EIROPAS
KOMISIJA

Briselē, 29.5.2019.
COM(2019) 250 final

KOMISIJAS PAZIŅOJUMS EIROPAS PARLAMENTAM UN PADOMEI

Vadlīnijas par Regulu par satvaru nepersondatu brīvai plūsmai Eiropas Savienībā

Satura rādītājs

1. Ievads ... 2

Norādījumu mērķis ... 3

2. Nepersondatu brīvas plūsmas regulas un Vispārīgās datu aizsardzības regulas mijdarbība. Jauktas datu kopas ... 4

2.1. Nepersondatu jēdziens Nepersondatu brīvas plūsmas regulā ... 4

Persondati ... 4

Nepersondati ... 5

2.2. Jauktas datu kopas ... 7

3. Brīva datu plūsma un datu teritoriālas ierobežošanas atcelšana ... 10

3.1. Nepersondatu brīva plūsma ... 10

3.2. Persondatu brīva plūsma ... 12

3.3. Nepersondatu brīvas plūsmas regulas tvērums ... 13

3.4. Pasākumi sakarā ar dalībvalstu iekšējo organizāciju ... 14

4. Pašregulēšanās pieejas, kas balsta datu brīvo plūsmu ... 15

4.1. Datu pārnešana un mākoņpakalpojumu sniedzēja maiņa ... 15

Pārnesamības jēgums un mijdarbība ar Vispārīgo datu aizsardzības regulu ... 17

4.2. Persondatu aizsardzības rīcības kodeksi un sertifikācijas shēmas ... 18

4.3. Vairot uzticēšanos pārrobežu datu apstrādei – sertificēt drošību ... 19

Nobeiguma piebildes ... 20

Šo dokumentu Eiropas Komisija izdevusi informatīvām vajadzībām. Tajā nav autoritatīvi interpretēta Eiropas Parlamenta un Padomes 2018. gada 14. novembra Regula (ES) 2018/1807 par satvaru nepersondatu brīvai apritei Eiropas Savienībā un nav pausts Eiropas Komisijas lēmums vai nostāja. Tas neskar attiecīgus Eiropas Komisijas lēmumus un nostājas un Eiropas Savienības Tiesas varu minēto regulu interpretēt saskaņā ar ES Līgumiem.

1. Ievads

Tā kā tautsaimniecība arvien vairāk balstās uz datiem, visdažādākā lieluma uzņēmumos un visās nozarēs uzņēmējdarbības procesu centrā ir datu plūsmas. Jaunas ciparu tehnoloģijas Eiropas Savienībā ("ES") dāvā jaunas iespējas plašai sabiedrībai, uzņēmumiem un valsts pārvaldes iestādēm.

Lai vēl vairāk uzlabotu datu pārrobežu apmaiņu un veicinātu datu ekonomiku, Eiropas Parlaments un Padome 2018. gada novembrī pēc Eiropas Komisijas ("Komisija") priekšlikuma pieņēma Regulu (ES) 2018/1807 par satvaru nepersondatu brīvai apritei Eiropas Savienībā (Nepersondatu brīvas plūsmas regula)[1]. Regulas piemērošana sākas 2019. gada 28. maijā. Persondatu "brīvas aprites" (brīvas pārvietošanas) princips jau noteikts Eiropas Parlamenta un Padomes 2016. gada 27. aprīļa Regulā (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)[2]. Tādējādi izveidots vispārējs satvars kopīgai Eiropas datu telpai un visu datu brīvai apritei Eiropas Savienībā[3].

Nepersondatu brīvas plūsmas regula dod juridisku noteiktību uzņēmumiem, kuri apstrādā savus datus pašu izraudzītā Eiropas Savienības vietā, vieš lielāku uzticēšanos datu apstrādes pakalpojumu sniedzējiem un apkaro praksi pircēju padarīt atkarīgu no viena pārdevēja. Tā ES paplašināsies klientu izvēle, uzlabosies efektivitāte un tiks sekmēta mākoņdatošanas tehnoloģiju ieviešana, kas ļaus uzņēmumiem ievērojami ietaupīt. Ir pētījums[4], kas liecina: pārejot uz mākoņdatošanu, uzņēmumi ES var ietaupīt 20–50 % IT izmaksu.

Ar abu regulu palīgu dati var brīvi plūst no dalībvalsts uz dalībvalsti, ļaujot datu apstrādes pakalpojumu lietotājiem dažādos ES tirgos savāktos datus izmantot ražīguma celšanai un konkurētspējas uzlabošanai. Tāpēc lietotāji var ietaupīt, visnotaļ izmantojot plašā ES tirgus sagādātos apjomus, tā uzlabojot savu spēju konkurēt pasaulē un Eiropas datu ekonomikas iekšējo savienojamību.

Nepersondatu brīvas plūsmas regulai ir trīs svarīgas iezīmes:

- Ar vispārīgu normu tā aizliedz dalībvalstīm izvirzīt prasības par to, kur datiem jāatrodas. Izņēmumus no šās normas var balstīt tikai uz sabiedriskās drošības apsvērumiem, ievērojot proporcionalitātes principu.
- Tā izveido sadarbības mehānismu, lai nodrošinātu, ka kompetentās iestādes nezaudē iespēju izmantot savas tiesības piekļūt datiem, kas tiek apstrādāti citā dalībvalstī.

---

[1] Eiropas Parlamenta un Padomes Regula (ES) 2018/1807 (2018. gada 14. novembris) par satvaru nepersondatu brīvai apritei Eiropas Savienībā (OV L 303, 28.11.2018., 59. lpp.)

[2] 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.).

[3] Vispārīgā datu aizsardzības regula attiecas arī uz Eiropas Ekonomikas zonu (EEZ), kur ietilpst Islande, Lihtenšteina un Norvēģija. Arī Nepersondatu brīvas plūsmas regulā ir atzīme, ka tā attiecas uz EEZ.

[4] Deloitte: *Measuring the economic impact of cloud computing in Europe*, SMART 2014/0031, 2016. Pieejams tiešsaistē: http://ec.europa.eu/newsroom/document.cfm?doc_id=41184.

- Ar Komisijas atbalstu tā stimulē nozari izstrādāt pašregulējošus rīcības kodeksus par pakalpojumu sniedzēju maiņu un datu pārnešanu.

Norādījumu mērķis

Šie norādījumi atbilst Nepersondatu brīvas plūsmas regulas 8. panta 3. punktam, kas liek Komisijai publicēt "informatīvas pamatnostādnes" par minētās regulas un Vispārīgās datu aizsardzības regulas mijdarbību, sevišķi "attiecībā uz datu kopām, kas sastāv gan no personatiem, gan no nepersondatiem".

Norādījumu mērķis ir palīdzēt lietotājiem, visvairāk – maziem un vidējiem uzņēmumiem, izprast Nepersondatu brīvas plūsmas regulas un Vispārīgās datu aizsardzības regulas mijdarbību[5]. Tāpēc norādījumos sevišķi iztirzāti: i) jēdzieni "nepersondati" un "personadati", ii) abu regulu datu brīvas aprites principi un datu teritoriālas ierobežošanas aizliegums, iii) datu pārnesamības jēgums Nepersondatu brīvas plūsmas regulā. Aplūkotas arī pašregulācijas prasības, kas noteiktas abās regulās.

Nepersondatu brīvas plūsmas regula attiecas tikai uz Vispārīgajā datu aizsardzības regulā noteiktajiem “datiem, kas nav personadati”. Vispārīgā datu aizsardzības regula regulē personadatu apstrādi, kas ir būtiska ES datu aizsardzības sistēmas sastāvdaļa[6]. Dalībvalstīs tā stājās spēkā 2018. gada 25. maijā. Regulā izklāstīti saskaņoti noteikumi, kas ES/EEZ iedzīvotājus aizsargā viņu personadatu apstrādes un brīvas aprites aspektā. Vispārīgā datu aizsardzības regula: i) nosaka, kāda informācija uzskatāma par personadatiem, ii) izveido to apstrādes tiesisko pamatu, iii) nosaka tiesības un pienākumus, kas jāievēro tādu datu apstrādē[7], kā arī citas normas. Par persondatu brīvas aprites principu Vispārīgās datu

---

[5] Eiropas Parlamenta un Padomes Regula (ES) 2018/1807 (2018. gada 14. novembris) par satvaru nepersondatu brīvai apritei Eiropas Savienībā, 37. apsvērums.

[6]
- Eiropas Parlamenta un Padomes Regula (ES) Nr. 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 119/1, 4.5.2016., 1. lpp.).
- Eiropas Parlamenta un Padomes Regula (ES) 2018/1725 (2018. gada 23. oktobris) par fizisku personu aizsardzību attiecībā uz personas datu apstrādi Savienības iestādēs, struktūrās, birojos un aģentūrās un par šādu datu brīvu apriti un ar ko atceļ Regulu (EK) Nr. 45/2001 un Lēmumu Nr. 1247/2002/EK (OV L 295, 21.11.2018., 39. lpp.).
- Direktīva (ES) 2016/680 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.).
- 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.) (patlaban tiek pārskatīta).

