Pamatnostādnes 04/2020 par atrašanās vietas datu un kontaktu izsekošanas rīku izmantošanu saistībā ar Covid-19 uzliesmojumu

Pieņemtas 2020. gada 21. aprīlī

Translations proofread by EDPB Members.
This language version has not yet been proofread.

pieņemts

Versiju vēsture

Versija 1.1	2020. gada 5. maijs	Nelielas izmaiņas
Versija 1.0	2020. gada 21. aprīlis	Pamatnostādņu pieņemšana

Satura rādītājs

Eiropas Datu aizsardzības kolēģija,

ņemot vērā 70. panta 1. punkta e) apakšpunktu Eiropas Parlamenta un Padomes 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 (turpmāk tekstā — VDAR),

ņemot vērā EEZ līgumu un jo īpaši tā XI pielikumu un 37. protokolu, kas grozīts ar EEZ Apvienotās komitejas Lēmumu Nr. 154/2018 (2018. gada 6. jūlijs)[1],

ņemot vērā Parlamenta Reglamenta 12. pantu un 22. pantu,

IR PIEŅĒMUSI ŠĪS PAMATNOSTĀDNES.

1 IEVADS UN KONTEKSTS

1 Reaģējot uz Covid-19 pandēmiju, valdības un privātā sektora dalībnieki pievēršas uz datiem balstītu risinājumu izmantošanai, kas rada bažas par privātumu.

2 EDAK uzsver, ka datu aizsardzības tiesiskais regulējums tika izstrādāts tā, lai tas būtu elastīgs, un kā tāds tas spēj sasniegt abus mērķus: gan efektīvi reaģēt, ierobežojot pandēmiju, gan aizsargāt cilvēka pamattiesības un pamatbrīvības.

3 EDAK ir stingri pārliecināta, ka gadījumos, kad personas datu apstrāde ir nepieciešama Covid-19 pandēmijas pārvaldībai, datu aizsardzība ir neaizstājama, lai veidotu uzticēšanos, radītu apstākļus jebkura risinājuma sociālajai pieņemamībai un tādējādi garantētu šo pasākumu efektivitāti. Tā kā vīruss nepazīst robežas, reaģējot uz pašreizējo krīzi, būtu vēlams izstrādāt kopēju Eiropas pieeju vai vismaz izveidot sadarbspējīgu sistēmu.

4 EDAK kopumā uzskata, ka dati un tehnoloģijas, ko izmanto cīņā pret Covid-19, būtu jāizmanto, lai indivīdiem dotu iespējas, nevis lai tos kontrolētu, stigmatizētu vai apspiestu. Turklāt, lai gan dati un tehnoloģijas var būt svarīgi instrumenti, tiem ir raksturīgi ierobežojumi un tos var izmantot tikai, lai uzlabotu citu sabiedrības veselības pasākumu efektivitāti. Pasākumiem, kurus dalībvalstis vai ES iestādes pieņēmušas nolūkā cīnīties pret Covid-19 un kuri ietver personas datu apstrādi, ir jābūt balstītiem vispārējos efektivitātes, nepieciešamības un proporcionalitātes principos.

5 Šajās pamatnostādnēs ir precizēti nosacījumi un principi atrašanās vietas datu un kontaktu izsekošanas rīku samērīgai izmantošanai divos konkrētos nolūkos:

- atrašanās vietas datu izmantošana, kuras mērķis ir atbalstīt reaģēšanu uz pandēmiju, modelējot vīrusa izplatību, lai novērtētu ierobežošanas pasākumu vispārējo efektivitāti;
- kontaktu izsekošana, kuras mērķis ir informēt indivīdus par to, ka viņi ir atradušies tāda cilvēka tiešā tuvumā, kurš, iespējams, tiks apstiprināts kā vīrusa nēsātājs, lai pēc iespējas ātrāk pārtrauktu inficēšanās ķēdi.

6 Kontaktu izsekošanas lietotņu efektivitāte pandēmijas pārvaldīšanā ir atkarīga no daudziem faktoriem (piemēram, to cilvēku īpatsvara, kuriem vajadzētu to lejupielādēt; "kontakta" definīcijas attiecībā uz tuvumu un ilgumu). Turklāt šādām lietotnēm ir jābūt daļai no visaptverošas sabiedrības veselības stratēģijas pandēmijas apkarošanai, kas cita starpā ietver testēšanu un turpmāku manuālu kontaktu izsekošanu nolūkā kliedēt šaubas. To ieviešana būtu jāpapildina ar atbalsta pasākumiem, lai nodrošinātu lietotājiem sniegtās informācijas

1 Atsauces uz "dalībvalstīm" šajā dokumentā jāsaprot kā atsauces uz "EEZ dalībvalstīm".

kontekstualizāciju un to, ka brīdinājumi var būt noderīgi sabiedrības veselības sistēmai. Pretējā gadījumā šīs lietotnes, iespējams, nespēs sasniegt to mērķus pilnā mērā.

7 EDAK uzsver, ka VDAR un Direktīvā 2002/58/EK (turpmāk tekstā — Direktīva) ir ietverti īpaši noteikumi, kas ļauj izmantot anonīmus vai personas datus, lai valsts un ES līmeņa publiskajām iestādēm un citiem dalībniekiem palīdzētu uzraudzīt un ierobežot SARS-CoV-2 vīrusa izplatību[2].

8 Šajā saistībā EDAK jau ir pieņēmusi nostāju par to, ka kontaktu izsekošanas lietotņu izmantošanai vajadzētu būt brīvprātīgai un tai nevajadzētu balstīties uz indivīdu kustības izsekošanu, bet drīzāk uz informāciju par attālumu starp lietotājiem[3].

[2] Skatīt EDAK iepriekšējo paziņojumu par Covid-19 uzliesmojumu.
[3] [3] https://edpb.europa.eu/sites/edpb/files/files/file1/edpbletterecadvisecodiv-appguidance_final.pdf

2 ATRAŠANĀS VIETAS DATU IZMANTOŠANA

2.1 Atrašanās vietas datu avoti

9 Vīrusa izplatības un ierobežošanas pasākumu vispārējās efektivitātes modelēšanai ir pieejami divi galvenie atrašanās vietas datu avoti:

- atrašanās vietas dati, ko ievākuši elektronisko sakaru pakalpojumu sniedzēji (piemēram, mobilo telekomunikāciju operatori), sniedzot savus pakalpojumus; kā arī
- atrašanās vietas dati, ko ievāc informācijas sabiedrības pakalpojumu sniedzēju lietotnes, kuru funkcionalitāte prasa šādu datu izmantošanu (piemēram, navigācija, transporta pakalpojumi utt.).

10 EDAK atgādina, ka atrašanās vietas datus[4] , kas ievākti no elektronisko komunikāciju pakalpojumu sniedzējiem, var apstrādāt tikai saskaņā ar Direktīvas 6. un 9. pantu. Tas nozīmē, ka šos datus iestādēm vai citām trešām personām var nosūtīt tikai tad, ja pakalpojumu sniedzējs tos ir anonimizējis, vai – attiecībā uz datiem, kas norāda lietotāja galiekārtas ģeogrāfisko atrašanās vietu un kas nav informācija par datu plūsmu, – ar lietotāju iepriekšēju piekrišanu[5].

