā ar šo regulu.

(6) Lai arī Eiropas Parlamenta un Padomes Direktīvas 2002/58/EK[5] principi un galvenie noteikumi joprojām ir kopumā pareizi, minētā direktīva vairs nav pilnībā atbilstīga tehnoloģiju un tirgus faktiskajai attīstībai, un tādēļ elektronisko sakaru jomā privātuma un konfidencialitātes aizsardzība kļūst nekonsekventa vai nepietiekami efektīva. Šāda attīstība cita starpā skar tādu elektronisko sakaru pakalpojumu ieviešanu tirgū, kas no patērētāju viedokļa var aizvietot tradicionālos pakalpojumus, bet attiecībā uz kuriem nav jāpanāk atbilstība tam pašam noteikumu kopumam. Tā attiecas arī uz jaunām metodēm, kas ļauj izsekot Direktīvā 2002/58/EK neaptverto galalietotāju uzvedību tiešsaistē. Tāpēc Direktīva 2002/58/EK būtu jāatceļ un jāaizstāj ar šo regulu.

(7) Lai nodrošinātu šīs regulas noteikumu efektīvu piemērošanu un interpretēšanu, dalībvalstīm būtu jādod iespēja, ievērojot šajā regulā noteiktos ierobežojumus, saglabāt vai ieviest valstu noteikumus, kuri vēl vairāk precizētu un izskaidrotu šīs regulas noteikumu piemērošanu. Tāpēc saistībā ar rīcības brīvību, kas šajā sakarā piešķirta dalībvalstīm, būtu jāievēro līdzsvars starp privātās dzīves un personas datu aizsardzību, no vienas puses, un elektronisko sakaru datu brīvu apriti, no otras puses.

(8) Šī regula būtu jāpiemēro elektronisko sakaru pakalpojumu sniedzējiem, publiski pieejamu abonentu sarakstu pakalpojumu sniedzējiem un programmatūras

---

[4] Eiropas Parlamenta un Padomes 2016. gada 27. aprīļa Regula (ES) 2016/679 par fizisku personu aizsardzību attiecībā uz personas datu apstrādi un šādu datu brīvu apriti un ar ko atceļ Direktīvu 95/46/EK (Vispārīgā datu aizsardzības regula) (OV L 119, 4.5.2016., 1.–88. lpp.).

[5] Eiropas Parlamenta un Padomes 2002. gada 12. jūlija Direktīva 2002/58/EK par personas datu apstrādi un privātās dzīves aizsardzību elektronisko komunikāciju nozarē (direktīva par privāto dzīvi un elektronisko komunikāciju) (OV L 201, 31.7.2002., 37. lpp.).

nodrošinātājiem, kuri dod iespēju izmantot elektroniskos sakarus, tostarp saistībā ar informācijas izguvi un parādīšanu internetā. Šī regula būtu jāpiemēro arī tādām fiziskām un juridiskām personām, kuras izmanto elektronisko sakaru pakalpojumus, lai nosūtītu tiešās tirgvedības komercpaziņojumus vai vāktu informāciju, kas saistīta ar galalietotāju galiekārtām vai tiek tajās saglabāta.

(9) Šī regula būtu jāpiemēro elektronisko sakaru datiem, kuri apstrādāti saistībā ar elektronisko sakaru pakalpojumu sniegšanu un izmantošanu Savienībā, neatkarīgi no tā, vai apstrāde notiek Savienībā vai ārpus tās. Turklāt, lai Savienībā galalietotājiem neliegtu efektīvu aizsardzību, šī regula būtu jāpiemēro arī elektronisko sakaru datiem, kas apstrādāti saistībā ar elektronisko sakaru pakalpojumiem, kurus no ārpussavienības valstīm sniedz galalietotājiem Savienībā.

(10) Savienības iekšējā tirgū laistajām radioiekārtām un to programmatūrai ir jāatbilst Eiropas Parlamenta un Padomes Direktīvai 2014/53/ES[6]. Šai regulai nevajadzētu skart Direktīvas 2014/53/ES prasību piemērojamību un Komisijas pilnvaras saskaņā ar Direktīvu 2014/53/ES pieņemt deleģētus aktus, kuros noteikts, ka konkrētās radioiekārtu kategorijās vai klasēs būtu jāietver drošības pasākumi, kuri nodrošinātu galalietotāju personas datu un privātuma aizsardzību.

(11) Pakalpojumi, ko izmanto sakaru nodrošināšanai, un to tehniskie līdzekļi ir ievērojami attīstījušies. Galalietotāji arvien vairāk aizstāj tradicionālos balss telefonijas, īsziņu (SMS) un elektroniskā pasta pārvades pakalpojumus ar funkcionāli līdzvērtīgiem tiešsaistes pakalpojumiem, kā IP balss pārraide, ziņapmaiņa un tīmekļa e-pasta pakalpojumi. Lai nodrošinātu, ka funkcionāli līdzvērtīgu pakalpojumu izmantošanā galalietotāji tiek efektīvi un vienādi aizsargāti, šajā regulā ir izmantota elektronisko sakaru pakalpojumu definīcija, kas sniegta [Eiropas Parlamenta un Padomes direktīvā par Eiropas Elektronisko sakaru kodeksa izveidi[7]]. Minētā definīcija ietver ne tikai interneta piekļuves pakalpojumus un pakalpojumus, kas pilnīgi vai daļēji ir signālu pārvade, bet arī starppersonu sakaru pakalpojumus, kas var būt un var nebūt numuratkarīgi, piemēram, piemēram, IP balss pārraidi, ziņapmaiņu un tīmekļa e-pasta pakalpojumus. Sakaru konfidencialitātes aizsardzībai ir būtiska nozīme arī starppersonu sakaru pakalpojumos, kurus sniedz papildus citam pakalpojumam; tādēļ šī regula būtu jāpiemēro šāda veida pakalpojumiem, kam arī ir saziņas funkcijas.

(12) Starp internetam pievienotām ierīcēm un iekārtām jeb mašīnām arvien vairāk iespējama saziņa elektronisko sakaru tīklos (lietu internets). Mašīnas-mašīnas sakaru pārraide ietver signālu pārvadi tīklā, un tādēļ to parasti uzskata par elektronisko sakaru pakalpojumu. Lai nodrošinātu tiesību uz privātumu un sakaru konfidencialitāti pilnīgu aizsardzību un veicinātu uzticamu un drošu lietu internetu digitālajā vienotajā tirgū, ir jāprecizē, ka šī regula būtu jāpiemēro mašīnas-mašīnas sakaru pārraidei. Tāpēc šajā regulā ietvertais konfidencialitātes princips būtu jāpiemēro arī attiecībā uz mašīnas-mašīnas sakaru pārraidi. Varētu noteikt arī konkrētus aizsardzības pasākumus saskaņā ar nozares tiesību aktiem, piemēram, Direktīvu 2014/53/ES.

(13) Attīstoties ātrām un efektīvām bezvadu tehnoloģijām, interneta pakalpojumi kļuvuši arvien pieejamāki sabiedrībai bezvadu tīklos, kuri publiskās un daļēji privātās vietās,

---

6 Eiropas Parlamenta un Padomes 2014. gada 16. aprīļa Direktīva 2014/53/ES par dalībvalstu tiesību aktu saskaņošanu attiecībā uz radioiekārtu pieejamību tirgū un ar ko atceļ Direktīvu 1999/5/EK (OV L 153, 22.5.2014., 62. lpp.).

7 Komisijas priekšlikums Eiropas Parlamenta un Padomes direktīvai par Eiropas Elektronisko sakaru kodeksa izveidi (pārstrādāta redakcija) (COM/2016/0590 *final* – 2016/0288 (COD)).

piemēram, dažādās pilsētas daļās, lielveikalos, tirdzniecības centros un slimnīcās, izvietotos tīklājos kļuvuši pieejami ikvienam. Šādos tīklos pārraidītu sakaru konfidencialitāte būtu jāaizsargā, ciktāl minētie sakaru tīkli ir paredzēti nenoteiktai galalietotāju grupai. Iespēja papildus citiem pakalpojumiem sniegt bezvadu elektronisko sakaru pakalpojumus nedrīkstētu radīt šķēršļus sakaru datu konfidencialitātes nodrošināšanai un šīs regulas piemērošanai. Tāpēc šī regula būtu jāpiemēro elektronisko sakaru datiem, kuru pārraidīšanai tiek izmantoti elektronisko sakaru pakalpojumi un publiskie sakaru tīkli. Taču tā nebūtu jāpiemēro slēgtām galalietotāju grupām, piemēram, korporatīviem tīkliem, kuriem piekļūt var tikai konkrētās organizācijas locekļi.

(14) Elektronisko sakaru dati ir jādefinē pietiekami plaši un tehnoloģiju ziņā neitrāli tā, lai aptvertu visu informāciju, kas attiecas uz pārraidīto vai apmaiņā nosūtīto saturu (elektronisko sakaru saturu), un informāciju par elektronisko sakaru pakalpojumu galalietotāju, kas apstrādāta nolūkā to pārraidīt, izplatīt vai nodrošināt iespēju veikt elektronisko sakaru satura apmaiņu; tas attiecas arī uz datiem, ko izmanto, lai izsekotu un identificētu paziņojuma avotu un galamērķi, ģeogrāfisko atrašanās vietu, kā arī saziņas datumu, laiku, ilgumu un veidu. Neatkarīgi no tā, vai šādu signālu un saistīto datu pārvadē izmanto vadus, radioviļņus, optiskos vai elektromagnētiskus līdzekļus, ieskaitot satelītsakaru tīklus, kabeļtīklus, fiksētos (ķēžu un pakešu komutācijas, ieskaitot internetu) un mobilos zemes tīklus, elektrokabeļu sistēmas, ar šādiem signāliem saistītie dati būtu jāuzskata par elektronisko sakaru metadatiem, un tāpēc tiem būtu piemērojami šīs regulas noteikumi. Elektronisko sakaru metadati var ietvert informāciju, kura sniegta saistībā ar pakalpojuma abonēšanu, ja šādu informāciju apstrādā nolūkā to pārraidīt, izplatīt vai veikt elektronisko sakaru satura apmaiņu.

(15) Elektronisko sakaru dati būtu jāapstrādā kā konfidenciāla informācija. Tas nozīmē, ka iejaukšanās elektronisko sakaru datu pārraidē – vai nu tieši ar cilvēka dalību, vai ar iekārtu veiktu automatizētu apstrādi – būtu jāaizliedz, ja nav saņemta piekrišana no visiem saziņā iesaistītajiem. Sakaru datu pārtveršanas aizliegums būtu jāpiemēro tad, kad notiek datu pārvade, proti, kamēr paredzētais adresāts nav saņēmis elektroniskās saziņas saturu. Elektronisko sakaru datu pārtveršana var notikt, piemēram, kad kāda persona, kas nav saziņā iesaistītā puse, noklausās telefonsarunas, izlasa, noskenē vai saglabā elektronisko sakaru saturu vai saistītos metadatus un dara to nolūkā, kas nav saistīts ar informācijas apmaiņu. Pārtveršana notiek arī tad, ja trešās personas bez attiecīgo galalietotāju piekrišanas uzmana apmeklētās tīmekļa vietnes, apmeklējumu laikus, sakarus ar citiem un citus aspektus. Līdz ar tehnoloģiju attīstību palielinājušās ir arī pārtveršanas tehniskās iespējas. Iespējas ir dažādas – var tikt uzstādītas iekārtas, kas vāc datus no galiekārtām konkrēti izvēlētās teritorijās, piemēram, tā sauktās starptautiskās mobilo sakaru abonenta identitātes (*IMSI*) uztvērēji, vai izmantotas tādas programmas un metodes, kas, piemēram, ļauj slepeni uzraudzīt pārlūkošanas paradumus nolūkā izveidot galalietotāja profilu. Citi pārtveršanas piemēri ietver ar *RPAS* aprīkojumu (*payload*) iegūtu datu vai satura datu pārtveršanu no nešifrētiem bezvadu tīkliem un maršrutētājiem, tostarp bez galalietotāja piekrišanas pārtverot datus saistībā ar pārlūkošanas paradumiem.

