Gairės

Gairės Nr. 04/2020 dėl buvimo vietos duomenų ir sąlytį turėjusių asmenų išaiškinimo priemonių naudojimo COVID-19 protrūkio aplinkybėmis

Priimta 2020 m. balandžio 21 d.

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

priimta

Informacija apie versijas

1.1 versija	2020 m. gegužės 5 d.	Nedideli pataisymai
1.0 versija	2020 m. balandžio 21 d.	Gairių priėmimas

Turinys

Europos duomenų apsaugos valdyba,

atsižvelgdama į 2016 m. balandžio 27 d. Europos Parlamento ir Tarybos reglamento (ES) 2016/679 dėl fizinių asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo ir kuriuo panaikinama Direktyva 95/46/EB (toliau – BDAR) 70 straipsnio 1 dalies e punktą,

atsižvelgdama į Europos ekonominės erdvės (EEE) susitarimą, ypač į jo XI priedą ir 37 protokolą, su pakeitimais, padarytais 2018 m. liepos 6 d. EEE jungtinio komiteto sprendimu Nr. 154/2018[1],

atsižvelgdama į savo Darbo taisyklių 12 ir 22 straipsnius,

PRIĖMĖ ŠIAS GAIRES:

1 ĮVADAS IR BENDROSIOS APLINKYBĖS

1 Reaguodamos į COVID-19 pandemiją, vyriausybės ir privačiojo sektoriaus subjektai vis dažniau naudoja duomenimis grindžiamus technologinius sprendimus, dėl to iškyla daug susirūpinimą dėl privatumo keliančių klausimų.

2 Europos duomenų apsaugos valdyba (EDAV) atkreipia dėmesį į tai, kad duomenų apsaugos teisinė sistema buvo sukurta taip, kad ją būtų galima pritaikyti pagal poreikį ir todėl ja naudojantis būtų galima tiek užtikrinti veiksmingą atsaką siekiant apriboti pandemijos plitimą, tiek apsaugoti pagrindines žmogaus teises ir laisves.

3 EDAV tvirtai laikosi nuomonės, kad tais atvejais, kai, siekiant suvaldyti COVID-19 pandemiją, reikia tvarkyti asmens duomenis, duomenų apsauga yra būtina siekiant užsitikrinti žmonių pasitikėjimą, taip pat siekiant sukurti sąlygas, kad bet koks technologinis sprendimas būtų socialiai priimtinas, ir taip užtikrinti šių priemonių veiksmingumą. Kadangi virusas nepaiso sienų, reaguojant į dabartinę krizę veikiausiai būtų geriau plėtoti bendrą Europos požiūrį arba bent įdiegti sąveikią sistemą.

4 EDAV bendra pozicija yra tokia, kad duomenys ir technologijos, kurie naudojami siekiant veiksmingiau kovoti su COVID-19, turėtų būti naudojami žmonėms įgalinti, o ne juos kontroliuoti, stigmatizuoti ar valdyti. Be to, nors duomenys ir technologijos gali būti svarbios priemonės, jie turi tam tikrų esminių trūkumų ir vargu ar savo veiksmingumu būtų pranašesni už kitas visuomenės sveikatos priemones. Visos valstybių narių ar ES institucijų priimamos priemonės, susijusios su asmens duomenų tvarkymu kovojant su COVID-19, turi būti pagrįstos bendraisiais veiksmingumo, būtinumo ir proporcingumo principais.

5 Šiose gairėse paaiškinamos buvimo vietos duomenų ir sąlytį turėjusių asmenų išaiškinimo priemonių proporcingo naudojimo sąlygos ir principai, kai jie naudojami dviem konkrečiais tikslais:

- kai buvimo vietos duomenys naudojami siekiant užtikrinti veiksmingesnį atsaką į pandemiją, modeliuojant viruso plitimą, kad būtų galima įvertinti bendrą izoliavimo priemonių veiksmingumą;
- kai siekiama išaiškinti sąlytį turėjusius asmenis, kad juos būtų galima informuoti apie tai, kad jie buvo labai arti asmens, kuris galiausiai buvo patvirtintas kaip viruso nešiotojas, siekiant kuo anksčiau nutraukti užsikrėtimo grandines.

1 Šiame dokumente minimos valstybės narės – tai EEE valstybės narės.

6 Sąlytį turėjusių asmenų išaiškinimo programėlių naudojimo efektyvumas siekiant suvaldyti pandemiją priklauso nuo daugelio veiksnių (pvz., žmonių, kuriems reikėtų ją įsidiegti, procentinės dalies; sąvokos „sąlytį turėjęs asmuo“ apibrėžtyje nustatyto sąlyčio artumo ir trukmės). Be to, tokias programėles reikia naudoti įgyvendinant visapusišką kovos su pandemija visuomenės sveikatos strategiją, kuri, be kita ko, apimtų tyrimus ir tolesnį mechaninį sąlytį turėjusių asmenų išaiškinimą siekiant pašalinti dvejones. Jos turėtų būti diegiamos kartu naudojant pagalbines priemones, siekiant užtikrinti, kad naudotojams informacija būtų teikiama kartu su tam tikru kontekstu ir kad perspėjimai būtų naudingi visuomenės sveikatos sistemai. Priešingu atveju gali nepavykti išnaudoti viso šių programėlių potencialo.

7 EDAV pabrėžia, kad tiek BDAR, tiek Direktyvoje 2002/58/EB (toliau – Direktyva) nustatytos konkrečios taisyklės, pagal kurias anoniminius arba asmens duomenis leidžiama naudoti, siekiant nacionaliniu ir ES lygmenimis padėti valdžios institucijoms ir kitiems subjektams vykdyti SARS-CoV-2 plitimo stebėseną ir jį suvaldyti[2].

8 Šiuo klausimu EDAV jau išreiškė poziciją, kad sąlytį turėjusių asmenų išaiškinimo programėlės turėtų būti naudojamos savanoriškai ir jų naudojimas turėtų būti grindžiamas ne atskirų asmenų judėjimo atsekimu, o su naudotojais susijusia artumo informacija[3].

[2] Žr. ankstesnį EDAV pranešimą dėl COVID-19 protrūkio.
[3] [3] https://edpb.europa.eu/sites/edpb/files/files/file1/edpbletterecadvisecodiv-appguidance_final.pdf

2 BUVIMO VIETOS DUOMENŲ NAUDOJIMAS

2.1 Buvimo vietos duomenų šaltiniai

9 Yra du pagrindiniai buvimo vietos duomenų šaltiniai, kuriais galima pasinaudoti modeliuojant viruso plitimą ir bendrą izoliavimo priemonių veiksmingumą:

- buvimo vietos duomenys, kuriuos elektroninių ryšių paslaugų teikėjai (pvz., mobiliųjų telekomunikacijų operatoriai) renka teikdami savo paslaugas, ir
- buvimo vietos duomenys, kurie renkami informacinės visuomenės paslaugų teikėjų programėlėmis, kurių funkcijoms (pvz., navigacijai, susisiekimo paslaugoms ir pan.) būtinas tokių duomenų naudojimas.

10 EDAV primena, kad iš elektroninių ryšių paslaugų teikėjų surinktus buvimo vietos duomenis[4] galima tvarkyti tik laikantis Direktyvos 6 ir 9 straipsnių. Tai reiškia, kad valdžios institucijoms arba kitoms trečiosioms šalims šiuos duomenis galima perduoti tik paslaugų teikėjui juos anoniminus arba, jeigu tai yra duomenys, iš kurių matoma naudotojo galinio įrenginio geografinė padėtis, bet kurie nėra srauto duomenys – gavus išankstinį naudotojų sutikimą[5].

