II

(Neleģislatīvi akti)

LĒMUMI

KOMISIJAS ĪSTENOŠANAS LĒMUMS (ES) 2020/1023

(2020. gada 15. jūlijs),

ar ko attiecībā uz datu pārrobežu apmaiņu starp nacionālajām kontaktu izsekošanas un brīdināšanas mobilajām lietotnēm cīņā pret Covid-19 pandēmiju groza Īstenošanas lēmumu (ES) 2019/1765

(Dokuments attiecas uz EEZ)

EIROPAS KOMISIJA,

ņemot vērā Līgumu par Eiropas Savienības darbību,

ņemot vērā Eiropas Parlamenta un Padomes Direktīvu 2011/24/ES (2011. gada 9. marts) par pacientu tiesību piemērošanu pārrobežu veselības aprūpē ([1]) un jo īpaši tās 14. panta 3. punktu,

tā kā:

(1) Direktīvas 2011/24/ES 14. pantā ir noteikts, ka Savienība atbalsta un veicina sadarbību un informācijas apmaiņu starp dalībvalstīm, kas strādā brīvprātīgā tīklā, kurā apvienotas par e-veselību atbildīgās valstu iestādes ("e-veselības tīkls"), ko nozīmējušas dalībvalstis.

(2) Komisijas Īstenošanas lēmums (ES) 2019/1765 ([2]) paredz par e-veselību atbildīgo valsts iestāžu tīkla izveidošanas, pārvaldības un darbības noteikumus. Minētā lēmuma 4. pants e-veselības tīklam uztic uzdevumu veicināt valstu informācijas un komunikācijas tehnoloģijas sistēmu lielāku sadarbspēju un elektronisko veselības datu pārrobežu nodrošināmību pārrobežu veselības aprūpē.

(3) Ņemot vērā Covid-19 pandēmijas izraisīto sabiedrības veselības krīzi, vairākas dalībvalstis ir izstrādājušas mobilās lietotnes, kas atbalsta kontaktu izsekošanu un ļauj šādu lietotņu lietotājus brīdināt, ja konstatēts, ka viņi varētu būt bijuši pakļauti saskarei ar šo vīrusu, atrodoties cita šādu lietotņu lietotāja tuvumā, kurš ir paziņojis pozitīvu diagnozi, – lai viņi varētu attiecīgi rīkoties, piemēram, testēties vai pašizolēties. Šādas lietotnes izmanto *Bluetooth* tehnoloģiju, lai atklātu tuvumā esošas ierīces. Kopš 2020. gada jūnija ceļošanas ierobežojumi starp dalībvalstīm ir atcelti, tāpēc valstu informācijas un komunikācijas tehnoloģijas sistēmu lielāka sadarbspēja e-veselības tīklā būtu jāpanāk tādējādi, ka tiek nodrošināta digitālā infrastruktūra, kas sekmē sadarbspēju starp valstu mobilajām lietotnēm, kuras atbalsta kontaktu izsekošanu un brīdināšanu.

([1]) OV L 88, 4.4.2011., 45. lpp.

([2]) Komisijas Īstenošanas lēmums (ES) 2019/1765 (2019. gada 22. oktobris), ar ko paredz par e-veselību atbildīgo valsts iestāžu tīkla izveidošanas, pārvaldības un darbības noteikumus un atceļ Īstenošanas lēmumu 2011/890/ES (OV L 270, 24.10.2019., 83. lpp.).

(4) Komisija atbalsta dalībvalstis attiecībā uz iepriekš minētajām mobilajām lietotnēm. Komisija 2020. gada 8. aprīlī pieņēma Ieteikumu par kopīgu Savienības rīkkopu tehnoloģiju un datu izmantošanai ar mērķi apkarot Covid-19 krīzi un iziet no tās, it īpaši attiecībā uz mobilajām lietotnēm un anonimizētu mobilitātes datu izmantošanu ("Komisijas ieteikums") ([3]). E-veselības tīklā esošās dalībvalstis ar Komisijas atbalstu pieņēma dalībvalstīm kopīgu ES rīkkopu par mobilajām lietotnēm, kuras atbalsta kontaktu izsekošanu ([4]) un norādījumus par apstiprinātu kontaktu izsekošanas mobilo lietotņu sadarbspēju ES ([5]). Rīkkopā ir izskaidrotas valstu prasības attiecībā uz nacionālajām kontaktu izsekošanas un brīdināšanas mobilajām lietotnēm, it īpaši, ka to instalēšanai jābūt brīvprātīgai, tām jābūt attiecīgās valsts veselības iestādes apstiprinātām, tām jānodrošina lietotāju privātums un, kolīdz vairs nav vajadzīgas, tās jāatinstalē. Pēc nesenajiem notikumiem Covid-19 krīzes attīstībā Komisija ([6]) un Eiropas Datu aizsardzības kolēģija ([7]) ir izdevušas katra savus norādījumus par mobilajām lietotnēm un kontaktu izsekošanas rīkiem saistībā ar datu aizsardzību. Dalībvalstu mobilo lietotņu un digitālās infrastruktūras, kas nodrošina to sadarbspēju, veidošanas pamatā ir kopīgā ES rīkkopa, iepriekš minētie norādījumi un tehniskās specifikācijas, par kurām vienojies e-veselības tīkls.