(16) Sakaru informācijas glabāšanas aizliegums nav noteikts ar nodomu aizliegt automātisku, pagaidu un īslaicīgu šādas informācijas saglabāšanu, ja tā veikta tikai un vienīgi ar mērķi veikt pārraidīšanu elektronisko sakaru tīklā. Šādā veidā nedrīkstētu aizliegt ne elektronisko sakaru datu apstrādi, ko veic nolūkā nodrošināt elektronisko sakaru pakalpojumu drošību un nepārtrauktību, citstarp pārbaudot, vai nepastāv drošības apdraudējumi un vai nav izveidota ļaunprogrammatūra, ne metadatu apstrādi,

kuras mērķis ir nodrošināt pakalpojumu kvalitātes prasību vajadzīgo līmeni, piemēram, latentuma, trīces un citādā ziņā.

(17) Elektronisko sakaru datu apstrāde var būt lietderīga uzņēmumiem, patērētājiem un sabiedrībai kopumā. Salīdzinot ar Direktīvu 2002/58/EK, šī regula paplašina elektronisko sakaru pakalpojumu sniedzēju iespējas apstrādāt elektronisko sakaru metadatus, ja galalietotāji tam devuši piekrišanu. Tomēr galalietotāji lielu nozīmi piešķir konfidencialitātei savos sakaros, tostarp savās tiešsaistes darbībās, un iespējai kontrolēt elektronisko sakaru datu izmantošanu arī citā nolūkā, ne tikai saistībā ar pārvadi. Tādēļ šajā regulā būtu jānosaka, ka elektronisko sakaru pakalpojumu sniedzējiem ir jāsaņem galalietotāju piekrišana un tikai tad viņi drīkst apstrādāt elektronisko sakaru metadatus, kas ietver tādus datus par iekārtas atrašanās vietu, kuri ģenerēti pakalpojuma piekļuves piešķiršanas un saglabāšanas un pieslēguma izveidošanas vajadzībām. Atrašanās vietas dati, kas nav ģenerēti elektronisko sakaru pakalpojumu sniegšanas saistībā, nebūtu jāuzskata par metadatiem. Kā piemēru situācijām, kad elektronisko sakaru pakalpojumu sniedzēji izmanto elektronisko sakaru metadatus komerciālos nolūkos, var minēt intensitātes kartes, kurās ar krāsām grafiski attēloti dati, kas norāda cilvēku koncentrēšanās vietas. Lai attēlotu satiksmes plūsmu konkrētos virzienos noteiktā laika periodā, ir jāizmanto identifikators, kas ļauj savienot atsevišķu cilvēku atrašanās vietas noteiktos laika intervālos. Šo identifikatoru nevarētu izmantot, ja tiktu izmantoti anonīmi dati, un šādu plūsmu nevarētu attēlot. Šādā veidā izmantojot elektronisko sakaru metadatus, iespējamie ieguvēji būtu, piemēram, publiskās iestādes un sabiedriskā transporta operatori, kuri varētu noteikt, kur, pamatojoties uz jau izveidotās struktūras izmantojumu un slodzi, veidot jaunu infrastruktūru. Ja elektronisko sakaru metadatu apstrādes veids – jo īpaši, izmantojot jaunās tehnoloģijas un ņemot vērā apstrādes raksturu, tvērumu, kontekstu un mērķus – varētu stipri apdraudēt fizisku personu tiesības un brīvības, pirms apstrādes būtu jāveic novērtējums par ietekmi uz datu aizsardzību un attiecīgā gadījumā jāapspriežas ar uzraudzības iestādi, kā paredzēts Regulas (ES) 2016/679 35. un 36. pantā.

(18) Lai saņemtu konkrētus pakalpojumus, piemēram, aizsardzību pret krāpnieciskām darbībām (analizējot izmantošanas datus, atrašanās vietu un klienta kontu reāllaikā), galalietotāji var dot piekrišanu savu metadatu apstrādei. Digitālajā ekonomikā pakalpojumu bieži sniedz pret citu pakalpojumu, nevis par naudu, piemēram, galalietotājus pakļaujot reklāmai. Šajā regulā galalietotāja – tiklab fiziskas, kā juridiskas personas – piekrišanai vajadzētu būt tādai pašai nozīmei, kāda ir Regulā (ES) 2016/679 paredzētajai datu subjekta piekrišanai, un attiecīgi tai būtu jāpiemēro tādi paši nosacījumi. Pamatpiekļuve platjoslas internetam un balss sakaru pakalpojumi ir jāuzskata par cilvēkiem svarīgiem pakalpojumiem, kas tiem ļauj sazināties un izmantot digitālās ekonomikas priekšrocības. Attiecībā uz tādu datu apstrādi dota piekrišana, kas iegūti no izmantotajiem interneta un balss sakaru pakalpojumiem, nav uzskatāma par derīgu, ja datu subjektam nav bijusi dota īsta vai brīva izvēle vai viņš nav varējis atteikties vai atsaukt savu izvēli bez nelabvēlīgām sekām.

(19) Elektronisko sakaru saturs ir cieši saistīts ar to pamattiesību būtību, kas paredz privātās un ģimenes dzīves, mājokļa un saziņas neaizskaramību un ir aizsargātas saskaņā ar Hartas 7. pantu. Iejaukšanās elektronisko sakaru saturā būtu jāatļauj vienīgi skaidri noteiktos apstākļos un atbilstīgi īpašiem nolūkiem, un būtu tai jāpiemēro pienācīga aizsardzība pret ļaunprātīgu izmantošanu. Šajā regulā ir paredzēta iespēja elektronisko sakaru pakalpojumu sniedzējiem apstrādāt tranzītā esošus elektronisko sakaru datus, ja visi attiecīgie galalietotāji ir snieguši apzinātu piekrišanu. Piemēram, pakalpojumu sniedzēji var piedāvāt pakalpojumus, kuri ietver e-pastu skenēšanu, lai

tādējādi izdzēstu konkrētu, iepriekš noteiktu materiālu. Ņemot vērā sakaru satura sensitivitāti, šajā regulā ir ietverts pieņēmums, ka šāda satura datu apstrāde stipri apdraudēs fizisku personu tiesības un brīvības. Apstrādājot šāda veida datus, elektronisko sakaru pakalpojumu sniedzējam vienmēr pirms apstrādes būtu jāapspriežas ar uzraudzības iestādi. Apspriežoties būtu jāievēro atbilstība Regulas (ES) 2016/679 36. panta 2. un 3. punktam. Pieņēmums neattiecas uz satura datu apstrādi, kas veikta, lai sniegtu galalietotāja pieprasītos pakalpojumus, ja galalietotājs ir piekritis šādai apstrādei un ja tā tiek veikta tādā nolūkā un tik ilgi, cik tas ir noteikti nepieciešams un samērīgi attiecībā uz šādu pakalpojumu. Kad galalietotājs ir nosūtījis elektronisko sakaru saturu, bet paredzētais galalietotājs vai paredzētie galalietotāji to ir saņēmuši, to var ierakstīt vai saglabāt galalietotājs, galalietotāji vai trešā persona, kurai galalietotāji ir uzticējuši ierakstīt vai saglabāt šādus datus. Jebkurai šādu datu apstrādei ir jāatbilst Regulai (ES) 2016/679.

(20) Elektronisko sakaru tīklu galalietotāju galiekārtas un jebkura informācija, kas saistīta ar šādu galiekārtu izmantošanu neatkarīgi no tā, vai tā tiek īpaši saglabāta šādās iekārtās vai iekārtas to emitē, pieprasa vai apstrādā, lai tās varētu savienoties ar citu ierīci un/vai tīkla iekārtām, ir daļa no galalietotāju privātās sfēras, kuras aizsardzība jānodrošina saskaņā ar Eiropas Savienības Pamattiesību hartu un Eiropas Cilvēktiesību un pamatbrīvību aizsardzības konvenciju. Ņemot vērā, ka šādas iekārtas satur vai apstrādā informāciju, kas var atklāt informāciju par indivīda emocionālajiem, politiskajiem, sociālajiem sarežģījumiem, ieskaitot sakaru saturu, attēlus, datus par indivīda atrašanās vietu, ko atklāj pieslēgšanās ierīces GPS informācijai, adresātu sarakstus un citu informāciju, kas jau ir saglabāta ierīcē, ir jānodrošina lielāka privātuma aizsardzība attiecībā uz informāciju, kas saistīta ar šādu iekārtu. Turklāt tā sauktā spiegprogrammatūra, neredzamie pikseļi (*web bugs*), slēptie identifikatori, pastāvīgās sīkdatnes un tamlīdzīgi nevēlamas izsekošanas rīki var iekļūt galalietotāju galiekārtās bez viņu ziņas un iegūt pieeju informācijai, saglabāt iekārtā apslēptu informāciju un izsekot darbības. Ar galalietotāja ierīci saistīto informāciju var vākt arī attālināti, lai pēc tam to izmantotu identificēšanas un izsekošanas vajadzībām, izmantojot tādas metodes kā "pirkstu nospiedumu lasītāju", kas bieži vien notiek bez galalietotāju ziņas, un tādējādi var tikt nopietni pārkāpta šo galalietotāju privātuma neaizskaramība. Metodes, ar kurām slepeni tiek uzraudzītas galalietotāju darbības, piemēram, tādas, ar kurām tiek izsekotas darbības tiešsaistē vai viņu galiekārtas atrašanās vieta vai apturēta galalietotāju galiekārtu darbība, nopietni apdraud galalietotāju privātuma neaizskaramību. Tāpēc jebkāda šāda iejaukšanās attiecībā uz galalietotāja galiekārtu būtu jāatļauj vienīgi ar galalietotāja piekrišanu un tikai tad, ja tās nolūki ir konkrēti un pārredzami.

(21) Izņēmumi attiecībā uz pienākumu iegūt piekrišanu par galiekārtas apstrādes un saglabāšanas spēju izmantošanu vai piekļuvi galiekārtā saglabātai informācijai būtu jāpiemēro tikai tādās situācijās, kad nenotiek iejaukšanās privātajā sfērā vai arī tā ir ļoti ierobežota. Piemēram, piekrišana nebūtu jāpieprasa tad, ja vajadzīga atļauja tehniskai glabāšanai vai piekļuvei, kas ir noteikti nepieciešama un samērīga likumīgā nolūkā, lai nodrošinātu tāda konkrēta pakalpojuma izmantošanu, kuru galalietotājs ir nepārprotami pieprasījis. Tas var ietvert sīkdatņu saglabāšanu uz atsevišķas sesijas laiku tīmekļa vietnē, lai izsekotu ievaddatiem, kurus galalietotājs norādījis, aizpildot tiešsaistes veidlapas vairākās lapās. Sīkdatnes var būt arī likumīgs un lietderīgs rīks, ko izmanto, piemēram, lai novērtētu tīmekļa datplūsmu uz tīmekļa vietni. Informācijas sabiedrības pakalpojumu sniedzējiem veicot konfigurācijas pārbaudes, lai nodrošinātu pakalpojumu atbilstību galalietotāju iestatījumiem, un reģistrējot tikai to, ka galalietotāja ierīce nespēj saņemt galalietotāja pieprasīto saturu, nedrīkstētu rasties

situācija, kad tiek nodrošināta piekļuve šādai ierīcei vai izmantotas šādas ierīces apstrādes iespējas.