11 Dėl tiesiogiai iš galinio įrenginio gaunamos informacijos, įskaitant buvimo vietos duomenis, taikoma Direktyvos 5 straipsnio 3 dalis. Taigi, saugoti informaciją naudotojo įrenginyje arba pasinaudoti galimybe susipažinti su jau saugoma informacija galima tik, jeigu i) naudotojas davė sutikimą[6] arba ii) informacijos saugojimas ir (arba) galimybė susipažinti su ja yra visiškai būtina naudotojo aiškiai prašomai informacinės visuomenės paslaugai teikti.

12 Vis dėlto, vadovaujantis 15 straipsniu, galimi nukrypimai nuo Direktyvoje numatytų teisių ir pareigų, kai tuo naudojamasi kaip būtina, tinkama ir proporcinga priemone, siekiant tam tikrų tikslų demokratinėje visuomenėje[7].

13 Kalbant apie informacinės visuomenės paslaugų teikėjo renkamų buvimo vietos duomenų pakartotinį naudojimą modeliavimo tikslais (pvz., naudojant operacinę sistemą arba kokią nors anksčiau įdiegtą programėlę), pažymėtina, kad turi būti įvykdytos papildomos sąlygos. Iš tiesų, jeigu duomenys surinkti laikantis Direktyvos 5 straipsnio 3 dalies, jie gali būti toliau tvarkomi tik gavus papildomą duomenų subjekto sutikimą arba remiantis Sąjungos arba valstybės narės teise, kai tuo naudojamasi kaip būtina ir proporcinga priemone demokratinėje visuomenėje, siekiant BDAR 23 straipsnio 1 dalyje nurodytų tikslų[8].

2.2 Pirmenybė anonimintų buvimo vietos duomenų naudojimui

14 EDAV atkreipia dėmesį į tai, kad, kalbant apie buvimo vietos duomenų naudojimą, visais atvejais pirmenybę reikėtų teikti anonimintų, o ne asmens duomenų tvarkymui.

15 Anoniminimas – tai tam tikrų metodų rinkinio naudojimas, siekiant panaikinti galimybę nesunkiai susieti duomenis su fiziniu asmeniu, kurio tapatybė žinoma arba gali būti nustatyta. Vertinant šį „nesunkaus susiejimo“ kriterijų, turi būti atsižvelgta tiek į objektyvius aspektus (laiką, technines priemones), tiek į kontekstinius elementus, kurie kiekvienu atveju gali skirtis (reiškinio retumą, atsižvelgiant, pvz., į gyventojų tankį, duomenų pobūdį ir kiekį). Jeigu duomenys neatitinka šio kriterijaus, tai reiškia, kad jie neanoniminti, todėl jiems vis tiek taikomas BDAR.

---

[4] Žr. Direktyvos 2 straipsnio c punktą.
[5] Žr. Direktyvos 6 ir 9 straipsnius.
[6] Direktyvoje apibrėžta sutikimo sąvoka atitinka BDAR apibrėžtą sutikimo sąvoką ir turi tenkinti visus BDAR 4 straipsnio 11 dalyje ir 7 straipsnyje nustatytus sutikimo reikalavimus.
[7] Direktyvos 15 straipsnio aiškinimą taip pat rasite 2008 m. sausio 29 d. Europos Sąjungos Teisingumo Teismo (ESTT) sprendime byloje C-275/06 *Productores de Música de España (Promusicae)* prieš *Telefónica de España SAU*.
[8] Žr. Gairių Nr. 1/2020 dėl asmens duomenų tvarkymo, susijusio su susietųjų transporto priemonių naudojimu, 1.5.3 skyrių.

16 Anoniminimo patikimumas vertinamas remiantis trimis kriterijais: i) pagal galimybę išskirti asmenį (remiantis duomenimis, atskirti asmenį didesnėje grupėje), ii) pagal galimybę susieti (susieti du su tuo pačiu asmeniu susijusius įrašus) ir iii) pagal galimybę suprasti (dedukcijos būdu ganėtinai tiksliai nustatyti nežinomą informaciją apie asmenį).

17 Anoniminimo sąvoka dažnai neteisingai suprantama ir neretai painiojama su pseudoniminimu. Nors anoniminimas suteikia galimybę naudoti duomenis be jokių apribojimų, pseudoniminiams duomenims vis tiek taikomas BDAR.

18 Yra daug būdų veiksmingai anoniminti duomenis[9], bet yra ir tam tikrų kliūčių. Duomenų negalima anoniminti atskirai, t. y. galima (arba negalima) anoniminti tik visą duomenų rinkinį. Šiuo požiūriu bet kokią su vienu duomeniu susijusią intervenciją (jo kodavimą arba kitokią matematinę transformaciją) geriausiu atveju galima laikyti pseudoniminimu.

19 Anoniminimo procesai ir mėginimai išanoniminti duomenis yra mokslininkų aktyviai tyrinėjamos sritys. Itin svarbu, kad bet kuris anoniminimo technologinius sprendimus diegiantis duomenų valdytojas stebėtų šioje srityje vykstančius pokyčius, ypač susijusius su buvimo vietos duomenimis (gaunamus iš telekomunikacijų operatorių ir (arba) informacinės visuomenės paslaugų teikėjų), kuriuos, kaip žinia, labai sunku anoniminti.

20 Iš tiesų, buvo atlikta nemažai mokslinių tyrimų, kurie atskleidė[10], kad *buvimo vietos duomenys, kurie laikyti anonimintais,* iš tikrųjų gali būti neanoniminti. Asmenų judumo pėdsakai yra savaime labai susiję ir unikalūs. Todėl tam tikromis aplinkybėmis, mėginant išanoniminti duomenis, šie asmenys gali būti pažeidžiami.

21 Vieno duomenų modelio, ilgą laiką naudojamo asmens buvimo vietai nustatyti, neįmanoma visiškai anoniminti. Toks vertinimas gali būti tikslus, jeigu registruojamų geografinių koordinačių tikslumas nepakankamai sumažinamas arba jeigu išsamūs kelio duomenys pašalinami, išsaugant duomenis tik apie vietų, kuriose duomenų subjektas būna ilgą laiką, buvimo vietą. Tai taip pat taikytina netinkamai agreguojamiems buvimo vietos duomenims.

22 Siekiant užtikrinti anonimiškumą, buvimo vietos duomenys turi būti tvarkomi atidžiai, kad atitiktų pagrįstumo kriterijų. Šiuo požiūriu, siekiant atidžiai tvarkyti duomenis, buvimo vietos duomenų rinkiniai turi būti vertinami kaip visuma, taip pat turi būti tvarkomi pakankamai didelės asmenų grupės duomenys ir tai turi būti daroma naudojant esamus patikimus anoniminimo metodus, užtikrinant, kad jie būtų naudojami tinkamai ir veiksmingai.

23 Galiausiai, atsižvelgiant į anoniminimo procesų sudėtingumą, primygtinai raginama užtikrinti anoniminimo metodų skaidrumą.

---

[9] „Dėl mobiliųjų telefonų duomenų naudojimo laikantis privatumo apsaugos principų“ (angl. *On the privacy-conscientious use of mobile phone data*), de Montjoye *et al.*, 2018 m.

[10] „Unikalus minioje. Žmonių judumo privatumo ribos“ (angl. *Unique in the Crowd: The privacy bounds of human mobility* (de Montjoye *et al.*, 2013 m.) ir „Tuk-tuk. Kas ten? Narystės numanymas remiantis bendrais buvimo vietos duomenimis“ (angl. *Knock Knock, Who's There? Membership Inference on Aggregate Location Data* (Pyrgelis *et al.*, 2017 m.).