11 Attiecībā uz informāciju, tostarp atrašanās vietas datiem, kas iegūti tieši no gala iekārtām, piemēro Direktīvas 5. panta 3. punktu. Tādējādi informācijas glabāšana par lietotāja ierīci vai piekļuves iegūšana jau uzglabātajai informācijai ir atļauta tikai tad, ja i) lietotājs ir devis piekrišanu[6] vai ii) glabāšana un/vai piekļuve ir noteikti nepieciešama informācijas sabiedrības pakalpojumam, ko lietotājs skaidri pieprasījis.

12 Atkāpes no tiesībām un pienākumiem, kas paredzēti Direktīvā, tomēr ir iespējamas saskaņā ar 15. pantu, ja tās ir nepieciešams, atbilstīgs un samērīgs pasākums demokrātiskā sabiedrībā attiecībā uz konkrētiem mērķiem[7].

13 Attiecībā uz informācijas sabiedrības pakalpojumu sniedzēja ievākto atrašanās vietas datu atkalizmantošanu modelēšanas vajadzībām (piemēram, izmantojot operētājsistēmu vai kādu iepriekš uzstādītu lietotni) ir jāievēro papildu nosacījumi. Ja dati ir ievākti saskaņā ar Direktīvas 5. panta 3. punktu, tos var papildus apstrādāt tikai ar datu subjekta papildu piekrišanu vai pamatojoties uz Savienības vai dalībvalsts tiesību aktiem, kas demokrātiskā sabiedrībā ir nepieciešams un samērīgs pasākums, lai aizsargātu VDAR 23. panta 1. punktā minētos mērķus[8].

2.2 Uzsvars uz anonimizētu atrašanās vietas datu izmantošanu

14 EDAK uzsver, ka attiecībā uz atrašanās vietas datu izmantošanu priekšroka vienmēr būtu dodama anonimizētu datu, nevis personas datu apstrādei.

15 Anonimizācija attiecas uz metožu kopuma izmantošanu nolūkā novērst iespēju ar jebkāda veida "pamatotiem" centieniem sasaistīt datus ar identificētu vai identificējamu fizisku personu. Šajā "pamatotības pārbaudē" jāņem vērā gan objektīvie aspekti (laiks, tehniskie līdzekļi), gan kontekstuālie elementi, kas katrā gadījumā var atšķirties (parādības retums, ņemot vērā iedzīvotāju blīvumu, datu veidu un apjomu). Ja dati neiztur šo testu, tie nav anonimizēti un tādējādi uz tiem attiecas VDAR darbības joma.

---

[4] Skatīt Direktīvas 2. panta c) punktu.

[5] Skatīt Direktīvas 6. un 9. pantu.

[6] Direktīvā lietotais "piekrišanas" jēdziens ir tāds pats kā VDAR lietotais "piekrišanas" jēdziens, un tam jāatbilst visām piekrišanas prasībām, kas paredzētas VDAR 4. panta 11. punktā un 7. pantā.

[7] Direktīvas 15. panta interpretācijai sk. arī EST 2008. gada 29. janvāra spriedumu lietā C-275/06, *Productores de Música de España* (*Promusicae*) *v. Telefónica de España SAU*.

[8] Skatīt 1.5.3. iedaļu Pamatnostādnēs 1/2020 par personas datu apstrādi saistībā ar savienotiem transportlīdzekļiem.

16 Anonimizācijas noturīguma novērtēšanas pamatā ir trīs kritēriji: i) nošķiršana (atsevišķas personas izolēšana lielākā grupā, pamatojoties uz datiem); ii) sasaistāmība (divu ierakstu sasaistīšana par vienu un to pašu indivīdu); un iii) secināšana (ar ievērojamu varbūtību secināt nezināmu informāciju par personu).

17 Anonimizācijas jēdziens ir pārprotams un bieži tiek kļūdaini jaukts ar pseidonimizāciju. Anonimizētus datus var izmantot bez jebkādiem ierobežojumiem, bet uz pseidonimizētiem datiem joprojām attiecas VDAR darbības joma.

18 Pastāv daudzas iespējas efektīvi anonimizēt datus[9], bet jāņem vērā atruna. Datus pašus par sevi nevar padarīt anonīmus, anonimizēt var tikai datu kopas kopumā. Šajā ziņā jebkuru viena datu modeļa pārveidošanu (ar šifrēšanu vai jebkurām citām matemātiskām darbībām) labākajā gadījumā var uzskatīt par pseidonimizāciju.

19 Tiek veikta intensīva pētniecība par anonimizācijas procesiem un atkārtotas identifikācijas uzbrukumiem. Ir būtiski, lai ikviens pārzinis, kas īsteno anonimizācijas risinājumus, sekotu līdzi jaunākajām norisēm šajā jomā, jo īpaši attiecībā uz atrašanās vietas datiem (kuri iegūti no telesakaru operatoriem un/vai informācijas sabiedrības pakalpojumiem), par kuriem ir zināms, ka tos ir ļoti grūti anonimizēt.

20 Daudzi pētījumi liecina,[10] ka *atrašanās vietas dati, kas tiek uzskatīti par anonimizētiem*, patiesībā var tādi nebūt. Personu mobilitātes pēdas pēc savas būtības ir cieši saistītas un unikālas. Tāpēc noteiktos apstākļos tās var būt neaizsargātas pret atkārtotas identifikācijas mēģinājumiem.

21 Atsevišķu datu modeli, kas izseko personas atrašanās vietu ievērojamā laikposmā, nevar pilnībā anonimizēt. Šis novērtējums joprojām var būt patiess, ja reģistrēto ģeogrāfisko koordinātu precizitāte nav pietiekami mazināta vai ja informācija par pēdām ir dzēsta, un pat ja tiek saglabātas tikai tās atrašanās vietas, kurās datu subjekts uzturas ievērojamu laiku. Tas attiecas arī uz atrašanās vietas datiem, kuri nav pietiekami apkopoti.

22 Lai panāktu anonimizāciju un izturētu pamatotības pārbaudi, atrašanās vietas dati ir rūpīgi jāapstrādā. Šajā nozīmē šāda apstrāde ietver atrašanās vietas datu kopu izskatīšanu kopumā, kā arī pietiekami liela indivīdu kopuma datu apstrādi, izmantojot pieejamas stabilas anonimizācijas metodes, ar nosacījumu, ka tās tiek pienācīgi un efektīvi īstenotas.

23 Visbeidzot, ņemot vērā anonimizācijas procesu sarežģītību, ir ļoti vēlams nodrošināt anonimizācijas metodikas pārredzamību.

---

[9] (de Montjoye et al., 2018) "On the privacy-conscientious use of mobile phone data"
[10] (*de Montjoye et al.*, 2013) "Unique in the Crowd: The privacy bounds of human mobility" un (*Pyrgelis et al.*, 2017) "Knock Knock, Who's There? Membership Inference on Aggregate Location Data"

3 KONTAKTU IZSEKOŠANAS LIETOTNES

3.1 Vispārīga juridiskā analīze

24 Fizisku personu atrašanās vietas un/vai kontaktu sistemātiska un plaša mēroga uzraudzība ir nopietna iejaukšanās šo personu privātajā dzīvē. To var leģitimizēt tikai tad, ja lietotāji sniedz brīvprātīgu piekrišanu katram no attiecīgajiem mērķiem. Tas jo īpaši nozīmē, ka personas, kas nolemj neizmantot vai nevar izmantot šādas lietotnes, nesaskaras ar nelabvēlīgām sekām.