(5) Lai sekmētu to, ka nacionālās kontaktu izsekošanas un brīdināšanas mobilās lietotnes ir sadarbspējīgas, tās e-veselības tīklā esošās dalībvalstis, kas nolēmušas savu sadarbību šajā jomā brīvprātīgi pastiprināt, ar Komisijas atbalstu ir izstrādājušas digitālu infrastruktūru kā IT rīku, ar ko apmainīties ar datiem. Šī digitālā infrastruktūra tiek dēvēta par federatīvo vārteju.

(6) Šajā lēmumā ir noteikti noteikumi par to, kāda ir iesaistīto dalībvalstu un Komisijas loma federatīvajā vārtejā attiecībā uz nacionālo mobilo kontaktu izsekošanas un brīdināšanas lietotņu pārrobežu sadarbspēju.

(7) Kontaktu izsekošanas un brīdināšanas mobilo lietotņu lietotāju persondatu apstrādei, par ko atbild dalībvalstis vai citas dalībvalstīs esošas publiskas organizācijas vai oficiālas struktūras, būtu jānotiek saskaņā ar Eiropas Parlamenta un Padomes Regulu (ES) 2016/679 ([8]) ("Vispārīgā datu aizsardzības regula") un Eiropas Parlamenta un Padomes Direktīvu 2002/58/EK ([9]). Persondatu apstrādei, par ko atbild Komisija un ko veic ar nolūku pārvaldīt federatīvo vārteju un garantēt tās drošību, būtu jāatbilst Eiropas Parlamenta un Padomes Regulai (ES) 2018/1725 ([10]).

(8) Federatīvajai vārtejai būtu jāsastāv no drošas IT infrastruktūras, kas nodrošina kopēju saskarni, kur nozīmētās valstu iestādes vai oficiālās struktūras var dalīties minimālā datu kopumā, kas attiecas uz kontaktēšanos ar *SARS-CoV*-2 inficētām personām, lai informētu citus par viņu varbūtējo saskari ar minēto infekciju un veicinātu efektīvu sadarbību starp dalībvalstīm veselības aprūpes plānā, atvieglojot attiecīgās informācijas apmaiņu.

(9) Tāpēc šajā lēmumā būtu jānosaka, kādā kārtībā Eiropas Savienībā ir veicama datu pārrobežu apmaiņa starp nozīmētajām valstu iestādēm vai oficiālajām struktūrām, izmantojot federatīvo vārteju.

([3]) Komisijas Ieteikums (ES) 2020/518 (2020. gada 8. aprīlis) par vienotu Savienības rīkkopu tehnoloģiju un datu izmantošanai ar mērķi apkarot Covid-19 krīzi un iziet no tās, it īpaši attiecībā uz mobilajām lietotnēm un anonimizētu mobilitātes datu izmantošanu (OV L 114, 14.4.2020., 7. lpp.).

([4]) https://ec.europa.eu/health/sites/health/files/ehealth/docs/covid-19_apps_en.pdf

([5]) https://ec.europa.eu/health/sites/health/files/ehealth/docs/contacttracing_mobileapps_guidelines_en.pdf

([6]) Komisijas paziņojums "Norādījumi par lietotnēm, kas sniedz atbalstu cīņā pret Covid-19 pandēmiju saistībā ar datu aizsardzību" (OV C 124I, 17.4.2020., 1. lpp.).

([7]) 2020. gada aprīļa Norādījumi par atrašanās vietas datu un kontaktu izsekošanas rīku izmantošanu Covid-19 uzliesmojuma kontekstā un EDAK 2020. gada 16. jūnija Paziņojums par kontaktu izsekošanas lietotņu sadarbspējas ietekmi uz datu aizsardzību, abi pieejami šeit: https://edpb.europa.eu.

([8]) 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.).

([9]) 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.).

([10]) 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.).

(10) Iesaistītās dalībvalstis, ko pārstāv nozīmētās valstu iestādes vai oficiālās struktūras, kopīgi nosaka, kādā nolūkā un ar kādiem līdzekļiem federatīvajā vārtejā var apstrādāt persondatus, un tāpēc tās ir kopīgi pārziņi. Vispārīgās datu aizsardzības regulas 26. pants persondatu apstrādes darbību kopīgajiem pārziņiem uzliek pienākumu pārredzamā veidā noteikt to attiecīgos pienākumus, lai izpildītu minētajā regulā uzliktās saistības. Tajā arī paredzēta iespēja, ka šos pienākumus var noteikt Savienības vai dalībvalsts tiesību aktos, kas attiecas uz pārziņiem. Katram pārzinim būtu jānodrošina, lai tam būtu valsts līmeņa juridiskais pamats datu apstrādei federatīvajā vārtejā.

