Suunised

# Suunised 04/2020 asukohaandmete ja nakatunuga kokku puutunud isikute kindlakstegemist võimaldavate vahendite kasutamise kohta seoses COVID-19 pandeemiaga

## Vastu võetud 21. aprillil 2020

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

Vastu võetud

# Versioonid

| | | |
|---|---|---|
| Versioon 1.1 | 5. mai 2020 | Väheolulised parandused |
| Versioon 1.0 | 21. aprill 2020 | Suuniste vastuvõtmine |

# Sisukord

**Euroopa Andmekaitsenõukogu,**

võttes arvesse Euroopa Parlamendi ja nõukogu 27. aprilli 2016. aasta määruse (EL) 2016/679 (füüsiliste isikute kaitse kohta isikuandmete töötlemisel ja selliste andmete vaba liikumise ning direktiivi 95/46/EÜ kehtetuks tunnistamise kohta) (edaspidi „isikuandmete kaitse üldmäärus“) artikli 70 lõike 1 punkti e,

võttes arvesse EMP lepingut, eriti selle XI lisa ja protokolli nr 37, mida on muudetud EMP ühiskomitee 6. juuli 2018. aasta otsusega nr 154/2018[1],

võttes arvesse andmekaitsenõukogu töökorra artikleid 12 ja 22,

**ON VASTU VÕTNUD JÄRGMISED SUUNISED**

# 1 SISSEJUHATUS JA TAUST

1 Võitluses COVID-19 pandeemiaga pöörduvad valitsused ja erasektori osalejad andmepõhiste lahenduste poole, mis tekitab mitmeid privaatsusega seotud probleeme.

2 Euroopa Andmekaitsenõukogu toonitab, et andmekaitsealane õigusraamistik on loodud paindlikuna ning võimaldab sellisena ühtaegu nii tõhusat tegutsemist pandeemia piiramisel kui ka inimeste põhiõiguste ja -vabaduste kaitset.

3 Euroopa Andmekaitsenõukogu on kindlal seisukohal, et kui COVID-19 pandeemia ohjeldamiseks on vaja töödelda isikuandmeid, on andmekaitse möödapääsmatu selleks, et tekitada usaldus, luua tingimused mis tahes lahenduse ühiskondlikult vastuvõetavaks muutmiseks ning tagada seeläbi asjaomaste meetmete tõhusus. Kuna viirus ei tunne piire, oleks parem töötada välja ühtne Euroopa lähenemisviis praegusele kriisile reageerimiseks või vähemalt panna paika koostalitlusvõime raamistik.

4 Euroopa Andmekaitsenõukogu on üldiselt seisukohal, et COVID-19 vastu võitlemisel kasutatavad andmed ja tehnoloogia peaksid andma üksikisikutele võimaluse anda oma panus, mitte aitama neid kontrollida, häbimärgistada või represseerida. Ehkki andmed ja tehnoloogia võivad olla olulised abivahendid, on nad oma olemuselt piiratud ning saavad vaid võimendada teiste rahvatervise meetmete tõhusust. Kõik meetmed, mille liikmesriigid või ELi institutsioonid kehtestavad COVID-19 vastu võitlemiseks ning mis hõlmavad isikuandmete töötlemist, peavad lähtuma tõhususe, vajalikkuse ja proportsionaalsuse üldpõhimõtetest.

5 Käesolevates suunistes selgitatakse tingimusi ja põhimõtteid, mis tagavad asukohaandmete ning nakatunuga kokku puutunud isikute kindlakstegemist võimaldavate vahendite proportsionaalse kasutamise kahel konkreetsel eesmärgil:

- asukohaandmete kasutamine, et toetada võitlust pandeemiaga, koostades liikumispiirangute üldise tõhususe hindamiseks viiruse leviku mudeli;
- nakatunuga kokku puutunud isikute kindlakstegemine eesmärgiga teavitada üksikisikuid, kui nad on olnud niisuguse isiku vahetus läheduses, kelle kohta saadakse hiljem kinnitus, et ta kannab viirust. See võimaldab katkestada nakkusahelad võimalikult vara.