25 Lai nodrošinātu pārskatatbildību, būtu skaidri jānosaka ikvienas kontaktu izsekošanas lietotnes pārzinis. EDAK uzskata, ka šādas lietotnes pārziņi[11] varētu būt valstu veselības aizsardzības iestādes; var noteikt arī citus pārziņus. Jebkurā gadījumā, ja kontaktu izsekošanas lietotņu ieviešanā iesaistīti dažādi dalībnieki, to lomas un pienākumi ir skaidri jānosaka jau pašā sākumā un jāizskaidro lietotājiem.

26 Turklāt attiecībā uz mērķa ierobežojuma principu mērķiem jābūt pietiekami specifiskiem, lai izslēgtu turpmāku apstrādi nolūkos, kas nav saistīti ar Covid-19 veselības krīzes pārvaldību (piemēram, komerciālos vai tiesībaizsardzības nolūkos). Tiklīdz mērķis būs skaidri noteikts, būs jānodrošina, ka personas datu izmantošana ir atbilstīga, nepieciešama un samērīga.

27 Kontaktu izsekošanas lietotnes kontekstā būtu rūpīgi jāapsver datu minimizēšanas un integrētas datu aizsardzības un datu aizsardzības pēc noklusējuma princips:

- kontaktu izsekošanas lietotnēm nav nepieciešams sekot individuālu lietotāju atrašanās vietai. Tā vietā būtu jāizmanto dati par attālumu.
- Tā kā kontaktu izsekošanas lietotnes var darboties bez tiešas indivīdu identifikācijas, būtu jāievieš atbilstīgi pasākumi atkārtotas identifikācijas novēršanai;
- ievāktajai informācijai vajadzētu atrasties lietotāja gala iekārtā, un attiecīgā informācija būtu jāvāc tikai tad, kad tā ir absolūti nepieciešama.

28 Attiecībā uz apstrādes likumību EDAK norāda, ka kontaktu izsekošanas lietotnes paredz gala iekārtā jau uzglabātas informācijas glabāšanu un/vai piekļuvi tai, uz ko attiecas Direktīvas 5. panta 3. punkts. Ja minētās darbības ir absolūti nepieciešamas, lai lietotnes pakalpojuma sniedzējs varētu sniegt lietotāja nepārprotami pieprasīto pakalpojumu, viņa/viņas piekrišana apstrādei nebūtu vajadzīga. Attiecībā uz darbībām, kas nav absolūti nepieciešamas, pakalpojuma sniedzējam būtu jālūdz lietotāja piekrišana.

29 Turklāt EDAK norāda, ka tas vien, ka kontaktu meklēšanas lietotņu izmantošana notiek brīvprātīgi, nenozīmē, ka personas datu apstrāde noteikti būs balstīta uz piekrišanu. Ja valsts iestādes sniedz pakalpojumu, pamatojoties uz pilnvarojumu, kas piešķirts saskaņā ar tiesību aktos noteiktajām prasībām, visatbilstošākais datu apstrādes juridiskais pamats būtu nepieciešamība veikt uzdevumu sabiedrības interesēs, t. i., VDAR 6. panta 1. punkta e) apakšpunkts.

30 VDAR 6. panta 3. punktā ir precizēts, ka 6. panta 1. punkta e) apakšpunktā minētās apstrādes pamatu nosaka Savienības vai dalībvalstu tiesību akti, kas piemērojami pārzinim. Apstrādes nolūku nosaka minētajā juridiskajā pamatā vai – attiecībā uz 1. punkta e) apakšpunktā minēto apstrādi – tas ir vajadzīgs, lai izpildītu uzdevumu, ko veic sabiedrības interesēs vai īstenojot pārzinim likumīgi piešķirtās oficiālās pilnvaras.[12]

31 Tomēr juridiskajā pamatā vai likumdošanas pasākumā, kas nodrošina likumīgu pamatu kontaktu izsekošanas lietotņu izmantošanai, būtu jāiekļauj jēgpilni aizsardzības pasākumi, tostarp atsauce uz to, ka lietotnes izmantošana ir brīvprātīga. Būtu skaidri jānorāda personas datu turpmākas izmantošanas mērķis un skaidri ierobežojumi, kā arī skaidri jānorāda iesaistītais(-ie) pārzinis(-i). Būtu jānosaka arī datu kategorijas, kā arī kopas (un mērķi, ar

[11] Sk. arī Eiropas Komisijas Paziņojumu "Norādījumi par lietotnēm, kas sniedz atbalstu cīņā pret Covid-19 pandēmiju saistībā ar datu aizsardzību", Brisele, 16.4.2020., C (2020) 2523 *final*.
[12] Sk. 41. apsvērumu.

kuriem personas datus var izpaust). Atkarībā no iejaukšanās līmeņa būtu jāiekļauj papildu aizsardzības pasākumi, ņemot vērā apstrādes veidu, apjomu un nolūkus. Visbeidzot, EDAK arī iesaka, cik drīz vien iespējams, iekļaut kritērijus, lai noteiktu, kad lietotnes lietošana ir jāpārtrauc un kura struktūra ir atbildīga un atskaitās par šo lēmumu.

32 Tomēr, ja datu apstrādes pamatā ir cits juridiskais pamats, [13] piemēram, piekrišana (6. panta 1. punkta a) apakšpunkts), pārzinim būs jānodrošina, ka tiek izpildītas stingrās prasības, lai šāds juridiskais pamats būtu spēkā.

33 Turklāt lietotnes izmantošana Covid-19 pandēmijas apkarošanai varētu novest pie veselības datu vākšanas (piemēram, inficētas personas statuss). Šādu datu apstrāde ir atļauta, ja šāda apstrāde ir vajadzīga sabiedrības interešu dēļ sabiedrības veselības jomā, kas atbilst VDAR 9. panta 2. punkta i) apakšpunkta[14] nosacījumiem, vai veselības aprūpes nolūkos, kā aprakstīts VDAR 9. panta 2. punkta h) apakšpunktā[15]. Atkarībā no juridiskā pamata tās pamatā varētu būt arī nepārprotama piekrišana (VDAR 9. panta 2. punkta a) apakšpunkts).

34 Saskaņā ar sākotnējo mērķi VDAR 9. panta 2. punkta j) apakšpunkts ļauj apstrādāt arī veselības datus, ja tas nepieciešams zinātniskās pētniecības vai statistikas nolūkos.

35 Pašreizējo veselības krīzi nevajadzētu izmantot kā iespēju noteikt nesamērīgas datu glabāšanas pilnvaras. Glabāšanas ierobežojumos vajadzētu ņemt vērā patiesās vajadzības un medicīnisko nozīmīgumu (tas var ietvert epidemioloģiskus apsvērumus, piemēram, inkubācijas periodu utt.), un personas datus vajadzētu glabāt tikai Covid-19 krīzes laikā. Pēc tam visi personas dati būtu jādzēš vai jāanonimizē.