(11) Komisija, būdama tā, kas federatīvo vārteju nodrošina ar tehniskiem un organizatoriskiem risinājumiem, iesaistīto dalībvalstu kā kopīgo pārziņu uzdevumā federatīvajā vārtejā apstrādā pseidonimizētus persondatus un tāpēc ir datu pārzinis. Saskaņā ar Vispārīgās datu aizsardzības regulas 28. pantu un Regulas (ES) 2018/1725 29. pantu apstrādi, ko veic apstrādātājs, reglamentē ar līgumu vai citu juridisku aktu saskaņā ar Savienības vai dalībvalsts tiesību aktiem, kurš ir saistošs apstrādātājam attiecībā uz pārzini un kurā ir specificēta apstrāde. Šajā lēmumā ir izklāstīti noteikumi par apstrādi, ko kā apstrādātājs veic Komisija.

(12) Kad federatīvajā vārtejā tiek apstrādāti persondati, Komisijai ir saistošs Komisijas Lēmums (ES, Euratom) 2017/46 ([11]).

(13) Ņemot vērā nolūkus, kādos pārziņi apstrādā persondatus nacionālajās mobilajās lietojumprogrammās, kas paredzētas kontaktu izsekošanai un brīdināšanai, datu subjekts nav obligāti jāidentificē, tāpēc datu pārziņi ne vienmēr var nodrošināt datu subjektu tiesību piemērošanu. Tāpēc, ja ir izpildīti minētās regulas 11. panta nosacījumi, Vispārīgās datu aizsardzības regulas 15.–20. pantā minētās tiesības var nebūt piemērojamas.

(14) Īstenošanas lēmumam (ES) 2019/1765 tiek pievienoti vēl divi pielikumi, tāpēc tā tagadējam pielikumam jāpiešķir numurs.

(15) Tāpēc Īstenošanas lēmums (ES) 2019/1765 būtu attiecīgi jāgroza.

(16) Ņemot vērā Covid-19 pandēmijas izraisītās situācijas steidzamību, šis lēmums būtu jāpiemēro no nākamās dienas pēc tā publicēšanas *Eiropas Savienības Oficiālajā Vēstnesī*.

(17) Ir notikusi apspriešanās ar Eiropas Datu aizsardzības uzraudzītāju saskaņā ar Regulas (ES) 2018/1725 42. panta 1. punktu, un 2020. gada 9. jūlijā tas sniedza atzinumu.

(18) Šajā lēmumā paredzētie pasākumi ir saskaņā ar komitejas, kas izveidota saskaņā ar Direktīvas 2011/24/ES 16. pantu, atzinumu,

IR PIEŅĒMUSI ŠO LĒMUMU.

1. pants

Īstenošanas lēmumu (ES) 2019/1765 groza šādi:

1) lēmuma 2. panta 1. punktam pievieno šādu g), h), i), j), k), l), m), n) un o) apakšpunktu:

"g) "lietotnes lietotājs" ir persona, kuras īpašumā ir viedierīce un kura ir lejupielādējusi un izmanto apstiprinātu mobilo lietotni kontaktu izsekošanai un brīdināšanai;

h) "kontaktu izsekošana" ir pasākumi, kurus īsteno nolūkā atrast personas, kuras ir bijušas pakļautas nopietna pārrobežu veselības apdraudējuma izraisītāja iedarbībai, Eiropas Parlamenta un Padomes Lēmuma Nr. 1082/2013/ES (*) 3. panta c) punkta nozīmē;

([11]) Komisijas Lēmums (ES, Euratom) 2017/46 (2017. gada 10. janvāris) par komunikācijas un informācijas sistēmu drošību Eiropas Komisijā (OV L 6, 11.1.2017., 40. lpp.). Vairāk informācijas par drošības standartiem, kas piemērojami visām Eiropas Komisijas informācijas sistēmām, Komisija publicē šeit: https://ec.europa.eu/info/publications/security-standards-applying-all-european-commission-information-systems_en.