[7] Sīkākus norādījumus par dažādiem aspektiem Regulā (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 (Vispārīgajā datu aizsardzības regulā) un Eiropas tiesību aktos datu aizsardzības jomā sk. Eiropas Datu aizsardzības kolēģijas vietnē; kolēģija saskaņā ar Vispārīgās datu aizsardzības regulas 70. pantu ir izdevusi vairākus vadlīniju dokumentus, kas pieejami https://edpb.europa.eu/our-work-tools/general-guidance/gdpr-guidelines-recommendations-best-practices_en. Attiecīgajā vietnē ir arī norādes uz Eiropas Datu aizsardzības kolēģijas 29. panta darba grupas vadlīnijām, ieteikumiem un citiem dokumentiem. Bez tam, lai uzlabotu pilsoņu un uzņēmumu izpratni par Eiropas Parlamenta un Padomes Regulu (ES) 2016/679 (2016. gada

aizsardzības regulas 1. panta 3. punktā noteikts: “Personas datu [persondatu] brīvu apriti Savienībā neierobežo un neaizliedz tādu iemeslu dēļ, kas saistīti ar fizisku personu aizsardzību attiecībā uz personas datu apstrādi.”

Vairumā dzīves situāciju datu kopa veidojas gan no persondatiem, gan no nepersondatiem. Tādu bieži dēvē par „jauktu datu kopu”. Tālāk 2.2. iedaļā skaidrota Nepersondatu brīvas plūsmas regulas un Vispārīgās datu aizsardzības regulas mijdarbība, kas skar jauktas datu kopas.

Skaidrības labad jāpiezīmē, ka Vispārīgajā datu aizsardzības regulā un Nepersondatu brīvas plūsmas regulā nav pretrunīgu pienākumu.

2. Nepersondatu brīvas plūsmas regulas un Vispārīgās datu aizsardzības regulas mijdarbība. Jauktas datu kopas

2.1. Nepersondatu jēdziens Nepersondatu brīvas plūsmas regulā

Nepersondatu brīvas plūsmas regulas[8] mērķis ir nodrošināt brīvu plūsmu datiem, kas nav persondati. Visā regulas tekstā lietots termins “dati”, kas jāsaprot kā "dati, kas nav persondati, kā definēts Regulas (ES) 2016/679 [Vispārīgās datu aizsardzības regulas] 4. panta 1) punktā"[9]. Tādi dati – šajā dokumentā apzīmēti arī kā “**nepersondati**” – ir definēti kā pretstats Vispārīgās datu aizsardzības regulas persondatiem ("personas datiem").

Persondati

Vispārīgajā datu aizsardzības regulā lasām: ""personas dati" [persondati] ir jebkura informācija, kas attiecas uz identificētu vai identificējamu fizisku personu (“datu subjekts”); identificējama fiziska persona ir tāda, kuru var tieši vai netieši identificēt, jo īpaši atsaucoties uz identifikatoru, piemēram, minētās personas vārdu, uzvārdu, identifikācijas numuru, atrašanās vietas datiem, tiešsaistes identifikatoru vai vienu vai vairākiem minētajai fiziskajai personai raksturīgiem fiziskās, fizioloģiskās, ģenētiskās, garīgās, ekonomiskās, kultūras vai sociālās identitātes faktoriem."

Persondati tiek ar nodomu definēti plaši, un salīdzinājumā ar iepriekšējo tiesību aktu[10] Vispārīgajā datu aizsardzības regulā to definīcija nav mainījusies. Tādi persondatu definīcijas

---

27. aprīlis) par fizisku personu aizsardzību attiecībā uz personas datu apstrādi un šādu datu brīvu apriti un ar ko atceļ Direktīvu 95/46/EK (Vispārīgo datu aizsardzības regulu), Komisija ir izdevusi paziņojumu par datu aizsardzību – norādes par VDAR tiešu piemērošanu (COM(2018) 43 final), kas aplūkojamas https://eur-lex.europa.eu/legal-content/LV/TXT/HTML/?uri=CELEX:52018DC0043&from=EN.

[8] Eiropas Parlamenta un Padomes Regula (ES) 2018/1807 (2018. gada 14. novembris) par satvaru nepersondatu brīvai apritei Eiropas Savienībā, 1. pants.

[9] Sk. Eiropas Parlamenta un Padomes Regulas (ES) 2018/1807 (2018. gada 14. novembris) par satvaru nepersondatu brīvai apritei Eiropas Savienībā 3. panta 1. punktu.

[10] Sk. Eiropas Parlamenta un Padomes Direktīvas 95/46/EK (1995. gada 24. oktobris) par personu aizsardzību attiecībā uz personas datu apstrādi un šādu datu brīvu apriti (nav spēkā pēc 2018. gada 24. maija, atcelta ar Vispārīgo datu aizsardzības regulu) 2. panta a) punktu. Sk. arī Tiesas judikatūru par persondatu definīciju, kas atzīst tāda jēguma plašo interpretāciju, piem., sk. Tiesas 2009. gada 29. janvāra spriedumu lietā *Productores de Música de España (Promusicae)/Telefónica de España SAU*, C-275/06, ECLI:EU:C:2008:54;

aspekti kā "jebkura informācija", "kas attiecas uz", "identificēta vai identificējama" jau aplūkoti 29. panta darba grupas[11] 2007. gada 20. jūnija Atzinumā 4/2007 par persondatu jēdzienu, WP 136.

Tādās jomās kā pētniecība ierasts persondatus aizstāt ar pseidonīmu, maskējot personas identitāti. **Pseidonimizācija** ir persondatu apstrāde tādā veidā, ka bez papildinformācijas tos nav iespējams attiecināt uz konkrētu personu. Papildinformācija glabājas atsevišķi un tiek aizsargāta ar organizatoriskiem vai tehniskiem pasākumiem (piemēram, šifrēšanu)[12].[13] Tomēr pseidonimizēti dati joprojām tiek uzskatīti par ziņām par identificējamu personu, ja tos iespējams attiecināt uz šo personu, izmantojot papildinformāciju[14]. Tādi dati **ir persondati** saskaņā ar Vispārīgo datu aizsardzības regulu.

Nepersondati

Ja dati nav Vispārīgajā datu aizsardzības regulā noteiktie persondati, tie ir **nepersondati**. Nepersondati šādi iedalāmi izcelsmes kategorijās:

- pirmā – dati, kas sākotnēji nav attiekušies uz identificētu vai identificējamu fizisku personu, piemēram, tādi dati par laika apstākļiem, ko radījuši vēja ģeneratoros uzstādīti sensori, vai dati par rūpniecības iekārtu apkopes vajadzībām,

- otrā – dati, kas sākotnēji bijuši persondati, bet vēlāk padarīti **anonīmi**[15]. Personas datu anonimizācija atšķiras no pseidonimizācijas (sk. iepriekš), jo kārtīgi anonimizētus datus nevar attiecināt uz konkrētu personu pat tad, ja izmanto papilddatus[16], un tāpēc tie ir nepersondati.

Tiesas 2011. gada 24. novembra spriedumu lietā *Scarlet Extended SA/Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM)*, C-70/10, ECLI:EU:C:2011:771; Tiesas 2016. gada 19. oktobra spriedumu lietā *Patrick Breyer*/VFR, C-582/14, ECLI:EU:C:2016:779.

[11] 29. panta darba grupa bija padomdevēja struktūra, kas Komisiju konsultēja datu aizsardzības jautājumos un palīdzēja izstrādāt saskaņotu datu aizsardzības politiku ES. Pēc Vispārīgās datu aizsardzības regulas stāšanās spēkā 2018. gada 25. maijā 29. panta darba grupas vietā nāca Eiropas Datu aizsardzības kolēģija.

[12] Sk. pseidonimizācijas definīciju Eiropas Parlamenta un Padomes Regulas (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 (Vispārīgās datu aizsardzības regulas) 4. panta 5. punktā.

[13] Tā, pētījumu par jaunu zāļu iedarbību varētu kvalificēt kā pseidonimizētu, ja pētījuma dalībnieku persondati pētījuma dokumentācijā būtu aizstāti ar unikāliem atribūtiem (kā numuru vai kodu) un viņu persondati kopā ar piešķirtajiem unikālajiem atribūtiem atsevišķi glabātos drošā dokumentā (piemēram, ar paroli aizsargātā datubāzē).

[14] Sk. Eiropas Parlamenta un Padomes Regulas (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 (Vispārīgās datu aizsardzības regulas) 26. apsvērumu.

[15] Sk. Eiropas Parlamenta un Padomes 2016. gada 27. aprīļa Regulas (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 (Vispārīgās datu aizsardzības regulas) 26. apsvērumu, kur teikts: "datu aizsardzības principi nebūtu jāpiemēro anonīmai informācijai, proti, informācijai, kura neattiecas uz identificētu vai identificējamu fizisku personu, vai personas datiem, ko sniedz anonīmi tādā veidā, ka datu subjekts nav vai vairs nav identificējams".

[16] Sk. Tiesas 2016. gada 19. oktobra spriedumu lietā *Patrick Breyer*/VFR, C-582/14, ECLI:EU:C:2016:779. Tiesa noteica, ka interneta protokola (IP) dinamiskā adrese var sastādīt persondatus pat tad, ja trešai personai (piemēram, interneta pakalpojumu sniedzējam) ir papildu dati, pēc kuriem indivīdu var

Datu anonimizācijas pareizības noteikšana ir atkarīga no katra gadījuma specifiskiem un unikāliem apstākļiem[17]. Vairāki par anonimizētām uzskatītu datu kopu atpakaļidentificēšanas piemēri parādījuši, ka novērtēšana var prasīt daudz pūļu[18]. Lai noteiktu, vai personu iespējams identificēt, ir jāizskata visi līdzekļi, ko datu pārzinis vai cita persona pamatoti varētu izmantot tiešai vai netiešai indivīda identificēšanai[19].