6 Nakatunuga kokku puutunud isikute kindlakstegemist võimaldavate mobiilirakenduste tõhusus pandeemia ohjeldamisel sõltub paljudest teguritest (nt nende inimeste osakaalust, kes

1 Kõiki selle dokumendi viiteid liikmesriikidele tuleb mõista kui viiteid EMP liikmesriikidele.

peaksid selle oma seadmesse paigaldama; mõiste „nakatunuga kokku puutunud isiku“ määratlusest, arvestades kokkupuute vahemaad ja kestust). Lisaks sellele peavad niisugused mobiilirakendused moodustama osa terviklikust rahvatervise strateegiast pandeemiaga võitlemisel, sealhulgas testimisest ja sellele järgnevast nakatunuga kokku puutunud isikute automatiseerimata kindlakstegemisest kahtluste välistamiseks. Nende kasutuselevõtuga peaksid kaasnema tugimeetmed, millega tagatakse, et kasutajatele antud teave on kontekstipõhine ning märguannetest on rahvatervise süsteemis kasu. Vastasel juhul ei pruugi rakendused olla nii mõjusad kui võimalik.

7 Euroopa Andmekaitsenõukogu rõhutab, et nii isikuandmete kaitse üldmäärus kui ka direktiiv 2002/58/EÜ (edaspidi „e-privaatsuse direktiiv“) sisaldavad konkreetseid norme, millega on lubatud anonüümsete andmete või isikuandmete kasutamine selleks, et aidata avaliku sektori asutustel ja muudel riigi ja liidu tasandi osalejatel seirata ning piirata SARS-CoV-2 viiruse levikut[2].

8 Sellega seoses on Euroopa Andmekaitsenõukogu juba võtnud seisukoha, mille järgi peaks nakatunuga kokku puutunud isikute kindlakstegemist võimaldavate mobiilirakenduste kasutamine olema vabatahtlik ning need ei tohiks tugineda üksikisikute liikumise jälgimisele, vaid pigem kasutajatevahelist vahemaad kajastavale teabele[3].

[2] Vt Euroopa Andmekaitsenõukogu eelmine avaldus COVID-19 puhangu kohta.
[3] [3] https://edpb.europa.eu/sites/edpb/files/files/file1/edpbletterecadvisecodiv-appguidance_final.pdf.

# 2 ASUKOHAANDMETE KASUTAMINE

## 2.1 Asukohaandmete allikad

9 Viiruse leviku ja liikumispiirangute üldise tõhususe mudeldamiseks on olemas kaks põhilist asukohaandmete allikat:

- asukohaandmed, mida koguvad elektrooniliste sideteenuste osutajad (nt mobiilsideoperaatorid) oma teenuse osutamise käigus, ning
- asukohaandmed, mida kogutakse infoühiskonna teenuste osutajate rakenduste kaudu, kui kõnealuste rakenduste toimimine eeldab niisuguste andmete kasutamist (nt navigatsiooni- või veoteenused jne).

10 Euroopa Andmekaitsenõukogu tuletab meelde, et elektrooniliste sideteenuste osutajatelt kogutud asukohaandmeid[4] võib töödelda üksnes e-privaatsuse direktiivi artiklite 6 ja 9 raames. See tähendab, et neid andmeid võib ametiasutustele või muudele kolmandatele isikutele edastada vaid juhul, kui teenuseosutaja on need anonüümseks muutnud, või kasutaja lõppseadme geograafilist asukohta näitavate andmete puhul, mis ei ole liiklusandmed, kui kasutajad on selleks andnud eelneva nõusoleku[5].

11 Otse lõppseadmest kogutud andmete, sealhulgas asukohaandmete kohta kehtib e-privaatsuse direktiivi artikli 5 lõige 3. Seega on teabe salvestamine kasutaja seadmesse või juba salvestatud teabele juurdepääsu saamine lubatud üksnes juhul, kui i) kasutaja on andnud selleks nõusoleku[6] või ii) salvestamine ja/või juurdepääs on rangelt vajalik infoühiskonna teenuse jaoks, mida kasutaja on sõnaselgelt taotlenud.

12 E-privaatsuse direktiivis ettenähtud õigustest ja kohustustest on selle artikli 15 järgi siiski võimalik kõrvale kalduda, kui see on demokraatlikus ühiskonnas vajalik, otstarbekas ja proportsionaalne abinõu teatud eesmärkide saavutamiseks[7].