i) "nacionālā kontaktu izsekošanas un brīdināšanas mobilā lietotne" ir valsts līmenī apstiprināta programmatūra, kas darbojas viedierīcēs, jo īpaši viedtālruņos, parasti ir paredzēta plašai un specifiskai mijiedarbībai ar tīmekļa resursiem, un, lai izsekotu kontaktēšanos ar cilvēkiem, kas inficēti ar *SARS-CoV-2*, un brīdinātu cilvēkus, kas varētu būt bijuši pakļauti saskarei ar *SARS-CoV-2* vīrusu, apstrādā tuvuma datus un citu kontekstuālu informāciju, kas savākta ar daudziem viedierīcēs esošajiem sensoriem. Šīs mobilās lietotnes spēj konstatēt citu ierīču klātbūtni, izmantojot *Bluetooth* tehnoloģiju, un, izmantojot internetu, apmainīties ar informāciju ar aizmugursistēmas serveriem;

j) "federatīvā vārteja" ir Komisijas ekspluatēta tīkla vārteja, kas, lai nodrošinātu nacionālo kontaktu izsekošanas un brīdināšanas mobilo lietotņu sadarbspēju, ar drošu IT rīku saņem, uzglabā un dara pieejamu minimālu persondatu kopumu dalībvalstu aizmugursistēmas serveriem;

k) "atslēga" ir īslaicīgs unikāls identifikators, kas saistīts ar lietotnes lietotāju, kurš ziņo, ka ir inficēts ar *SARS-CoV-2*, vai kurš varētu būt bijis pakļauts saskarei ar *SARS-CoV-2* vīrusu;

l) "inficēšanās verifikācija" ir metode, ar kuru apstiprina inficēšanos ar *SARS-CoV-2*, proti, pārbauda, vai lietotnes lietotājs par inficēšanos paziņojis pats vai inficēšanos ir apstiprinājusi valsts veselības iestāde, vai inficēšanās konstatēta laboratorijas testā;

m) "interesējošās valstis" ir dalībvalsts vai dalībvalstis, kur lietotnes lietotājs ir bijis 14 dienas pirms atslēgu augšupielādēšanas datuma un ir lejupielādējis apstiprināto valsts kontaktu izsekošanas un brīdināšanas mobilo lietotni un/vai ceļojis;

n) "atslēgu izcelsmes valsts" ir dalībvalsts, kurā atrodas aizmugursistēmas serveris, kas atslēgas augšupielādējis federatīvajā vārtejā;

o) "žurnāla dati" ir automātiski reģistrēts ieraksts par darbību, kas saistīta ar federatīvajā vārtejā apstrādāto datu apmaiņu un piekļuvi tiem, un tie galvenokārt norāda apstrādes darbības veidu, datumu un laiku un tās personas identifikatoru, kas šos datus ir apstrādājusi.

(*) Eiropas Parlamenta un Padomes Lēmums Nr. 1082/2013/ES (2013. gada 22. oktobris) par nopietniem pārrobežu veselības apdraudējumiem un ar ko atceļ Lēmumu Nr. 2119/98/EK (OV L 293, 5.11.2013., 1. lpp.).";

2) lēmuma 4. panta 1. punktam pievieno šādu h) apakšpunktu:

"h) norādījumu sniegšana dalībvalstīm par persondatu pārrobežu apmaiņu federatīvajā vārtejā starp nacionālajām kontaktu izsekošanas un brīdināšanas mobilajām lietotnēm.";

3) lēmuma 6. panta 1. punktam pievieno šādu f) un g) apakšpunktu:

"f) lai nodrošinātu nacionālo kontaktu izsekošanas un brīdināšanas mobilo lietotņu sadarbspēju, izstrādāt, ieviest un saglabāt piemērotus tehniskos un organizatoriskos pasākumus, kas saistīti ar persondatu nosūtīšanas un izmitināšanas drošību federatīvajā vārtejā;

g) nodrošināt un veikt nepieciešamos testus un revīzijas, tādā veidā palīdzot e-veselības tīklam noteikt, vai valstu iestādes nodrošina tehnisku un organizatorisku atbilstību prasībām, kas izvirzītas persondatu pārrobežu apmaiņai federatīvajā vārtejā. Komisijas revidentiem var palīdzēt dalībvalstu eksperti.";

4) lēmuma 7. pantu groza šādi:

a) virsrakstu aizstāj ar "E-veselības digitālo pakalpojumu infrastruktūrā apstrādāto persondatu aizsardzība";

b) panta 2. punktā virsrakstu "Pielikums" aizstāj ar virsrakstu "I pielikums";

5) iekļauj šādu 7.a pantu:

"*7.a pants*

Datu pārrobežu apmaiņa federatīvajā vārtejā starp nacionālajām kontaktu izsekošanas un brīdināšanas mobilajām lietotnēm

1. Ja federatīvajā vārtejā apmainās ar persondatiem, apstrāde notiek tikai ar nolūku sekmēt nacionālo kontaktu izsekošanas un brīdināšanas mobilo lietotņu sadarbspēju federatīvajā vārtejā un kontaktu izsekošanas nepārtrauktību pārrobežu kontekstā.