Nepersondatu piemēri

- Datus, kas apkopoti tādā pakāpē, ka atsevišķus notikumus (piem., personas atsevišķus braucienus uz ārvalstīm vai ceļojumu maršrutus, kas var veidot persondatus) vairs nevar identificēt, var kvalificēt kā anonīmus[20]. Anonīmus datus izmanto tādās jomās kā statistika vai pārdošanas pārskati (piemēram, lai novērtētu produkta un tā īpašību popularitāti).
- Ātrās datorizētās tirdzniecības dati finanšu sektorā vai precīzijas lauksaimniecības dati, kas palīdz pārraudzīt un optimalizēt pesticīdu, barības vielu un ūdens izmantošanu.

Toties tad, kad nepersondatus var kaut kā saistīt ar indivīdu, viņu padarot tieši vai netieši identificējamu, dati jāuzskata par persondatiem.

Piemēram, ja kvalitātes kontroles ziņojums par ražošanas līniju ļauj datus saistīt ar konkrētiem rūpnīcas strādniekiem (piemēram, tiem, kas nosaka ražošanas parametrus), tad dati būtu uzskatāmi par persondatiem un jāpiemēro Vispārīgā datu aizsardzības regula. Tādi paši noteikumi ir spēkā gadījumos, kad tehnoloģijas un datu analītikas attīstība darījusi iespējamu anonimizētu datu pārvēršanu persondatos. [21]

---

identificēt. Iespējai identificēt indivīdu jāveidojas no līdzekļiem, kurus, kā var domāt, izmantos indivīda tiešai vai netiešai identificēšanai.

[17] Datu anonimizācija vienmēr veicama ar pašiem modernākajiem anonimizācijas paņēmieniem.

[18] Par anonimizētām uzskatītu datu kopu atpakaļidentificēšanas piemērus sk. pētījumā par nākotnes datu plūsmām, kurus Eiropas Parlamenta komisijas ITRE uzdevumā veikuši Blackman, C., Forge, S.: *Data Flows – Future Scenarios: In-Depth Analysis for the ITRE Committee,* 2017, 22. lpp., 2. rāmis. Pieejams tiešsaistē: http://www.europarl.europa.eu/RegData/etudes/IDAN/2017/607362/IPOL_IDA(2017)607362_EN.pdf

[19] Sk. Regulas (ES) 2016/679, Vispārīgās datu aizsardzības regulas, 26. apsvērumu, kur teikts: "Lai pārliecinātos, vai līdzekļus varētu saprātīgi izmantot fiziskas personas identificēšanai, būtu jāņem vērā visi objektīvie faktori, piemēram, identificēšanai nepieciešamās izmaksas un laiks, ņemot vērā apstrādes laikā pieejamo tehnoloģiju un tehnoloģiju attīstību."

[20] Sk. 29. panta darba grupas atzinumu *Opinion 05/2014 on Anonymisation Techniques*, pieņemts 2014. gada 10. aprīlī, WP216, 9. lpp.: "Iegūto datu kopu var kvalificēt kā anonīmu tikai tad, ja datu pārzinis apkopo datus tādā pakāpē, kad atsevišķi notikumi vairs nav identificējami. Piemēram, ja organizācija vāc datus par kāda ceļojuma atsevišķiem braucieniem, atsevišķā ceļojuma musturs notikumu līmenī tomēr uzskatāms par katras personas persondatiem, kamēr datu pārzinim (vai jebkurai citai personai) vēl ir pieejami sākotnējie jēldati, pat ja no trešām personām nodotās kopas ir izņemti tiešie identifikatori. Taču, ja datu pārzinis izdzēš jēldatus un dod tikai augstā līmenī apkopotu statistiku par trešām personām, piemēram, "maršrutā X pirmdienās ir par 160 % vairāk pasažieru nekā otrdienās", tā kvalificējama kā anonīmi dati."

[21] Ja personas datus apstrādā nelikumīgi vai apstrāde citādi pārkāpj Vispārīgo datu aizsardzības regulu, datu subjektiem (fiziskām personām) saskaņā ar Vispārīgo datu aizsardzības regulu ir tiesības iesniegt sūdzību valsts uzraudzības iestādei (datu aizsardzības iestādei) ES vai vērsties valsts tiesā pēc efektīvas tiesiskās

Tā kā persondatu definīcija attiecas uz fiziskām personām, datu kopas, kurās ir juridisko personu vārdi un kontaktinformācija, principā ir nepersondati[22]. Zināmos gadījumos tās tomēr var būt persondati[23]. Tā tas ir, piemēram, ja juridiskās personas firmas nosaukums sakrīt ar īpašnieka vārdu vai informācija attiecas uz identificētu vai identificējamu fizisku personu[24].

2.2. Jauktas datu kopas

Nepersondatu brīvas plūsmas regula un Vispārīgā datu aizsardzības regula datu brīvo apriti Eiropas Savienībā aplūko no diviem dažādiem skatpunktiem.

Nepersondatu brīvas plūsmas regula nosaka nepersondatu teritoriālas ierobežošanas vispārēju aizliegumu. Regulas 4. panta 1. punkts aizliedz datu teritoriālo ierobežošanu, kura nav pamatota ar sabiedriskās drošības apsvērumiem, ievērojot proporcionalitātes principu.

Vispārīgā datu aizsardzības regula papildus persondatu augsta līmeņa aizsardzībai nodrošina arī persondatu brīvu plūsmu. Saskaņā ar regulas 1. panta 3. punktu personas datu brīvu apriti Savienībā "neierobežo un neaizliedz tādu iemeslu dēļ, kas saistīti ar fizisku personu aizsardzību attiecībā uz personas datu apstrādi." Abas regulas kopā paredz "visu" datu brīvu apriti ES. Speciālās normas ir sīkāk aplūkotas 3.1. un 3.2. iedaļā.

Jauktu datu kopu veido gan persondati, gan nepersondati. Jauktas ir lielākā daļa datu kopu, kas tiek izmantotas datu ekonomikā, un tās ir sastopamas tādu tehnoloģiju attīstības dēļ kā lietu internets (t. i., priekšmetu digitāli savienojumi), mākslīgais intelekts un tehnoloģijas, kas ļauj veikt lielo datu analītiku.

Jauktu datu kopu piemēri:

- uzņēmuma nodokļu uzskaite, kur minēts uzņēmuma rīkotājdirektora uzvārds un tālruņa numurs;
- datu kopas bankā, sevišķi ar ziņām par klientiem un informāciju par darījumiem, piemēram, maksājumu pakalpojumi (kredītkartes un debetkartes), partneru attiecību pārvaldības (*PRM*) lietotnes un aizdevuma līgumi, dokumenti, kas apvieno datus par fiziskām un juridiskām personām;

---

aizsardzības. Valsts uzraudzības iestāžu uzdevumus, piekritību un pilnvaras reglamentē Vispārīgās datu aizsardzības regulas VI nodaļas 2. iedaļa.

[22] Eiropas Parlamenta un Padomes 2016. gada 27. aprīļa Regulas (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 (Vispārīgās datu aizsardzības regulas) 14. apsvērumā teikts: "Šī regula neattiecas uz tādu personas datu apstrādi, kas skar juridiskas personas un jo īpaši uzņēmumus, kuriem ir juridiskas personas statuss, tostarp juridiskās personas nosaukumu, uzņēmējdarbības formu un kontaktinformāciju." Tas tomēr jāsaprot, ievērojot arī persondatu definīciju Vispārīgās datu aizsardzības regulas 4. panta 1. punktā.

[23] Sk. Tiesas 2010. gada 9. novembra spriedumu apvienotajās lietās *Volker und Markus Schecke GbR*, C-92/09 un *Hartmut Eifert*, C-93/09 / Hesene, ECLI:EU:C:2010:662, 52. punkts.

[24] https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/application-regulation/do-data-protection-rules-apply-data-about-company_en

- anonimizēti pētniecības iestādes statistikas dati un sākotnēji ievākti jēldati, piemēram, atsevišķu respondentu atbildes uz statistiskas aptaujas jautājumiem;
- uzņēmuma zināšanu datubāze par IT problēmām un to risinājumiem, kas balstīta uz individuāliem ziņojumiem par IT starpgadījumiem;
- ar lietu internetu saistīti dati, ja kādi no tiem ļauj izdarīt pieņēmumus par identificējamām personām (piemēram, klātbūtne konkrētā adresē un lietošanas paradumi); un
- apstrādes rūpniecības ražošanas iekārtu darbības žurnālu datu analīze.

Piemērs ar klientu attiecību pārvaldības dienestu

Dažas bankas izmanto klientu attiecību pārvaldības (*CRM*) pakalpojumus, ko sniedz trešās personas, kuras pieprasa klienta datu pieejamību *CRM* vidē. *CRM* dienesta glabātajos datos ir visāda informācija, kas vajadzīga, lai efektīvi pārvaldītu mijdarbību ar klientu, piemēram, viņu pasta un e-pasta adrese, tālruņa numurs, preces un pakalpojumi, ko viņi iegādājas, un pārdošanas pārskati, kuros ir apkopoti dati. Tāpēc tajos var būt gan klientu persondati, gan nepersondati.

Attiecībā uz jaukta tipa datu kopām Nepersondatu brīvas plūsmas regula[25] nosaka:

"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."