3 SĄLYTĮ TURĖJUSIŲ ASMENŲ IŠAIŠKINIMO PROGRAMĖLĖS

3.1 Bendroji teisinė analizė

24 Sisteminė ir didelės apimties fizinių asmenų buvimo vietos ir (arba) asmenų, su kuriais jie turėjo sąlytį, stebėsena yra sunkus jų privatumo pažeidimas. Tokią stebėseną galima įteisinti tik naudotojams savanoriškai pradėjus naudoti tokias programėles kuriuo nors iš atitinkamų tikslų. Tai reikštų, kad visų pirma tie asmenys, kurie nuspręstų nenaudoti arba negalėtų naudoti tokių programėlių, neturėtų patirti jokių nepatogumų.

25 Siekiant užtikrinti atskaitomybę, turėtų būti aiškiai apibrėžtas bet kurios sąlytį turėjusių asmenų išaiškinimo programėlės duomenų valdytojas. EDAV laikosi nuomonės, kad tokios programėlės duomenų valdytojais galėtų būti nacionalinės sveikatos apsaugos institucijos[11]; būtų galima numatyti ir kitus duomenų valdytojus. Visais atvejais, jeigu sąlytį turėjusių asmenų išaiškinimo programėles diegia skirtingi subjektai, nuo pat pradžių turi būti aiškiai nustatytos ir naudotojams paaiškintos tų subjektų funkcijos ir pareigos.

26 Be to, kalbant apie tikslo apribojimo principą, pažymėtina, kad duomenų naudojimo tikslai turi būti pakankamai konkrečiai apibrėžti, kad jie nebūtų vėliau tvarkomi su COVID-19 sukeltos sveikatos apsaugos srities krizės valdymu nesusijusiais tikslais (pvz., komerciniais arba teisėsaugos tikslais). Aiškiai apibrėžus tikslą, bus būtina užtikrinti, kad asmens duomenys būtų naudojami tinkamai, tik esant būtinybei ir proporcingai.

27 Naudojant sąlytį turėjusių asmenų išaiškinimo programėlę, reikėtų atidžiai atsižvelgti į duomenų kiekio mažinimo ir pritaikytosios bei standartizuotosios duomenų apsaugos principą:

- sąlytį turėjusių asmenų išaiškinimo programėlėms nebūtinas atskirų naudotojų buvimo vietos sekimas. Vietoj šių duomenų galima naudoti artumo duomenis;
- kadangi sąlytį turėjusių asmenų išaiškinimo programėlės gali veikti tiesiogiai nenustatant asmenų tapatybės, reikėtų įgyvendinti atitinkamas priemones, kad būtų išvengta duomenų išanoniminimo;
- surinkta informacija turėtų būti saugoma naudotojo galiniame įrenginyje ir, kai tai yra visiškai būtina, turėtų būti renkama tik aktuali informacija.

28 Dėl duomenų tvarkymo teisėtumo EDAV atkreipia dėmesį į tai, kad, naudojant sąlytį turėjusių asmenų išaiškinimo programėles, saugoma galiniame įrenginyje jau saugoma informacija ir (arba) suteikiama galimybė su ja susipažinti, ir šioms operacijoms taikoma Direktyvos 5 straipsnio 3 dalis. Jeigu šios operacijos yra visiškai būtinos tam, kad programėlės tiekėjas galėtų teikti paslaugą, kurios aiškiai prašo naudotojas, jo sutikimas nėra būtinas tam, kad būtų galima tvarkyti duomenis. Kad galėtų atlikti operacijas, kurios nėra visiškai būtinos, teikėjas turėtų gauti naudotojo sutikimą.

29 Be to, EDAV atkreipia dėmesį į tai, kad, nors sąlytį turėjusių asmenų išaiškinimo programėlės naudojamos savanoriškai, tai nereiškia, kad asmens duomenys būtinai bus tvarkomi tik gavus sutikimą. Kai valdžios institucijos teikia paslaugą remdamosi teisės aktais joms suteiktais įgaliojimais ir laikydamosi teisės aktuose nustatytų reikalavimų, atrodo, kad svarbiausias duomenų tvarkymo teisinis pagrindas yra būtinybė atlikti užduotį viešojo intereso labui, t. y. BDAR 6 straipsnio 1 dalies e punktas.

30 BDAR 6 straipsnio 3 dalyje paaiškinama, kad 6 straipsnio 1 dalies e punkte nurodyto duomenų tvarkymo pagrindas nustatomas pagal duomenų valdytojui taikomus Sąjungos arba valstybių narių teisės aktus. Duomenų tvarkymo tikslas nustatomas tame teisiniame pagrinde arba, 1 dalies e punkte nurodyto duomenų tvarkymo atveju, yra būtinas, siekiant atlikti užduotį,

[11] Taip pat žr. Europos Komisijos komunikatą „Duomenų apsaugos gairės dėl kovai su COVID-19 pandemija naudojamų programėlių“, Briuselis, 2020 4 16, C(2020) 2523 *final*.

vykdomą viešojo intereso labui arba vykdant duomenų valdytojui pavestas viešosios valdžios funkcijas[12].

31 Vis dėlto teisiniame pagrinde arba teisėkūros priemonėje, kuriais užtikrinamas teisėtas pagrindas naudoti sąlytį turėjusių asmenų išaiškinimo programėles, turėtų būti numatytos svarbios apsaugos priemonės, įskaitant nuorodą į savanorišką programėlės naudojimo pobūdį. Tame teisiniame pagrinde arba teisėkūros priemonėje turėtų būti aiškiai nurodytas tolesnio asmens duomenų naudojimo tikslas ir aiškūs apribojimai, taip pat turėtų būti aiškiai nustatytas (-i) susijęs (-ę) duomenų valdytojas (-ai). Taip pat turėtų būti nustatytos duomenų kategorijos ir subjektai, kuriems (ir tikslai, kuriais) asmens duomenys gali būti atskleidžiami. Priklausomai nuo poveikio privačiam gyvenimui lygio, turėtų būti numatytos papildomos apsaugos priemonės, atsižvelgiant į duomenų tvarkymo pobūdį, apimtį ir tikslus. Galiausiai, EDAV taip pat rekomenduoja pagal galimybes kuo greičiau nustatyti kriterijus, kuriais remiantis būtų galima nuspręsti, kada programėlę būtina pašalinti ir kuris subjektas yra atsakingas ir atskaitingas už tokį sprendimą.

32 Vis dėlto, jeigu duomenys tvarkomi remiantis kitu teisiniu pagrindu, pvz., remiantis sutikimu (6 straipsnio 1 dalies a punktas)[13], duomenų valdytojas turės užtikrinti, kad būtų įvykdyti griežti reikalavimai, suteikiantys galimybę remtis tokiu teisiniu pagrindu.

33 Be to, programėlę naudojant kovai su COVID-19 pandemija, gali būti renkami sveikatos duomenys (pvz., duomenys apie užsikrėtusio asmens būklę). Tvarkyti tokius duomenis leidžiama, kai toks duomenų tvarkymas yra būtinas dėl su viešuoju interesu visuomenės sveikatos srityje susijusių priežasčių, atitinkančių BDAR 9 straipsnio 2 dalies i punkte[14] nustatytas sąlygas, arba BDAR 9 straipsnio 2 dalies h punkte[15] nustatytais sveikatos priežiūros tikslais. Priklausomai nuo teisinio pagrindo, duomenų tvarkymas taip pat gali būti grindžiamas aiškiu sutikimu (BDAR 9 straipsnio 2 dalies a punktas).

34 Atsižvelgiant į pirminį tikslą, pagal BDAR 9 straipsnio 2 dalies j punktą sveikatos duomenis taip pat leidžiama tvarkyti, kai tai yra būtina mokslinių tyrimų arba statistikos tikslais.

