EIROPAS PARLAMENTA UN PADOMES REGULA (ES) 2018/1807

(2018. gada 14. novembris)

par satvaru nepersondatu brīvai apritei Eiropas Savienībā

(Dokuments attiecas uz EEZ)

EIROPAS PARLAMENTS UN EIROPAS SAVIENĪBAS PADOME,

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

ņemot vērā Eiropas Komisijas priekšlikumu,

pēc leģislatīvā akta projekta nosūtīšanas valstu parlamentiem,

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

pēc apspriešanās ar Reģionu komiteju,

saskaņā ar parasto likumdošanas procedūru ([2]),

tā kā:

(1) Ekonomikas digitalizācija kļūst aizvien straujāka. Informācijas un komunikācijas tehnoloģijas vairs nav specifiska nozare, bet gan pamats visām mūsdienu inovatīvajām ekonomikas sistēmām un sabiedrībai. Šo sistēmu centrā ir elektroniskie dati, un, tos analizējot vai kombinējot ar pakalpojumiem un produktiem, tie var radīt lielu vērtību. Tajā pašā laikā datu ekonomikas straujā attīstība un jaunās tehnoloģijas, piemēram, mākslīgais intelekts, ar lietu internetu saistītie produkti un pakalpojumi, autonomas sistēmas un 5G, rada jaunas juridiskas problēmas saistībā ar piekļuvi datiem un to atkalizmantošanu, atbildību, ētiku un solidaritāti. Būtu jāpievēršas jautājumam par atbildību, jo īpaši ar pašregulējošu kodeksu un cita veida labākās prakses ieviešanas palīdzību, ņemot vērā ieteikumus un lēmumus, kas tiek pieņemti, un darbības, kas tiek veiktas bez cilvēka iejaukšanās visā datu apstrādes vērtības veidošanās ķēdē. Šā darba procesā varētu arī iekļaut atbilstošus mehānismus atbildības noteikšanai, atbildības nodošanai starp dienestiem, kas savstarpēji sadarbojas, apdrošināšanai un revīzijai.

(2) Datu vērtības veidošanās ķēdes balstās uz dažādām ar datiem veiktām darbībām: datu radīšanu un vākšanu, datu apkopošanu un organizēšanu, datu apstrādi, datu analīzi, tirgvedību un izplatīšanu, datu izmantošanu un atkalizmantošanu. Ikvienas datu vērtības veidošanās ķēdes svarīgs elements ir efektīva un lietderīga datu apstrāde. Tomēr efektīvu un lietderīgu datu apstrādi un datu ekonomikas attīstību Savienībā jo īpaši kavē divu veidu šķēršļi datu mobilitātei un iekšējam tirgum: dalībvalstu iestāžu ieviestās datu teritoriālas ierobežošanas prasības un tāda prakse kā piesaiste pārdevējam privātajā sektorā.

(3) Saskaņā ar Līgumu par Eiropas Savienības darbību (LESD) uz datu apstrādes pakalpojumiem attiecas brīvība veikt uzņēmējdarbību un pakalpojumu sniegšanas brīvība. Taču minēto pakalpojumu sniegšanu traucē un reizēm pat liedz atsevišķas valsts, reģionālās vai vietējās prasības, ka datiem ir jāatrodas konkrētā teritorijā.

(4) Šādus šķēršļus datu apstrādes pakalpojumu brīvai apritei un pakalpojumu sniedzēju tiesībām veikt uzņēmējdarbību rada dalībvalstu tiesību aktos ietvertās prasības, lai dati apstrādes vajadzībām atrastos konkrētā ģeogrāfiskā apgabalā vai teritorijā. Tāda pati ietekme ir citiem noteikumiem vai administratīvai praksei, kas paredz īpašas prasības, kuras apgrūtina datu apstrādi ārpus noteikta ģeogrāfiskā apgabala vai teritorijas Savienībā, piemēram, prasība izmantot konkrētā dalībvalstī sertificētus vai apstiprinātus tehnoloģiskos līdzekļus. Turklāt tirgus dalībniekiem un publiskajam sektoram pieejamās izvēles iespējas datu apstrādes vietas ziņā ierobežo arī juridiskā nenoteiktība par pamatotu un nepamatotu datu teritoriālu ierobežošanas prasību apmēru. Šī regula nekādā ziņā neierobežo uzņēmumu brīvību slēgt līgumus, kuros tiek precizēta vieta, kur datiem ir jāatrodas. Šī regula ir paredzēta tikai tam, lai aizsargātu minēto brīvību, nodrošinot, ka vieta, kurā vienojas turēt datus, var būt jebkur Savienības teritorijā.

([1]) OV C 227, 28.6.2018., 78. lpp.
([2]) Eiropas Parlamenta 2018. gada 4. oktobra nostāja (*Oficiālajā Vēstnesī* vēl nav publicēta) un Padomes 2018. gada 6. novembra lēmums.

(5) Tajā pašā laikā datu mobilitāti Savienībā kavē arī privāta rakstura ierobežojumi: juridiskas, līgumiskas un tehniskas problēmas, kas datu apstrādes pakalpojumu lietotājiem apgrūtina vai liedz savus datus pārnest no viena pakalpojumu sniedzēja pie cita vai atpakaļ uz savām informācijas tehnoloģiju (IT) sistēmām, jo īpaši tad, kad beidzas to līgums ar kādu pakalpojumu sniedzēju.

(6) Minēto šķēršļu kombinācija ir izraisījusi konkurences trūkumu starp mākoņpakalpojumu sniedzējiem Savienībā, dažādas problēmas, kas saistītas ar grūtībām mainīt pakalpojumu sniedzēju, un nopietnu datu mobilitātes trūkumu. Tāpat arī datu teritoriālas ierobežošanas politika ir mazinājusi pētniecības un izstrādes uzņēmumu spēju atvieglot sadarbību starp uzņēmumiem, augstskolām un citām pētniecības organizācijām nolūkā veicināt inovāciju.

(7) Juridiskās noteiktības labad un ņemot vērā nepieciešamību Savienībā nodrošināt vienlīdzīgus konkurences apstākļus, svarīgs iekšējā tirgus darbības elements ir visiem tirgus dalībniekiem vienots noteikumu kopums. Lai likvidētu šķēršļus tirdzniecībai un konkurences izkropļojumus, ko rada atšķirības starp valstu tiesību aktiem, un novērstu iespējamu tirdzniecības šķēršļu un būtisku konkurences izkropļojumu rašanos nākotnē, būtu jāpieņem visās dalībvalstīs piemērojami vienoti noteikumi.