Tas nozīmē, ka gadījumā, kad datu kopu veido gan persondati, gan nepersondati:

- datu kopas nepersondatu daļai piemēro Nepersondatu brīvas plūsmas regulu;
- datu kopas persondatu daļai piemēro Vispārīgās datu aizsardzības regulas[26] noteikumus par brīvu plūsmu; un
- ja personas datu daļa un personas datu daļas ir "nedalāmas", datu aizsardzības tiesības un pienākumi, kas izriet no Vispārīgās datu aizsardzības regulas, pilnībā attiecas uz visu jaukto datu kopu, arī tad, ja persondati ir tikai neliela datu kopas daļa[27].

Šāda interpretācija saskan ar tiesībām uz personas datu aizsardzību, kas garantētas Eiropas Savienības Pamattiesību hartā[28], un ar Nepersondatu brīvas plūsmas regulas 8. apsvērumu[29]. Tās 8. apsvērumā teikts: "Šī regula neskar tiesisko regulējumu attiecībā uz fizisku personu

[25] Tās 2. panta 2. punkts.

[26] 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 (Vispārīgās datu aizsardzības regulas), 1. panta 3. punkts. Sk. arī tās 3. panta 2. punktu.

[27] Komisijas dienestu darba dokumentā "Ietekmes novērtējums – pavaddokuments pie Eiropas Parlamenta un Padomes regulas priekšlikuma par satvaru nepersonizētu datu brīvai apritei Eiropas Savienībā (SWD(2017) 304 final), 1./2. daļa, 3. lpp., atgādināts: "neraugoties uz to, cik daudz persondatu ir iekļauts jauktās datu kopās, attiecībā uz kopas persondatu daļu ir pilnībā jāievēro VDAR [Vispārīgā datu aizsardzības regula]."

[28] Eiropas Savienības Pamattiesību harta (OV C 362, 26.10.2012., 391. lpp.).

[29] Tās 8. apsvērums.

aizsardzību saistībā ar persondatu apstrādi, .. īpaši Vispārīgo datu aizsardzības regulu un Eiropas Parlamenta un Padomes Direktīvas (ES) 2016/680 un 2002/58/EK."

Praktisks piemērs

Uzņēmums, kas darbojas ES, piedāvā pakalpojumus platformā. Uzņēmumi (klienti) tajā ielādē savus dokumentus, kuros ir jauktas datu kopas. Uzņēmums, kurš ielādē dokumentus, ir datu pārzinis, kam jāgādā, lai apstrāde atbilst Vispārīgajai datu aizsardzības regulai. Apstrādājot datu kopu pārziņa vārdā, uzņēmumam, kas piedāvā pakalpojumus ("apstrādātājam"), ir jāglabā un jāapstrādā dati saskaņā ar Vispārīgo datu aizsardzības regulu, piemēram, lai nodrošinātu, ka datiem tiek garantēts atbilstīgs drošības līmenis, cita starpā ar šifrēšanu.

Jēdziens "nedalāms" nevienā no abām regulām nav definēts[30]. Praktiskām vajadzībām tas var norādīt uz situāciju, kad datu kopa satur persondatus, kā arī nepersonizētus datus, un to nodalīšana pārzinim nebūtu iespējama vai tas to uzskatītu par ekonomiski neefektīvu vai tehniski neiespējamu. Piemēram, iegādājoties *CRM* un pārdošanas pārskatu sistēmas, uzņēmumam nāktos divkāršot savas programmatūras izmaksas, iegādājoties atsevišķu programmatūru *CRM* (personas datiem) un pārdošanas pārskatu sistēmām (apkopotiem datiem / nepersondatiem), kas balstās uz *CRM* datiem.

Datu kopas sadalīšana pie tam var ievērojami samazināt datu kopas vērtību. Turklāt, ņemot vērā datu mainīgumu (sk. 2.1. iedaļu), ir grūtāk atšķirt un līdz ar to nodalīt dažādas datu kategorijas.

Svarīgi ir tas, ka neviena no abām regulām neuzliek uzņēmumiem pienākumu dalīt datu kopas, ko tie kontrolē vai apstrādā.

Līdz ar to uz jauktu datu kopu parasti attiecas datu pārziņu un apstrādātāju pienākumi un tiek ievērotas datu subjektu tiesības, kas iedibinātas ar Vispārīgo datu aizsardzības regulu.

Medicīnisko datu apstrāde

Jauktā datu kopā var ietilpt dati par veselību. Piemēri: pacienta elektroniskā medicīniskā karte, klīniskie izmēģinājumi vai datu kopas, ko vāc dažādas mobilās lietotnes veselības aprūpei un labsajūtai (piemēram, veselības novērtēšanai, atgādinājumam ieņemt zāles vai sekot savai fiziskajai sagatavotībai)[31]. Robeža starp persondatiem un nepersondatiem šajās datu kopās kļūst aizvien neskaidrāka, ņemot vērā tehnoloģijas attīstību. Tāpēc to apstrādei jāatbilst Vispārīgajai datu aizsardzības regulai, sevišķi (ņemot vērā, ka saskaņā ar regulu medicīniskie dati ir īpaša datu kategorija) 9. pantam, kas nosaka vispārēju aizliegumu apstrādāt atsevišķu kategoriju datus un izņēmumus no šā aizlieguma.

30 Nepersondatu brīvas plūsmas regula un Vispārīgā datu aizsardzības regula.

31 Mobilo veselības aprūpes lietotņu izstrāde un darbība prasa stingru atbilstību Vispārīgās datu aizsardzības regulas normām. Prasības tiks sīkāk formulētas rīcības kodeksā par privātumu mobilajās veselības aprūpes lietotnēs, kas pašlaik tiek gatavots. Sīkāk par tā izstrādes stāvokli sk. https://ec.europa.eu/digital-single-market/en/privacy-code-conduct-mobile-health-apps.

Dati jauktajās datu kopās, kurās ir medicīniskie dati, var būt vērtīgs informācijas avots, piemēram, turpmākai medicīniskai pētniecībai, recepšzāļu blakņu noteikšanai, slimību statistikas vajadzībām vai jaunu veselības aprūpes pakalpojumu vai ārstniecības paņēmienu izstrādei. Tomēr, veicot sākotnējās un turpmākās datu apstrādes darbības, ir jāievēro Vispārīgā datu aizsardzības regula. Tāpēc šādai medicīnisko datu apstrādei jānotiek uz likumīga pamata[32] un ar atbilstīgu pamatojumu, jābūt drošai un jānodrošina pietiekami aizsardzības pasākumi.

Visbeidzot, ir svarīgi, lai personas un uzņēmumi iegūtu juridisku noteiktību un uzticēšanos datu apstrādei. Tas ir svarīgi arī datu ekonomikas pastāvēšanai. Abas regulas to nodrošina, un abu mērķis ir neaizskart datu brīvo apriti.

3. Brīva datu plūsma un datu teritoriālas ierobežošanas atcelšana

Šajā iedaļā ir paskaidroti jēdzieni, kas attiecas uz datu teritoriālu ierobežošanu saskaņā ar Nepersondatu brīvas plūsmas regulu un brīvas aprites principu Vispārīgajā datu aizsardzības regulā. Lai gan šie noteikumi domāti dalībvalstīm, tie var uzņēmumiem izveidot labāku priekšstatu par to, kā šīs divas regulas veicina visu ES datu brīvu apriti ES iekšienē.

3.1. Nepersondatu brīva plūsma

Nepersondatu brīvas plūsmas regula[33] nosaka: "Datu teritoriālas ierobežošanas prasības ir aizliegtas, ja vien tās nav pamatotas ar sabiedriskās drošības apsvērumiem, ievērojot proporcionalitātes principu."

Datu teritoriālas ierobežošanas prasības ir definētas[34] kā "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"[35].

Definīcija rāda, ka pasākumi, kas ierobežo datu brīvo apriti ES (datu teritoriāla ierobežošana jeb iežogošana), var izpausties dažādi. Tie var būt noteikti normatīvajos tiesību aktos un administratīvajā regulējumā vai pat būt vispārējas, konsekventas administratīvās prakses rezultāts. Turklāt datu iežogošanas aizliegums attiecas gan uz tiešiem, gan netiešiem pasākumiem, kas ierobežo nepersondatu brīvo apriti.

---

[32] Sk. Eiropas Parlamenta un Padomes Regulas (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 (Vispārīgās datu aizsardzības regulas) 6. panta 1. punktu.

[33] Tās 4. panta 1. punkts.

[34] Eiropas Parlamenta un Padomes Regula (ES) 2018/1807 (2018. gada 14. novembris) par satvaru nepersondatu brīvai apritei Eiropas Savienībā, 3. panta 5. punkts.

[35] Jāievēro, ka juridiskā nenoteiktība ar datu teritoriālās ierobežošanas likumīgo un nelikumīgo prasību apmēru vēl vairāk ierobežo tirgus dalībnieku un publiskā sektora izvēli datu apstrādes vietas ziņā (sk. Eiropas Parlamenta un Padomes 2018. gada 14. novembra Regulas (ES) 2018/1807 par satvaru nepersonizētu datu brīvai apritei Eiropas Savienībā 4. apsvērumu).

Tieša datu iežogošana var izpausties, piemēram, pienākumā glabāt datus īpašā ģeogrāfiskā vietā (piemēram, serverim jāatrodas noteiktā dalībvalstī) vai pienākumā ievērot valsts īpatnējās tehniskās prasības (piemēram, datiem jābūt specifiskā formātā).