35 Dabartine sveikatos apsaugos srities krize neturėtų būti naudojamasi kaip galimybe nustatyti neproporcingus įgaliojamus saugoti duomenis. Nustatant duomenų saugojimo apribojimus, reikėtų atsižvelgti į faktinius poreikius ir medicininę reikšmę (tai gali būti tokios epidemiologija grindžiamos aplinkybės kaip inkubacinis laikotarpis ir kt.), ir asmens duomenys turėtų būti laikomi tik COVID-19 sukeltos krizės laikotarpiu. Vėliau, įprastais atvejais, visi asmens duomenys turėtų būti sunaikinti arba anoniminti.

36 EDAV supratimu, tokiomis programėlėmis negalima pakeisti mechaninio sąlytį turėjusių asmenų išaiškinimo, kurį atlieka kvalifikuoti visuomenės sveikatos srities darbuotojai, galintys atskirti, ar artimas sąlytis galėjo lemti viruso perdavimą, ar ne (pvz., bendraujant su kuo nors, kas buvo apsisaugojęs tinkamomis priemonėmis, pvz., kasininku ir pan., arba nedėvėjo tokių priemonių). EDAV atkreipia dėmesį į tai, kad procedūros ir procesai, įskaitant sąlytį turėjusių asmenų išaiškinimo programėlėse įdiegtus atitinkamus algoritmus, turėtų būti vykdomi griežtai prižiūrint kvalifikuotiems darbuotojams, kad būtų kuo mažiau bet kokių klaidingai teigiamų ir neigiamų rezultatų atvejų. Visų pirma, konsultacijos dėl tolesnių veiksmų turėtų būti teikiamos remiantis ne vien automatinio duomenų tvarkymo rezultatais.

37 Siekiant užtikrinti algoritmų teisingumą, atskaitomybę ir, platesne prasme, atitiktį teisės aktams, turi būti galimybė juos tikrinti ir nepriklausomi ekspertai turėtų reguliariai juos

---

[12] Žr. 41 konstatuojamąją dalį.

[13] Duomenų valdytojai (ypač valdžios institucijos) turi atkreipti ypatingą dėmesį į tai, kad sutikimas neturėtų būti laikomas laisva valia duotu sutikimu, jeigu asmuo faktiškai neturėjo galimybės atsisakyti sutikti arba atšaukti sutikimą, nepatirdamas žalos.

[14] Duomenų tvarkymas turi būti grindžiamas Sąjungos arba valstybių narių teisės aktais, kuriuose numatomos tinkamos ir konkrečios priemonės duomenų subjekto teisėms ir laisvėms, ypač profesinei paslapčiai, apsaugoti.

[15] Žr. BDAR 9 straipsnio 2 dalies h punktą.

peržiūrėti. Programėlės programinis kodas turėtų būti viešai skelbiamas, kad jį būtų galima kuo plačiau patikrinti.

38 Visada tam tikra dalis rezultatų bus klaidingai teigiami. Kadangi užsikrėtimo pavojaus nustatymas tikriausiai gali turėti didelį poveikį atitinkamiems asmenims, pvz., jiems gali tekti izoliuotis, kol tyrimo rezultatas bus neigiamas, galimybė pakoreguoti duomenis ir (arba) tolesnės analizės rezultatus yra būtina. Be abejo, tai turėtų būti taikoma tik tiems scenarijams ir įgyvendinimo veiksmams, kai duomenys tvarkomi ir (arba) saugomi taip, kad toks koregavimas yra techniniu požiūriu įmanomas, ir kai pirmiau minėtas nepageidaujamas poveikis yra tikėtinas.

39 Galiausiai, EDAV laikosi nuomonės, kad prieš įgyvendinant tokią priemonę turi būti atliekamas poveikio duomenų apsaugai vertinimas (PDAV), kadangi duomenų tvarkymas vertinamas kaip galintis sukelti didelį pavojų (sveikatos duomenys, numatomas taikymas dideliu mastu, sisteminė stebėsena, naujo technologinio sprendimo naudojimas)[16]. EDAV primygtinai rekomenduoja viešai skelbti poveikio duomenų apsaugai vertinimus.

3.2 Rekomendacijos ir funkciniai reikalavimai

40 Vadovaujantis duomenų kiekio mažinimo principu, be kitų pritaikytosios ir standartizuotosios duomenų apsaugos priemonių[17], tvarkomų duomenų kiekis turėtų būti sumažintas iki minimumo, kad būtų tvarkomi tik tie duomenys, kurie yra tikrai būtini. Programėlė neturėtų rinkti nesusijusios arba nereikalingos informacijos, pvz., susijusios su civiline būkle, ryšių identifikatoriais, įrenginio kataloge esančiais aplankais, pranešimais, skambučių žurnalais, buvimo vietos duomenimis, prietaiso identifikatoriais.

41 Programėlių transliuojami duomenys turi apimti tik tam tikrus programėlės sugeneruotus ir tik su ja susijusius unikalius ir pseudoniminius identifikatorius. Tie identifikatoriai turi būti atnaujinami reguliariai, atsižvelgiant į tikslą suvaldyti viruso plitimą tinkamu dažnumu, kurio pakaktų asmenų tapatybės nustatymo ir fizinio atsekamumo pavojui sumažinti.

42 Sąlytį turėjusių asmenų išaiškinimas gali būti įgyvendinamas centralizuotai arba decentralizuotai[18]. Abu šie būdai turėtų būti vertinami kaip priimtinos galimybės, jeigu bus nustatytos tinkamos saugumo priemonės, nes abu jie turi tam tikrų pranašumų ir trūkumų. Taigi, programėlės koncepcijos kūrimo etape visada reikėtų gerai apsvarstyti abi koncepcijas, atidžiai pasveriant atitinkamą poveikį duomenų apsaugai ir (arba) privatumui ir galimą poveikį asmenų teisėms.

43 Bet kuris sąlytį turėjusių asmenų išaiškinimo sistemos serveris turi kaupti tik naudotojo, kuriam – sveikatos priežiūros institucijoms atlikus tinkamą vertinimą ir naudotojui savanoriškai atlikus tam tikrus veiksmus – buvo diagnozuota infekcija, kontaktų istoriją arba pseudoniminius identifikatorius. Arba užsikrėtusių naudotojų pseudoniminių identifikatorių sąrašą arba jų kontaktų istoriją serveris turi kaupti tik tiek laiko, kiek jo reikia tam, kad būtų galima informuoti galimai užsikrėtusius naudotojus apie tai, kad jie galėjo užsikrėsti, ir neturėtų mėginti nustatyti užsikrėtusių naudotojų tapatybės.

44 Įgyvendinant visuotinį sąlytį turėjusių asmenų išaiškinimo metodą, apimantį ir programėles, ir mechaninį sąlytį turėjusių asmenų išaiškinimą, kai kuriais atvejais gali tekti tvarkyti papildomą informaciją. Tokiomis aplinkybėmis ši papildoma informacija turėtų likti

---

[16] Žr. 29 straipsnio darbo grupės parengtas (EDAV priimtas) poveikio duomenų apsaugai vertinimo (PDAV) gaires, kuriomis Reglamento 2016/679 taikymo tikslais nurodoma, kaip nustatyti, ar duomenų tvarkymo operacijos gali sukelti didelį pavojų.

[17] Žr. EDAV gaires Nr. 4/2019 dėl 25 straipsnio „Pritaikytoji duomenų apsauga ir standartizuotoji duomenų apsauga“.

[18] Apskritai, decentralizuotas sprendimas labiau atitinka duomenų kiekio mažinimo principą.

naudotojo galiniame įrenginyje ir turėtų būti tvarkoma tik, kai tai yra visiškai būtina ir tik gavus jo konkretų išankstinį sutikimą.

45 Siekiant apsaugoti serveriuose ir programėlėse saugomus duomenis, taip pat tarp programėlių ir nuotolinio serverio vykstančius duomenų mainus, turi būti įdiegti pažangiausi kriptografijos metodai. Taip pat turi būti vykdomas abipusis programėlės ir serverio autentiškumo tikrinimas.