(8) Šī regula neskar tiesisko regulējumu attiecībā uz fizisku personu aizsardzību saistībā ar persondatu apstrādi, kā arī attiecībā uz privātās dzīves neaizskaramību un persondatu aizsardzību elektroniskajos sakaros un jo īpaši Eiropas Parlamenta un Padomes Regulu (ES) 2016/679 ([1]) un Eiropas Parlamenta un Padomes Direktīvas (ES) 2016/680 ([2]) un 2002/58/EK ([3]).

(9) Būtiski nepersondatu avoti ir lietu internets, mākslīgais intelekts un mašīnmācīšanās – parādības, kas vēršas plašumā –, piemēram, kad tie tiek izmantoti automatizētos rūpnieciskās ražošanas procesos. Konkrēti nepersondatu piemēri ir apkopotas un anonimizētas datu kopas, ko izmanto lielo datu analīzei, dati par precīzo lauksaimniecību, kuri var palīdzēt uzraudzīt un optimizēt pesticīdu un ūdens izmantošanu, un dati par vajadzībām, kas saistītas ar rūpniecības iekārtu uzturēšanu. Ja tehnoloģiskā attīstība dod iespēju anonimizētus datus pārveidot par persondatiem, šādi dati uzskatāmi par persondatiem un attiecīgi ir piemērojama Regula (ES) 2016/679.

(10) Saskaņā ar Regulu (ES) 2016/679 dalībvalstis nedrīkst nedz ierobežot, nedz aizliegt brīvu persondatu apriti Savienībā tādu iemeslu dēļ, kas saistīti ar fizisku personu aizsardzību attiecībā uz persondatu apstrādi. Šī regula paredz tādu pašu brīvas aprites principu Savienībā arī attiecībā uz nepersondatiem, izņemot gadījumus, kad šāds ierobežojums vai aizliegums ir pamatots sabiedriskās drošības apsvērumu dēļ. Regula (ES) 2016/679 un šī regula paredz saskaņotu noteikumu kopumu, ar kuriem nodrošina dažāda veida datu brīvu apriti. Turklāt šī regula neuzliek pienākumu šo dažādo veidu datus glabāt atsevišķi.

(11) Lai izveidotu satvaru nepersondatu brīvai plūsmai Savienībā un pamatus datu ekonomikas attīstībai un Savienības rūpniecības konkurētspējas uzlabošanai, nepieciešams noteikt skaidru, visaptverošu un paredzamu tiesisko regulējumu datu, kas nav persondati, apstrādei iekšējā tirgū. Uz principiem balstītai pieejai, kas paredz sadarbību starp dalībvalstīm un pašregulāciju, būtu jānodrošina, ka šis satvars ir pietiekami elastīgs, lai ņemtu vērā jaunās lietotāju, pakalpojumu sniedzēju un valsts iestāžu vajadzības Savienībā. Lai izvairītos no iespējamas pārklāšanās ar pastāvošajiem mehānismiem, tādējādi novēršot lielāku slogu gan dalībvalstīm, gan uzņēmumiem, nebūtu jānosaka detalizēti tehniskie noteikumi.

(12) Šai regulai nebūtu jāskar datu apstrāde, ja to veic kā daļu no darbības, kas neietilpst Savienības tiesību aktu piemērošanas jomā. Jo īpaši būtu jāatgādina, ka saskaņā ar Līguma par Eiropas Savienību (LES) 4. pantu valsts drošība ir vienīgi katras dalībvalsts atbildībā.

([1]) Eiropas Parlamenta un Padomes Regula (ES) 2016/679 (2016. gada 27. aprīlis) 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. lpp.).

([2]) Eiropas Parlamenta un Padomes Direktīva (ES) 2016/680 (2016. gada 27. aprīlis) par fizisku personu aizsardzību attiecībā uz personas datu apstrādi, ko veic kompetentās iestādes, lai novērstu, izmeklētu, atklātu noziedzīgus nodarījumus vai sauktu pie atbildības par tiem vai izpildītu krimināsodus, un par šādu datu brīvu apriti, ar ko atceļ Padomes Pamatlēmumu 2008/977/TI (OV L 119, 4.5.2016., 89. lpp.).

([3]) Eiropas Parlamenta un Padomes Direktīva 2002/58/EK (2002. gada 12. jūlijs) 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.).

(13) Brīvai datu plūsmai Savienībā būs svarīga loma datu virzītas izaugsmes un inovācijas nodrošināšanā. Tāpat kā uzņēmumi un patērētāji arī dalībvalstu publiskās iestādes un publisko tiesību subjekti var gūt labumu no lielākas no datiem atkarīgu pakalpojumu sniedzēju izvēles brīvības, konkurētspējīgākām cenām un efektīvākas pakalpojumu sniegšanas iedzīvotājiem. Ņemot vērā lielos datu apjomus, ar ko rīkojas publiskās iestādes un publisko tiesību subjekti, ir ļoti svarīgi, lai tie rādītu piemēru, izmantojot datu apstrādes pakalpojumus, un atturētos no ierobežojumiem datu teritoriālas ierobežošanas jomā, kad tie izmanto datu apstrādes pakalpojumus. Tādēļ šīs regulas piemērošanas jomā būtu jāiekļauj publiskās iestādes un publisko tiesību subjekti. No iepriekš minētā izriet, ka šajā regulā paredzētais brīvas nepersondatu plūsmas princips būtu arī jāpiemēro vispārējai un konsekventai administratīvajai praksei un citām datu teritoriālas ierobežošanas prasībām publiskā iepirkuma jomā, neskarot Eiropas Parlamenta un Padomes Direktīvu 2014/24/ES ([1]).

(14) Tāpat kā Direktīva 2014/24/ES šī regula neskar normatīvos un administratīvos aktus, kas attiecas uz dalībvalstu iekšējo organizāciju un ar ko publiskām iestādēm un publisko tiesību subjektiem piešķir pilnvaras un pienākumus datu apstrādes jomā bez līgumā noteikta privāto tiesību subjektu atalgojuma, kā arī tādus dalībvalstu normatīvos un administratīvos aktus, kuros paredzēta minēto pilnvaru un pienākumu īstenošana. Lai gan publiskās iestādes un publisko tiesību subjekti tiek mudināti apsvērt ekonomiskos un citus ieguvumus, ko sniedz ārpakalpojumu sniedzēju nolīgšana, tiem varētu būt pamatoti iemesli izvēlēties pakalpojumus nodrošināt pašiem vai izraudzīties to sniedzēju no sava vidus. Līdz ar to nekas šajā regulā dalībvalstīm neuzliek par pienākumu slēgt līgumus par ārpakalpojumiem vai izmantot ārpakalpojumu sniedzējus tādu pakalpojumu sniegšanai, kurus tās vēlas sniegt pašas vai organizēt to sniegšanu, izmantojot līdzekļus, kas nav publiskā iepirkuma līgumi.