Netieša datu iežogošana, kas mēdz kavēt nepersondatu apstrādi citās dalībvalstīs; tā var izpausties dažnedažādi. Te var būt prasības izmantot tehnoloģiskās iekārtas, kas ir sertificētas vai apstiprinātas noteiktā dalībvalstī, vai citas prasības, kuru dēļ ir grūtāk datus apstrādāt ārpus noteiktā Eiropas Savienības ģeogrāfiskā apgabala vai teritorijas[36].[37]

Vērtējot, vai konkrētais pasākums ir netieša datu iežogošana, ir jāņem vērā katra gadījuma īpašie apstākļi.

Nepersondatu brīvas plūsmas regula[38] atsaucas uz Eiropas Savienības Tiesas judikatūrā aprādīto **sabiedriskās drošības** konceptu. Sabiedriskā drošība "aptver gan dalībvalsts iekšējo, gan ārējo drošību[39], 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[40], 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."

Turklāt datu iežogošanai, ko pamato ar sabiedrisko drošību, jābūt samērīgai. Saskaņā ar Eiropas Savienības Tiesas judikatūru proporcionalitātes princips prasa, lai pieņemtie pasākumi nodrošinātu, ka tiek sasniegts iecerētais mērķis un netiek darīts vairāk, kā šim nolūkam nepieciešams[41].

Skaidrības labad jāpasaka, ka datu iežogošanas aizliegums neskar ES tiesību aktos jau pastāvošos ierobežojumus[42].

---

[36] Eiropas Parlamenta un Padomes Regula (ES) 2018/1807 (2018. gada 14. novembris) par satvaru nepersondatu brīvai apritei Eiropas Savienībā, 4. apsvērums.

[37] Sk. divus pētījumus par datu iežogošanu, kas veikti pirms Nepersondatu brīvas plūsmas regulas pieņemšanas: 1) Godel, M. et al.: *Facilitating cross border data flows in the Digital Single Market*, SMART number 2015/2016, pieejams tiešsaistē: http://ec.europa.eu/newsroom/document.cfm?doc_id=41185, 2) Time.lex, Spark Legal Network and Tech4i2: *Cross-border data flow in the digital single market: study on data localisation restrictions*, SMART number 2015/0054, pieejams tiešsaistē: http://ec.europa.eu/newsroom/dae/document.cfm?doc_id=46695.

[38] Tās 19. apsvērums.

[39] Sk., piem., Tiesas 2010. gada 23. novembra spriedumu lietā *Bādene-Virtemberga* / *Tsakouridis*, C-145/09, ECLI:EU:C:2010:708, 43. punktu, un 2017. gada 4. aprīļa spriedumu lietā *Sahar Fahimian* / *VFR*, C-544/15, ECLI:EU:C:2017:225, 39. punktu.

[40] Sk., piem., Tiesas 2008. gada 22. decembra spriedumu lietā *Eiropas Kopienu Komisija* / *Austrijas Republika*, C-161/07, ECLI:EU:C:2008:759, 35. punktu un tajā minēto judikatūru, un 2009. gada 26. marta spriedumu lietā *Eiropas Kopienu Komisija* / *Itālijas Republika*, C-326/07, ECLI:EC:C:2009:193, 70. punktu un tajā minēto judikatūru.

[41] Sk., piemēram, Tiesas 2010. gada 8. jūlija spriedumu lietā *Afton Chemical Limited* / *Secretary of State for Transport*, C-343/09, ECLI:EU:C:2010:419, 45. punktu un arī tajā minēto judikatūru.

[42] Sk., piemēram, 2006. gada 28. novembra Direktīvas 2006/112/EK par kopējo pievienotās vērtības nodokļa sistēmu 245. panta 2. punktu, kur noteikts: „Dalībvalstis var prasīt, lai nodokļa maksātāji, kas veic uzņēmējdarbību to teritorijā, paziņo rēķinu glabāšanas vietu, ja tā ir ārpus dalībvalsts attiecīgās teritorijas". Taču

Turklāt Nepersondatu brīvas plūsmas regula ne uzliek uzņēmumiem pienākumu, ne ierobežo to līgumtiesisko brīvību lemt par datu apstrādes vietu.

Dalībvalstīm tiek prasīts sniegt informāciju par to teritorijā piemērojamām datu teritoriālas ierobežošanas prasībām, kas publiski pieejamas **valsts vienotā tiešsaistes informācijas punktā** (valsts vietnē). Tām informācija pastāvīgi jāatjaunina vai jāsniedz atjaunināta informācija centrālam informācijas punktam, kas izveidots uz cita ES tiesību akta pamata[43]. Uzņēmējdarbības ērtībai un labai attiecīgās informācijas piekļūstamībai visā Eiropas Savienībā Komisija portālā "Tava Eiropa"[44] publicē saites ar šiem informācijas punktiem.

3.2. Persondatu brīva plūsma

Vispārīgā datu aizsardzības regula[45] nosaka: "Personas datu brīvu apriti Savienībā neierobežo un neaizliedz tādu iemeslu dēļ, kas saistīti ar fizisku personu aizsardzību attiecībā uz personas datu apstrādi."

Ja datu teritoriālās ierobežošanas prasības dalībvalsts uzliek persondatiem tādu iemeslu dēļ, kas nav persondatu aizsardzība, ir jāizsver to atbilstība pamatbrīvību normām un Līgumā par Eiropas Savienības darbību atļautajam pamatam izņēmumiem no šīm brīvībām[46,47], un attiecīgiem ES aktiem, kā Pakalpojumu direktīva[48] un E-komercijas direktīva[49].

Piemērs

Valsts tiesību norma prasa, lai algu sarakstu pārskati atrodas konkrētā dalībvalstī ar regulatīvo kontroli saistītu iemeslu dēļ, piemēram, valsts nodokļu dienesta vajadzībām. Tādas normu Vispārīgās datu aizsardzības regulas 1. panta 3. punkts neaptver, jo to pamats nav persondatu aizsardzība. Taču tāda prasība jāvērtē atbilstīgi pamatbrīvību normām un Līgumā par Eiropas Savienības darbību atļautajam pamatam izņēmumiem no šīm brīvībām.

šī prasība lasāma kopā ar 249. pantu, kurā noteikts: "Ja nodokļa maksātājs rēķinus, ko tas izsniedz vai saņem, glabā elektroniski, garantējot tiešsaistes piekļuvi datiem, un ja glabāšanas vieta ir citā dalībvalstī nevis tajā, kurā tas veic uzņēmējdarbību, kompetentajām iestādēm dalībvalstī, kurā tas veic uzņēmējdarbību, šīs direktīvas nolūkiem ir tiesības elektroniski piekļūt šiem rēķiniem, lejupielādēt un izmantot tos, nepārsniedzot ierobežojumus, ko nosaka nodokļa maksātāja uzņēmējdarbības veikšanas dalībvalsts noteikumi, ciktāl minētajām iestādēm tas ir vajadzīgs kontroles nolūkā."

[43] Eiropas Parlamenta un Padomes Regula (ES) 2018/1807 (2018. gada 14. novembris) par satvaru nepersondatu brīvai apritei Eiropas Savienībā, 4. panta 4. punkts.

[44] https://europa.eu/youreurope/index.htm

[45] 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), 1. panta 3. punkts.

[46] Līguma par Eiropas Savienības darbību konsolidētā versija (OV C 326, 26.10.2012., 47.–390. lpp.).

[47] Sk. arī Tiesas 2008. gada 19. jūnija spriedumu lietā *Eiropas Kopienu Komisija* / *Luksemburgas Lielhercogiste*, C-319/06, ECLI:EU:C:2008:350, 90.–91. punktu. Tiesa uzskatīja, ka pienākums glabāt un paturēt zināmus dokumentus atsevišķā dalībvalstī ir pakalpojumu sniegšanas brīvības ierobežojums; pamatojums "iestādēm ir vieglāk pildīt uzraudzības uzdevumus" nav pietiekams.

[48] Eiropas Parlamenta un Padomes Direktīva 2006/123/EK (2006. gada 12. decembris) par pakalpojumiem iekšējā tirgū (OV L 376, 27.12.2006., 36.–68. lpp.).

[49] Eiropas Parlamenta un Padomes Direktīva 2000/31/EK (2000. gada 8. jūnijs) 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.).

Vispārīgā datu aizsardzības regula[50] atzīst, ka dalībvalstis var piemērot nosacījumus, to starpā ierobežojumus, ģenētisko datu, biometrisko datu vai medicīnisko datu apstrādei. Tomēr, kā norādīts 53. apsvērumā, tādi valsts ierobežojumi nedrīkst kavēt persondatu brīvu plūsmu ES, ja nosacījumi attiecas uz tādu datu pārrobežu apstrādi. Tas saskan ar Līguma par Eiropas Savienības darbību 16. pantu, kas nodrošina juridisko pamatu, uz kura pieņem noteikumus par tiesībām uz persondatu aizsardzību un noteikumus par tādu datu brīvu apriti.

3.3. Nepersondatu brīvas plūsmas regulas tvērums

Kā jau teikts, Nepersondatu brīvas plūsmas regula tiecas nodrošināt nepersondatu brīvu plūsmu "Savienībā"[51]. Tā neattiecas uz apstrādes darbībām ārpus ES un datu teritoriālas ierobežošanas prasībām, kas saistītas ar tādu apstrādi[52].[53]

Tāpēc regulas tvērums saskaņā ar 2. panta 1. punktu aprobežojas ar elektronisko nepersondatu apstrādi Eiropas Savienībā,

(a) ko nodrošina kā pakalpojumu lietotājiem, kuriem Savienībā ir pastāvīga dzīvesvieta vai iedibinājums, bez izšķirības, vai pakalpojuma sniedzējs ir vai nav reģistrēts Savienībā, vai
(b) ko savām vajadzībām veic fiziska vai juridiska persona, kurai ES ir pastāvīga dzīvesvieta vai iedibinājums.