46 Naudotojų programėlei teikiama informacija apie savo užsikrėtimą SARS-CoV-2 turi būti atitinkamai patvirtinama, pvz., pateikiamas vienkartinis kodas, susietas su pseudonimine užsikrėtusio asmens tapatybe ir atitinkama tyrimų stotimi arba sveikatos priežiūros specialistu. Nesant saugaus patvirtinimo galimybės, jokie duomenys neturėtų būti tvarkomi, kad nekiltų abejonių dėl naudotojo būklės pagrįstumo.

47 Duomenų valdytojas, bendradarbiaudamas su valdžios institucijomis, turi aiškiai ir išsamiai informuoti apie nuorodą, kurią spustelėjus galima parsisiųsti oficialią nacionalinę sąlytį turėjusių asmenų išaiškinimo programėlę, kad būtų kuo mažesnis pavojus, kad atitinkami asmenys naudos trečiųjų šalių programėlę.

4 IŠVADA

48 Šiuo metu pasaulis stengiasi įveikti didelio masto visuomenės sveikatos apsaugos srities krizę, kuri reikalauja imtis griežtų atsakomųjų veiksmų, kurių poveikis bus juntamas net ir pasibaigus šiai ekstremaliajai situacijai. Automatizuotas duomenų tvarkymas ir skaitmeninės technologijos gali būti itin svarbūs kovojant su COVID-19. Vis dėlto, reikėtų saugotis vadinamojo reketo efekto. Mūsų pareiga – užtikrinti, kad kiekviena priemonė, kurios imamasi šiomis ypatingomis aplinkybėmis, būtų būtina, taikoma laikinai ir minimaliu mastu ir būtų periodiškai iš esmės peržiūrima bei moksliškai įvertinama.

49 EDAV atkreipia dėmesį į tai, kad niekas neturėtų būti priverstas rinktis vieno iš dviejų tikslų – veiksmingai reaguoti į dabartinę krizę arba apsaugoti savo pagrindines teises: mes galime pasiekti juos abu, be to, duomenų apsaugos principai gali atlikti labai svarbų vaidmenį kovojant su virusu. ES teisės aktai, kuriais reglamentuojama duomenų apsauga, suteikia galimybę atsakingai naudoti asmens duomenis sveikatos priežiūros valdymo tikslais, kartu užtikrinant, kad šio proceso metu nebūtų pažeistos žmogaus teisės ir laisvės.

Europos duomenų apsaugos valdybos vardu

Pirmininkė

(Andrea Jelinek)

PRIEDAS. SĄLYTĮ TURĖJUSIŲ ASMENŲ IŠAIŠKINIMO PROGRAMĖLĖS. ANALITINIS VADOVAS

0. Atsakomybės ribojimas

Toliau pateikiamos gairės nėra norminamojo pobūdžio ir nėra išsamios; vienintelė šio vadovo paskirtis – pateikti bendras gaires sąlytį turėjusių asmenų išaiškinimo programėlių kūrėjams ir jas diegiantiems subjektams. Gali būti naudojami ir kiti šiame dokumente neaprašyti technologiniai sprendimai ir tokie sprendimai gali būti teisėti, jeigu atitinka susijusios teisinės sistemos (t. y. BDAR ir Direktyvos) nuostatas.

Taip pat būtina atkreipti dėmesį į tai, kad tai yra bendro pobūdžio vadovas. Taigi šiame dokumente pateikiamų rekomendacijų ir nustatytų prievolių negalima laikyti išsamiomis. Bet koks vertinimas turi būti atliekamas atsižvelgiant į konkrečias kiekvieno atvejo aplinkybes, be to, dėl tam tikrų konkrečių programėlių gali tekti imtis papildomų šiame vadovų neaptartų priemonių.

1. Santrauka

Daugelyje valstybių narių suinteresuotieji subjektai šiuo metu svarsto galimybę naudoti vadinamąsias *sąlytį turėjusių asmenų išaiškinimo* programėles, siekdami padėti gyventojams išsiaiškinti, ar jie nėra artimai bendravę su SARS-Cov-2 užsikrėtusiu asmeniu.

Dar nenustatytos sąlygos, kuriomis tokios programėlės turėtų padėti veiksmingai valdyti pandemiją. Šias sąlygas reikėtų nustatyti prieš įdiegiant bet kurią iš tokių programėlių. Vis dėlto svarbu pateikti gaires, kuriose būtų išdėstyta pirminiams programėlių kūrėjams aktuali informacija, kad asmens duomenų apsauga būtų užtikrinama nuo pat pirmųjų tokių programėlių kūrimo etapų.

Būtina atkreipti dėmesį į tai, kad tai yra bendro pobūdžio vadovas. Taigi, šiame dokumente pateikiamų rekomendacijų ir nustatytų prievolių negalima laikyti išsamiomis. Bet koks vertinimas turi būti atliekamas atsižvelgiant į konkrečias kiekvieno atvejo aplinkybes, be to, dėl tam tikrų konkrečių programėlių gali tekti imtis papildomų šiame vadovų neaptartų priemonių. Šio vadovo paskirtis – pateikti bendras gaires sąlytį turėjusių asmenų išaiškinimo programėlių kūrėjams ir jas diegiantiems subjektams.

Kai kurie kriterijai gali viršyti griežtus duomenų apsaugos sistemos reikalavimus. Jais siekiama užtikrinti aukščiausio lygio skaidrumą, kuris padėtų užtikrinti tokių sąlytį turėjusių asmenų išaiškinimo programėlių priimtinumą visuomenei.

Šiuo tikslu sąlytį turėjusių asmenų išaiškinimo programėlių leidėjai turėtų atsižvelgti į toliau nurodytus kriterijus.

- Tokia programėlė gali būti naudojama tik savanoriškai. Galimybė pasinaudoti teisėje įtvirtintomis teisėmis negali būti susieta su programėlės naudojimu. Asmenys turi galėti visada visapusiškai kontroliuoti savo duomenis ir turėtų turėti galimybę rinktis, ar naudoti tokią programėlę.
- Sąlytį turėjusių asmenų išaiškinimo programėlės gali kelti didelį pavojų fizinių asmenų teisėms ir laisvėms ir, prieš jas įdiegiant, gali reikėti atlikti poveikio duomenų apsaugai vertinimą.