2. Persondatus, kas minēti 3. punktā, federatīvajā vārtejā ievada pseidonimizētā veidā.

3. Federatīvajā vārtejā apmainītie un apstrādātie pseidonimizētie persondati ietver tikai šādu informāciju:

a) nacionālo kontaktu izsekošanas un brīdināšanas mobilo lietotņu atslēgas, kas nosūtītas līdz 14 dienām pirms šo atslēgu augšupielādēšanas datuma;

b) ar atslēgām saistītie žurnāla dati atbilstoši tehnisko specifikāciju protokolam, kuru izmanto atslēgu izcelsmes valstī;

c) inficēšanās verifikācija;

d) interesējošās valstis un atslēgu izcelsmes valsts.

4. Nozīmētās valstu iestādes vai oficiālās struktūras, kas persondatus apstrādā federatīvajā vārtejā, ir federatīvajā vārtejā apstrādāto datu kopīgi pārziņi. Kopīgie pārziņi savus pienākumus savstarpēji sadala atbilstoši II pielikumam. Katra dalībvalsts, kas vēlas piedalīties datu pārrobežu apmaiņā starp nacionālajām kontaktu izsekošanas un brīdināšanas mobilajām lietotnēm, pirms pievienošanās par savu nodomu paziņo Komisijai un nosauc par atbildīgo pārzini nozīmēto valsts iestādi vai oficiālo struktūru.

5. Federālajā vārtejā persondatu apstrādātājs ir Komisija. Apstrādātāja kapacitātē Komisija nodrošina persondatu apstrādes, arī nosūtīšanas un izmitināšanas, drošību federatīvajā vārtejā un pilda apstrādātāja pienākumus, kas noteikti III pielikumā.

6. Komisija un valstu iestādes, kam atļauts piekļūt federatīvajai vārtejai, regulāri testē, novērtē un izvērtē, vai tehniskie un organizatoriskie pasākumi, ar kuriem panāk persondatu apstrādes drošību federatīvajā vārtejā, ir efektīvi.

7. Neskarot kopīgo pārziņu lēmumu datu apstrādi federatīvajā vārtejā pārtraukt, federatīvā vārteja izbeidz darbību, kad ir pagājušas vismaz 14 dienas pēc tam, kad visas pieslēgtās nacionālās kontaktu izsekošanas un brīdināšanas mobilās lietotnes ir pārstājušas federatīvajā vārtejā pārsūtīt atslēgas.";

6) pielikums turpmāk ir I pielikums;

7) pievieno II un III pielikumu, kuru teksts ir dots šā lēmuma pielikumā.

2. pants

Šis lēmums stājas spēkā nākamajā dienā pēc tā publicēšanas *Eiropas Savienības Oficiālajā Vēstnesī*.

Briselē, 2020. gada 15. jūlijā

Komisijas vārdā –
priekšsēdētāja
Ursula VON DER LEYEN

PIELIKUMS

Īstenošanas lēmumam (ES) 2019/1765 pievieno šādu II un III pielikumu:

"II PIELIKUMS

IESAISTĪTO DALĪBVALSTU KĀ KOPĪGO PĀRZIŅU PIENĀKUMI FEDERATĪVAJĀ VĀRTEJĀ, KURĀ NOTIEK DATU PĀRROBEŽU APSTRĀDE STARP NACIONĀLAJĀM KONTAKTU IZSEKOŠANAS UN BRĪDINĀŠANAS MOBILAJĀM LIETOTNĒM

1. IEDAĻA

1. apakšiedaļa

Pienākumu sadale

1. Kopīgie pārziņi federatīvajā vārtejā apstrādā persondatus atbilstoši tehniskajām specifikācijām, kādas noteicis e-veselības tīkls ([1]).

2. Katrs pārzinis ir atbildīgs par persondatu apstrādi federatīvajā vārtejā saskaņā ar Vispārīgo datu aizsardzības regulu un Direktīvu 2002/58/EK.

3. Katrs pārzinis izveido kontaktpunktu ar funkcionālo pastkastīti, kas tiks izmantota saziņai starp kopīgajiem pārziņiem un starp kopīgajiem pārziņiem un apstrādātāju.

4. Pagaidu apakšgrupai, ko saskaņā ar 5. panta 4. punktu izveidojis e-veselības tīkls, uztic izskatīt visas iespējamās problēmas, kas rodas sakarā ar nacionālo kontaktu izsekošanas un brīdināšanas mobilo lietotņu sadarbspēju un izriet no kopīgās atbildības par persondatu attiecīgo apstrādi, un sekmēt Komisijai kā apstrādātājam domātu norādījumu koordinētu sagatavošanu. Cita starpā pārziņi drīkst pagaidu apakšgrupā strādāt pie kopējas pieejas, kā datus saglabāt attiecīgo valstu aizmugursistēmas serveros, ievērojot federatīvajā vārtejā noteikto saglabāšanas periodu.