Piemēri

Nepersondatu brīvas plūsmas regulas 2. panta 1. punkta a) apakšpunkts.

- ASV reģistrēts mākoņdatošanas pakalpojumu sniedzējs sniedz apstrādes pakalpojumus klientiem, kuri dzīvo vai veic saimniecisku darbību ES. Savu darbību mākoņpakalpojumu sniedzējs īsteno caur serveriem ES teritorijā, kur glabājas vai tiek apstrādāti tā Eiropas klientu dati. Mākoņpakalpojumu sniedzēja īpašumā nav jābūt ES bāzētai infrastruktūrai, bet tas var, piemēram, īrēt vietu ES serveros. Uz tādu datu apstrādi attiecas Nepersondatu brīvas plūsmas regula.
- Japānā reģistrēts mākoņpakalpojumu sniedzējs piedāvā pakalpojumus klientiem Eiropā. Pakalpojumu sniedzēja apstrādes jaudas ir Japānā, un visa apstrāde notiek tur. Ja visas

[50] 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 (Vispārīgās datu aizsardzības regulas), 9. panta 4. punkts.

[51] Sk. Eiropas Parlamenta un Padomes Regulas (ES) 2018/1807 (2018. gada 14. novembris) par satvaru nepersondatu brīvai apritei Eiropas Savienībā 1. pantu.

[52] Sk. Eiropas Parlamenta un Padomes Regulas (ES) 2018/1807 (2018. gada 14. novembris) par satvaru nepersondatu brīvai apritei Eiropas Savienībā 15. apsvērumu.

[53] Termins "apstrāde" ir definēts plaši (Eiropas Parlamenta un Padomes 2018. gada 14. novembra Regulas (ES) 2018/1807 par satvaru nepersonizētu datu brīvai apritei Eiropas Savienībā 3. panta 2. punktā), un, kā uzsvērts 17. apsvērumā, regula piemērojama apstrādei visplašākajā nozīmē, aptverot visdažādāko veidu IT sistēmu izmantošanu.

apstrādes darbības notiek ārpus ES, šajā gadījumā Nepersondatu brīvas plūsmas regula nav piemērojama[54].

Nepersondatu brīvas plūsmas regulas 2. panta 1. punkta b) apakšpunkts.

- Sīks Eiropas jaunuzņēmums no dalībvalsts A nolemj paplašināties, iedibinot uzņēmumu dalībvalstī B. Lai minimalizētu izmaksas, tas nolemj jaunizveidotā uzņēmuma datus centralizēti glabāt un apstrādāt savā serverī, kas atrodas dalībvalstī A. Tādu IT centralizēšanu dalībvalstis nedrīkst aizliegt, izņemot gadījumu, kad aizliegumu pamato ar sabiedrisko drošību, ievērojot proporcionalitātes principu.

Nepersondatu brīvas plūsmas regula nav piemērojama, ja visas persondatu apstrādes darbības notiek ārpus ES, taču, ja daļa no datu kopas ir persondati, ir jāievēro Vispārīgā datu aizsardzības regula. Galvenais, katrā gadījumā ir jāievēro noteikumi par persondatu nodošanu trešām valstīm vai starptautiskām organizācijām saskaņā ar Vispārīgo datu aizsardzības regulu[55].

3.4. Pasākumi sakarā ar dalībvalstu iekšējo organizāciju

Nepersondatu brīvas plūsmas regula neuzliek dalībvalstīm pienākumu ārpakalpojumu sniedzējiem uzticēt ar nepersondatiem saistītus pakalpojumus, kurus tās vēlas sniegt pašas vai organizēt bez publiskā iepirkuma[56].

Nepersondatu brīvas plūsmas regulas 2. panta 3. punkta otrā daļa nosaka:

"Šī regula neskar normatīvos un administratīvos aktus, kas ir saistīti ar dalībvalstu **iekšējo organizāciju** un ar ko publiskām iestādēm un Direktīvas 2014/24/ES[57] 2. panta 1. punkta

[54] Ievērosim, ka Eiropas Parlamenta un Padomes 2018. gada 14. novembra Regula (ES) 2018/1807 par satvaru nepersonizētu datu brīvai apritei Eiropas Savienībā neattiecas uz datu teritoriālas ierobežošanas prasībām, ko dalībvalstis noteikušas nepersondatu glabāšanai trešās valstīs, un tādas var pastāvēt valsts tiesību sistēmā. Skaidrības labad: Vispārīgā datu aizsardzības regula uz ES atrodošos datu subjektu persondatu apstrādi, ko veic pārzinis vai apstrādātājs, kuram ES nav uzņēmuma, attiecas tad, ja apstrādes darbības saistītas ar a) preču vai pakalpojumu piedāvāšanu šādiem datu subjektiem Savienībā neatkarīgi no tā, vai no datu subjekta tiek prasīta samaksa, vai b) "viņu uzvedības novērošanu, ciktāl viņu uzvedība notiek Savienībā" (sk. Vispārīgās datu aizsardzības regulas 3. panta 2. punktu).

[55] Par persondatu nodošanu trešām valstīm sk. Komisijas tīmekļa vietni https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/obligations/what-rules-apply-if-my-organisation-transfers-data-outside-eu_en un Komisijas paziņojumu Eiropas Parlamentam un Padomei "Apmaiņa ar personas datiem un šo datu aizsardzība globalizētā pasaulē", COM/2017/07 final, pieejams https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2017 %3A7 %3AFIN. 2019. gada 23. janvārī Komisija ir pieņēmusi lēmumu par datu aizsardzības līmeņa pietiekamību Japānā, ļaujot personas datiem brīvi plūst starp abiem reģioniem, pamatojoties uz to stingrām aizsardzības garantijām.

[56] Eiropas Parlamenta un Padomes Regulas (ES) 2018/1807 (2018. gada 14. novembris) par satvaru nepersondatu brīvai apritei Eiropas Savienībā 14. apsvērums.

[57] Eiropas Parlamenta un Padomes 2014. gada 26. februāra Direktīvas 2014/24/ES par publisko iepirkumu un ar ko atceļ Direktīvu 2004/18/EK, OV L 94, 28.3.2014., 65.–242. lpp., 2. panta 1. punkta 4. apakšpunktā noteikts: ""Publisko tiesību subjekti" ir struktūras, kurām piemīt visi turpmāk minētie raksturlielumi: a) tās ir nodibinātas ar konkrētu mērķi apmierināt vispārējas vajadzības, kurām nav rūpnieciska vai komerciāla rakstura; b) tām ir juridiskas personas statuss; un c) tās galvenokārt finansē valsts, reģionālās vai vietējās iestādes vai citi publisko tiesību subjekti; vai to pārvaldību uzrauga minētās iestādes vai struktūras; vai to vadībā, valdē vai uzraudzības padomē vairāk nekā pusi locekļu ieceļ valsts, reģionālās vai vietējās iestādes vai citi publisko tiesību subjekti."

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."[58]

Var pastāvēt leģitīmas intereses, kas attaisno tādu datu apstrādes pakalpojumu "pašnodrošināšanu", piemēram, pakalpojumu sniedzot pašu spēkiem vai vienojoties pārvaldes iestādēm. Par tipisku piemēru var minēt "valdības mākoņa" izmantošanu vai centralizētas IT aģentūras iesaisti valdības darbā, lai nodrošinātu datu apstrādes pakalpojumus valsts iestādēm un struktūrām.

Taču Nepersondatu brīvas plūsmas regula mudina dalībvalstis apsvērt ārpakalpojumu izmantošanas ekonomisko efektivitāti un citas priekšrocības[59].[60] Tiklīdz valsts iestādes sāk ārpakalpojumu izmantošanu datu apstrādei ar līgumisku atlīdzību privātpersonām un apstrāde notiek Eiropas Savienībā, uz apstrādi attiecas Nepersondatu brīvas plūsmas regula, un tas nozīmē, ka uz valsts iestāžu vispārējo un administratīvo praksi attiecas nepersondatu brīvas plūsmas princips. Svarīgākais – tām jāatturas no datu teritoriāliem ierobežojumiem, piemēram, publiskā iepirkuma konkursos[61].

4. Pašregulēšanās pieejas, kas balsta datu brīvo plūsmu

Pašregulācija veicina inovāciju un uzticēšanos tirgus dalībnieku starpā, un tai piemīt potenciāls reaģēt uz pārmaiņām tirgū. Šajā iedaļā dots pārskats par pašregulēšanās iniciatīvām gan persondatu, gan nepersondatu apstrādē.

4.1. Datu pārnešana un mākoņpakalpojumu sniedzēja maiņa

Viens no Nepersondatu brīvas plūsmas regulas mērķiem ir novērst iestigšanu pie viena vienīga pārdevēja. Tā notiek, kad lietotāji nevar nomainīt pakalpojuma sniedzēju tāpēc, ka viņu dati ir iestiguši pakalpojumu sniedzēja sistēmā, piemēram, īpaša formāta vai līguma noteikumu dēļ, un tos nevar dabūt ārā no pārdevēja IT sistēmas. Datu pārnešana bez traucēkļiem ir svarīga, lai lietotāji varētu brīvi izvēlēties datu apstrādes pakalpojumu sniedzējus un tirgū tiktu nodrošināta efektīva konkurence.