36 EDAK uzskata, ka šādas lietotnes nevar aizstāt, bet tikai atbalstīt manuālu kontaktu izsekošanu, ko veic kvalificēts valsts veselības aprūpes personāls, kurš var noskaidrot, vai tuvi kontakti var izraisīt vīrusa pārnešanu (piemēram, mijiedarbojoties ar personu, kas ir aizsargāta ar atbilstošu aprīkojumu – kasieriem utt.). EDAK uzsver, ka procedūrām un procesiem, tostarp attiecīgajiem algoritmiem, ko izmanto kontaktu izsekošanas lietotnes, vajadzētu darboties stingrā kvalificēta personāla uzraudzībā, lai ierobežotu kļūdaini pozitīvu un negatīvu rezultātu rašanos. Tikai automatizētu apstrādi nevajadzētu izmantot, lai sniegtu konsultācijas par turpmāk veicamiem pasākumiem.

37 Lai nodrošinātu to taisnīgumu, pārskatatbildību un – plašākā nozīmē – atbilstību tiesību aktiem, nepieciešams, lai algoritmi būtu revidējami, un neatkarīgiem ekspertiem tie būtu regulāri jāpārskata. Lietotnes pirmkods būtu jādara publiski pieejams pēc iespējas plašākai pārbaudei.

38 Vienmēr tiks konstatēts noteikts daudzums kļūdaini pozitīvu rezultātu. Tā kā inficēšanās riska identificēšana, iespējams, var lielā mērā ietekmēt indivīdus, piemēram, tiem paliekot pašizolācijā, kamēr testu rezultāti nav negatīvi, ir nepieciešama spēja vajadzības gadījumā labot datus un/vai turpmāko analīžu rezultātus. Tas, protams, būtu jāattiecina tikai uz tādiem scenārijiem un to īstenošanu, kuros dati tiek apstrādāti un/vai uzglabāti tādā veidā, ka šāda labošana ir tehniski iespējama, un gadījumos, kad ir iespējams, ka iestājas iepriekš minētā nelabvēlīgā ietekme.

39 Visbeidzot, EDAK uzskata, ka pirms šāda instrumenta ieviešanas ir jāveic novērtējums par ietekmi uz datu aizsardzību (NIDA), jo tiek uzskatīts, ka apstrāde, iespējams, rada augstu risku (veselības dati, paredzamā plaša mēroga pieņemšana, sistemātiska uzraudzība, jauna tehnoloģiskā risinājuma izmantošana)[16]. EDAK stingri iesaka publicēt NIDA.

---

[13] Pārziņiem (jo īpaši valsts iestādēm) jāpievērš īpaša uzmanība tam, ka piekrišana nebūtu jāuzskata par brīvi sniegtu, ja personai nav patiesas izvēles atteikt vai atsaukt savu piekrišanu bez nelabvēlīgām sekām.

[14] Apstrādei jābūt balstītai uz Savienības vai dalībvalsts tiesību aktiem, kuros paredzēti piemēroti un konkrēti pasākumi, kā aizsargāt datu subjekta tiesības un brīvības, jo īpaši profesionālo noslēpumu.

[15] Skatīt VDAR 9. panta 2. punkta h) apakšpunktu.

[16] Skatīt 29. panta darba grupas Pamatnostādnes (ko pieņēmusi EDAK) par datu aizsardzības ietekmes novērtējumu (NIDA) un par to, vai apstrāde "var radīt augstu risku" Regulas (EK) Nr. 2016/679 izpratnē.

3.2 Ieteikumi un funkcionālās prasības

40 Saskaņā ar datu minimizēšanas principu līdz ar citiem integrētās datu aizsardzības un datu aizsardzības pēc noklusējuma pasākumiem[17] apstrādātie dati būtu jāsamazina līdz striktam minimumam. Lietotnei nebūtu jāvāc nesaistīta vai nevajadzīga informācija, tostarp informācija par civilstāvokli, sakaru identifikatoriem, aprīkojuma sarakstu vienībām, ziņojumiem, zvanu sarakstiem, atrašanās vietas datiem, ierīču identifikatoriem utt.

41 Lietotņu pārraidītajos datos jāiekļauj tikai daži unikāli un pseidonimizēti identifikatori, ko ģenerējusi lietotne un kas ir tai specifiski. Šie identifikatori jāatjauno regulāri un tik bieži, cik vajadzīgs, lai ierobežotu vīrusa izplatību, un pietiekami, lai ierobežotu indivīdu identificēšanas un fiziskas izsekošanas risku.

42 Kontaktu izsekošanā var izmantot centralizētu vai decentralizētu pieeju[18]. Abas pieejas būtu jāuzskata par iespējamām ar nosacījumu, ka tiek īstenoti atbilstoši drošības pasākumi, jo katrai no tām ir savas priekšrocības un trūkumi. Tāpēc lietotņu izstrādes konceptuālajā posmā vienmēr būtu rūpīgi jāapsver abas pieejas, rūpīgi izvērtējot attiecīgo ietekmi uz datu aizsardzību/privātumu un iespējamo ietekmi uz personu tiesībām.

43 Ikvienam kontaktu izsekošanas sistēmā iesaistītajam serverim jāvāc tikai tādu lietotāju kontaktvēsture vai pseidonimizētie identifikatori, kuri veselības aizsardzības iestāžu veiktā atbilstīgā novērtējumā atzīti par inficētiem, un vākšanai jānotiek, pamatojoties uz lietotāju brīvprātīgu rīcību. Alternatīvā variantā serveris uzglabā inficēto lietotāju pseidonimizēto identifikatoru sarakstu vai viņu saskarsmes vēsturi tikai tik ilgi, lai informētu potenciāli inficētos lietotājus par viņu mijiedarbību, un serverim nevajadzētu mēģināt identificēt potenciāli inficētos lietotājus.

44 Ieviešot globālu kontaktu izsekošanas metodiku, kas ietver gan lietotnes, gan manuālu izsekošanu, dažos gadījumos var būt nepieciešama papildu informācijas apstrāde. Šajā kontekstā šai papildu informācijai būtu jāpaliek lietotāja gala iekārtā un tā būtu jāapstrādā tikai tad, kad tas ir absolūti nepieciešams un ar lietotāja iepriekšēju un konkrētu piekrišanu.

45 Jāievieš mūsdienīgas kriptogrāfijas metodes, lai nodrošinātu serveros un lietotnēs glabāto datu drošību, kā arī drošu apmaiņu starp lietotnēm un attālināto serveri. Starp lietotni un serveri jāveic arī savstarpēja autentifikācija.

46 Lai lietotnē ziņotu par lietotājiem, kuri inficēti ar SARS-CoV-2, jāsaņem pienācīga atļauja, piemēram, izmantojot vienreiz lietojamu kodu, kas piesaistīts inficētās personas pseidonimizētai identitātei un saistīts ar testēšanas iestādi vai veselības aprūpes speciālistu. Ja apstiprinājumu nevar iegūt drošā veidā, nebūtu jāveic tāda datu apstrāde, kurai vajadzīgs lietotāja statusa derīgums.