5. Norādījumus apstrādātājam nosūta jebkurš kopīgo pārziņu kontaktpunkts, vienojoties ar pārējiem kopīgajiem pārziņiem iepriekš minētajā apakšgrupā.

6. Federatīvajā vārtejā apmainītajiem lietotāju persondatiem drīkst piekļūt tikai nozīmēto valsts iestāžu vai oficiālo struktūru pilnvarotas personas.

7. Katra nozīmētā valsts iestāde vai oficiālā struktūra beidz pildīt kopīgā pārziņa pienākumus no datuma, kurā tā atsauc dalību federatīvajā vārtejā. Tā joprojām ir atbildīga par datu apstrādi federatīvajā vārtejā, kas notikusi pirms atsaukuma.

2. apakšiedaļa

Pienākumi un lomas attiecībā uz datu subjektu pieprasījumu izskatīšanu un viņu informēšanu

1. Katrs pārzinis saskaņā ar Vispārīgās datu aizsardzības regulas 13. un 14. pantu savas nacionālās kontaktu izsekošanas un brīdināšanas mobilās lietotnes lietotājiem ("datu subjekti") sniedz informāciju par viņu persondatu apstrādi federatīvajā vārtejā nacionālo kontaktu izsekošanas un brīdināšanas mobilo lietotņu sadarbspējas vajadzībām.

2. Katrs pārzinis savas nacionālo kontaktu izsekošanas un brīdināšanas mobilo lietotņu lietotājiem ir kontaktpunkts un izskata šo lietotāju vai viņu pārstāvju iesniegtos pieprasījumus par datu subjektu tiesību izmantošanu saskaņā ar Vispārīgo datu aizsardzības regulu. Katrs pārzinis nozīmē īpašu kontaktpunktu, kurš izskata no datu subjektiem saņemtos pieprasījumus. Ja kāds no kopīgajiem pārziņiem saņem pieprasījumu no datu subjekta, kas neietilpst tā atbildības jomā, tas to nekavējoties pārsūta atbildīgajam kopīgajam pārzinim. Pēc pieprasījuma kopīgie pārziņi cits citam palīdz izskatīt datu subjektu pieprasījumus un cits citam atbild bez liekas kavēšanās un vēlākais 15 dienu laikā pēc palīdzības pieprasījuma saņemšanas.

([1]) Proti, atbilstoši 2020. gada 16. jūnija sadarbspējas specifikācijām par datu pārrobežu nosūtīšanas ķēdēm starp apstiprinātām lietotnēm. Specifikācijas pieejamas šeit: https://ec.europa.eu/health/ehealth/key_documents_en#anchor0

3. Katrs pārzinis datu subjektiem dara pieejamu šā pielikuma saturu, arī 1. un 2. punktā noteikto.

2. IEDAĻA

Rīcība drošības incidentu, arī persondatu aizsardzības pārkāpumu, gadījumā

1. Kopīgie pārziņi cits citam palīdz identificēt un risināt drošības incidentus, arī persondatu aizsardzības pārkāpumus, kas saistīti ar datu apstrādi federatīvajā vārtejā.

2. Jo īpaši, kopīgie pārziņi cits citam paziņo:

a) jebkuru potenciālu vai faktisku risku federatīvajā vārtejā esošo apstrādājamo persondatu pieejamībai, konfidencialitātei un/vai integritātei;

b) jebkuru drošības incidentu, kas saistīts ar apstrādes darbību federatīvajā vārtejā;

c) jebkuru persondatu aizsardzības pārkāpumu, persondatu aizsardzības pārkāpuma iespējamās sekas un fizisku personu tiesību un brīvību riska novērtējumu, un jebkurus pasākumus, kas veikti, lai risinātu persondatu aizsardzības pārkāpumu un mazinātu risku fizisku personu tiesībām un brīvībām;

d) jebkuru apstrādes darbības tehnisko un/vai organizatorisko aizsardzības pasākumu pārkāpumu federatīvajā vārtejā.

3. Jebkurus persondatu aizsardzības pārkāpumus saistībā ar apstrādes darbību federatīvajā vārtejā kopīgie pārziņi saskaņā ar Regulas (ES) 2016/679 33. un 34. pantu vai pēc Komisijas paziņojuma paziņo Komisijai, kompetentajām uzraudzības iestādēm un vajadzības gadījumā datu subjektiem.

3. IEDAĻA

Novērtējums par ietekmi uz datu aizsardzību

Ja pārzinim, lai izpildītu Vispārīgās datu aizsardzības regulas 35. un 36. pantā norādītos pienākumus, vajadzīga informācija no cita pārziņa, tas sūta īpašu pieprasījumu uz 1. iedaļas 1. apakšiedaļas 3. punktā minēto funkcionālo pastkastīti. Minētais cits pārzinis dara visu iespējamo, lai šo informāciju sniegtu.