(22) Metodēm, ko izmanto informācijas sniegšanai un galalietotāju piekrišanas saņemšanai, vajadzētu būt pēc iespējas ērtākām lietotājiem. Ņemot vērā, ka pastāvīgo sīkdatņu un citu izsekošanas metožu izmantošana ir kļuvusi plaši izplatīta, galalietotājiem arvien biežāk tiek pieprasīts dot piekrišanu šādu pastāvīgo sīkfailu saglabāšanai viņu galiekārtās. Rezultātā galalietotāji ir pārslogoti ar prasībām dot piekrišanu. Taču šo problēmu var risināt, ja piekrišanas sniegšanā tiek, piemēram, izmantoti tādi tehniskie līdzekļi, kuru iestatījumi ir pārredzami un lietotājam ērti. Tādēļ šajā regulā būtu jāparedz iespēja sniegt piekrišanu, izmantojot atbilstīgus iestatījumus pārlūkprogrammā vai citā lietotnē. Izvēlēm, ko galalietotāji izdara, mainot vispārējos privātuma iestatījumus pārlūkprogrammā vai citā lietotnē, vajadzētu būt saistošām jebkurām trešām personām un tādām, ko šīs trešās personas var izpildīt. Tīmekļa pārlūkprogrammas ir tāda veida lietojumprogrammatūra, kas ļauj no interneta izgūt informāciju un to tur arī parādīt. Tādas pašas spējas ir arī cita veida lietotnēm, piemēram, tām, kas ļauj veikt izsaukumus un sūtīt īsziņas vai dot maršruta norādījumus. Tīmekļa pārlūkprogrammas nodrošina lielu daļu sakaru starp galalietotāju un tīmekļa vietni. No šāda viedokļa raugoties, tām ir priekšrocība, ko dod vajadzība tās aktīvi izmantot, lai galalietotājam būtu vieglāk kontrolēt informācijas plūsmu no galiekārtām un uz tām. Konkrētāk, tīmekļa pārlūkprogrammas var izmantot kā "vārtsargus", kas tādējādi palīdz galalietotājiem nodrošināt, ka viņu galiekārtās (piemēram, viedtālrunī, planšetdatorā vai datorā) saglabātajai informācijai neviens nepiekļūs un neviens to nesaglabās.

(23) Principi "integrēta datu aizsardzība" un "datu aizsardzība pēc noklusējuma" tika kodificēti saskaņā ar Regulas (ES) 2016/679 25. pantu. Patlaban sīkdatņu noklusējuma iestatījumi vairumā pārlūkprogrammu ir iestatīti kā "pieņemt visas sīkdatnes". Tādēļ tās programmatūras nodrošinātājiem, kas ļauj izgūt no interneta informāciju un to tur parādīt, būtu jānosaka pienākums veikt tādu programmatūras konfigurāciju, lai būtu iespējams liegt trešajām personām saglabāt informāciju galiekārtās; bieži vien šī iespēja ir iestatīta kā "noraidīt trešās personas sīkdatnes". Galalietotājiem vajadzētu būt piedāvātai virknei privātuma iestatījumu iespēju, sākot no augstāka līmeņa (piemēram, "nekad nepieņemt sīkdatnes") līdz vidējam līmenim (piemēram, "noraidīt trešās personas sīkdatnes" vai "pieņemt tikai pirmās puses sīkdatnes") un, visbeidzot, zemākam līmenim (piemēram, "vienmēr pieņemt sīkdatnes"). Šādu privātuma iestatījumu attēlojumam vajadzētu būt viegli pamanāmam un saprotamam.

(24) Lai tīmekļa pārlūkprogrammās būtu iespējams saņemt galalietotāju piekrišanu, kā noteikts Regulā (ES) 2016/679, piemēram, par trešās personas pastāvīgo sīkdatņu datu saglabāšanu, tajās būtu jāpieprasa galiekārtas galalietotājam veikt skaidru apstiprinošu darbību, kas apliecinātu galalietotāja brīvu, konkrētu, apzinātu un viennozīmīgu piekrišanu šādu sīkdatņu saglabāšanai un piekļuvei galiekārtās vai no galiekārtām. Šādu darbību var uzskatīt par apstiprinošu, piemēram, ja galalietotājiem prasa apzināti izvēlēties "pieņemt trešās personas sīkdatnes", lai apstiprinātu savu piekrišanu, un ja viņiem tiek sniegta šādas izvēles izdarīšanai nepieciešamā informācija. Šajā nolūkā jāpieprasa, lai tās programmatūras instalēšanas brīdī, kas sniedz piekļuvi internetam, programmatūras nodrošinātāji informētu galalietotājus par iespēju no dažādiem variantiem izvēlēties privātuma iestatījumus un lūgtu tiem izdarīt izvēli. Sniegtā informācija nedrīkstētu atturēt galalietotājus no augstāka līmeņa privātuma iestatījumiem, un tajā būtu jāiekļauj attiecīgā informācija par riskiem, ko var radīt trešo personu sīkdatņu saglabāšana datorā, ieskaitot datu apkopošanu par personas

pārlūkošanas vēsturi ilgtermiņā, un par šādu datu izmantošanu mērķētas reklāmas sūtījumos. Tīmekļa pārlūkprogrammas tiek mudinātas sniegt galalietotājiem iespējas vienkāršā veidā mainīt privātuma iestatījumus jebkurā lietošanas brīdī un ļaut lietotājam izdarīt izņēmumus attiecībā uz dažām tīmekļa vietnēm vai iekļaut tās "baltajā sarakstā" vai precizēt, kurām tīmekļa vietnēm (trešās) personas sīkdatnes vienmēr ir vai nekad nav atļautas.

(25) Lai varētu nodrošināt piekļuvi elektronisko sakaru tīkliem, regulāri būtu jāemitē noteiktas datu paketes, lai izveidotu vai saglabātu savienojumu ar tīklu vai citu ierīci šajā tīklā. Turklāt ierīcēm jābūt izveidotai unikālai adresei, lai tās minētajā tīklā būtu identificējamas. Bezvadu un mobilo tālruņu standarti līdzīgā veidā paredz izstarot aktīvos signālus, kas satur unikālus identifikatorus, piemēram, *MAC* adresi, *IMEI* (starptautiskā mobilā aprīkojuma identitāte), *IMSI* utt. Atsevišķai bezvadu bāzes stacijai (t. i., raidītājs un uztvērējs), piemēram, bezvadu piekļuves punktam, ir konkrēts diapazons, kādā var uztvert šādu informāciju. Ir parādījušies pakalpojumu sniedzēji, kas piedāvā izsekošanas pakalpojumus, kuru pamatā tiek izmantota ar iekārtu saistītās dažādas funkcionalitātes informācijas skenēšana, tostarp iedzīvotāju skaitīšana, datu sniegšana par rindā esošo cilvēku skaitu, cilvēku skaita noskaidrošana konkrētā teritorijā utt. Šādu informāciju var izmantot tādos nolūkos, kas paredz lielāku iejaukšanos, piemēram, lai brīdī, kad galalietotājs ieiet veikalā, nosūtītu viņam komerciņojumu ar personalizētiem piedāvājumiem. Lai arī dažas no šīm funkciju iespējām nerada augstu risku saistībā ar privātuma neaizskaramību, ir arī tādas, kas to rada, piemēram, tādas, kas saistītas ar indivīdu izsekošanu ilgākā laika posmā, tostarp saistībā ar atkārtotiem apmeklējumiem konkrēti noteiktās vietās. Pakalpojumu sniedzējiem, kuri izmanto šādu praksi, pie pārklājuma zonas robežlīnijas būtu jāsniedz nepārprotams paziņojums, informējot galalietotājus pirms ieiešanas noteiktajā zonā par to, ka konkrētā tehnoloģija darbojas attiecīgajā perimetrā, kā arī par izsekošanas mērķi, šajā saistībā atbildīgo personu un pasākumiem, ko galalietotājs var veikt, lai samazinātu vai apturētu datu vākšanu. Ja personas dati tiek vākti saskaņā ar Regulas (ES) 2016/679 13. pantu, būtu jāsniedz papildu informācija.

(26) Ja elektronisko sakaru datu apstrāde, ko veic elektronisko sakaru pakalpojumu sniedzēji, ietilpst šīs regulas piemērošanas jomā, tad šajā regulā būtu jāparedz iespēja Savienībai vai dalībvalstīm īpašos apstākļos ar likumu ierobežot konkrētus pienākumus un tiesības, ja šāda ierobežošana demokrātiskā sabiedrībā ir nepieciešams un samērīgs pasākums, lai aizsargātu īpaši svarīgas sabiedrības intereses, tostarp valsts drošību, aizsardzību, sabiedrības drošību, lai novērstu, izmeklētu, atklātu noziedzīgus nodarījumus vai sauktu pie atbildības par tiem vai izpildītu krimināLsodus, tostarp lai pasargātu no draudiem sabiedriskajai drošībai un tos novērstu, kā arī garantētu citas svarīgas Savienības vai dalībvalsts vispārējo sabiedrības interešu mērķus, jo īpaši svarīgas Savienības vai dalībvalsts ekonomiskās vai finansiālās intereses, vai uzraudzības, pārbaudes vai regulatīvo funkciju, kas saistīta ar oficiālu pilnvaru īstenošanu šādu interešu aizsardzības nolūkā. Tādēļ saskaņā ar Eiropas Savienības Pamattiesību hartu un Eiropas Cilvēktiesību un pamatbrīvību aizsardzības konvenciju, kā to interpretē Eiropas Savienības Tiesa un Eiropas Cilvēktiesību tiesa, šai regulai nevajadzētu skart dalībvalstu spējas veikt elektronisko sakaru likumīgu pārtveršanu vai citus pasākumus, ja tie ir nepieciešami un samērīgi nolūkā aizsargāt iepriekš minētās sabiedrības intereses. Elektronisko sakaru pakalpojumu sniedzējiem būtu jānodrošina piemērotas procedūras, kuras palīdzētu izskatīt kompetento iestāžu likumīgos pieprasījumus, vajadzības gadījumā ņemot vērā arī saskaņā ar 3. panta 3. punktu ieceltā pārstāvja pienākumus.

(27) Attiecībā uz izsaucošā numura noteikšanu ir jāaizsargā izsaucēja tiesības neuzrādīt numuru, no kura veikts izsaukums, kā arī izsauktā tiesības noraidīt zvanus no nenosakāmiem numuriem. Atsevišķi galalietotāji, jo īpaši palīdzības dienesti un līdzīgas organizācijas, ir ieinteresēti garantēt savu zvanītāju anonimitāti. Attiecībā uz savienotā numura noteikšanu ir jāaizsargā izsauktā tiesības un likumīgās intereses neuzrādīt numuru, ar kuru izsaucošais ir faktiski savienots.