47 Lai mazinātu risku, ka indivīdi izmanto trešo personu lietotnes, pārzinim sadarbībā ar valsts iestādēm ir skaidri un nepārprotami jāinformē par saiti, no kuras var lejupielādēt oficiālo valsts kontaktu izsekošanas lietotni.

---

[17] Skatīt EDAK Pamatnostādnes 4/2019 par "Integrētas datu aizsardzības un datu aizsardzības pēc noklusējuma" 25. pantu.

[18] Decentralizētais risinājums kopumā vairāk atbilst minimizēšanas principam.

4 SECINĀJUMS

48 Pasaule saskaras ar ievērojamu sabiedrības veselības krīzi, kura prasa stingru atbildes reakciju un kuras ietekme pārsniegs šo ārkārtas situāciju. Automatizēta datu apstrāde un digitālās tehnoloģijas var būt svarīgi elementi cīņā pret Covid-19. Tomēr vajadzētu izvairīties no "sprūdrata efekta". Mūsu pienākums ir nodrošināt, lai ikviens pasākums, ko veic šajos ārkārtas apstākļos, būtu nepieciešams, ierobežots laikā, minimāls un tiktu periodiski un godīgi pārskatīts, kā arī zinātniski novērtēts.

49 EDAK uzsver, ka nevajadzētu izvēlēties starp efektīvu reakciju uz pašreizējo krīzi un mūsu pamattiesību aizsardzību: mēs varam sasniegt abus mērķus, turklāt datu aizsardzības principiem var būt ļoti liela nozīme cīņā pret vīrusu. Eiropas datu aizsardzības tiesību akti ļauj atbildīgi izmantot personas datus veselības pārvaldības nolūkos, vienlaikus nodrošinot, ka šajā procesā netiek grautas personas tiesības un brīvības.

Eiropas Datu aizsardzības kolēģijas vārdā

priekšsēdētāja

(Andrea Jelineka)

PIELIKUMS – KONTAKTU IZSEKOŠANAS LIETOTNES ANALĪZES PAMATNOSTĀDNES

0. Atruna

Šie norādījumi nav ne preskriptīvi, ne izsmeļoši, un to vienīgais mērķis ir sniegt vispārīgus norādījumus kontaktu izsekošanas lietotņu izstrādātājiem un īstenotājiem. Var izmantot citus risinājumus, nevis šeit aprakstītos, un tie var būt likumīgi, ja vien tie atbilst attiecīgajam tiesiskajam regulējumam (t. i., VDAR un Direktīvai).

Jāņem vērā arī, ka šīs pamatnostādnes ir vispārīgas. Līdz ar to šajā dokumentā ietvertie ieteikumi un pienākumi nav uzskatāmi par izsmeļošiem. Katrs gadījums jāizvērtē atsevišķi, un konkrētām lietotnēm var būt nepieciešami papildu pasākumi, kas nav iekļauti šajās pamatnostādnēs.

1. Kopsavilkums

Daudzās dalībvalstīs ieinteresētās personas apsver iespēju izmantot *kontaktu izsekošanas* lietotnes, lai palīdzētu iedzīvotājiem noskaidrot, vai viņiem ir bijusi saskarsme ar personu, kas inficēta ar SARS-CoV-2.

Nosacījumi, saskaņā ar kuriem šādas lietotnes efektīvi veicinātu pandēmijas pārvaldību, vēl nav noteikti. Šie nosacījumi būtu jānosaka pirms šādas lietotnes ieviešanas. Tomēr ir svarīgi sniegt pamatnostādnes, ar kurām izstrādes grupām iepriekš sniedz attiecīgo informāciju, lai jau agrīnā izstrādes posmā varētu garantēt personas datu aizsardzību.

Jāņem vērā, ka šīs pamatnostādnes ir vispārīgas. Līdz ar to šajā dokumentā ietvertie ieteikumi un pienākumi nav uzskatāmi par izsmeļošiem. Katrs gadījums jāizvērtē atsevišķi, un konkrētām lietotnēm var būt nepieciešami papildu pasākumi, kas nav iekļauti šajās pamatnostādnēs. Šo pamatnostādņu mērķis ir sniegt vispārīgus norādījumus kontaktu izsekošanas lietotņu izstrādātājiem un īstenotājiem.

Daži kritēriji varētu pārsniegt stingrās prasības, kas izriet no datu aizsardzības regulējuma. To mērķis ir nodrošināt visaugstāko pārredzamības līmeni, lai veicinātu šādu kontaktu izsekošanas lietotņu pieņemšanu sabiedrībā.

Šajā nolūkā kontaktu izsekošanas lietotņu izdevējiem būtu jāņem vērā turpmāk minētie kritēriji.

- Šādas lietotnes izmantošanai jābūt pilnīgi brīvprātīgai. Tā nedrīkst ierobežot piekļuvi tiesībām, ko garantē tiesību akti. Indivīdiem vienmēr jābūt pilnīgai kontrolei pār saviem datiem un jābūt iespējai brīvi izvēlēties izmantot šādu lietotni.
- Kontaktu izsekošanas lietotnes var radīt augstu risku fizisku personu tiesībām un brīvībām un ir vajadzīgs, lai pirms to ieviešanas tiktu veikts novērtējums par to ietekmi uz datu aizsardzību.
- Informāciju par attālumu starp lietotnes lietotājiem var iegūt, nenorādot to atrašanās vietu. Šāda veida lietotnei nav nepieciešama atrašanās vietas datu izmantošana un tādēļ tai nevajadzētu ietvert šādu datu vākšanu.
- Ja lietotājam diagnosticē SARS-CoV-2, jāinformē tikai tās personas, ar kurām lietotājs ir bijis ciešā saskarē epidemioloģiski atbilstīgajā kontaktu izsekošanas saglabāšanas periodā.

- Atkarībā no izvēlētās struktūras šāda veida lietotņu darbībai var būt nepieciešams izmantot centralizētu serveri. Šādā gadījumā un saskaņā ar datu minimizēšanas un integrētas datu aizsardzības principiem centralizētajā serverī apstrādātie dati būtu jāierobežo līdz minimumam.
    - Ja konstatē, ka lietotājs ir inficēts, informāciju par viņa iepriekšējiem ciešiem kontaktiem vai lietotāja lietotnē pārraidītajiem identifikatoriem var vākt tikai ar lietotāja piekrišanu. Ir jānosaka pārbaudes metode, kas ļauj noteikt, ka persona patiešām ir inficēta, neidentificējot lietotāju. Tehniski to varētu panākt, brīdinot kontaktpersonas tikai pēc veselības aprūpes speciālista iesaistīšanās, piemēram, izmantojot īpašu vienreiz lietojamu kodu.
    - Centrālajā serverī glabātajai informācijai nebūtu jāļauj pārzinim identificēt lietotājus, kuriem ir diagnosticēta inficēšanās vai kuri ir kontaktējušies ar šiem lietotājiem, kā arī tai nevajadzētu ļaut izsekot kontaktēšanās vēsturi, kas nav vajadzīga, lai noteiktu attiecīgos kontaktus.
- Lai šāda veida lietotne darbotos, ir jāpārraida dati, ko uztver citu lietotāju ierīces, un jāuztver šādas pārraides.
    - Pietiek ar pseidonimizētu identifikatoru apmaiņu starp lietotāju mobilajām iekārtām (datoriem, planšetdatoriem, savienotiem pulksteņiem utt.), piemēram, pārraidot tos (piemēram, izmantojot *Bluetooth Low Energy* tehnoloģiju).
    - Identifikatorus jāģenerē, izmantojot mūsdienīgus kriptogrāfijas procesus.
    - Identifikatori ir regulāri jāatjauno, lai samazinātu fiziskas izsekošanas un sasaistes uzbrukumu risku.
- Šāda veida lietotnei jābūt nodrošinātai, lai garantētu drošus tehniskos procesus. Proti,
    - lietotnei nevajadzētu nodot lietotājiem informāciju, kas tiem ļauj izsecināt citu personu identitāti vai diagnozi. Centrālais serveris neidentificē lietotājus un nesecina informāciju par tiem.