III PIELIKUMS

KOMISIJAS KĀ DATU APSTRĀDĀTĀJA PIENĀKUMI FEDERATĪVAJĀ VĀRTEJĀ, KURĀ NOTIEK PĀRROBEŽU DATU APSTRĀDE STARP NACIONĀLAJĀM KONTAKTU IZSEKOŠANAS UN BRĪDINĀŠANAS MOBILAJĀM LIETOTNĒM

Komisija:

1) izveido un nodrošina drošu un uzticamu sakaru infrastruktūru, kas savstarpēji savieno to dalībvalstu kontaktu izsekošanas un brīdināšanas mobilās lietotnes, kuras iesaistītas federatīvajā vārtejā. Lai izpildītu federatīvās vārtejas datu apstrādātāja pienākumus, Komisija drīkst piesaistīt trešās personas kā apakšapstrādātājus; Komisija informē kopīgos pārziņus par plānotajām izmaiņām attiecībā uz citu apakšapstrādāju piesaistīšanu vai aizvietošanu, līdz ar to dodot iespēju pārziņiem kopīgi iebilst pret šādām izmaiņām, kā norādīts II pielikuma 1. iedaļas 1. apakšiedaļas 4. punktā. Komisija nodrošina, lai šādiem apakšapstrādātājiem būtu tādi paši datu aizsardzības pienākumi, kādi izklāstīti šajā lēmumā;

2) persondatus apstrādā, tikai pamatojoties uz pārziņu dotiem dokumentētiem norādījumiem, ja vien tas nav prasīts Savienības vai dalībvalstu tiesību aktos; šādā gadījumā Komisija pirms datu apstrādes par attiecīgo juridisko prasību informē pārziņus, ja vien šādas informācijas iesniegšana ar attiecīgo tiesību aktu nav aizliegta, ievērojot svarīgas sabiedrības intereses;

3) apstrādes ietvaros Komisija:

a) autentificē valstu aizmugursistēmas serverus, pamatojoties uz valstu aizmugursistēmas serveru sertifikātiem;

b) saņem īstenošanas lēmuma 7.a panta 3. punktā minētos un valstu aizmugursistēmas serveru augšupielādētos datus, nodrošinot lietojumprogrammas saskarni, ar kuras palīdzību valstu aizmugursistēmas serveri attiecīgos datus var augšupielādēt;

c) datus glabā federatīvajā vārtejā, kad tie saņemti no valstu aizmugursistēmas serveriem;

d) dod iespēju datus lejupielādēt valstu aizmugursistēmas serveros;

e) datus dzēš, kad visi iesaistītie aizmugursistēmas serveri tos ir lejupielādējuši, vai 14 dienas pēc to saņemšanas, ja tas ir agrāk;

f) pēc pakalpojuma sniegšanas beigām dzēš visus atlikušos datus, ja vien Savienības vai dalībvalsts tiesību akti nepieprasa glabāt persondatus.

Apstrādātājs veic visus vajadzīgos pasākumus, lai saglabātu apstrādāto datu integritāti;

4) veic visus mūsdienīgos organizatoriskos, fiziskos un loģiskos drošības pasākumus, kādi vajadzīgi, lai uzturētu federatīvo vārteju. Šajā nolūkā Komisija:

a) nozīmē par federatīvās vārtejas drošību atbildīgo struktūru, paziņo pārziņiem tās kontaktinformāciju un nodrošina, lai tā būtu pieejama un reaģētu uz drošības draudiem;

b) uzņemas atbildību par federatīvās vārtejas drošību;

c) gādā, lai visiem cilvēkiem, kam ir dota piekļuve federatīvajai vārtejai, būtu jāievēro līgumisks, profesionāls vai ar likumu noteikts pienākums saglabāt konfidencialitāti;

5) veic visus vajadzīgos drošības pasākumus, lai nebūtu apdraudēta valstu aizmugursistēmas serveru raita darbība. Šajā nolūkā Komisija ievieš īpašas procedūras, kas saistītas ar aizmugursistēmas serveru pieslēgšanu federatīvajai vārtejai. Proti:

a) ievieš riska novērtēšanas procedūru, kurā nosaka un novērtē iespējamos sistēmas apdraudējumus;

b) ievieš revīzijas un pārbaudes procedūru, kurā:

i) pārbauda īstenoto drošības pasākumu atbilstību piemērojamajai drošības politikai;

ii) regulāri kontrolē sistēmas datņu integritāti, drošības parametrus un piešķirtos pilnvarojumus;

iii) novēro, lai atklātu drošības pārkāpumus un ielaušanos;

iv) ievieš izmaiņas, lai mazinātu pastāvošos drošības trūkumus;

v) dod iespēju, arī pēc pārziņu pieprasījuma, veikt neatkarīgas revīzijas, arī pārbaudes, un piedalīties tajās, un pārskatīt drošības pasākumus, ievērojot nosacījumus, kuros ir ņemts vērā LESD 7. protokols par privilēģijām un imunitāti Eiropas Savienībā ([2]);