Datu pārnesamība starp uzņēmumiem kļūst arvien svarīgāka visdažādākajās digitālajās nozarēs, ieskaitot mākoņpakalpojumus.

Saskaņā ar Nepersondatu brīvas plūsmas regulas 6. pantu Komisija veicina un atvieglo pašregulējošu ES līmeņa rīcības kodeksu ("rīcības kodeksi") izstrādi, lai veicinātu

[58] Eiropas Parlamenta un Padomes Regulas (ES) 2018/1807 (2018. gada 14. novembris) par satvaru nepersondatu brīvai apritei Eiropas Savienībā 13. apsvērums uzsver, ka regula neskar Direktīvu 2014/24/ES.

[59] Eiropas Parlamenta un Padomes Regula (ES) 2018/1807 (2018. gada 14. novembris) par satvaru nepersondatu brīvai apritei Eiropas Savienībā, 14. apsvērums.

[60] Ārpakalpojumu sniedzēji ir personas, kuras nav "publisko tiesību subjekti" tā, kā noteikts Eiropas Parlamenta un Padomes 2014. gada 26. februāra Direktīvas 2014/24/ES par publisko iepirkumu un ar ko atceļ Direktīvu 2004/18/EK (OV L 94, 28.3.2014., 65.–242. lpp.) 2. panta 1. punkta 4. apakšpunktā.

[61] Eiropas Parlamenta un Padomes Regulas (ES) 2018/1807 (2018. gada 14. novembris) par satvaru nepersondatu brīvai apritei Eiropas Savienībā 13. apsvērums.

konkurētspējīgu datu ekonomiku. Tas nozarei dod pamatu, uz kura izstrādāt pašregulējošus rīcības kodeksus par pakalpojumu sniedzēju maiņu un datu pārnešanu starp atšķirīgām IT sistēmām.

Izstrādājot šādus rīcības kodeksus datu pārnesamībai, jāņem vērā vairāki aspekti, sevišķi:

- **paraugprakse** pakalpojumu sniedzēju maiņas atvieglošanai un datu pārnešanai strukturētā, plaši izmantotā un mašīnlasāmā formātā;
- **minimālās informēšanas prasības**, kas nodrošinātu, ka pirms līguma noslēgšanas profesionāliem lietotājiem tiek sniegta pietiekami detalizēta un skaidra informācija par procesiem, tehniskajām prasībām, termiņiem un maksu, ko piemēro gadījumos, kad profesionāls lietotājs vēlas mainīt pakalpojumu sniedzēju vai pārnest datus atpakaļ savās IT sistēmās;
- tādas **pieejas sertifikācijas shēmām**, kas ļauj mākoņpakalpojumus vieglāk salīdzināt; un
- **ceļveži**, kas uzlabo informētību par rīcības kodeksiem.

Mākoņpakalpojumu tirgū Komisija ir sākusi atvieglot darbu digitālā vienotā tirgus (DVT) mākoņdatošanas ieinteresēto personu darba grupām, kas apvieno mākoņdatošanas ekspertus un profesionālos lietotājus, to vidū mazos un vidējos uzņēmumus. Patlaban viena apakšgrupa izstrādā pašregulējošus rīcības kodeksus datu pārnešanai un pakalpojumu sniedzēju maiņai (darba grupa *SWIPO*)[62] un cita apakšgrupa taisās izstrādāt mākoņdatošanas drošības sertifikāciju (darba grupa *CSCTERT*)[63].

SWIPO izstrādā rīcības kodeksus, kas aptver visu mākoņdatošanas pakalpojumu spektru: programmatūru kā pakalpojumu (*SaaS*), platformu kā pakalpojumu (*PaaS*) un infrastruktūru kā pakalpojumu (*IaaS*).

Komisija cer sagaidīt, ka dažādos rīcības kodeksus papildinās **līgumu standartklauzulas**[64]. Tas ļaus praktiski īstenot un piemērot tehniski un juridiski specifiskus rīcības kodeksus, kas būs īpaši svarīgi mazajiem un vidējiem uzņēmumiem. Līgumu standartklauzulu izstrāde tiek plānota pēc rīcības kodeksu izstrādes (kas jāpaveic līdz 2019. gada 29. novembrim).

Saskaņā ar Nepersondatu brīvas plūsmas regulas 8. pantu Komisija līdz 2022. gada 29. novembrim izvērtēs regulas īstenošanu. Tad būs iespējams novērtēt: i) ietekmi uz datu brīvu plūsmu Eiropā; ii) regulas piemērošanu, sevišķi – jauktām datu kopām; iii) kādā mērā dalībvalstis būs faktiski atcēlušas spēkā esošos nepamatotos teritoriālos ierobežojumus; iv) datu pārnešanas un mākoņpakalpojumu sniedzēju maiņas rīcības kodeksu ietekmi uz tirgu.

62 Mākoņpakalpojumu maiņas un datu pārnešanas darba grupa.

63 Eiropas Mākoņpakalpojumu sniedzēju sertifikācijas darba grupa. Sk. arī 4.3. iedaļu.

64 Sk. Eiropas Parlamenta un Padomes Regulas (ES) 2018/1807 (2018. gada 14. novembris) par satvaru nepersondatu brīvai apritei Eiropas Savienībā 30. apsvērumu.

Pārnesamības jēgums un mijdarbība ar Vispārīgo datu aizsardzības regulu

Abas regulas[65] attiecas uz datu pārnesamību un mērķi atvieglināt datu pārnesi no vienas IT vides uz otru, t. i., vai nu cita pakalpojuma sniedzēja sistēmā, vai objekta vietējā sistēmā. Tas novērš atkarību no viena pārdevēja un veicina pakalpojumu sniedzēju konkurenci. Tomēr regulās atšķiras pieeja pārnesamībai tādā plāksnē kā attiecības starp interešu mērķgrupām un noteikumu juridiskā daba.

Vispārīgās datu aizsardzības regulas 20. panta noteiktās tiesības uz persondatu pārnesamību galvenokārt vērstas uz attiecībām starp datu subjektu un datu pārzini. Tās attiecas uz datu subjekta tiesībām persondatus, kurus tas nodevis pārzinim, saņemt strukturētā, plaši izmantotā un mašīnlasāmā formā un pārvest tos pie cita pārziņa vai pašam savā glabāšanas iekārtā tā, ka to nekavē pārzinis, kuram personas dati bijuši nodoti[66]. Parastākie datu subjekti tādās attiecībās ir dažādu tiešsaistes pakalpojumu patērētāji, kuri vēlas mainīt pakalpojumu sniedzēju.

Nepersondatu brīvas plūsmas regulas 6. pants profesionālajiem lietotājiem neparedz tiesības pārnest datus, bet izmanto nozares pašregulēšanu ar brīvprātīgas rīcības kodeksiem. Tajā pašā laikā tas vērsts uz situāciju, kad profesionāls lietotājs datu apstrādi uzticējis ārpakalpojumu sniedzējam, kas ir treša persona, kura piedāvā datu apstrādes pakalpojumu[67]. Saskaņā ar Nepersondatu brīvas plūsmas regulas 3. panta 8. punktu starp "profesionāliem lietotājiem" var būt fiziskas vai juridiskas personas, "tostarp publiska iestāde vai publisko tiesību subjekts, kas izmanto vai pieprasa datu apstrādes pakalpojumu savām ar tirdzniecību, uzņēmējdarbību, arodu, profesiju vai uzdevumu saistītām vajadzībām".

Nepersondatu brīvas plūsmas regulas 6. pantā noteiktā pārnesamība praksē attiecas uz profesionāla lietotāja (kas gadījumos, kas ietver persondatu apstrādi, saskaņā ar Vispārīgo datu aizsardzības regulu tiek kvalificēts kā "pārzinis") un pakalpojumu sniedzēja (dažos gadījumos tiek kvalificēts kā "apstrādātājs") mijdarbību.

Neraugoties uz atšķirībām, var rasties situācijas, kad datu pārnešanu aptver gan Nepersondatu brīvas plūsmas regula, gan – attiecībā uz jauktām datu kopām – Vispārīgā datu aizsardzības regula.

Piemērs

[65] Eiropas Parlamenta un Padomes Regula (ES) 2018/1807 (2018. gada 14. novembris) par satvaru nepersondatu brīvai apritei Eiropas Savienībā, 6. pants, un 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), 20. pants.

[66] Sk. 29. panta darba grupas "Vadlīnijas par tiesībām uz datu pārnesamību". WP 242 rev.01, pieņemtas 2016. gada 13. decembrī, jaunākā pārskatītā redakcija pieņemta 2017. gada 5. aprīlī.

[67] Eiropas Parlamenta un Padomes Regulas (ES) 2018/1807 (2018. gada 14. novembris) par satvaru nepersondatu brīvai apritei Eiropas Savienībā 29. apsvērumā teikts: "Lai gan individuāli patērētāji gūst labumu no spēkā esošajiem Savienības tiesību aktiem [t. i., Vispārīgās datu aizsardzības regulas], tie neatvieglo tādu lietotāju iespējas mainīt pakalpojumu sniedzējus, kuri rīkojas uzņēmējdarbības vai profesionālās darbības veikšanas laikā."