Atruna: iepriekšminētie principi ir saistīti tikai un vienīgi ar norādīto *kontaktu izsekošanas* lietotņu mērķi, t.i., tikai automātiski informēt cilvēkus, kuri var būt pakļauti vīrusa iedarbībai (neidentificējot tos). Lietotņu operatorus un to infrastruktūru var kontrolēt kompetentā uzraudzības iestāde. Šo pamatnostādņu pilnīga vai daļēja ievērošana ne vienmēr ir pietiekama, lai nodrošinātu pilnīgu atbilstību datu aizsardzības regulējumam.

2. Definīcijas

Kontakts	Kontaktu izsekošanas lietotnē kontakts ir lietotājs, kas ir iesaistījies mijiedarbībā ar lietotāju, kurš ir apstiprināts kā vīrusa nesējs, un mijiedarbības ilgums un attālums rada būtisku inficēšanās risku. Parametrus attiecībā uz saskarsmes ilgumu un attālumu starp cilvēkiem nosaka veselības aizsardzības iestādes, un tos var iestatīt lietotnē.

Atrašanās vietas dati	Attiecas uz visiem datiem, kas apstrādāti elektronisko komunikāciju tīklā vai ko apstrādā elektronisko komunikāciju pakalpojumā, norādot publiski pieejamu elektronisko komunikāciju pakalpojumu lietotāja gala iekārtas ģeogrāfisko atrašanās vietu (kā definēts Direktīvā), kā arī datiem no iespējamiem citiem avotiem, kas attiecas uz: • galiekārtas ģeogrāfisko platumu, garumu vai augstumu; • lietotāja pārvietošanās virzienu; vai • atrašanās vietas informācijas reģistrēšanas laiku.
Mijiedarbība	Kontaktu izsekošanas lietotnes kontekstā mijiedarbība ir informācijas apmaiņa starp divām ierīcēm, kas atrodas tuvu viena otrai (telpā un laikā) izmantotās komunikācijas tehnoloģijas (piemēram, *Bluetooth*) diapazonā. Šī definīcija neietver abu mijiedarbībā iesaistīto lietotāju atrašanās vietu.
Vīrusa nesējs	Šajā dokumentā tiek pieņemts, ka vīrusa nesēji ir lietotāji, kuru veikto vīrusa testu rezultāts ir pozitīvs un kuri ir saņēmuši oficiālu diagnozi no ārstiem vai veselības aprūpes centriem.
Kontaktu izsekošana	Personām, kas bijušas ciešā kontaktā (saskaņā ar epidemiologu noteiktajiem kritērijiem) ar indivīdu, kurš inficēts ar vīrusu, ir ievērojams risks inficēties un inficēt citas personas. Kontaktu izsekošana ir slimību kontroles metode, kas paredz uzskaitīt visus cilvēkus, kuri ir bijuši vīrusa nēsātāja tiešā tuvumā, lai pārbaudītu, vai viņi ir pakļauti infekcijas riskam, un veiktu atbilstošus sanitāros pasākumus attiecībā uz viņiem.

3. Vispārīgas prasības

GEN-1	Lietotni izmanto kā līdzekli, kas papildina tradicionālās kontaktu izsekošanas metodes (jo īpaši intervijas ar inficētajām personām), t. i., tai jābūt daļai no plašākas sabiedrības veselības programmas. To izmanto tikai līdz brīdim, kad jaunu infekciju daudzumu var pārvaldīt tikai ar manuālās kontaktu izsekošanas metodēm.
GEN-2	Ne vēlāk kā tad, kad kompetentās valsts iestādes nolemj "atjaunot normālu režīmu", ir jāizstrādā procedūra, kā apturēt identifikatoru vākšanu (lietotnes vispārēja deaktivizācija, norādījumi par lietotnes atiestatīšanu, automātiska atiestatīšana utt.) un aktivizēt visu savākto datu dzēšanu no visām datubāzēm (mobilajām lietotnēm un serveriem).
GEN-3	Lietotnes un tās rezerves pirmkodam jābūt atklātam, un tehniskajām specifikācijām jābūt publiski pieejamām, lai ikviena ieinteresētā persona varētu veikt koda revīziju un attiecīgā gadījumā palīdzēt uzlabot kodu, labot iespējamos trūkumus un nodrošināt pārredzamību personas datu apstrādē.

GEN-4	Nosakot lietotnes ieviešanu vairākos posmos, var pakāpeniski validēt tās efektivitāti no sabiedrības veselības viedokļa. Šim nolūkam iepriekš jānosaka novērtēšanas protokols, kurā norādīti rādītāji, kas ļauj izmērīt lietotnes efektivitāti.

4. Mērķi

PUR-1	Lietotnes vienīgais mērķis ir kontaktu izsekošana nolūkā brīdināt un rūpēties par cilvēkiem, kas potenciāli pakļauti SARS-CoV-2 iedarbībai. To nedrīkst izmantot citiem mērķiem.
PUR-2	Lietotni nedrīkst novirzīt no tās primārās izmantošanas mērķa, lai uzraudzītu atbilstību karantīnas vai ierobežošanas pasākumiem un/vai sociālās distancēšanās pasākumiem.
PUR-3	Lietotni nedrīkst izmantot ar mērķi secināt lietotāju atrašanās vietu, pamatojoties uz viņu mijiedarbību un/vai citiem līdzekļiem.