(15) Šī regula būtu jāpiemēro fiziskām vai juridiskām personām, kas sniedz datu apstrādes pakalpojumus lietotājiem, kuriem Savienībā ir pastāvīga dzīvesvieta vai reģistrācijas vieta, tostarp personām, kuras Savienībā sniedz datu apstrādes pakalpojumus, lai gan tām tajā nav reģistrācijas vietas. Tādēļ šo regulu nevajadzētu attiecināt uz datu apstrādes pakalpojumiem, kas notiek ārpus Savienības, un datu teritoriālas ierobežošanas prasībām, kuras piemēro šādiem datiem.

(16) Šī regula neparedz noteikumus par komerclietās piemērojamu tiesību aktu noteikšanu, un tāpēc tā neskar Eiropas Parlamenta un Padomes Regulu (EK) Nr. 593/2008 ([2]). Jo īpaši – ciktāl līgumam piemērojamie tiesību akti nav izraudzīti saskaņā ar minēto regulu – pakalpojumu sniegšanas līgumu principā reglamentē tās valsts tiesību akti, kurā pakalpojumu sniedzējam ir parastā rezidences vieta.

(17) Šī regula būtu jāpiemēro datu apstrādei visplašākā nozīmē, aptverot visu veidu IT sistēmu izmantošanu neatkarīgi no tā, vai tās atrodas lietotāja telpās, vai ir uzticētas pakalpojumu sniedzējam. Tai būtu jāaptver dažādas intensitātes pakāpes datu apstrāde – no datu glabāšanas (infrastruktūra kā pakalpojums (*IaaS*)) līdz datu apstrādei platformās (platforma kā pakalpojums (*PaaS*)) vai lietotnēs (programmatūra kā pakalpojums (*SaaS*)).

(18) Datu teritoriālas ierobežošanas prasības ir nepārprotams šķērslis brīvai datu apstrādes pakalpojumu sniegšanai Savienības teritorijā, kā arī iekšējā tirgus darbībai. Šīs prasības pēc būtības būtu jāaizliedz, ja vien tās nav pamatotas ar sabiedriskās drošības apsvērumiem, kā noteikts Savienības tiesību aktos, jo īpaši LESD 52. panta nozīmē, un ja vien tās neatbilst LES 5. pantā noteiktajam proporcionalitātes principam. Lai īstenotu principu, kas paredz nepersondatu brīvu plūsmu pāri robežām, nodrošinātu spēkā esošo datu teritoriālas ierobežošanas prasību ātru atcelšanu un dotu iespēju operatīvu iemeslu dēļ datus apstrādāt dažādās vietās Savienības teritorijā un tā kā šī regula paredz pasākumus, kuru mērķis ir nodrošināt datu pieejamību regulatīvas kontroles veikšanai, būtu jāparedz, ka dalībvalstis datu teritoriālas ierobežošanas prasības var pamatot tikai ar sabiedriskās drošības apsvērumiem.

(19) Sabiedriskās drošības jēdziens LESD 52. panta nozīmē un atbilstoši Tiesas interpretācijai aptver gan dalībvalsts iekšējo, gan ārējo drošību, kā arī sabiedrības drošības jautājumus, jo īpaši, lai varētu sekmēt noziedzīgu nodarījumu izmeklēšanu, atklāšanu un saukšanu pie atbildības par tiem. Tas saprotams tā, ka pastāv reāli un pietiekami nopietni draudi, kas skar sabiedrības pamatintereses, piemēram, institūciju darbību, svarīgu sabiedrisko pakalpojumu sniegšanu un iedzīvotāju izdzīvošanu, kā arī risks, ka var nopietni tikt apdraudētas ārējās attiecības vai mierīga nāciju līdzāspastāvēšana, vai militāro interešu apdraudējums. Saskaņā ar proporcionalitātes principu datu teritoriālas ierobežošanas prasībām, kuru pamatojums ir sabiedriskās drošības apsvērumi, vajadzētu būt piemērotām izvirzītā mērķa sasniegšanai, un ar tām nevajadzētu pārsniegt to, kas ir nepieciešams šā mērķa sasniegšanai.

([1]) Eiropas Parlamenta un Padomes Direktīva 2014/24/ES (2014. gada 26. februāris) par publisko iepirkumu un ar ko atceļ Direktīvu 2004/18/EK (OV L 94, 28.3.2014., 65. lpp.).

([2]) Eiropas Parlamenta un Padomes Regula (EK) Nr. 593/2008 (2008. gada 17. jūnijs) par tiesību aktiem, kas piemērojami līgumsaistībām (Roma I) (OV L 177, 4.7.2008., 6. lpp.).

(20) Lai nodrošinātu, ka tiek efektīvi piemērots princips, kas paredz nepersondatu brīvu plūsmu pāri robežām, un novērstu to, ka rodas jauni šķēršļi vienmērīgai iekšējā tirgus darbībai, dalībvalstīm būtu nekavējoties jāpaziņo Komisijai par ikvienu akta projektu, kas ievieš jaunu datu teritoriālas ierobežošanas prasību vai ar ko groza kādu spēkā esošu datu teritoriālas ierobežošanas prasību. Minētie aktu projekti būtu jāiesniedz un jāizvērtē saskaņā ar Eiropas Parlamenta un Padomes Direktīvu (ES) 2015/1535 ([1]).

(21) Turklāt, lai novērstu iespējamus šķēršļus, dalībvalstīm 24 mēnešu pārejas perioda laikā pēc šīs regulas piemērošanas dienas būtu jāpārskata spēkā esošie vispārējie normatīvie un administratīvie akti, ar ko nosaka datu teritoriālas ierobežošanas prasības, un jāpaziņo Komisijai jebkādas šādas datu teritoriālas ierobežošanas prasības, kuras tās uzskata par atbilstošām šai regulai, pievienojot pamatojumu. Tam vajadzētu Komisijai dot iespēju pārbaudīt jebkādu atlikušo datu teritoriālas ierobežošanas prasību atbilstību. Komisijai vajadzētu būt iespējai nepieciešamības gadījumā attiecīgajai dalībvalstij sniegt komentārus. Šādi komentāri varētu ietvert ieteikumu grozīt vai atcelt konkrēto datu teritoriālas ierobežošanas prasību.

(22) Ar šo regulu noteiktais pienākums paziņot Komisijai spēkā esošās datu teritoriālas ierobežošanas prasības un aktu projektus būtu jāpiemēro regulatīvām datu teritoriālas ierobežošanas prasībām un vispārēja rakstura aktu projektiem, bet ne konkrētām fiziskām vai juridiskām personām adresētiem lēmumiem.