(28) Īpašos gadījumos ir pamats neievērot atteikšanos no izsaucošā numura uzrādīšanas iespējas. Būtu jāierobežo galalietotāju tiesības uz privātumu attiecībā uz izsaucošā numura noteikšanu tad, ja tas ir vajadzīgs traucējošu zvanu izsekošanai, un attiecībā uz izsaucošā numura noteikšanu un atrašanās vietas datiem – ja tas ir nepieciešams, lai ļautu palīdzības dienestiem, piemēram, eZvanam, izpildīt savus uzdevumus iespējami efektīvāk.

(29) Ir izstrādāta tehnoloģija, kas ļauj elektronisko sakaru pakalpojumu sniedzējiem piedāvāt galalietotājiem dažādas iespējas samazināt nevēlamu izsaukumu saņemšanu, tostarp bloķēt klusējošos izsaukumus un citus krāpnieciskus un traucējošus izsaukumus. Publiski pieejamu numuratkarīgu starppersonu sakaru pakalpojumu sniedzējiem būtu jāizmanto šī tehnoloģija un bez maksas jāaizsargā galalietotāji no traucējošu zvanu saņemšanas. Pakalpojumu sniedzējiem, piemēram, publicējot informāciju savā tīmekļa vietnē, būtu jānodrošina galalietotāju informēšana par iespēju izmantot šādas funkcijas.

(30) Publiski pieejami elektronisko sakaru pakalpojumu galalietotāju saraksti tiek plaši izplatīti. Publiski pieejams abonentu saraksts ir jebkurš abonentu saraksts vai pakalpojums, kas ietver informāciju par galalietotājiem, piemēram, tālruņa numurus (arī mobilo tālruņu numurus), e-pasta adreses kontaktinformāciju, turklāt tie ietver uzziņu dienestu pakalpojumus. Fiziskas personas tiesības uz privātumu un personas datu aizsardzību paredz, ka galalietotājiem, kas ir fiziskas personas, lūdz dot piekrišanu pirms viņu personas datu iekļaušanas abonentu sarakstā. Tiesību subjektu likumīgo interešu labad galalietotājiem, kuri ir tiesību subjekti, jābūt tiesībām iebilst pret tādu datu iekļaušanu abonentu sarakstā, kas saistīti ar šiem galalietotājiem.

(31) Ja galalietotāji, kas ir fiziskas personas, dod piekrišanu savu datu iekļaušanai šādos abonentu sarakstos, tiem, pamatojoties uz sniegto piekrišanu, vajadzētu būt iespējai noteikt, kuras personas datu kategorijas tiek iekļautas abonentu sarakstā (piemēram, vārds un uzvārds, e-pasta adrese, dzīvesvietas adrese, lietotāja vārds un uzvārds, tālruņa numurs). Turklāt publiski pieejamu abonentu sarakstu pakalpojumu sniedzējiem pirms galalietotāju datu iekļaušanas attiecīgajā sarakstā būtu jāinformē galalietotāji par abonentu saraksta izmantošanas nolūku un tajā izmantojamajām meklēšanas funkcijām. Galalietotājiem vajadzētu būt iespējai dot piekrišanu attiecībā uz personas datu kategorijām, kuras izmantojamas viņu kontaktinformācijas meklēšanā. Abonentu sarakstā iekļautajām personas datu kategorijām un tām personas datu kategorijām, kuras izmantojamas galalietotāju kontaktinformācijas meklēšanā, nav noteikti jābūt vienādām.

(32) Šajā regulā tiešā tirgvedība attiecas uz jebkura veida reklāmu, kurā fiziska vai juridiska persona tiešā veidā sūta tiešās tirgvedības paziņojumus vienam vai vairākiem identificētiem vai identificējamiem elektronisko sakaru pakalpojumu galalietotājiem. Papildus produktu un pakalpojumu piedāvāšanai komerciālos nolūkos tajā būtu jāiekļauj arī ziņojumi, ko popularitātes iemantošanas nolūkā sūta politiskās partijas, kuras ar fiziskām personām sazinās ar elektronisko sakaru pakalpojumu palīdzību. Tas

pats būtu jāattiecina uz ziņojumiem, ko savu mērķu sasniegšanas vārdā nosūtījušas citas bezpeļņas organizācijas.

(33) Lai aizsargātu galalietotājus pret nepasūtītiem paziņojumiem, kas, pārkāpjot galalietotāju privātās dzīves neaizskaramību, nosūtīti tiešās tirgvedības nolūkā, būtu jāparedz aizsardzības pasākumi. Iejaukšanās privātajā sfērā un traucējumu līmenis ir visai līdzīgs neatkarīgi no plašā tehnoloģiju un kanālu klāsta, kas tiek izmantots šajos elektroniskajos sakaros (automatizētas izsaukšanas un saziņas sistēmas, tūlītējās ziņapmaiņas lietotnes, e-pasti, SMS, MMS, *Bluetooth* utt.). Tādēļ ir pamats pieprasīt, lai galalietotāja piekrišana tiktu saņemta pirms tiešās tirgvedības nolūkā sagatavotu elektronisko komercpaziņojumu nosūtīšanas galalietotājiem, tādējādi efektīvi aizsargājot gan indivīdus no iejaukšanās viņu privātajā dzīvē, gan juridisku personu likumīgās intereses. Juridiskā noteiktība un nepieciešamība nodrošināt, lai noteikumi, kas aizsargā no nepasūtītiem elektroniskajiem paziņojumiem, joprojām atbilstu nākotnes prasībām, pamato vajadzību definēt tādu vienotu noteikumu kopumu, kas neatšķiras atkarībā no šādu nepasūtītu paziņojumu pārvadē izmantotās tehnoloģijas un vienlaikus garantē vienādu aizsardzības līmeni visiem iedzīvotājiem visā Savienības teritorijā. Tomēr, uzturot attiecības ar esošajiem klientiem, kuriem tiek piedāvāti jau izmantotajiem līdzīgi produkti vai pakalpojumi, ir lietderīgi atļaut izmantot e-pasta kontaktinformāciju. Šāda iespēja būtu izmantojama tikai tādam uzņēmumam, kas elektronisko kontaktinformāciju ieguvis saskaņā ar Regulu (ES) 2016/679.

(34) Ja galalietotāji ir devuši piekrišanu saņemt tiešās tirgvedības nolūkā nosūtītus nepasūtītus paziņojumus, viņiem vajadzētu būt iespējai katrā laikā vienkāršā veidā piekrišanu atsaukt. Lai veicinātu to Savienības noteikumu efektīvu izpildi, kuri attiecas uz tiešās tirgvedības nolūkā sagatavotiem nepasūtītiem ziņojumiem, ir jāaizliedz tiešās tirgvedības nolūkā sagatavotu nepasūtītu komercpaziņojumu izsūtīšanā slēpt identitāti un izmantot viltus identitāti, viltus atpakaļadresi vai viltus numurus. Tādēļ nepasūtītiem tirgvedības paziņojumiem vajadzētu būt skaidri atpazīstamiem un tajos būtu jānorāda tās juridiskās vai fiziskās personas identitāte, kas pārraidījusi paziņojumu vai kuras vārdā paziņojums ir pārraidīts, kā arī jāsniedz saņēmējiem vajadzīgā informācija, kas tiem ļautu izmantot tiesības iebilst pret turpmāku rakstisku un/vai mutisku tirgvedības ziņojumu saņemšanu.

(35) Lai piekrišanu varētu ērti atsaukt, juridiskām vai fiziskām personām, kas tiešās tirgvedības paziņojumus izsūta pa e-pastu, būtu jānorāda saite vai derīga e-pasta adrese, ko galalietotāji var viegli izmantot piekrišanas atsaukšanai. Juridiskām vai fiziskām personām, kas tiešās tirgvedības paziņojumu nosūtīšanai izmanto balss izsaukumus un automatizētu izsaukšanas un saziņas sistēmu veiktus izsaukumus, būtu jāatklāj savs tiešais identifikācijas numurs, pa kuru uzņēmumu var sazvanīt, vai jānorāda īpašs kods, kas norāda, ka tas ir tirgvedības izsaukums.

(36) Tiešās tirgvedības balss izsaukumi, kas nav saistīti ar automatizētām izsaukšanas un saziņas sistēmām, sūtītājam izmaksā daudz vairāk, bet galalietotājiem finansiālas izmaksas nerada. Tāpēc dalībvalstīm vajadzētu būt iespējai izveidot un/vai saglabāt valsts sistēmas, kas šādus izsaukumus ļauj adresēt tikai tiem galalietotājiem, kuri nav pret to iebilduši.

(37) Pakalpojumu sniedzējiem, kuri piedāvā elektronisko sakaru pakalpojumus, būtu jāinformē galalietotāji par pasākumiem, ko tie var veikt savu sakaru drošības aizsardzībai, piemēram, izmantojot īpaša veida programmatūru vai šifrēšanas tehnoloģijas. Prasība informēt galalietotājus par sevišķiem drošības riskiem neatbrīvo pakalpojumu sniedzēju no pienākuma par saviem līdzekļiem pieņemt atbilstīgus un

steidzamus pasākumus, lai novērstu jaunus, neparedzētus drošības riskus un atjaunotu normālu pakalpojuma drošības līmeni. Informācija par drošības riskiem būtu jāsniedz abonentam bez maksas. Drošības jautājums ir izvērtēts saskaņā ar Regulas (ES) 2016/679 32. pantu.

(38) Lai nodrošinātu pilnīgu atbilstību Regulai (ES) 2016/679, šīs regulas noteikumu īstenošana būtu jāuztic tām pašām iestādēm, kas atbild par Regulas (ES) 2016/679 noteikumu izpildi, un šī regula balstās uz Regulas (ES) 2016/679 konsekvences mehānismu. Atbilstīgi savai konstitucionālajai, organizatoriskajai un administratīvajai iekārtai dalībvalstīm būtu jāspēj nodrošināt, ka tajās ir vairāk nekā viena uzraudzības iestāde. Uzraudzības iestādēm vajadzētu būt atbildīgām arī par šīs regulas piemērošanas uzraudzību attiecībā uz juridisko personu elektronisko sakaru datiem. Šādu papildu uzdevumu veikšanai nevajadzētu apdraudēt uzraudzības iestādes spēju pildīt tai uzticētos uzdevumus, kas attiecas uz personas datu aizsardzību saskaņā ar Regulu (ES) 2016/679 un šo regulu. Katrai uzraudzības iestādei būtu jāpiešķir papildu finanšu līdzekļi un cilvēkresursi, telpas un infrastruktūra, kas vajadzīga efektīvai uzdevumu izpildei saskaņā ar šo regulu.

(39) Katrai uzraudzības iestādei vajadzētu būt kompetentai savas dalībvalsts teritorijā īstenot pilnvaras un pildīt uzdevumus, kas tai paredzēti šajā regulā. Lai nodrošinātu konsekventu šīs regulas piemērošanas uzraudzību un izpildi visā Savienībā, uzraudzības iestādēm, pievēršot tiesu iestāžu uzmanību šīs regulas pārkāpumiem un iesaistoties tiesvedībā, katrā dalībvalstī vajadzētu būt vieniem un tiem pašiem uzdevumiem un faktiskajām pilnvarām, neskarot saskaņā ar dalībvalsts tiesību aktiem noteiktās kriminālvajāšanas iestāžu pilnvaras. Dalībvalstis un to uzraudzības iestādes tiek mudinātas šīs regulas piemērošanā ņemt vērā mikrouzņēmumu, mazo un vidējo uzņēmumu konkrētās vajadzības.