5. Funkcionāli apsvērumi

FUNC-1	Lietotnei jānodrošina funkcija, kas ļauj informēt lietotājus par to, ka viņi potenciāli ir bijuši pakļauti vīrusa iedarbībai, un šīs informācijas pamatā jābūt inficēta lietotāja attālumam X dienu intervālā pirms pozitīvā skrīninga testa (X vērtību nosaka veselības aizsardzības iestādes).
FUNC-2	Lietotnē jāsniedz ieteikumi lietotājiem, par kuriem konstatēts, ka tie potenciāli ir saskārušies ar vīrusu. Tai vajadzētu sniegt norādījumus par pasākumiem, kas tiem būtu jāveic, un jādod lietotājam iespēja prasīt padomus. Šādos gadījumos cilvēka iesaiste būtu obligāta.
FUNC-3	Algoritmam, ar ko mēra infekcijas risku, ņemot vērā attāluma un laika faktorus un tādējādi nosakot, kad kontakts jāreģistrē kontaktu izsekošanas sarakstā, jābūt droši regulējamam, lai ņemtu vērā jaunākās zināšanas par vīrusa izplatību.
FUNC-4	**Lietotāji jāinformē, ja viņi bijuši pakļauti vīrusa iedarbībai**, vai arī tiem regulāri jāsaņem informācija par to, vai viņi bijuši pakļauti vīrusa iedarbībai vīrusa inkubācijas periodā.
FUNC-5	Lietotnei vajadzētu būt sadarbspējīgai ar citām lietotnēm, kas izstrādātas citās dalībvalstīs, lai varētu efektīvi informēt lietotājus, kuri ceļo citās dalībvalstīs.

6. Dati

DATA-1	Lai varētu veikt kontaktu izsekošanu, lietotnei jāspēj pārraidīt un uztvert datus, izmantojot tuvinājuma sakaru tehnoloģijas, piemēram, *Bluetooth Low Energy*.
DATA-2	Šajos apraides datos jāiekļauj kriptogrāfiski spēcīgi lietotnes ģenerēti un tai specifiski nejauši izvēlēti pseidonimizēti identifikatori.
DATA-3	Nejauši izvēlētu pseidonimizētu identifikatoru pārklāšanās riskam vajadzētu būt pietiekami zemam.
DATA-4	Nejauši izvēlētie pseidonimizētie identifikatori ir regulāri jāatjauno tik bieži, lai pietiekami ierobežotu risku, ka centrālo serveru operatori, citi lietotnes lietotāji vai ļaunprātīgas trešās personas varētu atkārtoti identificēt, fiziski izsekot vai sasaistīt personas. Šie identifikatori jāģenerē lietotāja lietotnē, iespējams, izmantojot centrālā servera sniegtu sagatavi.
DATA-5	Saskaņā ar datu minimizēšanas principu lietotne nedrīkst vākt citus datus kā tikai tos, kas ir noteikti nepieciešami kontaktu izsekošanai.
DATA-6	Lietotne nedrīkst vākt atrašanās vietas datus kontaktu izsekošanas vajadzībām. Atrašanās vietas datus var apstrādāt tikai ar mērķi ļaut lietotnei mijiedarboties ar līdzīgām lietotnēm citās valstīs, un šāda apstrāde būtu stingri jāierobežo tikai līdz šim mērķim absolūti nepieciešamai.
DATA-7	Lietotnei nevajadzētu vākt veselības datus papildus tiem, kas noteikti nepieciešami lietotnes vajadzībām, izņemot fakultatīvi un tikai ar mērķi palīdzēt pieņemt lēmumu par lietotāja informēšanu.
DATA-8	Lietotāji ir jāinformē par visiem personas datiem, kas tiks vākti. Šie dati būtu jāvāc tikai ar lietotāja atļauju.

7. Tehniskās īpašības

TECH-1	Lietotnē vajadzētu izmantot pieejamas tehnoloģijas, piemēram, tuvinājuma komunikācijas tehnoloģiju (piemēram, *Bluetooth Low Energy*), lai atklātu lietotājus tās ierīces tuvumā, kurā tiek izmantota šī lietotne.
TECH-2	Lietotnei noteiktu ierobežotu laikposmu ierīcē jāglabā lietotāja kontaktu vēsture.
TECH-3	Dažu lietotnes funkciju īstenošanā var izmantot centrālo serveri.
TECH-4	Lietotnei jābūt izstrādātai tā, lai tā pēc iespējas vairāk balstītos uz lietotāju ierīcēm.
TECH-5	Pēc to lietotāju iniciatīvas, par kuriem ir ziņots, ka viņi ir inficēti ar vīrusu, un pēc tam, kad atbilstoši sertificēts veselības aprūpes speciālists ir apstiprinājis šo statusu, viņu kontaktvēsture vai viņu pašu identifikatori būtu jānosūta uz centrālo serveri.

8. Drošība

SEC-1	Ir vajadzīgs mehānisms, kas pārbauda to lietotāju statusu, kuri lietotnē ir reģistrēti kā SARS-CoV-2 pozitīvi, piemēram, nodrošinot vienreiz lietojamu kodu, kas saistīts ar testēšanas iestādi vai veselības aprūpes speciālistu. Ja apstiprinājumu nevar iegūt drošā veidā, datus nedrīkst apstrādāt.
SEC-2	Uz centrālo serveri nosūtītie dati jāpārraida, izmantojot drošu kanālu. OS platformas pakalpojumu sniedzēju sniegto paziņošanas pakalpojumu izmantošana būtu rūpīgi jāizvērtē, un tās rezultātā nekādus datus nedrīkst izpaust trešām personām.
SEC-3	Pieprasījumus nedrīkst ietekmēt ļaunprātīgu lietotāju veiktas ļaunprātīgas manipulācijas.
SEC-4	Ir jāievieš mūsdienīgas kriptogrāfijas tehnikas, lai garantētu drošu apmaiņu starp lietotni un serveri, kā arī starp lietotnēm un lai aizsargātu lietotnēs un serverī glabāto informāciju. Tehniskie paņēmieni, ko var izmantot, ir, piemēram, šādi: simetriska un asimetriska šifrēšana, jaucējfunkcijas, privātas piederības tests, privātas kopas krustpunkts, Blūma filtri, privātas informācijas izguve, homomorfa šifrēšana utt.
SEC-5	Centrālais serveris nedrīkst glabāt lietotāju tīkla savienojuma identifikatorus (piemēram, IP adreses), tostarp tādu lietotāju, kuri ir saņēmuši pozitīvu diagnozi un pārsūtījuši savu kontaktu vēsturi vai savus identifikatorus.
SEC-6	Lai izvairītos no izlikšanās par citu personu vai viltus lietotāju radīšanas, serverim ir jāapliecina lietotnes autentiskums.
SEC-7	Lietotnei ir jāapliecina centrālā servera autentiskums.
SEC-8	Servera funkcijas būtu jāaizsargā pret atkārtošanas uzbrukumiem.
SEC-9	Lai autentificētu centrālā servera pārraidītās informācijas izcelsmi un integritāti, tai jābūt parakstītai.
SEC-10	Piekļuve visiem datiem, kas glabājas centrālajā serverī un nav publiski pieejami, ir jāatļauj tikai pilnvarotām personām.
SEC-11	Ierīces atļaujas pārvaldītājam operētājsistēmas līmenī jāpieprasa tikai atļaujas, kas vajadzīgas, lai piekļūtu komunikācijas moduļiem un vajadzības gadījumā tos izmantotu, uzglabātu datus gala iekārtā un apmainītos ar informāciju ar centrālo serveri.

9. Fizisku personu personas datu un privātās dzīves aizsardzība

Atgādinājums: šīs pamatnostādnes attiecas uz lietotni, kuras vienīgais mērķis ir kontaktu izsekošana.