13 Niisuguste asukohaandmete uuesti kasutamise korral, mille infoühiskonna teenuse osutaja on kogunud mudeldamise eesmärgil (nt operatsioonisüsteemi või mõne varasemalt paigaldatud rakenduse kaudu), tuleb järgida lisatingimusi. Kui andmed on kogutud kooskõlas e-privaatsuse direktiivi artikli 5 lõikega 3, võib neid edasi töödelda üksnes andmesubjekti täiendaval nõusolekul või liidu või liikmesriigi õigusakti alusel, mis on demokraatlikus ühiskonnas vajalik ja proportsionaalne meede isikuandmete kaitse üldmääruse artikli 23 lõikes 1 nimetatud eesmärkide tagamiseks[8].

## 2.2 Rõhk anonüümitud asukohaandmete kasutamisele

14 Euroopa Andmekaitsenõukogu rõhutab, et asukohaandmete kasutamise korral tuleks alati eelistada anonüümitud andmete, mitte isikuandmete töötlemist.

15 Anonüümimine tähendab, et teatavate meetoditega kaotatakse võimalus seostada mõistlike jõupingutustega andmeid tuvastatud või tuvastatava füüsilise isikuga. Selle mõistlikkuse kriteeriumi puhul tuleb võtta arvesse nii objektiivseid tegureid (aeg, tehnilised vahendid) kui ka konteksti, mis võib iga juhtumi puhul erineda (mingi nähtuse harukordsus, võttes arvesse näiteks rahvastiku tihedust ning andmete laadi ja mahtu). Kui andmed ei vasta sellele kriteeriumile, ei ole need anonüümitud ja seetõttu jäävad need isikuandmete kaitse üldmääruse kohaldamisalasse.

---

[4] Vt e-privaatsuse direktiivi artikli 2 punkt c.
[5] Vt e-privaatsuse direktiivi artiklid 6 ja 9.
[6] E-privaatsuse direktiivis sisalduv nõusoleku mõiste jääb isikuandmete kaitse üldmääruses samaks ning peab vastama kõikidele selle määruse artikli 4 punktis 11 ja artiklis 7 sätestatud nõusoleku nõuetele.
[7] E-privaatsuse direktiivi artikli 15 tõlgendamise kohta vt ka Euroopa Kohtu otsus, 29. jaanuar 2008, Promusicae, C-275/06, ECLI:EU:C:2008:54.
[8] Vt suunised 1/2020 isikuandmete töötlemise kohta seoses ühendatud sõidukitega, punkt 1.5.3.

16 Anonüümimise usaldusväärsuse hindamisel lähtutakse kolmest tingimusest: i) eraldamine (andmete alusel üksikisiku suuremast rühmast eraldamine); ii) seostatavus (sama üksikisikut puudutava kahe andmekogumi omavaheline seostamine) ning iii) järeldamine (üksikisiku kohta mitte teada oleva teabe suure tõenäosusega tuletamine).

17 Anonüümimise mõistest kiputakse valesti aru saama ja sageli aetakse seda segi pseudonüümimisega. Kui anonüümimine võimaldab andmeid kasutada piiranguteta, siis pseudonüümitud andmed jäävad isikuandmete kaitse üldmääruse kohaldamisalasse.

18 Andmete tõhusaks anonüümimiseks on palju võimalusi,[9] kuid siin kehtib üks tingimus. Andmeid ei saa anonüümida eraldi, mis tähendab, et anonüümseks saab muuta vaid andmekogumeid tervikuna. Seega saab igasugust sekkumist ühte andmestruktuuri (krüpteerimise või mis tahes muu matemaatilise muundamise teel) parimal juhul pidada pseudonüümimiseks.

19 Anonüümimisprotsesse ja andmete taasidentifitseerimise katseid uuritakse aktiivselt. Kõik anonüümimislahendusi rakendavad vastutavad töötlejad peavad jälgima selles vallas toimuvat arengut, eriti seoses asukohaandmetega (mis pärinevad telekommunikatsioonivõrgu operaatoritelt ja/või infoühiskonna teenuste osutajatelt), kuna on teada, et neid on ülimalt keeruline anonüümseks muuta.