([2]) 7. protokols par privilēģijām un imunitāti Eiropas Savienībā (OV C 326, 26.10.2012., 266. lpp.).

c) maina kontroles procedūru, lai dokumentētu un novērtētu izmaiņu ietekmi pirms to ieviešanas un pastāvīgi informētu pārziņus par jebkurām izmaiņām, kas var ietekmēt komunikāciju ar to infrastruktūrām un/vai šo infrastruktūru drošību;

d) nosaka apkopes un remonta procedūru, lai precizētu noteikumus un nosacījumus, kādi jāievēro, kad jāveic aprīkojuma apkope un/vai remonts;

e) nosaka drošības incidenta procedūru, lai noteiktu ziņošanas un eskalācijas shēmu, nekavējoties informētu pārziņus un Eiropas Datu aizsardzības uzraudzītāju par jebkuru persondatu aizsardzības pārkāpumu un noteiktu disciplinārlietu, kurā risina drošības pārkāpumus;

6) veic mūsdienīgus fiziskus un/vai loģiskus drošības pasākumus objektiem, kuros atrodas federatīvās vārtejas aprīkojums, un loģisko datu un drošības piekļuves kontrolei. Šajā nolūkā Komisija:

a) pastiprina fizisko drošību, lai izveidotu norobežotus drošības perimetrus un varētu atklāt pārkāpumus;

b) kontrolē piekļuvi objektiem un uztur apmeklētāju reģistru izsekošanas vajadzībām;

c) nodrošina, lai ārējus cilvēkus, kam dota piekļuve telpām, eskortētu pienācīgi pilnvarots personāls;

d) gādā, lai aprīkojumu nevarētu pievienot, nomainīt vai izņemt bez iepriekšējas nozīmēto atbildīgo struktūru atļaujas;

e) kontrolē valstu aizmugursistēmas serveru un federatīvās vārtejas savstarpējo piekļuvi;

f) nodrošina, lai cilvēki, kas piekļūst federatīvajai vārtejai, tiktu identificēti un autentificēti;

g) drošības pārkāpuma gadījumā, kas skar šo infrastruktūru, pārbauda tiesības piekļūt federatīvajai vārtejai;

h) saglabā caur federatīvo vārteju nosūtītās informācijas integritāti;

i) īsteno tehniskus un organizatoriskus drošības pasākumus, lai nepieļautu neatļautu piekļuvi persondatiem;

j) vajadzības gadījumā īsteno pasākumus, kas bloķē neatļautu piekļuvi federatīvajai vārtejai no valstu iestāžu domēna (t. i., bloķē vietas/IP adresi);

7) veic pasākumus, lai aizsargātu savu domēnu, arī sarauj sakarus, ja ir būtiska novirze no kvalitātes vai drošības principiem vai jēdzieniem;

8) uztur riska pārvaldības plānu, kas attiecas uz tās atbildības jomu;

9) reāllaikā pārrauga visu savu pakalpojumu komponentu veiktspēju federatīvajā vārtejā, regulāri sagatavo statistiku un kārto uzskaiti;

10) visu diennakti un cauru gadu pa tālruni, e-pastu vai tīmekļa portālā sniedz atbalstu angļu valodā attiecībā uz visiem federatīvās vārtejas pakalpojumiem un atbild, ja zvana apstiprināti zvanītāji: federatīvās vārtejas koordinatori un viņu attiecīgie palīdzības dienesti, projektu vadītāji un nozīmētas personas no Komisijas;

11) ar attiecīgiem tehniskiem un organizatoriskiem pasākumiem, cik vien iespējams, palīdz pārziņiem pildīt pārziņu pienākumu atbildēt uz pieprasījumiem, kuros datu subjekti vēlas izmantot tiesības, kas noteiktas Vispārīgās datu aizsardzības regulas III nodaļā;

12) atbalsta pārziņus, sniedzot informāciju par federatīvo vārteju, lai pildītu Vispārīgās datu aizsardzības regulas 32., 35. un 36. pantā noteiktos pienākumus;

13) gādā, lai federatīvajā vārtejā apstrādātie dati būtu nesaprotami personām, kam nav atļauts tiem piekļūt;

14) veic visus nepieciešamos pasākumus, lai nepieļautu, ka federatīvās vārtejas operatoriem būtu neatļauta piekļuve nosūtītajiem datiem;

15) veic pasākumus, lai atvieglotu sadarbspēju un saziņu starp nozīmētajiem federatīvās vārtejas pārziņiem;

16) Saskaņā ar Regulas (ES) 2018/1725 31. panta 2. punktu uztur pārziņu vārdā veikto apstrādes darbību reģistru.”