PRIV-1	Datu apmaiņā jāievēro lietotāju privātums (un jo īpaši datu minimizēšanas princips).
PRIV-2	Lietotne nedrīkst ļaut tieši identificēt lietotājus, kad tie izmanto lietotni.
PRIV-3	Lietotne nedrīkst ļaut izsekot lietotāju kustībai.
PRIV-4	Izmantojot lietotni, lietotāji nedrīkstētu iegūt informāciju par citiem lietotājiem (un jo īpaši par to, vai viņi ir vīrusa nēsātāji).
PRIV-5	Uzticībai centrālajam serverim jābūt ierobežotai. Centrālā servera pārvaldībā jāievēro skaidri definēti pārvaldības noteikumi un jāīsteno visi pasākumi, kas vajadzīgi, lai garantētu tā drošību. Centrālajam serverim vajadzētu atrasties vietā, kas ļauj kompetentajai uzraudzības iestādei veikt efektīvu uzraudzību.
PRIV-6	Ir jāveic un jāpublisko datu aizsardzības ietekmes novērtējums.
PRIV-7	Lietotnei būtu tikai jāatklāj lietotājam, vai viņš ir bijis pakļauts vīrusa iedarbībai, un, ja iespējams, neatklājot informāciju par citiem lietotājiem, mijiedarbības reižu skaitu un to datumiem.
PRIV-8	Lietotnē sniegtā informācija nedrīkst ļaut lietotājiem identificēt lietotājus, kuri ir vīrusa nēsātāji, vai viņu pārvietošanos.
PRIV-9	Lietotnē sniegtā informācija nedrīkst ļaut veselības aizsardzības iestādēm identificēt vīrusam, iespējams, pakļautos lietotājus bez viņu piekrišanas.
PRIV-10	Pieprasījumi, ko lietotne iesniedz centrālajam serverim, nedrīkst saturēt nekādu informāciju par vīrusa nesēju.
PRIV-11	Pieprasījumi, ko lietotne iesniedz centrālajam serverim, nedrīkst atklāt nevajadzīgu informāciju par lietotāju, izņemot tikai tad, ja tas ir nepieciešams, par tās pseidonimizētajiem identifikatoriem un kontaktu sarakstu.
PRIV-12	Nedrīkst pieļaut sasaistes uzbrukumus.
PRIV-13	Lietotājiem ir jābūt iespējai izmantot savas tiesības ar lietotnes starpniecību.
PRIV-14	Lietotnes dzēšanas rezultātā ir jādzēš visi vietēji savāktie dati.
PRIV-15	Lietotnē būtu jāapkopo tikai dati, ko nosūtījusi lietotne vai sadarbspējīgas līdzvērtīgas lietotnes. Nevāc datus, kas attiecas uz citām lietotnēm un/vai tuvinājuma komunikācijas ierīcēm.
PRIV-16	Lai novērstu centrālā servera veiktu atkārtotu identifikāciju, būtu jāievieš starpniekserveri. Šo *nesadarbīgo serveru* mērķis ir sajaukt vairāku lietotāju identifikatorus (gan vīrusa nesēju, gan pieprasītāju nosūtītos) pirms to paziņošanas centrālajam serverim, lai centrālajam serverim nebūtu zināmi lietotāju identifikatori (piemēram, IP adreses).

PRIV-17	Lietotne un serveris ir rūpīgi jāizstrādā un jākonfigurē, lai novērstu nevajadzīgu datu vākšanu (piemēram, serveru žurnālos nebūtu jāiekļauj identifikatori utt.) un lai izvairītos no tā, ka kāda trešā persona, kas nodarbojas ar programmatūras izstrādi, vāc datus citiem mērķiem.

Vairumā kontaktu izsekošanas lietotņu, kas pašlaik tiek apspriestas, pamatā tiek izmantotas divas pieejas gadījumiem, kad lietotājs tiek atzīts par inficētu: tās var vai nu nosūtīt uz serveri to tuvo kontaktu vēsturi, kurus tās ir ieguvušas skenējot, vai arī nosūtīt pašas savu pārraidīto identifikatoru sarakstu. Saskaņā ar šīm divām pieejām tiek piemēroti turpmāk minētie principi._Lai gan šajās pamatnostādnēs tiek apspriestas minētās pieejas, tas nenozīmē, ka citas pieejas nav iespējamas vai pat vēlamas, piemēram, pieejas, ar kurām īsteno kādu E2E šifrēšanas veidu vai izmanto citas drošību vai privātumu uzlabojošas tehnoloģijas.

9.1. Principi, ko piemēro tikai **tad, ja lietotne nosūta serverim kontaktpersonu sarakstu**:

CON-1	Centrālais serveris apkopo to lietotāju kontaktvēsturi, par kuriem ziņots kā par SARS-CoV-2 pozitīviem, un apkpošana notiek, pamatojoties uz minēto lietotāju brīvprātīgu rīcību.
CON-2	Centrālais serveris nedrīkst uzturēt un izplatīt to lietotāju pseidonīmidentifikatoru sarakstu, kuri pārnēsā vīrusu.
CON-3	Centrālajā serverī saglabāto kontaktu vēsturi dzēš, tiklīdz lietotājiem ir paziņots par to, ka viņi ir atradušies pozitīvi diagnosticētu personu tuvumā.
CON-4	Izņemot gadījumus, kad lietotājs, kura vīrusa testa rezultāts ir pozitīvs, paziņo savu kontaktu vēsturi centrālajam serverim vai kad lietotājs pieprasa serverim noskaidrot savu potenciālo saskarsmi ar vīrusu, nekādi dati nedrīkst atstāt lietotāja iekārtu.
CON-5	Visus vietējās vēstures identifikatorus dzēš pēc X dienām pēc to savākšanas (X vērtību nosaka veselības aprūpes iestādes).
CON-6	Kontaktvēstures, ko iesnieguši atsevišķi lietotāji, papildus neapstrādā, piemēram, tās savstarpēji saistot nolūkā izveidot pasaules mēroga attāluma kartes.
CON-7	Serveru žurnāli satur pēc iespējas mazāk datu, un tiem atbilst datu aizsardzības prasībām.

9.2. Principi, ko piemēro tikai tad, ja lietotne nosūta serverim savu identifikatoru sarakstu

ID-1	Centrālais serveris apkopo identifikatorus, ko pārraida tādu lietotāju lietotnes, par kuriem ziņots kā par SARS-CoV-2 pozitīviem, un apkopošana notiek, pamatojoties uz minēto lietotāju brīvprātīgu rīcību.
ID-2	Centrālais serveris nesaglabā un neizplata to lietotāju kontaktvēsturi, kuri pārnēsā vīrusu.

ID-3	Centrālajā serverī saglabātos identifikatorus dzēš, tiklīdz tie ir izplatīti citām lietotnēm.
ID-4	Izņemot gadījumus, kad lietotājs, kura vīrusa testa rezultāts ir pozitīvs, dalās ar saviem identifikatoriem ar centrālo serveri vai kad lietotājs pieprasa serverim noskaidrot savu potenciālo saskarsmi ar vīrusu, nekādi dati nedrīkst atstāt lietotāja iekārtu.
ID-5	Serveru žurnāli satur pēc iespējas mazāk datu, un tiem atbilst datu aizsardzības prasībām.