(23) Lai dalībvalstīs fiziskām un juridiskām personām, piemēram, pakalpojumu sniedzējiem un datu apstrādes pakalpojumu lietotājiem, nodrošinātu vispārējos normatīvajos un administratīvajos aktos paredzēto datu teritoriālas ierobežošanas prasību pārredzamību, dalībvalstīm informācija par šādām prasībām būtu jāpublicē valsts vienotā tiešsaistes informācijas punktā un minētā informācija regulāri jāatjaunina. Alternatīvi dalībvalstīm atjaunināta informācija par šādām prasībām būtu jāsniedz centrālajam informācijas punktam, kas izveidots saskaņā ar citu Savienības tiesību aktu. Lai par datu teritoriālas ierobežošanas prasībām pienācīgi informētu fiziskas un juridiskas personas visā Savienībā, dalībvalstīm būtu jāpaziņo Komisijai šādu valsts vienotu informācijas punktu adreses. Komisijai šī informācija kopā ar regulāri atjauninātu visu dalībvalstīs spēkā esošo datu teritoriālas ierobežošanas prasību konsolidētu sarakstu, tostarp īsi apkopotu informāciju par minētajām prasībām, būtu jāpublicē savā tīmekļa vietnē.

(24) Datu teritoriālas ierobežošanas prasību noteikšanas pamatā bieži vien ir neuzticēšanās datu pārrobežu apstrādei, un šī neuzticēšanās izriet no iedomātas datu nepieejamības dalībvalstu kompetento iestāžu vajadzībām, piemēram, regulatīvas vai ar uzraudzību saistītas kontroles nolūkos veiktai pārbaudei vai revīzijai. Šādu neuzticēšanos nevar pārvarēt, tikai atzīstot par spēkā neesošiem līguma noteikumus, kas kompetentajām iestādēm liedz likumīgu piekļuvi datiem, kas nepieciešami to oficiālo pienākumu pildīšanai. Tādēļ ar šo regulu būtu skaidri jānosaka, ka tā neskar kompetento iestāžu pilnvaras pieprasīt vai saņemt piekļuvi datiem saskaņā ar Savienības vai valstu tiesību aktiem un ka kompetentajām iestādēm piekļuvi datiem nedrīkst atteikt, pamatojoties uz to, ka dati ir apstrādāti citā dalībvalstī. Kompetentās iestādes varētu noteikt funkcionālas prasības, lai atbalstītu piekļuvi datiem, piemēram, prasību, ka sistēmu apraksti ir jāglabā attiecīgajā dalībvalstī.

(25) Fiziskas vai juridiskas personas, uz kurām attiecas pienākums sniegt datus kompetentajām iestādēm, šādu pienākumu var izpildīt, nodrošinot un garantējot kompetentajām iestādēm efektīvu un laicīgu elektronisku piekļuvi datiem neatkarīgi no dalībvalsts, kuras teritorijā tie tiek apstrādāti. Šādu piekļuvi var nodrošināt, paredzot konkrētus noteikumus līgumos starp fizisku vai juridisku personu, uz kuru attiecas pienākums nodrošināt piekļuvi, un pakalpojumu sniedzēju.

(26) Ja uz fizisku vai juridisku personu attiecas pienākums sniegt datus un tā šo pienākumu neizpilda, būtu jāparedz, ka kompetentā iestāde var lūgt palīdzību kompetentajām iestādēm citās dalībvalstīs. Šādos gadījumos atkarībā no katrā atsevišķajā gadījumā skatītā jautājuma kompetentajām iestādēm būtu jāizmanto specifiski sadarbības instrumenti, kas pieejami Savienības tiesībās vai starptautiskos nolīgumos, tādi kā, piemēram, policijas sadarbības,

([1]) Eiropas Parlamenta un Padomes Direktīva (ES) 2015/1535 (2015. gada 9. septembris), ar ko nosaka informācijas sniegšanas kārtību tehnisko noteikumu un Informācijas sabiedrības pakalpojumu noteikumu jomā (OV L 241, 17.9.2015., 1. lpp.).

krimināltiesību, civiltiesību vai administratīvo tiesību jomā, attiecīgi Padomes Pamatlēmums 2006/960/TI ([1]), Eiropas Parlamenta un Padomes Direktīva 2014/41/ES ([2]), Eiropas Padomes Konvencija par kibernoziegumiem ([3]), Padomes Regula (EK) Nr. 1206/2001 ([4]), Padomes Direktīva 2006/112/EK ([5]) un Padomes Regula (ES) Nr. 904/2010 ([6]). Ja šādu specifisku sadarbības mehānismu nav, kompetentajām iestādēm būtu savstarpēji jāsadarbojas ar izraudzīto vienoto kontaktpunktu starpniecību, lai nodrošinātu piekļuvi pieprasītajiem datiem.

(27) Ja palīdzības pieprasījuma izpildes nolūkā lūgumu saņēmušajai iestādei ir jāiegūst piekļuve jebkādām fiziskas vai juridiskas personas telpām, tostarp jebkādam datu apstrādes aprīkojumam un līdzekļiem, šādai piekļuvei ir jāatbilst Savienības tiesību aktiem vai valsts procesuālajiem noteikumiem, tostarp ievērojot jebkādas prasības saņemt iepriekšēju tiesas atļauju.

(28) Ar šo regulu nevajadzētu dot iespēju lietotājiem mēģināt izvairīties no valstu tiesību aktu piemērošanas. Tādēļ tajā būtu jāparedz, ka dalībvalstis piemēro efektīvus, samērīgus un atturošus sodus lietotājiem, kuri kompetentajām iestādēm liedz iespēju piekļūt saviem datiem, kas vajadzīgi kompetento iestāžu oficiālo pienākumu pildīšanai saskaņā ar Savienības un valstu tiesību aktiem. Steidzamos gadījumos, kad lietotājs ļaunprātīgi izmanto savas tiesības, dalībvalstīm vajadzētu būt iespējai piemērot stingri samērīgus pagaidu pasākumus. Jebkādi pagaidu pasākumi, kas paredz datu teritoriālu ierobežošanu no jauna uz laiku, kas pārsniedz 180 dienas pēc atkārtotas teritoriālas ierobežošanas, ievērojamu periodu neatbilstu datu brīvas aprites principam, un tāpēc par tiem būtu jāpaziņo Komisijai, lai tā varētu pārbaudīt to atbilstību Savienības tiesību aktiem.