(40) Lai stiprinātu šīs regulas noteikumu izpildes nodrošināšanu, papildus citiem šajā regulā paredzētiem atbilstošiem pasākumiem vai šādu pasākumu vietā katrai uzraudzības iestādei vajadzētu būt piešķirtām pilnvarām piemērot sankcijas, tostarp administratīvus naudas sodus par šīs regulas pārkāpumiem. Šajā regulā būtu jānorāda pārkāpumi un jānosaka attiecīgā administratīvā naudas soda maksimālais apmērs un kritēriji tā noteikšanai, kas katrā konkrētā gadījumā būtu jānosaka uzraudzības iestādei, ņemot vērā visus attiecīgos konkrētās situācijas apstākļus un pienācīgi ņemot vērā jo īpaši pārkāpuma būtību, smagumu, ilgumu un sekas, kā arī pasākumus, kas veikti, lai nodrošinātu šajā regulā paredzēto pienākumu ievērošanu un novērstu vai mazinātu pārkāpuma sekas. Nosakot naudas sodu saskaņā ar šo regulu, uzņēmums būtu jāsaprot kā uzņēmums saskaņā ar Līguma 101. un 102. pantu.

(41) Lai sasniegtu šīs regulas mērķus, proti, aizsargātu fizisku personu pamattiesības un pamatbrīvības, jo īpaši tiesības uz personas datu aizsardzību, un nodrošinātu personas datu brīvu apriti Savienībā, Komisijai, papildinot šo regulu, būtu jādeleģē pilnvaras pieņemt aktus saskaņā ar Līguma 290. pantu. Jo īpaši, deleģētie akti būtu jāpieņem attiecībā uz sniedzamo informāciju, arī to, ko sniedz ar standartizētām ikonām, kuras palīdz viegli pamanāmā un saprotamā veidā sniegt pārskatu par galiekārtas emitētās informācijas vākšanu, tās mērķi, atbildīgo personu un visiem pasākumiem, ko galalietotājs var veikt, lai minimalizētu šādu informācijas vākšanu. Deleģētie akti būtu arī jāpieņem, lai precizētu kodu, ar kuru tiek identificēti tiešās tirgvedības izsaukumi, tostarp tie, kas veikti automatizētās izsaukšanas un saziņas sistēmās. Sevišķi svarīgi ir Komisijai pienācīgi apspriesties saskaņā ar principiem, kas noteikti 2016. gada

13. aprīļa Iestāžu nolīgumā par labāku likumdošanas procesu[8]. Jo īpaši, lai deleģēto aktu sagatavošanā nodrošinātu vienlīdzīgu dalību, Eiropas Parlaments un Padome visus dokumentus saņem vienlaicīgi ar dalībvalstu ekspertiem un minēto iestāžu ekspertiem ir sistemātiska piekļuve Komisijas ekspertu grupu sanāksmēm, kurās notiek deleģēto aktu sagatavošana. Turklāt, lai nodrošinātu vienādus nosacījumus šīs regulas īstenošanai, Komisijai būtu jāsaņem īstenošanas pilnvaras, ja tas paredzēts šajā regulā. Minētās pilnvaras būtu jāīsteno saskaņā ar Regulu (ES) Nr. 182/2011.

(42) Ņemot vērā ka šīs regulas mērķi, proti, nodrošināt fiziskām un juridiskām personām vienādu aizsardzības līmeni un brīvu elektronisko sakaru datu apriti visā Savienībā, nevar pietiekami labi sasniegt atsevišķās dalībvalstīs, un rīcības mēroga vai seku dēļ tos var labāk sasniegt Savienības līmenī, Savienība var pieņemt pasākumus saskaņā ar Līguma par Eiropas Savienību 5. pantā noteikto subsidiaritātes principu. Saskaņā ar minētajā pantā noteikto proporcionalitātes principu šajā regulā paredz vienīgi tos pasākumus, kas ir vajadzīgi minētā mērķa sasniegšanai.

(43) Direktīva 2002/58/EK būtu jāatceļ.

IR PIEŅĒMUŠI ŠO REGULU.

[8] Iestāžu 2016. gada 13. aprīļa Nolīgums starp Eiropas Parlamentu, Eiropas Savienības Padomi un Eiropas Komisiju par labāku likumdošanas procesu (OV L 123, 12.5.2016., 1.–14. lpp.).

I NODAĻA
VISPĀRĪGI NOTEIKUMI

1. pants
Priekšmets

1. Šajā regulā ir izklāstīti noteikumi par fizisku un juridisku personu pamattiesību un pamatbrīvību aizsardzību elektronisko sakaru pakalpojumu sniegšanā un izmantošanā, un īpaši par tiesībām uz privātās dzīves un sakaru neaizskaramību un par fizisku personu aizsardzību saistībā ar personas datu apstrādi.

2. Šī regula nodrošina elektronisko sakaru datu un elektronisko sakaru pakalpojumu brīvu apriti Savienībā, ko neierobežo un neaizliedz tādu iemeslu dēļ, kuri saistīti ar fizisku un juridisku personu privātās dzīves un sakaru neaizskaramību un fizisku personu aizsardzību saistībā ar personas datu apstrādi.

3. Šīs regulas noteikumi, 1. un 2. punkta vajadzībām izklāstot īpašus noteikumus, konkretizē un papildina Regulu (ES) 2016/679.

2. pants
Materiālā piemērošanas joma

1. Šo regulu piemēro elektronisko sakaru datu apstrādei, ko veic saistībā ar elektronisko sakaru pakalpojumu sniegšanu un izmantošanu, kā arī informācijai, kas ir saistīta ar galalietotāju galiekārtām.

2. Šo regulu nepiemēro:

(a) darbībām, kuras neietilpst Savienības tiesību piemērošanas jomā;

(b) dalībvalstu darbībām, kuras ietilpst Līguma par Eiropas Savienību V sadaļas 2. nodaļas piemērošanas jomā;

(c) elektronisko sakaru pakalpojumiem, kas nav publiski pieejami;

(d) darbībām, ko kompetentās iestādes veic, lai novērstu, izmeklētu vai atklātu noziedzīgus nodarījumus vai sauktu pie atbildības par tiem, vai izpildītu krimināsodus, tostarp pasargāšanai no sabiedriskās drošības apdraudējumiem un to novēršanai.

3. Elektronisko sakaru datu apstrādi, ko veic Savienības iestādes, struktūras, biroji un aģentūras, reglamentē Regula (ES) 00/0000 [jaunā regula, ar ko aizstāj Regulu 45/2001].

4. Šī regula neskar Direktīvas 2000/31/EK[9] piemērošanu, jo īpaši attiecībā uz minētās direktīvas 12.–15. panta noteikumiem par starpnieku pakalpojumu sniedzēju atbildību.

5. Šī regula neskar Direktīvas 2014/53/ES noteikumus.

[9] Eiropas Parlamenta un Padomes 2000. gada 8. jūnija Direktīva 2000/31/EK par dažiem informācijas sabiedrības pakalpojumu tiesiskiem aspektiem, jo īpaši elektronisko tirdzniecību, iekšējā tirgū ("Direktīva par elektronisko tirdzniecību") (OV L 178, 17.7.2000., 1.–16. lpp.).

3. pants
Teritoriālā piemērošanas joma un pārstāvis

1. Šo regulu piemēro:

(a) elektronisko sakaru pakalpojumu sniegšanai galalietotājiem Savienībā, neatkarīgi no tā, vai no galalietotāja prasa maksu;

(b) šādu pakalpojumu izmantošanai;

(c) tādas informācijas aizsardzībai, kas saistīta ar galalietotāju galiekārtām, kuras atrodas Savienībā.

2. Ja elektronisko sakaru pakalpojumu sniedzējs neveic uzņēmējdarbību Savienībā, tas rakstiski ieceļ sev pārstāvi Savienībā.

3. Pārstāvis ir tāds, kas veic uzņēmējdarbību vienā no dalībvalstīm, kurās atrodas šādu elektronisko sakaru pakalpojumu galalietotāji.

4. Lai nodrošinātu atbilstību šai regulai, pārstāvis ir pilnvarots atbildēt uz jautājumiem un sniegt informāciju papildus pakalpojumu sniedzējam vai tā vietā, jo īpaši uzraudzības iestādēm un galalietotājiem, par visiem jautājumiem, kas saistīti ar elektronisko sakaru datu apstrādi.

5. Pārstāvja iecelšana saskaņā ar šā panta 2. punktu neskar tiesiskās prasības, kuras varētu celt pret fizisku vai juridisku personu, kas apstrādā elektronisko sakaru datus saistībā ar elektronisko sakaru pakalpojumiem, kurus no valstīm ārpus Savienības sniedz galalietotājiem Savienībā.

4. pants
Definīcijas

1. Šajā regulā piemēro šādas definīcijas:

(a) Regulā (ES) 2016/679 noteiktās definīcijas;

(b) definīcijas "elektronisko sakaru tīkls", "elektronisko sakaru pakalpojums", "starppersonu sakaru pakalpojums", "numuratkarīgs starppersonu sakaru pakalpojums", "numurneatkarīgs starppersonu sakaru pakalpojums", "galalietotājs" un "izsaukums", kas attiecīgi minētas [Direktīvas par Eiropas Elektronisko sakaru kodeksa izveidi] 2. panta 1., 4., 5., 6., 7., 14. un 21. punktā;

(c) definīciju "galiekārta" ["termināliekārta"], kas minēta Komisijas Direktīvas 2008/63/EK[10] 1. panta 1. punktā.

2. Piemērojot 1. punkta b) apakšpunktu, definīcijā "starppersonu sakaru pakalpojums" ietilpst pakalpojumi, kuros interaktīva starppersonu saziņa ir tikai ar citu pakalpojumu saistīta sīka palīgfunkcija.

3. Turklāt šajā regulā piemēro šādas definīcijas:

(a) "elektronisko sakaru dati" ir elektronisko sakaru saturs un elektronisko sakaru metadati;

[10] Komisijas 2008. gada 20. jūnija Direktīva 2008/63/EK par konkurenci telekomunikāciju terminālieka̅rtu tirgos (OV L 162, 21.6.2008., 20.–26. lpp.).

(b) "elektronisko sakaru saturs" ir saturs, ar kuru notiek apmaiņa, izmantojot elektronisko sakaru pakalpojumus, piemēram, teksts, balss ieraksti, video, attēli skaņa;

(c) "elektronisko sakaru metadati" ir dati, kas elektronisko sakaru tīklā tiek apstrādāti nolūkā tos pārraidīt, izplatīt vai veikt elektronisko sakaru satura apmaiņu; tie ir arī dati, ko izmanto, lai izsekotu un identificētu saziņas avotu un galamērķi, dati par ierīces atrašanās vietu, kas ģenerēti saistībā ar elektronisko sakaru pakalpojumu sniegšanu, kā arī saziņas datums, laiks, ilgums un veids;

(d) "publiski pieejams abonentu saraksts" ir elektronisko sakaru pakalpojumu galalietotāju saraksts iespiestā vai elektroniskā formā, kas tiek publicēts vai darīts pieejams sabiedrībai vai kādai sabiedrības daļai, arī caur uzziņu dienestu;

(e) "elektroniskais pasts" ir jebkurš elektronisks ziņojums, kas satur elektronisko sakaru tīklā nosūtītu informāciju, piemēram, tekstu, balss ierakstu, video, skaņu vai attēlu, ko var saglabāt tīklā, ar to saistītajās datošanas iekārtās vai šāda ziņojuma saņēmēja galiekārtā;

(f) "tiešās tirgvedības paziņojumi" ir katra rakstiska vai mutiska reklāma, ko nosūta vienam vai vairākiem identificētiem vai identificējamiem elektronisko sakaru pakalpojumu galalietotājiem, ieskaitot automatizētas izsaukšanas un saziņas sistēmas izmantošanu ar cilvēka dalību vai bez tās, elektronisko pastu, SMS, utt.;

(g) "tiešās tirgvedības balss izsaukumi" ir tiešie izsaukumi, kuru veikšanai nav jāizmanto automatizētas izsaukšanas un saziņas sistēmas;

(h) "automatizētas izsaukšanas un saziņas sistēmas" ir sistēmas, kas spēj automātiski veikt viena vai vairāku saņēmēju izsaukumus saskaņā ar konkrētajai sistēmai noteiktajiem norādījumiem, un pārraidīt skaņu, kas nav tieši pārraidīta runa, tostarp izsaukumus, ko veic automatizētā izsaukšanas un saziņas sistēma, kas izsaukto personu savieno ar citu personu.