20 Paljud teadusuuringud on näidanud,[10] et *anonüümituks peetavad asukohaandmed* ei pruugi seda tegelikult olla. Üksikisikute liikumisest jäävad jäljed on olemuslikult omavahel tihedas korrelatsioonis ja kordumatud. Seetõttu võivad need teatud juhtudel olla taasidentifitseerimiskatsete suhtes kaitsetud.

21 Ühte andmestruktuuri, mis jälgib üksikisiku asukohta märkimisväärse ajavahemiku vältel, ei saa täielikult anonüümseks muuta. See võib kehtida ka juhul, kui salvestatud geograafiliste koordinaatide täpsusaste ei ole viidud piisavalt väikseks, kui liikumistee üksikasjad eemaldatakse või isegi kui säilitatakse vaid nende asukohtade andmed, kus andmesubjekt viibib pikka aega. Samuti kehtib see halvasti koondatud asukohaandmete korral.

22 Anonüümimiseks tuleb asukohaandmeid hoolikalt töödelda, et mõistlikkuse kriteerium oleks täidetud. See tähendab, et asukohaandmete kogumeid võetakse tervikuna ja et töödeldakse suhteliselt suure üksikisikute rühma andmeid, kasutades olemasolevaid usaldusväärseid anonüümimismeetodeid, mida tuleb rakendada nõuetekohaselt ja tõhusalt.

23 Võttes arvesse anonüümimise keerukust, on tungivalt soovitatav, et anonüümimise metoodika oleks läbipaistev.

---

[9] De Montjoye, Y.–A. jt, „On the privacy-conscientious use of mobile phone data“, 2018.
[10] De Montjoye, Y.–A. jt, „Unique in the Crowd: The privacy bounds of human mobility“, 2013 ning Pyrgelis, A. jt, „Knock, Who's There? Membership Inference on Aggregate Location Data“, 2017.

# 3 NAKATUNUGA KOKKU PUUTUNUD ISIKUTE KINDLAKSTEGEMIST VÕIMALDAVAD MOBIILIRAKENDUSED

## 3.1 Üldine õiguslik analüüs

24 Süstemaatiline ja ulatuslik asukoha ja/või füüsiliste isikute vaheliste kokkupuudete seire tähendab tõsist sekkumist isikute privaatsusse. Selle saab õiguspäraseks muuta üksnes juhul, kui kasutajad võtavad selle iga eesmärgi puhul kasutusele vabatahtlikult. Eelkõige tähendaks see, et kasutajad, kes otsustavad niisuguseid mobiilirakendusi mitte kasutada või ei saa seda teha, ei tohiks sellepärast kuidagi kannatada.

25 Aruandekohustuse tagamiseks peaks nakatunuga kokku puutunud isikute kindlakstegemist võimaldava mobiilirakenduse vastutav töötleja olema selgelt kindlaks määratud. Euroopa Andmekaitsenõukogu arvates võiks niisuguse rakenduse vastutavaks töötlejaks[11] olla riikide tervishoiuasutused; kaaluda võib ka muid vastutavaid töötlejaid. Alati, kui nakatunuga kokku puutunud isikute kindlakstegemist võimaldavate mobiilirakenduste kasutuselevõtt hõlmab erinevaid osalejaid, peavad nende rollid ja vastutusalad olema kohe selgelt kindlaks määratud ning neid tuleb kasutajatele selgitada.

26 Lisaks sellele, pidades silmas eesmärgi piiramise põhimõtet, peavad eesmärgid olema piisavalt konkreetsed, et välistatud oleks andmete edasine töötlemine COVID-19 haigusest tuleneva rahvatervise kriisi juhtimisega mitteseotud põhjustel (nt kommerts- või õiguskaitsealastel eesmärkidel). Kui eesmärk on selgelt määratletud, tuleb tagada, et isikuandmete kasutamine on asjakohane, vajalik ja proportsionaalne.

27 Nakatunuga kokku puutunud isikute kindlakstegemisel tuleks igakülgselt arvestada võimalikult väheste andmete kogumise ning lõimitud andmekaitse ja vaikimisi andmekaitse põhimõtteid:

- nakatunuga kokku puutunud isikute kindlakstegemist võimaldavate mobiilirakenduste tarbeks ei ole vaja jälgida üksikute kasutajate asukohta. Selle asemel tuleks kasutada lähedusandmeid;
- kuna nakatunuga kokku puutunud isikute kindlakstegemist võimaldavad mobiilirakendused saavad toimida ilma üksikisikuid otseselt tuvastamata, tuleks näha ette sobivad meetmed taasidentifitseerimise vältimiseks;
- kogutud teave peaks asuma kasutaja lõppseadmes ja asjakohast teavet tuleks koguda vaid äärmise vajaduse korral.