(29) Iespēja netraucēti pārnest datus ir svarīgs faktors, lai atvieglotu lietotāju izvēli un sekmētu efektīvu konkurenci datu apstrādes pakalpojumu tirgos. Faktiskās vai šķietamās grūtības datus pārnest pāri robežām arī apdraud profesionālo lietotāju uzticēšanos, izvēloties pārrobežu piedāvājumus, un līdz ar to arī viņu uzticēšanos iekšējam tirgum. Lai gan individuāli patērētāji gūst labumu no spēkā esošajiem Savienības tiesību aktiem, tie neatvieglo tādu lietotāju iespējas mainīt pakalpojumu sniedzējus, kuri rīkojas uzņēmējdarbības vai profesionālās darbības veikšanas laikā. Konsekventu tehnisko prasību noteikšana visā Savienībā – attiecībā uz tehnisku saskaņošanu, savstarpēju atzīšanu vai brīvprātīgu saskaņošanu – arī veicina konkurētspējīga datu apstrādes pakalpojumu iekšējā tirgus izveidi.

(30) Lai pilnībā izmantotu priekšrocības, ko sniedz vide, kurā valda konkurence, profesionāliem lietotājiem būtu jāspēj izdarīt uz informāciju balstītu izvēli un viegli salīdzināt dažādu iekšējā tirgū piedāvātu datu apstrādes pakalpojumu atsevišķos komponentus, tostarp attiecībā uz līguma noteikumiem par datu pārnešanu, kad beidzas līgums. Lai pielāgotos tirgus inovācijas potenciālam un ņemtu vērā pakalpojumu sniedzēju un datu apstrādes pakalpojumu profesionālo lietotāju pieredzi un speciālās zināšanas, tirgus subjektiem, izmantojot pašregulāciju – uz ko mudinātu un ko atvieglotu un uzraudzītu Komisija – attiecībā uz datu pārnešanu būtu jānosaka detalizēta informācija un operatīvas prasības tādu Savienības rīcības kodeksu veidā, kuri varētu ietvert līguma paraugnoteikumus.

(31) Lai šādi rīcības kodeksi būtu efektīvi un lai tie atvieglotu pakalpojumu sniedzēja maiņu un datu pārnešanu, šiem kodeksiem vajadzētu būt visaptverošiem un būtu jāietver vismaz vairāki tādi aspekti, kas ir svarīgi datu pārnešanas procesā, piemēram, procesi, ko izmanto datu dublēšanai, un to atrašanās vieta; pieejamie datu formāti un nesēji; nepieciešamā IT konfigurācija un minimālais tīkla joslas platums; laiks, kas vajadzīgs pirms pārnešanas procesa, periods, kurā datus varēs pārnest; un garantija, ka datiem varēs piekļūt pakalpojumu sniedzēja bankrota gadījumā. Rīcības kodeksos arī būtu skaidri jānorāda, ka šķēršļu likšana pakalpojumu sniedzēja maiņai nav pieņemama uzņēmējdarbības prakse, kā arī būtu jāparedz uzticēšanos veicinošas tehnoloģijas, un tie būtu regulāri jāatjaunina, lai ietu kopsolī ar tehnoloģiju attīstību. Komisijai būtu jānodrošina, ka minētajā procesā notiek apspriešanās ar visām attiecīgajām ieinteresētajām personām, tostarp mazo un vidējo uzņēmumu (MVU) asociācijām un jaunuzņēmumiem, lietotājiem un mākoņpakalpojumu sniedzējiem. Komisijai būtu jāizvērtē šādu rīcības kodeksu izstrāde un īstenošanas efektivitāte.

([1]) Padomes Pamatlēmums 2006/960/TI (2006. gada 18. decembris) par Eiropas Savienības dalībvalstu tiesībaizsardzības iestāžu informācijas un izlūkdatu apmaiņas vienkāršošanu (OV L 386, 29.12.2006., 89. lpp.).

([2]) Eiropas Parlamenta un Padomes Direktīva 2014/41/ES (2014. gada 3. aprīlis) par Eiropas izmeklēšanas rīkojumu krimināllietās (OV L 130, 1.5.2014., 1. lpp.).

([3]) Eiropas Padomes Konvencija par kibernoziegumiem, CETS Nr. 185.

([4]) Padomes Regula (EK) Nr. 1206/2001 (2001. gada 28. maijs) par sadarbību starp dalībvalstu tiesām pierādījumu iegūšanā civillietās un krimināllietās (OV L 174, 27.6.2001., 1. lpp.).

([5]) Padomes Direktīva 2006/112/EK (2006. gada 28. novembris) par kopējo pievienotās vērtības nodokļa sistēmu (OV L 347, 11.12.2006., 1. lpp.).

([6]) Padomes Regula (ES) Nr. 904/2010 (2010. gada 7. oktobris) par administratīvu sadarbību un krāpšanas apkarošanu pievienotās vērtības nodokļa jomā (OV L 268, 12.10.2010., 1. lpp.).

(32) Ja kādas dalībvalsts kompetentā iestāde lūdz citas dalībvalsts palīdzību, lai iegūtu piekļuvi datiem saskaņā ar šo regulu, tai ar izraudzīta vienota kontaktpunkta palīdzību būtu jāiesniedz pienācīgi pamatots pieprasījums šīs citas dalībvalsts izraudzītajam vienotajam kontaktpunktam, pieprasījumā iekļaujot rakstisku skaidrojumu par nepieciešamās datu piekļuves iemesliem un juridiskajiem pamatiem. Vienotajam kontaktpunktam, ko izraudzījusies dalībvalsts, kurai tiek lūgta palīdzība, būtu jāatvieglo pieprasījuma nosūtīšana attiecīgajai kompetentajai iestādei dalībvalstī, kurai tiek lūgta palīdzība. Lai nodrošinātu efektīvu sadarbību, iestādei, kurai tiek nodots pieprasījums, bez liekas kavēšanās būtu jāsniedz palīdzība, lai reaģētu uz konkrēto pieprasījumu, vai jāinformē par grūtībām izpildīt šādu pieprasījumu, vai jāsniedz pamatojums tā izpildes atteikšanai.

(33) Uzticēšanās palielināšanai pārrobežu datu apstrādes drošībai būtu jāmazina tirgus dalībnieku un publiskā sektora tieksme izmantot datu teritoriālu ierobežošanu kā datu drošības aizstājēju. Tam arī uzņēmumiem būtu jāuzlabo juridiskā noteiktība attiecībā uz atbilstību piemērojamām drošības prasībām, kad tie datu apstrādes darbības uztic ārpakalpojumu sniedzējiem, tostarp pakalpojumu sniedzējiem citās dalībvalstīs.