II NODAĻA
FIZISKU UN JURIDISKU PERSONU ELEKTRONISKO SAKARU UN VIŅU GALIEKĀRTĀS GLABĀTĀS INFORMĀCIJAS AIZSARDZĪBA

5. pants
Elektronisko sakaru datu konfidencialitāte

Elektronisko sakaru dati ir konfidenciāli. Jebkāda iejaukšanās elektronisko sakaru datos, piemēram, elektronisko sakaru datu noklausīšanās, ierakstīšana, saglabāšana, uzraudzība, skenēšana vai citāda pārtveršana, pārraudzība vai apstrāde, ko veic personas, kuras nav galalietotāji, ir aizliegta, izņemot gadījumus, kad to atļauj šī regula.

6. pants
Atļautā elektronisko sakaru datu apstrāde

1. Elektronisko sakaru tīklu un pakalpojumu sniedzēji drīkst apstrādāt elektronisko sakaru datus, ja:

(a) tas ir jādara, lai nodrošinātu saziņas pārraidīšanu tik ilgi, cik nepieciešams šim nolūkam, vai

(b) tas ir jādara, lai saglabātu vai atjaunotu elektronisko sakaru tīklu un pakalpojumu drošību vai konstatētu tehniskos bojājumus un/vai kļūdas elektronisko sakaru pārraidīšanā tik ilgi, cik tas nepieciešams šim nolūkam.

2. Elektronisko sakaru un pakalpojumu sniedzēji drīkst apstrādāt elektronisko sakaru metadatus, ja:

(a) tas ir jādara, lai tik ilgi, cik nepieciešams šim nolūkam, nodrošinātu pakalpojumu kvalitātes obligāto līmeni saskaņā ar [Direktīvu par Eiropas Elektronisko sakaru kodeksa izveidi] vai Regulu (ES) 2015/2120[11], vai

(b) tas ir jādara saistībā ar rēķinu sagatavošanu, starpsavienojumu maksas aprēķināšanu, elektronisko pakalpojumu krāpnieciskas vai ļaunprātīgas izmantošanas atklāšanu vai apturēšanu vai elektronisko sakaru pakalpojumu abonēšanu, vai

(c) attiecīgais galalietotājs ir devis piekrišanu viņa sakaru metadatu apstrādei vienam vai vairākiem konkrētiem nolūkiem, tostarp attiecībā uz konkrētu pakalpojumu sniegšanu šādiem galalietotājiem, ar nosacījumu, ka attiecīgo nolūku vai nolūkus nevar sasniegt, apstrādājot anonimizētu informāciju.

3. Elektronisko sakaru un pakalpojumu sniedzēji drīkst apstrādāt elektronisko sakaru saturu tikai tad, ja:

(a) tas tiek darīts vienīgi tāpēc, lai galalietotājam sniegtu konkrētu pakalpojumu, ja attiecīgais galalietotājs vai galalietotāji ir devuši piekrišanu viņu elektronisko sakaru satura apstrādei un minētā pakalpojuma sniegšana nav iespējama bez šāda satura apstrādes, vai

(b) ja visi attiecīgie galalietotāji ir devuši piekrišanu viņu elektronisko sakaru satura apstrādei vienam vai vairākiem konkrētiem nolūkiem, kurus nevar sasniegt, apstrādājot anonimizētu informāciju, un pakalpojumu sniedzējs ir apspriedies ar uzraudzības iestādi. Attiecībā uz apspriešanos ar uzraudzības iestādi piemēro Regulas (ES) 2016/679 36. panta 2. un 3. punktu.

7. pants
Elektronisko sakaru datu glabāšana un dzēšana

1. Neskarot 6. panta 1. punkta b) apakšpunktu un 6. panta 3. punkta a) un b) apakšpunktu, kad elektronisko sakaru saturu ir saņēmis paredzētais saņēmējs vai saņēmēji, elektronisko sakaru pakalpojumu sniedzējs dzēš elektronisko sakaru saturu vai padara minētos datus anonīmus. Šādus datus var ierakstīt vai saglabāt galalietotāji vai trešā persona, kurai galalietotāji ir uzticējuši tos ierakstīt, saglabāt vai citādi apstrādāt saskaņā ar Regulu (ES) 2016/679.

2. Neskarot 6. panta 1. punkta b) apakšpunktu un 6. panta 2. punkta a) un c) apakšpunktu, elektronisko sakaru pakalpojumu sniedzējs dzēš elektronisko sakaru metadatus vai padara minētos datus anonīmus tad, kad tie vairs nav vajadzīgi paziņojuma pārraidīšanai.

[11] Eiropas Parlamenta un Padomes 2015. gada 25. novembra Regula (ES) 2015/2120, ar ko nosaka pasākumus sakarā ar piekļuvi atvērtam internetam un groza Direktīvu 2002/22/EK par universālo pakalpojumu un lietotāju tiesībām attiecībā uz elektronisko sakaru tīkliem un pakalpojumiem un Regulu (ES) Nr. 531/2012 par viesabonēšanu publiskajos mobilo sakaru tīklos Savienībā (OV L 310, 26.11.2015., 1.–18. lpp.).

3. Ja elektronisko sakaru metadati tiek apstrādāti rēķinu sagatavošanas nolūkā saskaņā ar 6. panta 2. punkta b) apakšpunktu, attiecīgos metadatus var glabāt līdz tā termiņa beigām, kura laikā saskaņā ar valsts tiesību aktiem rēķinu var likumīgi apstrīdēt vai saņemt maksājumu.

8. pants

Galalietotāja galiekārtā glabātās un ar to saistītās informācijas aizsardzība

1. Galiekārtas apstrādes un saglabāšanas spēju izmantošana un informācijas vākšana no galalietotāju galiekārtām, tostarp par to programmatūru un aparatūru, ja to neveic attiecīgais galalietotājs, ir aizliegta, izņemot gadījumus, ja:

(a) tas ir jādara tikai un vienīgi tādēļ, lai veiktu elektroniskās saziņas pārraidīšanu elektronisko sakaru tīklā, vai

(b) galalietotājs ir devis piekrišanu, vai

(c) tas ir jādara, lai sniegtu galalietotāja pieprasītu informācijas sabiedrības pakalpojumu, vai

(d) tas ir jādara, lai veiktu tīmekļa mērķauditorijas mērījumus, ar nosacījumu, ka tos veic informācijas sabiedrības pakalpojumu sniedzējs, kam to lūdzis galalietotājs.

2. Tādas informācijas vākšana, ko galiekārta emitē, lai būtu iespējama tās savienošana ar citu ierīci vai tīklu iekārtu, ir aizliegta, izņemot gadījumus, ja:

(a) tas tiek darīts tikai un vienīgi savienojuma izveidošanas nolūkā un tikai uz tam nepieciešamo laiku, vai

(b) parādās skaidrs un nepārprotams paziņojums vismaz par šādas vākšanas kārtību, tās mērķi, atbildīgo personu un citiem aspektiem, par kuriem jāinformē saskaņā ar Regulas (ES) 2016/679 13. pantu gadījumos, kad tiek vākti personas dati, kā arī jebkuru pasākumu, ko galalietotājs var veikt, lai apturētu vai minimalizētu šādu informācijas vākšanu.

Šādas informācijas vākšana ir atkarīga no tā, vai ir veikti piemēroti tehniski un organizatoriski pasākumi, kuru mērķis ir nodrošināt riskiem atbilstošas pakāpes drošību, kā noteikts Regulas (ES) 2016/679 32. pantā.

3. Informāciju, kas jāsniedz saskaņā ar 2. punkta b) apakšpunktu, var sniegt apvienojumā ar standartizētām ikonām, lai viegli uztveramā, saprotamā un skaidri salasāmā veidā sniegtu jēgpilnu pārskatu par savākto.

4. Komisija tiek pilnvarota saskaņā ar 27. pantu pieņemt deleģētos aktus, kuros nosaka ar standartizēto ikonu sniedzamo informāciju un procedūras standartizētu ikonu nodrošināšanai.

9. pants

Piekrišana

1. Attiecībā uz piekrišanu piemēro definīciju un nosacījumus, kas paredzēti Regulas (ES) 2016/679 4. panta 11. punktā un 7. pantā.

2. Neskarot 1. punktu – ja vien tas ir tehniski iespējami un rentabli, 8. panta 1. punkta b) apakšpunkta vajadzībām piekrišanu var dot, izmantojot atbilstīgus tehniskos iestatījumus pārlūkprogrammā, kas ļauj piekļūt internetam.

3. Galalietotājiem, kuri snieguši piekrišanu elektronisko sakaru datu apstrādei, kā noteikts 6. panta 2. punkta c) apakšpunktā un 6. panta 3. punkta a) un b) apakšpunktā, ir iespēja jebkurā laikā piekrišanu atsaukt, kā noteikts Regulas (ES) 2016/679 7. panta 3. punktā, un viņiem periodiski, ik pēc 6 mēnešiem, kamēr vien apstrāde turpinās, tiek atgādināts par šo iespēju.

10. pants

Sniedzamā informācija un iespējas attiecībā uz privātuma iestatījumiem

1. Tirgū laistā programmatūra, kas nodrošina elektroniskos sakarus, tostarp informācijas izguvi un parādīšanu internetā, piedāvā izvēlēties iespēju, kas liedz trešām personām saglabāt informāciju galalietotāja galiekārtā vai apstrādāt šādā galiekārtā jau saglabāto informāciju.

2. Uzreiz pēc instalēšanas programmatūra informē galalietotāju par privātuma iestatījumu iespējām un pirms instalēšanas turpināšanas pieprasa, lai galalietotājs piekristu iestatījumiem.

3. Ja 2018. gada 25. maijā programmatūra jau ir uzstādīta, 1. un 2. punktā minētās prasības ir jāievēro tad, kad tiek veikts pirmais programmatūras atjauninājums, taču ne vēlāk par 2018. gada 25. augustu.

11. pants

Ierobežojumi

1. Savienības vai dalībvalsts tiesību akti ar leģislatīvu pasākumu var ierobežot 5.–8. pantā paredzēto pienākumu un tiesību tvērumu, ja vien ar šādu ierobežojumu tiek ievērota pamattiesību un pamatbrīvību būtība un ja tas ir nepieciešams, piemērots un samērīgs demokrātiskas sabiedrības pasākums, kura mērķis ir garantēt vienu vai vairākas sabiedrības vispārējās intereses, kas minētas Regulas (ES) 2016/679 23. panta 1. punkta a)–e) apakšpunktā, vai uzraudzības, pārbaudes vai regulatīvo funkciju, kas saistīta ar oficiālu pilnvaru īstenošanu šādu interešu aizsardzības nolūkā.