- Informaciją apie arti esančius programėlės naudotojus galima gauti nenustatant jų buvimo vietos. Tokios rūšies programėlės veikimui užtikrinti nereikia buvimo vietos duomenų, todėl ji turėtų veikti nenaudodama tokių duomenų.
- Naudotojui diagnozavus SARS-Cov-2 infekciją, apie tai turėtų būti informuojami tik tie asmenys, su kuriais šis naudotojas artimai bendravo per epidemiologiniu požiūriu sąlytį turėjusių asmenų išaiškinimui aktualų laikotarpį.
- Priklausomai nuo pasirinktos architektūros, kad tokio tipo programėlė veiktų, gali reikėti centralizuoto serverio. Tokiu atveju ir vadovaujantis duomenų kiekio mažinimo ir pritaikytosios duomenų apsaugos principu, centralizuotas serveris turėtų tvarkyti tik tuos duomenis, kurie yra tikrai būtini.
    - Naudotojui diagnozavus infekciją, informacija, susijusi su jo ankstesniais artimais kontaktais arba naudotojo programėlės transliuojamais identifikatoriais, gali būti kaupiama tik naudotojui sutikus. Turėtų būti nustatytas tam tikras tikrinimo metodas, kuris suteiktų galimybę, nenustatant naudotojo tapatybės, patvirtinti, kad asmuo iš tikrųjų užsikrėtęs. Techniniu požiūriu šią galimybę būtų galima įgyvendinti sąlytį turėjusius asmenis įspėjant tik įsikišus sveikatos priežiūros specialistui, pvz., naudojant specialų vienkartinį kodą.
    - Centriniame serveryje saugoma informacija neturėtų suteikti galimybės duomenų valdytojams nustatyti naudotojų, kuriems diagnozuota infekcija arba kurie bendravo su tais naudotojais, tapatybės, taip pat neturėtų leisti jiems dedukcijos būdu nustatyti su kontaktais susijusių ypatumų, kurie nėra būtini siekiant nustatyti atitinkamus sąlytį turėjusius asmenis.
- Kad tokio tipo programėlė veiktų, ji turi transliuoti duomenis, kuriuos nuskaito kitų naudotojų prietaisai, ir reikia klausytis šių transliacijų.
    - Pakanka, kad tarp naudotojų mobiliųjų įrenginių (kompiuterių, planšečių, susietųjų rankinių laikrodžių ir kt.) būtų keičiamasi pseudoniminiais identifikatoriais, pvz., juos transliuojant (naudojant energiją tausojančią „Bluetooth“ technologiją).
    - Identifikatoriai turi būti generuojami naudojant pažangiausius kriptografijos procesus.
    - Identifikatoriai turi būti reguliariai atnaujinami, siekiant sumažinti fizinio atsekamumo ir mėginimų susieti pavojų.
- Tokio tipo programėlė turi būti apsaugota, kad būtų užtikrintas techninių procesų saugumas. Visų pirma
    - programėlė neturėtų naudotojams perduoti informacijos, kuri suteiktų jiems galimybę numanyti kitų naudotojų tapatybę arba diagnozę. Centrinis serveris negali nei nustatyti naudotojų tapatybės, nei dedukcijos būdu nustatyti jokios informacijos apie juos.

Atsakomybės ribojimas. Pirmiau minėti principai susiję su nurodyta *sąlytį turėjusių asmenų išaiškinimo* programėlių paskirtimi ir tik su ja, t. y. tik automatiškai informuoti žmones, kurie galimai galėjo užsikrėsti virusu (nesant tikslo nustatyti jų tapatybę). Programėlės ir jos infrastruktūros valdytojus gali kontroliuoti kompetentinga priežiūros institucija. Vadovavimosi visomis arba dalimi šių gairių nebūtinai pakaks, siekiant užtikrinti visapusišką atitiktį duomenų apsaugos sistemai.

2. Sąvokų apibrėžtys

Sąlytį turėjęs asmuo	Kalbant apie sąlytį turėjusių asmenų išaiškinimo programėlę, sąlytį turėjęs asmuo – tai naudotojas, bendravęs su naudotoju, kuris patvirtintas kaip viruso nešiotojas, ir kurio bendravimo su užsikrėtusiu naudotoju trukmė ir atstumas leidžia manyti, kad pavojus užsikrėsti virusine infekcija buvo labai didelis. Bendravimo su užsikrėtusiu asmeniu trukmės ir atstumo tarp žmonių parametrus turi įvertinti sveikatos priežiūros institucijos ir jie gali būti nustatyti programėlėje.
Buvimo vietos duomenys	Tai yra visi elektroninių ryšių tinkle arba elektroninių ryšių paslaugų teikėjų tvarkomi duomenys, iš kurių matoma viešai prieinamų elektroninių ryšių paslaugų naudotojo (kaip apibrėžta Direktyvoje) galinio įrenginio geografinė padėtis, taip pat duomenys iš galimų kitų šaltinių, susiję su: • galinio įrenginio buvimo vietos geografine platuma, ilguma arba aukščiu virš jūros lygio; • naudotojo kelionės kryptimi arba • laiku, kuriuo buvo užregistruota buvimo vietos informacija.
Sąveika	Kalbant apie sąlytį turėjusių asmenų išaiškinimo programėlę, sąveika – tai informacijos mainai tarp dviejų (erdvės ir laiko požiūriu) arti vienas kito esančių prietaisų, naudojantis tam tikromis ryšių technologijomis (pvz., „Bluetooth“ technologija). Į šią apibrėžtį neįtraukta dviejų šioje sąveikoje dalyvaujančių naudotojų buvimo vieta.
Viruso nešiotojas	Šiame dokumente viruso nešiotojais laikomi tie naudotojai, kurių tyrimo dėl viruso rezultatas buvo teigiamas ir kurių diagnozė oficialiai patvirtinta gydytojo arba sveikatos priežiūros centro.
Sąlytį turėjusių asmenų išaiškinimas	Žmonėms, kurie (pagal epidemiologų apibrėžtus kriterijus) artimai bendravo su virusu užsikrėtusiu asmeniu, taip pat kyla didelis pavojus užsikrėsti ir kartu jie patys kelia tokį pavojų kitiems. Sąlytį turėjusių asmenų išaiškinimas – tai ligų kontrolės metodas, kai išvardijami visi arti viruso nešiotojo buvę žmonės, siekiant patikrinti, ar jiems nekyla pavojus užsikrėsti ir imtis atitinkamų sanitarinių priemonių jų atžvilgiu.

3. Bendroji dalis

GEN-1	Programėlė turi būti naudojama kaip papildoma priemonė kartu su tradiciniais sąlytį turėjusių asmenų išaiškinimo metodais (būtent, pokalbiais su užsikrėtusiais asmenimis), t. y. naudojama vykdant platesnę visuomenės sveikatos programą. Ji turi būti naudojama tik tol, kol dėl didelio naujų

	užsikrėtimo atvejų skaičiaus nepajėgiama vien mechaniniu būdu išaiškinti sąlytį turėjusius asmenis.
GEN-2	Vėliausiai tuo metu, kai kompetentingos valdžios institucijos nuspręs, kad laikas grįžti prie įprastų sąlygų, turi būti nustatyta procedūra, kuria vadovaujantis būtų nutrauktas identifikatorių rinkimas (visuotino programėlės išjungimo procedūra, programėlės išinstaliavimo instrukcijos, automatinio išinstaliavimo procedūra ir pan.) ir būtų pradėtas visų iš visų duomenų bazių (mobiliųjų programėlių ir serverių) surinktų duomenų sunaikinimas.
GEN-3	Programėlės ir jos duomenų saugyklos pradinė programa turi būti atvira, o techninės specifikacijos turi būti viešai skelbiamos, kad bet kuri suinteresuotoji šalis galėtų patikrinti tą programą ir, jei reikia, padėti patobulinti ją, ištaisyti galimas klaidas ir užtikrinti asmens duomenų tvarkymo skaidrumą.
GEN-4	Programėlės diegimo etapai turi suteikti galimybę laipsniškai patvirtinti jos veiksmingumą visuomenės sveikatos apsaugos požiūriu. Šiuo tikslu turi būti apibrėžtas programėlės kūrėjams skirtas vertinimo protokolas, kuriame būtų nurodyti rodikliai, pagal kuriuos būtų galima įvertinti programėlės veiksmingumą.

4. Tikslai

PUR-1	Programėlė turi būti naudojama vieninteliu tikslu – siekiant išaiškinti sąlytį turėjusius asmenis, kad būtų galima įspėti galimai užsikrėsti SARS-Cov-2 galėjusius žmones ir jais pasirūpinti. Programėlė negali būti naudojama kitais tikslais.
PUR-2	Programėlės negalima naudoti ne pagal pirminę paskirtį, t. y. stebėjimui, kaip laikomasi karantino arba izoliavimo priemonių ir (arba) socialinio atsiribojimo reikalavimų.
PUR-3	Programėlė negali būti naudojama siekiant padaryti išvadas dėl naudotojų buvimo vietos, atsižvelgiant į jų bendravimą ir (arba) naudojant kitas priemones.