(34) Jebkādas ar datu apstrādi saistītas drošības prasības, ko atbilstoši Savienības tiesību aktiem vai Savienības tiesību aktiem atbilstīgiem dalībvalstu tiesību aktiem pamatoti un samērīgi piemēro tādu fizisku vai juridisku personu dzīvesvietas vai reģistrācijas vietas dalībvalstī, uz kuru datiem attiecas šāda apstrāde, arī turpmāk būtu jāpiemēro šādu datu apstrādei citā dalībvalstī. Minētajām fiziskajām vai juridiskajām personām būtu jāspēj izpildīt šādas prasības vai nu pašām, vai arī līgumos ar pakalpojumu sniedzējiem iekļaujot attiecīgas līgumiskas klauzulas.

(35) Valsts līmenī noteiktām drošības prasībām vajadzētu būt nepieciešamām un samērīgām ar riskiem, kas apdraud datu apstrādes drošību, uz kuru attiecas valsts tiesību akts, ar ko šīs prasības ir noteiktas.

(36) Eiropas Parlamenta un Padomes Direktīva (ES) 2016/1148 ([1]) paredz juridiskus pasākumus, kuru mērķis ir paaugstināt vispārējo kiberdrošības līmeni Savienībā. Datu apstrādes pakalpojumi ir viens no minētās direktīvas piemērošanas jomā ietilpstošiem digitālo pakalpojumu veidiem. Saskaņā ar minēto direktīvu dalībvalstīm ir jānodrošina, ka digitālo pakalpojumu sniedzēji nosaka un veic atbilstošus un samērīgus tehniskus un organizatoriskus pasākumus, lai pārvaldītu riskus, kas apdraud šo pakalpojumu sniedzēju izmantoto tīklu un informācijas sistēmu drošību. Ar šādiem pasākumiem būtu jānodrošina pastāvošajam riskam atbilstošs drošības līmenis un būtu jāņem vērā sistēmu un iekārtu drošība; incidentu novēršana; darbības nepārtrauktības pārvaldība; uzraudzība, revīzija un testēšana; un atbilstība starptautiskiem standartiem. Šie elementi Komisijai sīkāk būtu jāprecizē minētajā direktīvā paredzētajos īstenošanas aktos.

(37) Komisijai būtu jāiesniedz ziņojums par šīs regulas īstenošanu, jo īpaši ar mērķi noteikt, vai nav nepieciešamas izmaiņas saistībā ar tehnoloģisko attīstību vai norisēm tirgū. Minētajā ziņojumā jo īpaši būtu jāizvērtē šīs regulas piemērošana, jo īpaši tās piemērošana attiecībā uz datu kopām, kas sastāv gan no persondatiem, gan nepersondatiem, kā arī sabiedriskās drošības izņēmuma piemērošana. Pirms šīs regulas piemērošanas – lai uzņēmumi, tostarp MVU, labāk izprastu mijiedarbību starp šo regulu un Regulu (ES) 2016/679 un lai nodrošinātu abu regulu ievērošanu –, Komisijai arī būtu jāpublicē informatīvi norādījumi par to, kā rīkoties ar datu kopām, kas sastāv gan no persondatiem, gan no nepersondatiem.

(38) Šajā regulā ir ievērotas pamattiesības un principi, kas ir atzīti Eiropas Savienības Pamattiesību hartā, un tā būtu jāinterpretē un jāpiemēro saskaņā ar šīm tiesībām un principiem, tostarp tiesībām uz persondatu aizsardzību, vārda un informācijas brīvību un darījumdarbības brīvību.

(39) Ņemot vērā to, ka šīs regulas mērķi, proti, datu, kas nav persondati, brīvu plūsmu Savienībā, nevar pietiekami labi sasniegt atsevišķās dalībvalstīs, bet tā mēroga un ietekmes dēļ to var labāk sasniegt Savienības līmenī, Savienība var pieņemt pasākumus saskaņā ar LES 5. pantā noteikto subsidiaritātes principu. Saskaņā ar minētajā pantā noteikto proporcionalitātes principu šajā regulā paredz vienīgi tos pasākumus, kas ir vajadzīgi minētā mērķa sasniegšanai,

([1]) Eiropas Parlamenta un Padomes Direktīva (ES) 2016/1148 (2016. gada 6. jūlijs) par pasākumiem nolūkā panākt vienādi augsta līmeņa tīklu un informācijas sistēmu drošību visā Savienībā (OV L 194, 19.7.2016., 1. lpp.).

IR PIEŅĒMUŠI ŠO REGULU.

1. pants

Priekšmets

Šīs regulas mērķis ir nodrošināt datu, kas nav persondati, brīvu plūsmu Savienībā, paredzot noteikumus par datu teritoriālas ierobežošanas prasībām un datu pieejamību kompetentām iestādēm, kā arī profesionāliem lietotājiem paredzētus noteikumus par datu pārnešanu.

2. pants

Piemērošanas joma

1. Šo regulu piemēro Savienībā veiktai elektronisku datu, kas nav persondati, apstrādei:

a) ko nodrošina kā pakalpojumu lietotājiem, kuriem Savienībā ir pastāvīga dzīvesvieta vai reģistrācijas vieta, neatkarīgi no tā, vai pakalpojuma sniedzējs ir vai nav reģistrēts Savienībā; vai

b) ko savām vajadzībām veic fiziska vai juridiska persona, kurai Savienībā ir pastāvīga dzīvesvieta vai reģistrācijas vieta.

2. Tādu datu kopu gadījumā, kas sastāv gan no persondatiem, gan no nepersondatiem, šo regulu piemēro datu kopas nepersondatu daļai. Ja persondati un nepersondati datu kopā ir nedalāmi saistīti, šī regula neskar Regulas (ES) 2016/679 piemērošanu.

3. Šo regulu nepiemēro darbībai, kas neietilpst Savienības tiesību aktu piemērošanas jomā.

Šī regula neskar normatīvos un administratīvos aktus, kas ir saistīti ar dalībvalstu iekšējo organizāciju un ar ko publiskām iestādēm un Direktīvas 2014/24/ES 2. panta 1. punkta 4) apakšpunktā definētiem publisko tiesību subjektiem piešķir pilnvaras un pienākumus attiecībā uz datu apstrādi bez līgumā noteikta privāto tiesību subjektu atalgojuma, kā arī dalībvalstu normatīvos un administratīvos aktus, ar ko paredz minēto pilnvaru un pienākumu īstenošanu.