2. Elektronisko sakaru pakalpojumu sniedzēji, pamatojoties uz leģislatīvu pasākumu, kas pieņemts atbilstīgi 1. punktam, izstrādā iekšējās procedūras, kas izmantojamas, lai atbildētu uz pieprasījumiem piekļūt galalietotāju elektronisko sakaru datiem. Elektronisko sakaru pakalpojumu sniedzēji pēc kompetentās uzraudzības iestādes pieprasījuma sniedz tai informāciju par minētajām procedūrām, saņemto pieprasījumu skaitu, attiecīgo juridisko pamatojumu un pakalpojumu sniedzēju atbildēm.

III NODAĻA
FIZISKU UN JURIDISKU PERSONU TIESĪBAS KONTROLĒT ELEKTRONISKOS SAKARUS

12. pants

Izsaucošā numura un savienotā numura uzrādīšana un uzrādīšanas ierobežošana

1. Ja izsaucošā un savienotā numura uzrādīšana tiek piedāvāta saskaņā ar [Direktīvas par Eiropas Elektronisko sakaru kodeksa izveidi] [107]. pantu, publiski pieejamu numuratkarīgu starppersonu sakaru pakalpojumu sniedzēji nodrošina, ka:

(a) izsaucošajam galalietotājam ir iespēja liegt izsaucošā numura uzrādīšanu atsevišķam izsaukumam, atsevišķam savienojumam vai pastāvīgi;

(b) izsauktajam galalietotājam ir iespēja liegt ienākošo izsaukumu izsaucošā numura uzrādīšanu;

(c) izsauktajam galalietotājam ir iespēja noraidīt ienākošos izsaukumus, ja izsaucošā numura uzrādīšanu ir liedzis izsaucošais galalietotājs;

(d) izsauktajam galalietotājam ir iespēja liegt savienotā numura uzrādīšanu izsaucošajam galalietotājam.

2. Iespējas, kas minētas 1. punkta a), b), c) un d) apakšpunktā, galalietotājiem tiek nodrošinātas ar vienkāršiem līdzekļiem un bez maksas.

3. Šā panta 1. punkta a) apakšpunkts attiecas arī uz izsaukumiem, kas no Savienības veikti uz trešām valstīm. Šā punkta 1. punkta b), c) un d) apakšpunkts attiecas arī uz ienākošajiem izsaukumiem no trešām valstīm.

4. Ja tiek piedāvāta izsaucošā vai savienotā numura uzrādīšana, publiski pieejamu numuratkarīgu starppersonu sakaru pakalpojumu sniedzēji informē sabiedrību par 1. punkta a), b), c) un d) apakšpunktā izklāstītajām iespējām.

13. pants

Izsaucošā numura un savienotā numura uzrādīšanas un ierobežošanas izņēmumi

1. Neatkarīgi no tā, vai izsaucošais galalietotājs ir liedzis uzrādīt izsaucošo numuru gadījumos, kad tas ir bijis neatliekamās palīdzības dienestu izsaukums, publiski pieejamu numuratkarīgu starppersonu sakaru pakalpojumu sniedzēji, lai nodrošinātu atbildi šādos sakaros, vērtē atsevišķi katru numuru organizācijām, kuru darbība ir saistīta ar neatliekamās palīdzības dienesta, tostarp ārkārtas izsaukumu centrāļu, sakariem, un attiecīgā gadījumā neievēro atteikšanos uzrādīt izsaucošo numuru un galalietotāja atteikšanos sniegt piekrišanu metadatu apstrādei vai tās neesamību.

2. Ja galalietotāji pieprasa ļaunprātīgu vai traucējošu izsaukumu izsekošanu, dalībvalstis izstrādā konkrētākus noteikumus par ieviešamajām procedūrām un apstākļiem, kad publiski pieejamu numuratkarīgu starppersonu sakaru pakalpojumu sniedzēji uz pagaidu laiku neievēro atteikšanos uzrādīt izsaucošo numuru.

14. pants

Ienākošā izsaukuma bloķēšana

Publiski pieejamu numuratkarīgu starppersonu sakaru pakalpojumu sniedzēji veic pasākumus, kuri atbilst jaunākajiem tehniskajiem sasniegumiem un ļauj galalietotājiem samazināt nevēlamu izsaukumu saņemšanu, turklāt izsauktajiem galalietotājiem bez maksas nodrošina šādas iespējas:

(a) bloķēt ienākošos izsaukumus no konkrētiem numuriem vai anonīmiem avotiem;

(b) pārtraukt izsaukumu automātisku pāradresēšanu uz galalietotāja galiekārtu, ko veic trešā persona.

15. pants
Publiski pieejami abonentu saraksti

1. Publiski pieejamu abonentu sarakstu pakalpojumu sniedzēji saņem piekrišanu no galalietotājiem, kas ir fiziskas personas, un tikai pēc tam to personas datus iekļauj abonentu sarakstā, un attiecīgi no minētajiem galalietotājiem saņem piekrišanu par katras personas datu kategorijas iekļaušanu, ciktāl šādi dati ir būtiski šāda abonentu saraksta izveidē atbilstīgi tam, kā noteicis saraksta pakalpojumu sniedzējs. Galalietotājiem, kuri ir fiziskas personas, sarakstu pakalpojumu sniedzēji nodrošina iespējas pārbaudīt, labot vai dzēst šādus datus.

2. Galalietotājus, kas ir fiziskas personas, kuru personas dati ir iekļauti publiski pieejamā abonentu sarakstā, attiecīgā saraksta pakalpojumu sniedzēji informē par izmantojamajām meklēšanas funkcijām un saņem galalietotāju piekrišanu pirms šādu meklēšanas funkciju aktivizēšanas saistībā ar viņu datiem.

3. Galalietotājiem, kuri ir juridiskas personas, publiski pieejamu abonentu sarakstu pakalpojumu sniedzēji nodrošina iespēju iebilst pret tādu datu iekļaušanu abonentu sarakstā, kas saistīti ar šiem galalietotājiem. Šādiem galalietotājiem, kuri ir juridiskas personas, sarakstu pakalpojumu sniedzēji nodrošina iespējas pārbaudīt, labot vai dzēst šādus datus.

4. Iespēja galalietotājiem izvēlēties netikt iekļautiem publiski pieejamā abonentu sarakstā vai pārbaudīt, labot vai dzēst jebkurus datus, kas saistīti ar šiem galalietotājiem, ir izmantojama bez maksas.

16. pants
Nepasūtīti paziņojumi

1. Fiziskas vai juridiskas personas drīkst izmantot elektronisko sakaru pakalpojumus, lai nosūtītu tiešās tirgvedības paziņojumus galalietotājiem, kas ir fiziskas personas, kuras tam sniegušas piekrišanu.

2. Ja saskaņā ar Regulu (ES) 2016/679 saistībā ar produkta vai pakalpojuma pārdošanu fiziska vai juridiska persona no sava klienta iegūst elektronisko kontaktinformāciju elektroniskā pasta nosūtīšanai, tad minētā fiziskā vai juridiskā persona var izmantot šo elektronisko kontaktinformāciju savu līdzīgu produktu vai pakalpojumu tiešajā tirgvedībā tikai tad, ja klientiem skaidri un nepārprotami ir dota iespēja bez maksas un vienkāršā veidā izteikt iebildumus pret šādu izmantošanu. Tiesības izteikt iebildumus tiek dotas ikreiz, kad tiek vākta informācija un nosūtīts paziņojums.

3. Neskarot 1. un 2. punktu, fiziskas vai juridiskas personas, kas izmanto elektronisko sakaru pakalpojumus tiešās tirgvedības izsaukumiem:

(a) uzrāda tā tiešā numura identifikatoru, kuru izmantojot, var sazināties ar attiecīgo personu, vai

(b) uzrāda īpašu kodu vai prefiksu, kas norāda uz to, ka tas ir tirgvedības izsaukums.

4. Neskarot 1. punktu, dalībvalstis tiesību aktos var paredzēt, ka tiešās tirgvedības balss izsaukumi, kas adresēti galalietotājiem, kuri ir fiziskas personas, ir atļauti tikai attiecībā uz tiem galalietotājiem, kas ir fiziskas personas, kuras nav izteikušas iebildumus pret šo paziņojumu saņemšanu.

5. Saskaņā ar Savienības tiesību aktiem un spēkā esošajiem valsts tiesību aktiem dalībvalstis nodrošina, lai pietiekami tiktu aizsargātas galalietotāju, kas ir juridiskas

personas, likumīgās intereses attiecībā uz nepasūtītiem paziņojumiem, kuri nosūtīti ar 1. punktā paredzētajiem līdzekļiem.

6. Jebkura fiziska vai juridiska persona, kas izmanto elektronisko sakaru pakalpojumus tiešās tirgvedības paziņojumu pārraidīšanai, informē galalietotājus par paziņojumu tirgvedības raksturu un tās juridiskās vai fiziskās personas identitāti, kuras vārdā šie paziņojumi tiek pārraidīti, kā arī sniedz informāciju, kas saņēmējiem ir vajadzīga, lai izmantotu savas tiesības vienkāršā veidā atsaukt savu piekrišanu attiecībā uz turpmāku tirgvedības paziņojumu saņemšanu.

7. Komisija ir pilnvarota saskaņā ar 26. panta 2. punktu pieņemt īstenošanas pasākumus, kuros tā precizē kodu vai prefiksu, kas norāda uz to, ka tas ir tirgvedības izsaukums atbilstīgi 3. punkta b) apakšpunktam.

17. pants
Informācija par konstatētajiem drošības riskiem

Pastāvot īpašam riskam, kas var apdraudēt tīklu un elektronisko sakaru pakalpojumu drošību, elektronisko sakaru pakalpojumu sniedzējs informē attiecīgos galalietotājus par šādu risku, un, ja šāds risks neietilpst pakalpojuma sniedzēja pieņemamo pasākumu tvērumā, informē galalietotājus par jebkuriem tiesiskās aizsardzības līdzekļiem, iekļaujot norādi par iespējamām saistītajām izmaksām.

IV NODAĻA
NEATKARĪGAS UZRAUDZĪBAS IESTĀDES UN NOTEIKUMU IZPILDE

18. pants
Neatkarīgās uzraudzības iestādes

1. Neatkarīgā uzraudzības iestāde vai iestādes, kas ir atbildīgas par Regulas (ES) 2016/679 piemērošanu, ir atbildīgas arī par šīs regulas piemērošanas uzraudzību. Regulas (ES) 2016/679 VI un VII nodaļu piemēro pēc analoģijas. Uzraudzības iestāžu uzdevumus un pilnvaras īsteno attiecībā uz galalietotājiem.

2. Uzraudzības iestāde vai iestādes, kuras minētas 1. punktā, vajadzības gadījumā sadarbojas ar valsts regulatīvajām iestādēm, kas izveidotas saskaņā ar [Direktīvu par Eiropas Elektronisko sakaru kodeksa izveidi].