5. Funkciniai aspektai

FUNC-1	Programėlėje turi būti funkcija, suteikianti galimybę naudotojams būti informuotiems apie tai, kad jie galimai galėjo užsikrėsti virusu; ši informacija turėtų būti grindžiama buvimu arti užsikrėtusio naudotojo, likus X dienoms (-ų) iki jam atliekant tyrimą dėl užsikrėtimo, kurio rezultatas buvo teigiamas (X vertę turi nustatyti sveikatos priežiūros institucijos).
FUNC-2	Programėlė turėtų pateikti rekomendacijas tiems naudotojams, kurie nustatyti kaip asmenys, galimai galėję užsikrėsti virusu. Programėlė turėtų pateikti nurodymus dėl priemonių, kurių jie turėtų toliau imtis, ir ji turėtų suteikti

	galimybę naudotojui paprašyti konsultacijos. Tokiais atvejais žmogaus įsikišimas būtų būtinas.
FUNC-3	Turi būti galimybė, remiantis naujausiomis žiniomis apie viruso plitimą, saugiai priderinti algoritmą, pagal kurį, atsižvelgiant į tokius veiksnius kaip atstumas ir laikas, vertinamas užsikrėtimo pavojus ir nustatoma, ar sąlytį turėjusį asmenį reikia įtraukti į sąlytį turėjusių asmenų išaiškinimui skirtą sąrašą.
FUNC-4	**Naudotojai turi būti informuoti, jeigu jie galėjo užsikrėsti virusu**, arba turi visą viruso inkubacinį laikotarpį reguliariai gauti informaciją apie tai, ar jie galėjo, ar negalėjo užsikrėsti virusu.
FUNC-5	Programėlė turėtų būti sąveiki su kitomis valstybėse narėse sukurtomis programėlėmis, kad skirtingose valstybėse narėse keliaujančius naudotojus būtų galima veiksmingai informuoti.

6. Duomenys

DATA-1	Programėlėje turi būti užtikrinta galimybė siųsti ir priimti duomenis naudojant artimumo principu veikiančias ryšių technologijas, kaip antai energiją tausojančią „Bluetooth“ technologiją, kad būtų galima vykdyti sąlytį turėjusių asmenų išaiškinimo procesą.
DATA-2	Šie transliuojami duomenys turi apimti kriptoanalizei atsparius programėlės sugeneruotus ir tik su ja susijusius pseudoatsitiktinius identifikatorius.
DATA-3	Pseudoatsitiktinių identifikatorių kolizijos rizika turėtų būti pakankamai maža.
DATA-4	Pseudoatsitiktiniai identifikatoriai turi būti atnaujinami reguliariai, tokiu dažnumu, kurio pakaktų sumažinti pavojų, kad kas nors, įskaitant centrinio serverio operatorius, kitus programėlės naudotojus arba piktų ketinimų turinčias trečiąsias šalis, išanonimins kurių nors asmenų duomenis, fiziškai juos atseks arba susies. Šie identifikatoriai turi būti sugeneruoti naudotojo programėlės, galimai pagal centrinio serverio pateiktą pradinę reikšmę.
DATA-5	Pagal duomenų kiekio mažinimo principą programėlė negali rinkti jokių kitų duomenų, išskyrus tuos duomenis, kurie yra visiškai būtini sąlytį turėjusių asmenų išaiškinimui.
DATA-6	Programėlė negali rinkti buvimo vietos duomenų sąlytį turėjusių asmenų išaiškinimo tikslais. Buvimo vietos duomenys gali būti tvarkomi tik vienu tikslu – siekiant užtikrinti galimybę programėlei sąveikauti su panašiomis programėlėms kitose valstybėse, ir tai turėtų būti tiksliai tik tie duomenys, kurie yra visiškai būtini šiam vieninteliam tikslui pasiekti.
DATA-7	Programėlė neturėtų rinkti sveikatos duomenų – be tų duomenų, kurie yra visiškai būtini tam, kad programėlė galėtų veikti pagal paskirtį, –išskyrus tuos atvejus, kai jų neprivaloma pateikti ir tik kai tuo siekiama padėti priimti sprendimą dėl naudotojo informavimo.

DATA-8	Naudotojai turi būti informuojami apie visus asmens duomenis, kurie bus renkami. Šie duomenys turėtų būti renkami tik naudotojui leidus.

7. Techninės savybės

TECH-1	Programėlė turėtų, naudodama tokias esamas technologijas kaip keitimosi duomenimis trumpu atstumu sistemas (pvz., energiją tausojančią „Bluetooth“ technologiją), nustatyti naudotojus, esančius netoli įrenginio, kuriame ši programėlė veikia.
TECH-2	Programėlė turėtų saugoti naudotojų kontaktų istoriją įrenginyje iš anksto apibrėžtą ribotą laiką.
TECH-3	Kai kurių programėlės funkcijų veikimui gali būti reikalingas centrinis serveris.
TECH-4	Programėlės architektūra turi būti kuo artimesnė naudotojų įrenginių architektūrai.
TECH-5	Naudotojų, apie kuriuos pranešta, kaip apie užsikrėtusius virusu, iniciatyva ir tinkamai sertifikuotam sveikatos priežiūros specialistui patvirtintus jų būklę, jų kontaktų istorija arba jų pačių identifikatoriai turėtų būti perduoti centriniam serveriui.

8. Saugumas

SEC-1	Turi būti įdiegta sistema, suteikianti galimybę patikrinti programėlei informaciją apie savo užsikrėtimą SARS-CoV-2 pateikiančių naudotojų būklę, pvz., pateikiamas vienkartinis kodas, susietas su atitinkama tyrimų stotimi arba sveikatos priežiūros specialistu. Jeigu negalima saugiai gauti patvirtinimo, duomenų negalima tvarkyti.
SEC-2	Centriniam serveriui siunčiami duomenys turi būti perduodami saugiu kanalu. Reikėtų atidžiai įvertinti operacinės sistemos platformos paslaugos teikėjų teikiamų pranešimo paslaugų naudojimą - naudojantis tokiomis paslaugomis, trečiosioms šalims neturėtų būti atskleidžiami jokie duomenys.
SEC-3	Užklausos turi būti atsparios neteisėtam keitimui, kurį gali mėginti atlikti piktų ketinimų turintys naudotojai.
SEC-4	Siekiant apsaugoti tarp programėlės ir serverio bei skirtingų programėlių vykstančius duomenų mainus, taip pat, kaip įprasta, apsaugoti programėlėse ir serveryje saugomą informaciją, turi būti įdiegti pažangiausi kriptografijos metodai. Gali būti naudojami šie metodai: simetrinis ir asimetrinis šifravimas, maišos funkcijos, konfidencialus aibės elementų tyrimas, konfidencialus rinkinių palyginimas, „Bloom“ filtrai, konfidencialus informacijos išrinkimas, homomorfinis šifravimas ir kt.
SEC-5	Centrinis serveris negali saugoti jokių naudotojų, įskaitant tuos naudotojus, kuriems diagnozuota infekcija ir kurie perdavė savo kontaktų istoriją arba savo pačių identifikatorių, prisijungimo prie tinklo identifikatorių (pvz., IP adresų).

SEC-6	Siekiant išvengti apsimetimo kitais naudotojais arba netikrų naudotojų sukūrimo, serveris turi nustatyti programėlės tapatumą.
SEC-7	Programėlė turi nustatyti centrinio serverio tapatumą.
SEC-8	Serveris turėtų būti apsaugotas nuo mėginimų pakartoti jau atliktas funkciją.
SEC-9	Centrinio serverio perduodama informacija turi būti pasirašyta, kad būtų galima patvirtinti jos kilmę ir vientisumą.
SEC-10	Galimybė susipažinti su visais centriniame serveryje saugomais ir vieši neskelbiamais duomenimis, turi būti suteikiama tik įgaliotiems asmenims.
SEC-11	Įrenginio leidimų tvarkytuvė operacinės sistemos lygmeniu turi reikalauti tik tų leidimų, kurie yra būtini siekiant prisijungti prie ryšio modulių ir, esant būtinybei, jais naudotis, taip pat siekiant saugoti duomenis galiniame įrenginyje ir keistis informacija su centriniu serveriu.