28 Andmete töötlemise seaduslikkuse kohta märgib Euroopa Andmekaitsenõukogu, et nakatunuga kokku puutunud isikute kindlakstegemist võimaldavate mobiilirakendustega salvestatakse teavet ja/või saadakse juurdepääs lõppseadmesse salvestatud teabele ning sellise salvestamise ja juurdepääsu suhtes kehtib e-privaatsuse direktiivi artikli 5 lõige 3. Kui sellised toimingud on hädavajalikud selleks, et mobiilirakenduse pakkuja saaks osutada teenust, mida kasutaja on sõnaselgelt taotlenud, ei oleks töötlemiseks kasutaja nõusolekut vaja. Sellisteks toiminguteks, mis ei ole hädavajalikud, peaks rakenduse pakkuja küsima kasutaja nõusoleku.

29 Lisaks sellele märgib Euroopa Andmekaitsenõukogu, et üksnes tõsiasi, et nakatunuga kokku puutunud isikute kindlakstegemist võimaldavaid mobiilirakendusi kasutatakse vabatahtlikult, ei tähenda, et isikuandmete töötlemise aluseks on tingimata nõusolek. Kui avaliku sektori asutused osutavad teenust õigusaktidega neile antud volituse piires ja vastavalt õigusaktidega ettenähtud nõuetele, siis näib kõige asjakohasemaks isikuandmete töötlemise õiguslikuks aluseks olevat avalikes huvides oleva ülesande täitmise vajadus, s.t isikuandmete kaitse üldmääruse artikli 6 lõike 1 punkt e.

[11] Vt ka Euroopa Komisjoni teatis „Andmekaitsega seotud suunised COVID-19 pandeemia vastast võitlust toetavate mobiilirakenduste kohta“, Brüssel, 16.4.2020, C(2020) 2523 final.

30 Isikuandmete kaitse üldmääruse artikli 6 lõikes 3 on selgitatud, et artikli 6 lõike 1 punktis e osutatud isikuandmete töötlemise alus kehtestatakse liidu õigusega või vastutava töötleja suhtes kohaldatava liikmesriigi õigusega. Isikuandmete töötlemise eesmärk määratakse kindlaks selles õiguslikus aluses või see on lõike 1 punktis e osutatud isikuandmete töötlemise osas vajalik avalikes huvides oleva ülesande täitmiseks või vastutava töötleja avaliku võimu teostamiseks[12].

31 Õiguslik alus või seadusandlik meede, mis loob seadusliku aluse nakatunuga kokku puutunud isikute kindlakstegemist võimaldavate mobiilirakenduste kasutamiseks, peaks siiski hõlmama asjakohaseid kaitsemeetmeid, sealhulgas viidet sellele, et mobiilirakenduse kasutamine on vabatahtlik. Selgelt peaks olema ära näidatud eesmärk ja sõnaselgelt märgitud isikuandmete edasise kasutamise piirangud, samuti peab (peavad) üheselt olema kindlaks määratud kaasatud vastutav(ad) töötleja(d). Veel peaks olema määratletud andmete liigid ning üksused, kellele (ja eesmärgid, milleks) isikuandmeid võidakse avaldada. Sõltuvalt sekkumise astmest tuleks rakendada täiendavaid kaitsemeetmeid, võttes arvesse andmete töötlemise laadi, ulatust ja eesmärke. Samuti soovitab Euroopa Andmekaitsenõukogu lisada esimesel võimalusel ka tingimused, millest lähtuvalt määratakse, millal mobiilirakenduse kasutamine lõpetatakse ning milline üksus selle otsuse tegemise eest vastutab.

32 Kui aga andmete töötlemine põhineb muul õiguslikul alusel, näiteks nõusolekul (artikli 6 lõike 1 punkt a),[13] peab vastutav töötleja tagama, et järgitud on asjaomase õigusliku aluse kehtivust käsitlevaid rangeid nõudeid.