19. pants
Eiropas Datu aizsardzības kolēģija

Eiropas Datu aizsardzības kolēģijai, kas izveidota saskaņā ar Regulas (ES) 2016/679 68. pantu, ir pilnvaras nodrošināt šīs regulas konsekventu piemērošanu. Šādā nolūkā Eiropas Datu aizsardzības kolēģija veic uzdevumus, kas izklāstīti Regulas (ES) 2016/679 70. pantā. Kolēģijai ir arī šādi uzdevumi:

(a) dot padomus Komisijai par visiem ierosinātajiem šīs regulas grozījumiem;

(b) pēc pašas kolēģijas iniciatīvas, pēc sava locekļa vai Komisijas pieprasījuma izskatīt jautājumus, kas attiecas uz šīs regulas piemērošanu, un nākt klajā ar

pamatnostādnēm, ieteikumiem un paraugpraksi, lai veicinātu šīs regulas konsekventu piemērošanu.

20. pants
Sadarbība un konsekvences nodrošināšanas procedūras

Katra uzraudzības iestāde palīdz nodrošināt šīs regulas konsekventu piemērošanu visā Savienībā. Šajā nolūkā saskaņā ar Regulas (ES) 2016/679 VII nodaļu uzraudzības iestādes sadarbojas cita ar citu un ar Komisiju jautājumos, uz ko attiecas šī regula.

V NODAĻA
TIESISKĀS AIZSARDZĪBAS LĪDZEKĻI, ATBILDĪBA UN SANKCIJAS

21. pants
Tiesiskās aizsardzības līdzekļi

1. Neskarot citus administratīvās vai tiesiskās aizsardzības līdzekļus, katram elektronisko sakaru pakalpojumu galalietotājam ir izmantojami tādi paši tiesiskās aizsardzības līdzekļi, kādi paredzēti Regulas (ES) 2016/679 77., 78., un 79. pantā.

2. Jebkurai fiziskai vai juridiskai personai, kas nav galalietotājs, bet kuru negatīvi ietekmējuši šīs regulas pārkāpumi un kurai ir likumīgas intereses izbeigt vai aizliegt iespējamos pārkāpumus, ieskaitot elektronisko sakaru pakalpojumu sniedzēju, kurš aizsargā savas likumīgās darījumdarbības intereses, ir tiesības vērsties tiesā pret tādiem pārkāpumiem.

22. pants
Tiesības uz kompensāciju un atbildība

Elektronisko sakaru pakalpojumu galalietotājiem, kuriem šīs regulas pārkāpuma rezultātā ir nodarīts materiāls vai nemateriāls kaitējums, ir tiesības no regulas pārkāpēja saskaņā ar Regulas (ES) 2016/679 82. pantu saņemt kompensāciju par nodarīto kaitējumu, ja vien pārkāpējs nepierāda, ka nekādā veidā nav atbildīgs par notikumu, ar ko nodarīts attiecīgais kaitējums.

23. pants
Vispārīgi nosacījumi par administratīvo naudas sodu piemērošanu

1. Piemērojot šo pantu, šīs regulas noteikumu pārkāpumiem piemēro Regulas (ES) 2016/679 VII nodaļu.

2. Administratīvus naudas sodus apmērā līdz EUR 10 000 000 vai, uzņēmuma gadījumā, līdz 2 % no tā kopējā visā pasaulē iepriekšējā finanšu gadā gūtā gada apgrozījuma atkarībā no tā, kuras summas apmērs ir lielāks, saskaņā ar 1. punktu piemēro par šādiem šīs regulas noteikumu pārkāpumiem:

(a) pienākumi, kas saskaņā ar 8. pantu noteikti jebkurai juridiskai vai fiziskai personai, kura apstrādā elektronisko sakaru datus;

(b) pienākumi, kas saskaņā ar 10. pantu noteikti programmatūras nodrošinātājam, kurš ļauj veikt elektronisko sakarus;

(c) pienākumi, kas saskaņā ar 15. pantu noteikti publiski pieejamu abonentu sarakstu pakalpojumu sniedzējiem;

(d) pienākumi, kas saskaņā ar 16. pantu noteikti jebkurai juridiskai vai fiziskai personai, kura izmanto elektronisko sakaru pakalpojumus.

3. Par 5., 6. un 7. pantā paredzētā sakaru konfidencialitātes principa, elektronisko sakaru datu atļautās apstrādes un datu dzēšanai paredzēto termiņu neievērošanu saskaņā ar šā panta 1. punktu piemēro administratīvus naudas sodus apmērā līdz EUR 20 000 000 vai, uzņēmuma gadījumā, līdz 4 % no tā kopējā visā pasaulē iepriekšējā finanšu gadā gūtā gada apgrozījuma atkarībā no tā, kuras summas apmērs ir lielāks.

4. Dalībvalstis pieņem noteikumus par sodiem, ko piemēro par 12., 13., 14. un 17. panta pārkāpumiem.

5. Par 18. pantā minētās uzraudzības iestādes rīkojuma neievērošanu piemēro administratīvus naudas sodus apmērā līdz EUR 20 000 000 vai, uzņēmuma gadījumā, līdz 4 % no tā kopējā visā pasaulē iepriekšējā finanšu gadā gūtā gada apgrozījuma atkarībā no tā, kuras summas apmērs ir lielāks.

6. Neskarot 18. pantā paredzētās uzraudzības iestāžu korektīvās pilnvaras, katra dalībvalsts var izstrādāt noteikumus par to, vai un līdz kādam apjomam administratīvos naudas sodus var piemērot publiskām iestādēm un struktūrām, kas ir iedibinātas minētajā dalībvalstī.

7. Uzraudzības iestādes pilnvaru veikšanai saskaņā ar šo pantu piemēro atbilstošas procesuālas garantijas saskaņā ar Savienības un dalībvalsts tiesību aktiem, tostarp efektīvu tiesību aizsardzību tiesā un pienācīgu procedūru ievērošanu.

8. Ja dalībvalsts tiesību sistēmā nav paredzēti administratīvi naudas sodi, šo pantu var piemērot tā, ka naudas sodu ierosina kompetentā uzraudzības iestāde, bet uzliek kompetentās valsts tiesas, vienlaikus nodrošinot, ka minētie tiesiskās aizsardzības līdzekļi ir efektīvi un tiem ir līdzvērtīga iedarbība ar uzraudzības iestāžu uzliktiem administratīviem naudas sodiem. Jebkurā gadījumā uzliktie naudas sodi ir iedarbīgi, samērīgi un atturoši. Līdz [...] minētās dalībvalstis Komisijai dara zināmus to tiesību aktu noteikumus, ko tās pieņem, ievērojot šo punktu, un nekavējoties paziņo Komisijai par turpmākiem grozījumu aktiem vai šo noteikumu grozījumiem.

24. pants
Sankcijas

1. Dalībvalstis paredz noteikumus par citām sankcijām, ko piemēro par šīs regulas pārkāpumiem, jo īpaši pārkāpumiem, par kuriem nav paredzēti administratīvi naudas sodi saskaņā ar 23. pantu, un veic visus nepieciešamos pasākumus, lai nodrošinātu, ka šos noteikumus īsteno. Šādas sankcijas ir iedarbīgas, samērīgas un atturošas.

2. Ne vēlāk kā 18 mēnešus pēc 29. panta 2. punktā noteiktās dienas katra dalībvalsts paziņo Komisijai to tiesību aktu noteikumus, ko tā pieņem, ievērojot 1. punktu, un nekavējoties paziņo Komisijai par jebkuriem turpmākiem šo noteikumu grozījumiem.

VI NODAĻA
DELEĢĒTIE AKTI UN ĪSTENOŠANAS AKTI

25. pants
Deleģēšanas īstenošana

1. Pilnvaras pieņemt deleģētos aktus Komisijai piešķir, ievērojot šajā pantā izklāstītos nosacījumus.

2. Pilnvaras pieņemt 8. panta 4. punktā minētos deleģētos aktus Komisijai piešķir uz nenoteiktu laiku no [šīs regulas spēkā stāšanās dienas].

3. Eiropas Parlaments vai Padome jebkurā laikā var atsaukt 8. panta 4. punktā minēto pilnvaru deleģēšanu. Ar lēmumu par atsaukšanu izbeidz tajā norādīto pilnvaru deleģēšanu. Lēmums stājas spēkā nākamajā dienā pēc tā publicēšanas *Eiropas Savienības Oficiālajā Vēstnesī* vai vēlākā dienā, kas tajā norādīta. Tas neskar jau spēkā esošos deleģētos aktus.

4. Pirms deleģētā akta pieņemšanas Komisija apspriežas ar ekspertiem, kurus katra dalībvalsts iecēlusi saskaņā ar principiem, kas noteikti 2016. gada 13. aprīļa Iestāžu nolīgumā par labāku likumdošanas procesu.

5. Tiklīdz Komisija pieņem deleģētu aktu, tā par to paziņo vienlaikus Eiropas Parlamentam un Padomei.

6. Saskaņā ar 8. panta 4. punktu pieņemts deleģētais akts stājas spēkā tikai tad, ja divos mēnešos no dienas, kad minētais akts paziņots Eiropas Parlamentam un Padomei, ne Eiropas Parlaments, ne Padome nav izteikuši iebildumus, vai ja pirms minētā laikposma beigām gan Eiropas Parlaments, gan Padome ir informējuši Komisiju par savu nodomu neizteikt iebildumus. Pēc Eiropas Parlamenta vai Padomes iniciatīvas šo laikposmu pagarina par diviem mēnešiem.

26. pants
Komiteju procedūra

1. Komisijai palīdz Sakaru komiteja, kas ir ar [Direktīvas par Eiropas Elektronisko sakaru kodeksa izveidi] 110. pantu izveidotā Komunikāciju komiteja. Minētā komiteja ir komiteja Regulas (ES) Nr. 182/2011[12] nozīmē.

2. Ja ir atsauce uz šo punktu, piemēro Regulas (ES) Nr. 182/2011 5. pantu.

VII NODAĻA
NOBEIGUMA NOTEIKUMI

27. pants
Atcelšana

1. Direktīvu 2002/58/EK atceļ no 2018. gada 25. maija.

[12] Eiropas Parlamenta un Padomes 2011. gada 16. februāra Regula (ES) Nr. 182/2011, ar ko nosaka normas un vispārīgus principus par dalībvalstu kontroles mehānismiem, kuri attiecas uz Komisijas īstenošanas pilnvaru izmantošanu (OV L 55, 28.2.2011., 13.–18. lpp.).

2. Atsauces uz atcelto direktīvu uzskata par atsaucēm uz šo regulu.

28. pants
Uzraudzības un izvērtēšanas klauzula

Ne vēlāk kā 2018. gada 1. janvārī Komisija sagatavo sīki izstrādātu programmu, lai uzraudzītu šīs regulas efektivitāti.

Ne vēlāk kā trīs gadus pēc šīs regulas stāšanās spēkā un pēc tam reizi trijos gados Komisija veic šīs regulas izvērtēšanu un ziņo par galvenajiem konstatējumiem Eiropas Parlamentam, Padomei un Eiropas Ekonomikas un sociālo lietu komitejai. Izvērtējumā vajadzības gadījumā, ņemot vērā juridisko, tehnisko un ekonomisko attīstību, informē par priekšlikumu izdarīt grozījumus šajā regulā vai to atcelt.

29. pants
Stāšanās spēkā un piemērošana

1. Šī regula stājas spēkā divdesmitajā dienā pēc tās publicēšanas *Eiropas Savienības Oficiālajā Vēstnesī.*

2. To piemēro no 2018. gada 25. maija.

Šī regula uzliek saistības kopumā un ir tieši piemērojama visās dalībvalstīs.

Briselē,

Eiropas Parlamenta vārdā —	*Padomes vārdā —*
priekšsēdētājs	*priekšsēdētājs*