3. pants

Definīcijas

Šajā regulā piemēro šādas definīcijas:

1) "dati" ir dati, kas nav persondati, kā definēts Regulas (ES) 2016/679 4. panta 1) punktā;

2) "apstrāde" ir jebkura operācija vai operāciju kopums, ko ar elektroniskiem datiem vai datu kopām veic ar vai bez automatizētiem līdzekļiem, piemēram, vākšana, reģistrācija, organizēšana, strukturēšana, glabāšana, pielāgošana vai pārveidošana, atgūšana, aplūkošana, izmantošana, atklāšana nosūtot, izplatot vai citādi datus darot pieejamus, sakārtošana vai kombinēšana, ierobežošana, dzēšana vai iznīcināšana;

3) "akta projekts" ir teksts, kas izstrādāts ar mērķi to ieviest kā vispārīgu normatīvu vai administratīvu aktu un kas ir tādā sagatavošanas pakāpē, kad vēl ir iespējams izdarīt būtiskus grozījumus;

4) "pakalpojumu sniedzējs" ir fiziska vai juridiska persona, kas sniedz datu apstrādes pakalpojumus;

5) "datu teritoriālas ierobežošanas prasība" ir jebkāds dalībvalstu normatīvajos vai administratīvajos aktos noteikts vai no dalībvalstu un publisku tiesību subjektu vispārējas un konsekventas prakses – tostarp publiskā iepirkuma jomā, neskarot Direktīvu 2014/24/ES, – izrietošs pienākums, aizliegums, nosacījums, ierobežojums vai cita prasība, kas paredz datu apstrādi konkrētas dalībvalsts teritorijā vai kavē datu apstrādi jebkurā citā dalībvalstī;

6) "kompetentā iestāde" ir dalībvalsts iestāde vai jebkura cita struktūra, kurai ar valsts tiesību aktiem ir atļauts pildīt publisku funkciju vai īstenot valsts varu un kura ir pilnvarota iegūt piekļuvi fiziskas vai juridiskas personas apstrādātiem datiem savu oficiālo pienākumu pildīšanas nolūkā, kā noteikts Savienības vai valsts tiesību aktos;

7) "lietotājs" ir fiziska vai juridiska persona, tostarp publiska iestāde vai publisko tiesību subjekts, kas izmanto vai pieprasa datu apstrādes pakalpojumu;

8) "profesionāls lietotājs" ir fiziska vai juridiska persona, tostarp publiska iestāde vai publisko tiesību subjekts, kas izmanto vai pieprasa datu apstrādes pakalpojumu savām ar tirdzniecību, uzņēmējdarbību, arodu, profesiju vai uzdevumu saistītām vajadzībām.

4. pants

Brīva datu aprite Savienībā

1. Datu teritoriālas ierobežošanas prasības ir aizliegtas, ja vien tās nav pamatotas ar sabiedriskās drošības apsvērumiem, ievērojot proporcionalitātes principu.

Šā punkta pirmā daļa neskar 3. punktu un datu teritoriālas ierobežošanas prasības, kas noteiktas, pamatojoties uz spēkā esošajiem Savienības tiesību aktiem.

2. Dalībvalstis nekavējoties paziņo Komisijai par ikvienu akta projektu, ar kuru ievieš jaunu datu teritoriālas ierobežošanas prasību vai groza kādu spēkā esošu datu teritoriālas ierobežošanas prasību, atbilstīgi Direktīvas (ES) 2015/1535 5., 6. un 7. pantā paredzētajām procedūrām.

3. Līdz 2021. gada 30. maijam dalībvalstis nodrošina, ka tiek atcelta ikviena spēkā esoša ar vispārēja rakstura normatīvu vai administratīvu aktu noteikta datu teritoriālas ierobežošanas prasība, kas neatbilst šā panta 1. punktam.

Ja dalībvalsts uzskata, ka kāds spēkā esošs pasākums, kas ietver datu teritoriālas ierobežošanas prasību, atbilst šā panta 1. punktam un tāpēc var palikt spēkā, tā līdz 2021. gada 30. maijam par minēto pasākumu paziņo Komisijai, pievienojot pamatojumu tā paturēšanai spēkā. Neskarot LESD 258. pantu, Komisija sešu mēnešu laikā pēc šāda paziņojuma saņemšanas dienas pārbauda minētā pasākuma atbilstību šā panta 1. punktam un attiecīgā gadījumā dalībvalstij sniedz komentārus, tostarp nepieciešamības gadījumā iesakot pasākumu grozīt vai atcelt.

4. Dalībvalstis, izmantojot valsts vienotu tiešsaistes informācijas punktu, kuru tās pastāvīgi atjaunina, tiešsaistē dara publiski pieejamu detalizētu informāciju par visām ar vispārēja rakstura normatīvu vai administratīvu aktu noteiktām un to teritorijā piemērojamām datu teritoriālas ierobežošanas prasībām vai arī sniedz centrālajam informācijas punktam, kas izveidots ar citu Savienības tiesību aktu, atjauninātu detalizētu informāciju par visām šādām teritoriālas ierobežošanas prasībām.

5. Šā panta 4. punktā minētā vienotā informācijas punkta adresi dalībvalstis paziņo Komisijai. Komisija savā tīmekļa vietnē publicē saiti(-es) uz šādu(-iem) punktu(-iem), kā arī regulāri atjauninātu konsolidētu sarakstu ar visām 4. punktā minētajām datu teritoriālas ierobežošanas prasībām, tostarp kopsavilkuma informāciju par šīm prasībām.

5. pants

Datu pieejamība kompetentajām iestādēm

1. Šī regula neskar kompetento iestāžu pilnvaras pieprasīt vai iegūt piekļuvi datiem savu oficiālo pienākumu pildīšanai saskaņā ar Savienības vai valsts tiesību aktiem. Kompetentajām iestādēm nedrīkst atteikt piekļuvi datiem, pamatojoties uz to, ka šie dati tiek apstrādāti citā dalībvalstī.

2. Ja kompetentā iestāde pēc tam, kad ir pieprasījusi piekļuvi lietotāja datiem, to neiegūst un ja nepastāv īpašs ar Savienības tiesību aktiem vai starptautiskiem nolīgumiem izveidots sadarbības mehānisms datu apmaiņai starp dažādu dalībvalstu kompetentajām iestādēm, minētā kompetentā iestāde var saskaņā ar 7. pantā izklāstīto procedūru lūgt palīdzību kompetentajai iestādei citā dalībvalstī.

3. Ja palīdzības pieprasījuma izpildes nolūkā lūgumu saņēmušajai iestādei ir jāiegūst piekļuve fiziskas vai juridiskas personas telpām, tostarp jebkādam datu apstrādes aprīkojumam un līdzekļiem, šādai piekļuvei ir jāatbilst Savienības tiesību aktiem vai valstu procesuālajiem noteikumiem.

4. Dalībvalstis saskaņā ar Savienības un valstu tiesību aktiem par datu sniegšanas pienākuma neizpildi var piemērot efektīvus, samērīgus un atturošus sodus.