9. Fizinių asmenų asmens duomenų ir privatumo apsauga

Priminimas. Toliau pateikiamos gairės susijusios su programėle, kurios vienintelė paskirtis yra išaiškinti sąlytį turėjusius asmenis.

PRIV-1	Duomenimis turi būti keičiamasi gerbiant naudotojų privatumą (ir ypač laikantis duomenų kiekio mažinimo principo).
PRIV-2	Programėlė negali suteikti galimybės tiesiogiai nustatyti programėle besinaudojančių naudotojų tapatybę.
PRIV-3	Programėlė negali suteikti galimybės atsekti naudotojų judėjimą.
PRIV-4	Naudodami programėlę, naudotojai neturėtų turėti galimybės sužinoti jokios informacijos apie kitus naudotojus (ir ypač tai, ar jie yra viruso nešiotojai ar ne).
PRIV-5	Negalima visiškai pasikliauti centriniu serveriu. Centrinis serveris turi būti valdomas pagal aiškiai apibrėžtas valdymo taisykles ir taikant visas būtinas priemones jo saugumui užtikrinti. Centrinio serverio lokalizavimas turėtų suteikti galimybę kompetentingai priežiūros institucijai vykdyti veiksmingą priežiūrą.
PRIV-6	Turi būti atliktas ir paviešintas poveikio duomenų apsaugai vertinimas.
PRIV-7	Naudotojui programėlė turėtų atskleisti tik tai, ar jis galėjo užsikrėsti virusu, jei įmanoma, neatskleisdama informacijos apie kitus naudotojus ir apie tai, kiek kartų ir kuriomis datomis jis galėjo užsikrėsti.
PRIV-8	Programėlės perduodama informacija negali suteikti galimybės naudotojams nustatyti virusą nešiojančių asmenų tapatybę ir judėjimą.
PRIV-9	Programėlės perduodama informacija negali suteikti galimybės sveikatos priežiūros institucijoms nustatyti galimai užsikrėsti galėjusių naudotojų tapatybę be jų sutikimo.
PRIV-10	Programėlės centriniam serveriui pateikiamose užklausose negali būti atskleidžiama jokios informacijos apie viruso nešiotoją.
PRIV-11	Programėlės centriniam serveriui pateikiamose užklausose negali būti atskleidžiama jokios nebūtinos informacijos apie naudotoją, išskyrus galbūt tuos atvejus, kai to reikia dėl pseudoniminių identifikatorių ir kontaktų sąrašo, ir tik jei tai yra būtina.
PRIV-12	Negali būti galimybės mėginti susieti duomenis.
PRIV-13	Naudotojai turi turėtų galimybę naudodamiesi programėle naudotis savo teisėmis.
PRIV-14	Pašalinus programėlę, turi būti sunaikinti visi vietoje surinkti duomenys.
PRIV-15	Programėlė turėtų rinkti tik tuos duomenis, kuriuos perduoda tos programėlės ar sąveikių lygiaverčių programėlių klasės egzemplioriai. Nerenkami duomenys, susiję su kitomis programėlėmis ir (arba) artumo principu veikiančiais ryšio įrenginiais.

PRIV-16	Siekiant išvengti, kad centrinis serveris neišanonimintų duomenų, turėtų būti įdiegtas įgaliotasis serveris. Šių *slaptai duomenimis nesidalijančių serverių* paskirtis – sumaišyti kelių naudotojų (tiek viruso nešiotojų, tiek užklausas pateikusių naudotojų atsiųstus) identifikatorius, prieš jais pasidalijant su centriniu serveriu, kad centrinis serveris nesužinotų naudotojų identifikatorių (pvz., IP adresų).
PRIV-17	Programėlė ir serveris turi būti atidžiai kuriami ir konfigūruojami taip, kad nebūtų renkami jokie nebūtini duomenys (pvz., į serverių žurnalus neturėtų būti įtraukiami jokie identifikatoriai ir pan.) ir kad nebūtų naudojamas joks trečiųjų šalių programinės įrangos kūrimo priemonių rinkinys, kuriuo renkami duomenys kitais tikslais.

Patvirtinus, kad naudotojas užsikrėtęs, dauguma aptariamų sąlytį turėjusių asmenų išaiškinimo programėlių veikia iš esmės dviem būdais – jos arba nusiunčia serveriui peržiūrėjus duomenis nustatytų artimų kontaktų istoriją, arba gali nusiųsti savo pačių ištransliuotų identifikatorių sąrašą. Jeigu veikimas grindžiamas šiais dviem būdais, atsisakoma toliau nurodytų principų. Nepaisant to, kad šiame dokumente aptariami būtent šie būdai, tai nereiškia, kad nėra kitų galimų ar tinkamesnių būdų, pvz., kuriuos taikant būtų atliekamas tam tikros formos E2E šifravimas arba taikomos kitos saugumą didinančios arba privatumą saugančios technologijos.

9.1. Principai, kurie taikomi tik, **kai serveriui programėlė nusiunčia sąlytį turėjusių asmenų sąrašą:**

CON-1	Centrinis serveris turi kaupti naudotojų, kuriems nustatyta SARS-CoV-2 infekcija, kontaktų istoriją, jei jie savanoriškų tai leidžia.
CON-2	Centrinis serveris negali nei sudaryti, nei platinti virusą nešiojančių naudotojų pseudoniminių identifikatorių sąrašo.
CON-3	Centriniame serveryje saugoma kontaktų istorija turi būti sunaikinta, kai naudotojams pranešama apie jų buvimą arti asmens, kuriam diagnozuota infekcija.
CON-4	Jokie duomenys negali būti išsiunčiami iš naudotojo įrenginio, išskyrus tuos atvejus, kai naudotojas, kuriam nustatyta infekcija, dalijasi savo kontaktų istorija su centriniu serveriu arba kai naudotojas pateikia serveriui prašymą sužinoti, ar jis galėjo užsikrėsti virusu.
CON-5	Bet koks į vietinę istoriją įtrauktas identifikatorius turi būti sunaikintas praėjus X dienų nuo jo surinkimo (X vertę nustato sveikatos priežiūros institucijos).
CON-6	Skirtingų naudotojų pateiktos kontaktų istorijos neturėtų būti toliau tvarkomos, pvz., abipusiai koreliuojamos, siekiant sukurti visuotinius artumo žemėlapius.
CON-7	Serverio žurnaluose turi būti kuo mažiau duomenų ir jie turi atitikti duomenų apsaugos reikalavimas.

9.2. Principai, kurie taikomi tik, kai serveriui programėlė nusiunčia savo pačios identifikatorių sąrašą:

ID-1	Centrinis serveris turi rinkti identifikatorius, kurie dėl naudotojų, kuriems nustatyta SARS-CoV-2 infekcija, savanoriškų veiksmų siunčiami iš jų programėlės.
ID-2	Centrinis serveris negali nei kaupti, nei platinti virusą nešiojančių naudotojų kontaktų istorijos.
ID-3	Centriniame serveryje saugomi identifikatoriai turi būti panaikinti vos tik jie išsiunčiami į kitas programėles.
ID-4	Jokie duomenys negali būti išsiunčiami iš naudotojo įrenginio, išskyrus tuos atvejus, kai naudotojas, kuriam nustatyta infekcija, dalijasi savo identifikatoriais su centriniu serveriu arba kai naudotojas pateikia serveriui prašymą sužinoti, ar jis galėjo užsikrėsti virusu.
ID-5	Serverio žurnaluose turi būti kuo mažiau duomenų ir jie turi atitikti duomenų apsaugos reikalavimas.