Uzņēmums, kas izmanto mākoņpakalpojumu, nolemj pāriet pie cita pakalpojumu sniedzēja un pārnest pie tā visus datus. Pakalpojumu sniedzēja maiņa un datu pārnešana ir ietverta klienta un mākoņpakalpojuma sniedzēja līgumā. Ja vecais mākoņpakalpojumu sniedzējs ievēro rīcības kodeksus, kas izstrādāti saskaņā ar Nepersondatu brīvas plūsmas regulu, datu pārnešanai jānotiek saskaņā ar tajā noteiktajām prasībām.

Ja persondati ietilpst arī pārnesamajās datu kopās, pārnešanai jāatbilst visiem attiecīgajiem Vispārīgās datu aizsardzības regulas noteikumiem, it īpaši – nodrošinot, ka jaunais mākoņpakalpojumu sniedzējs atbilst piemērojamajām prasībām, piemēram, drošības prasībām[68].

Piemērs

Banka nolemj mainīt klientu attiecību pārvaldības (*CRM*) pakalpojumu sniedzēju, un kādi dati (persondati un nepersondati) ir jāpārceļ no vecā pakalpojumu sniedzēja pie jaunā. Tad uz šiem datiem attiecas atšķirīgas regulatīvās prasības, no kurām vienas izriet no Vispārīgās datu aizsardzības regulas, otras – no Nepersondatu brīvas plūsmas regulas.

4.2. Persondatu aizsardzības rīcības kodeksi un sertifikācijas shēmas

Lai pierādītu Vispārīgajā datu aizsardzības regulā (sk. 24. panta 3. punktu un 28. panta 5. punktu) noteikto pienākumu izpildi, var izmantot rīcības kodeksus un sertifikācijas shēmas.

Saskaņā ar Vispārīgās datu aizsardzības regulas 40. panta 1. punktu un 42. panta 1. punktu dalībvalstīm, uzraudzības iestādēm, Eiropas Datu aizsardzības kolēģijai un Komisijai jāmudina nozare izstrādāt rīcības kodeksus un veidot datu aizsardzības sertifikācijas mehānismus.

Apvienības vai citas struktūras, kas pārstāv kādu pārziņu vai apstrādātāju kategoriju, var sagatavot rīcības kodeksu attiecīgajai nozarei. Kodeksa projekts iesniedzams apstiprināšanai attiecīgajā kompetentajā uzraudzības iestādē[69]. Ja rīcības kodeksa projekts attiecas uz apstrādes darbībām vairākās dalībvalstīs, uzraudzības iestādei tas pirms apstiprināšanas jāiesniedz Eiropas Datu aizsardzības kolēģijai. Tad kolēģija sniedz atzinumu par to, vai kodeksa projekts atbilst Vispārīgajai datu aizsardzības regulai.

Eiropas Datu aizsardzības kolēģija saskaņā ar Vispārīgo datu aizsardzības regulu publicēja vadlīnijas 1/2019 par rīcības kodeksiem un uzraudzības struktūrām[70]. Vadlīnijās ir informācija

[68] Sk. 29. panta darba grupas 2012. gada 1. jūlijā pieņemto atzinumu 05/2012 par mākoņdatošanu, WP196, kur sīkāk precizēti mākoņdatošanas lietotāju un mākoņdatošanas pakalpojumu sniedzēju statuss un pienākumi persondatu apstrādē.

[69] Sk. Eiropas Parlamenta un Padomes Regulas (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 (Vispārīgās datu aizsardzības regulas) 40. panta 5. punktu un 55. pantu.

[70] Eiropas Datu aizsardzības kolēģija, *Guidelines 1/2019 on Codes of Conduct and Monitoring Bodies under Regulation 2016/679*, pieņemts 2019. gada 12. februārī, versija sabiedriskai apspriešanai, pieejams

par rīcības kodeksu izstrādi, to apstiprināšanas kritēriji un citas noderīgas ziņas. Līdzīgā veidā Eiropas Datu aizsardzības kolēģijas vadlīnijas 1/2018 par sertifikāciju un sertifikācijas kritēriju noteikšanu saskaņā ar Vispārīgās datu aizsardzības regulas 42. un 43. pantu sniedz informāciju par sertifikāciju atbilstīgi šai regulai un sertifikācijas kritēriju izstrādi un apstiprināšanu[71].

Mākoņdatošanas nozares izstrādāti rīcības kodeksi

ES Mākoņdatošanas rīcības kodekss, kura izstrādi veicināja Komisija, izstrādāts sadarbībā ar Mākoņdatošanas nozares grupu (*C-SIG*), pamatojoties uz Datu aizsardzības direktīvu[72] un vēlāk uz Vispārīgo datu aizsardzības regulu. ES Mākoņdatošanas rīcības kodekss aptver visus mākoņpakalpojumus: programmatūru kā pakalpojumu (*SaaS*), platformu kā pakalpojumu (*PaaS*) un infrastruktūru kā pakalpojumu (*IaaS*)[73].

Eiropas mākoņdatošanas infrastruktūras pakalpojumu sniedzēju (*CISPE*) rīcības kodekss[74] domāts *IaaS* pakalpojumu sniedzējiem. *CISPE* rīcības kodeksā ir prasības, kas attiecas uz *IaaS* pakalpojumu sniedzējiem, kuri darbojas kā datu apstrādātāji saskaņā ar Vispārīgo datu aizsardzības regulu. Tajā arī izklāstīti noteikumi par kodeksa īstenošanas un piemērošanas pārvaldes struktūru.

Mākoņdatošanas drošības alianses rīcības kodekss atbilstībai VDAR attiecas uz tādām mākoņdatošanas un Eiropas persondatu jomas tiesību aktu aspektā ieinteresētajām personām kā mākoņdatošanas pakalpojumu sniedzēji, viņu klienti un potenciālie klienti, mākoņdatošanas revidenti un mākoņdatošanas mākleri. Rīcības kodekss aptver visu mākoņpakalpojumu sniedzēju loku[75].

4.3. Vairot uzticēšanos pārrobežu datu apstrādei – sertificēt drošību

Nepersondatu brīvas plūsmas regulas 33. apsvērumā norādīts, ka lielāka uzticēšanās pārrobežu datu apstrādei vājina tirgus dalībnieku un publiskā sektora noslieci datu teritoriālo ierobežošanu izmantot par datu drošības aizstājēju. Līdztekus Komisijas 2017. gadā ierosinātajai kiberdrošības paketei[76] darba grupa *CSPCERT* Eiropas mākoņdatošanas sertifikācijas shēmas izveides vajadzībām izstrādā ieteikumus, kas tiks iesniegti Komisijai. Tāda shēma spētu veicināt datu brīvo apriti, uzlabot mākoņdatošanas pakalpojumu salīdzināmību un plašāk izmantot mākoņdatošanu. Saskaņā ar attiecīgajiem Kiberdrošības

---

tiešsaistē https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-12019-codes-conduct-and-monitoring-bodies-under_en

[71] Eiropas Datu aizsardzības kolēģija, *Guidelines 1/2018 on certification and identifying certification criteria in accordance with Articles 42 and 43 of the Regulation 2016/679*, pieņemts 2019. gada 23. janvārī, pieejams tiešsaistē: https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-12018-certification-and-identifying-certification_en

[72] Eiropas Parlamenta un Padomes Direktīva 95/46/EK (1995. gada 24. oktobris) par personu aizsardzību attiecībā uz personas datu apstrādi un šādu datu brīvu apriti (spēkā esības beigas – 2018. gada 24. maijs).

[73] Sīkāk par ES mākoņdatošanas kodeksu sk. https://eucoc.cloud/en/home.html

[74] Sīkāk par *CISPE* kodeksu sk. https://cispe.cloud/code-of-conduct/

[75] Sīkāk par *CSA* rīcības kodeksu sk. https://gdpr.cloudsecurityalliance.org/

[76] Sīkāk sk. https://ec.europa.eu/digital-single-market/en/cyber-security

akta[77] noteikumiem Komisija var pieprasīt no *ENISA* (Eiropas Savienības Kiberdrošības aģentūras) kandidātshēmu. Kandidātshēma varētu attiekties gan uz persondatiem, gan nepersondatiem. Papildus Kiberdrošības aktam un tā, kā uzsvērts 4.2. iedaļā, VDAR ir izmantojama arī piemērotu datu drošības aizsardzības pasākumu pastāvēšanas pierādīšanai[78].

Nobeiguma piebildes

Lai panāktu juridisko noteiktību un uzticēšanos datu apstrādei, ir būtiski, lai ES spētu pilnīgi izmantot datu potenciālu, turklāt tā, ka vērtības veidošanas ķēdes attīstās gan starp nozarēm, gan pāri robežām. Abas regulas to nodrošina, un abu mērķis ir datiem nodrošināt brīvu apriti. Nepersondatu brīvas plūsmas regula un Vispārīgā datu aizsardzības regula kopīgi liek pamatus brīvai visu datu plūsmai Eiropas Savienībā un augsti konkurētspējīgai Eiropas datu ekonomikai.

[77] Eiropas Parlamenta un Padomes Regula (2019. gada 17. aprīlis) par *ENISA* (Eiropas Savienības Kiberdrošības aģentūru) un informācijas un sakaru tehnoloģiju kiberdrošības sertifikāciju un par Regulas (ES) Nr. 526/2013 atcelšanu (Kiberdrošības akts).

[78] Sk. Kiberdrošības akta 74. apsvērumu.