Ja kāds lietotājs ļaunprātīgi izmanto tiesības, dalībvalsts tam var piemērot stingri samērīgus pagaidu pasākumus, ja tam par pamatojumu kalpo nepieciešamība steidzami piekļūt datiem un tiek ņemtas vērā attiecīgo pušu intereses. Ja pagaidu pasākums paredz datu atkārtotu teritoriālu ierobežošanu uz laiku, kas pārsniedz 180 dienas pēc atkārtotas teritoriālas ierobežošanas, par to minētajā 180 dienu periodā paziņo Komisijai. Komisija pēc iespējas īsākā laikā pārbauda minēto pasākumu un tā saderību ar Savienības tiesību aktiem un attiecīgā gadījumā veic nepieciešamos pasākumus. Komisija veic informācijas apmaiņu ar 7. pantā minētajiem dalībvalstu vienotajiem kontaktpunktiem par šajā sakarā iegūto pieredzi.

6. pants

Datu pārnešana

1. Lai veicinātu konkurētspējīgu datu ekonomiku, kas balstās uz pārredzamības un sadarbspējas principu un pienācīgi ņemot vērā atvērtos standartus, Komisija rosina un atvieglo pašregulējošu rīcības kodeksu ("rīcības kodeksi") izstrādi Savienības līmenī, kuri cita starpā aptver šādus aspektus:

a) labākā prakse nolūkā atvieglot pakalpojumu sniedzēja maiņu un datu pārnešanu strukturētā, plaši izmantotā un mašīnlasāmā formātā, tostarp atvērto standartu formātā, ja pakalpojumu sniedzējam, kurš datus saņem, tas ir vajadzīgs vai viņš to pieprasa;

b) minimālās informācijas sniegšanas prasības, lai nodrošinātu, ka pirms līguma par datu apstrādi noslēgšanas profesionāliem lietotājiem tiek sniegta pietiekami detalizēta, skaidra un pārredzama informācija par procesiem, tehniskajām prasībām, termiņiem un maksu, ko piemēro gadījumos, kad profesionāls lietotājs vēlas mainīt pakalpojumu sniedzēju vai pārnest datus atpakaļ uz savām IT sistēmām;

c) pieejas sertificēšanas shēmām, kas profesionāliem lietotājiem atvieglo datu apstrādes produktu un pakalpojumu salīdzināšanu, ņemot vērā valsts noteiktās vai starptautiskās normas, lai atvieglotu minēto produktu un pakalpojumu salīdzināmību. Šādas pieejas cita starpā var ietvert arī kvalitātes pārvaldību, informācijas drošības pārvaldību, uzņēmējdarbības nepārtrauktības pārvaldību un vides pārvaldību;

d) komunikācijas ceļveži, kuros izmantota daudzdisciplīnu pieeja, lai veicinātu attiecīgo ieinteresēto personu izpratni par rīcības kodeksiem.

2. Komisija nodrošina, ka rīcības kodeksus izstrādā ciešā sadarbībā ar visām attiecīgajām ieinteresētajām personām, tostarp mazo un vidējo uzņēmumu (MVU) asociācijām un jaunuzņēmumiem, lietotājiem un mākoņpakalpojumu sniedzējiem.

3. Komisija mudina pakalpojumu sniedzējus rīcības kodeksu izstrādi pabeigt līdz 2019. gada 29. novembrim un tos efektīvi īstenot līdz 2020. gada 29. maijam.

7. pants

Iestāžu sadarbības procedūra

1. Katra dalībvalsts izraugās vienotu kontaktpunktu, kas attiecībā uz šīs regulas piemērošanu uztur sakarus ar citu dalībvalstu vienotajiem kontaktpunktiem un Komisiju. Dalībvalstis izraudzītos vienotos kontaktpunktus un jebkādas turpmākas ar tiem saistītas izmaiņas paziņo Komisijai.

2. Ja kādas dalībvalsts kompetentā iestāde, ievērojot 5. panta 2. punktu, lūdz citas dalībvalsts palīdzību, lai iegūtu piekļuvi datiem, tā šīs citas dalībvalsts izraudzītajam vienotajam kontaktpunktam iesniedz pienācīgi pamatotu pieprasījumu. Pieprasījumā iekļauj rakstisku skaidrojumu par nepieciešamās datu piekļuves iemesliem un juridiskajiem pamatiem.

3. Vienotais kontaktpunkts nosaka attiecīgo savas dalībvalsts kompetento iestādi un nosūta tai saskaņā ar 2. punktu saņemto pieprasījumu.

4. Attiecīgā kompetentā iestāde bez liekas kavēšanās un laikā, kas ir samērīgs ar pieprasījuma steidzamību, sniedz atbildi, nosūtot prasītos datus vai informējot pieprasījumu iesniegušo kompetento iestādi par to, ka tā neuzskata, ka pieprasījums atbilst šajā regulā noteiktajiem palīdzības lūgšanas nosacījumiem.

5. Jebkādu informāciju, kas saņemta lūgtās palīdzības kontekstā un sniegta saskaņā ar 5. panta 2. punktu, izmanto tikai saistībā ar jautājumu, kura risināšanai tā pieprasīta.

6. Vienotie kontaktpunkti lietotājiem sniedz vispārēju informāciju par šo regulu, tostarp par rīcības kodeksu izstrādi.

8. pants

Izvērtēšana un pamatnostādnes

1. Ne vēlāk kā 2022. gada 29. novembrī Komisija iesniedz Eiropas Parlamentam, Padomei un Eiropas Ekonomikas un sociālo lietu komitejai ziņojumu, kurā izvērtē šīs regulas īstenošanu, jo īpaši attiecībā uz:

a) šīs regulas piemērošanu – jo īpaši datu kopām, kuras sastāv gan no persondatiem, gan no nepersondatiem, – ņemot vērā norises tirgū un tehnoloģisko attīstību, kas varētu paplašināt datu deanonimizācijas iespējas;

b) to, kā dalībvalstis īsteno 4. panta 1. punktu, un jo īpaši sabiedriskās drošības izņēmumu; un

c) rīcības kodeksu izstrādi un efektīvu īstenošanu un pakalpojumu sniedzēju veiktu efektīvu informācijas sniegšanu.

2. Dalībvalstis sniedz Komisijai informāciju, kas nepieciešama 1. punktā minētā ziņojuma sagatavošanai.

3. Līdz 2019. gada 29. maijam Komisija publicē informatīvas pamatnostādnes par šīs regulas un Regulas (ES) 2016/679 mijiedarbību attiecībā uz datu kopām, kas sastāv gan no persondatiem, gan no nepersondatiem.

9. pants

Nobeiguma noteikumi

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

Šo regulu sāk piemērot sešus mēnešus pēc tās publicēšanas.

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

Strasbūrā, 2018. gada 14. novembrī

Eiropas Parlamenta vārdā –	*Padomes vārdā –*
priekšsēdētājs	*priekšsēdētāja*
A. TAJANI	K. EDTSTADLER