33 Lisaks sellele võib mobiilirakenduse kasutamine COVID-19 pandeemiaga võitlemiseks tuua kaasa terviseandmete (nt nakatunu seisundi kohta) kogumise. Niisuguste andmete töötlemine on lubatud, kui see on vajalik rahvatervise valdkonna avalikes huvides, järgides isikuandmete kaitse üldmääruse artikli 9 lõike 2 punktis i[14] sätestatud tingimusi, või tervishoiualastel eesmärkidel kooskõlas nimetatud määruse artikli 9 lõike 2 punktiga h[15]. Sõltuvalt õiguslikust alusest võib töötlemine põhineda ka sõnaselgel nõusolekul (isikuandmete kaitse üldmääruse artikli 9 lõike 2 punkt a).

34 Kooskõlas algse eesmärgiga võimaldab isikuandmete kaitse üldmääruse artikli 9 lõike 2 punkt j ka terviseandmete töötlemist, kui see on vajalik teadusuuringute või statistilisel eesmärgil.

35 Praegust rahvatervise kriisi ei tohiks kasutada võimalusena kehtestada ebaproportsionaalseid andmete säilitamise õigusi. Säilitamise piirangu puhul tuleks võtta arvesse tegelikke vajadusi ja meditsiinilist asjakohasust (muu hulgas võivad selleks olla epidemioloogilised kaalutlused, näiteks peiteaeg jne) ning isikuandmeid tuleks säilitada üksnes COVID-19 kriisi vältel. Pärast seda tuleks kõik isikuandmed üldreeglina kustutada või muuta anonüümseks.

36 Euroopa Andmekaitsenõukogu on seisukohal, et kõnealused mobiilirakendused ei saa asendada, vaid ainult toetada nakatunuga kokku puutunud isikute automatiseerimata kindlakstegemist väljaõppinud tervishoiutöötajate poolt, kes saavad välja selgitada, kas lähikontaktid võisid tõenäoliselt tuua kaasa viiruse edasikandumise või mitte (nt olukorras, kus suheldi kellegagi, kes kasutas nõuetekohaseid kaitsevahendeid, nagu kassapidajad jne, või siis kellegagi, kes selliseid vahendeid ei kasutanud). Euroopa Andmekaitsenõukogu toonitab, et menetlusi ja protsesse, sealhulgas nakatunuga kokku puutunud isikute kindlakstegemist võimaldavates mobiilirakendustes kasutatavaid vastavaid algoritme, tuleks rakendada väljaõppinud personali range järelevalve all, et piirata valepositiivsete ja -negatiivsete

[12] Vt põhjendus 41.

[13] Vastutavad töötlejad (eriti avaliku sektori asutused) peavad pöörama erilist tähelepanu tõigale, et nõusolekut ei tohiks pidada vabatahtlikult antuks, kui inimesel pole tegelikku võimalust teda kahjustavate tagajärgedeta nõusoleku andmisest keelduda või seda tagasi võtta.

[14] Andmete töötlemine peab tuginema liidu või liikmesriigi õigusele, millega nähakse ette sobivad ja konkreetsed meetmed andmesubjekti õiguste ja vabaduste, eelkõige ametisaladuse kaitseks.

[15] Vt isikuandmete kaitse üldmääruse artikli 9 lõike 2 punkt h.

tulemuste esinemist. Eelkõige ei tohiks edasise tegevuse jaoks juhiste andmine põhineda üksnes andmete automatiseeritud töötlemisel.

37 Selleks, et tagada algoritmide erapooletus ja usaldusväärsus ning üldisemalt nende vastavus õigusaktidele, peavad need olema kontrollitavad ja sõltumatud eksperdid peaks neid korrapäraselt üle vaatama. Mobiilirakenduse lähtekood peaks olema avalikult kättesaadav, et saaks teha võimalikult ulatuslikku järelevalvet.

38 Teatud määral tekib alati valepositiivseid tulemusi. Kuna nakatumisohu tuvastamisel võib tõenäoliselt olla üksikisikutele suur mõju (näiteks kohustus jääda kuni negatiivse testitulemuseni isolatsiooni), peab olema võimalik andmeid ja/või hilisemaid analüüsitulemusi parandada. Mõistagi peaks see kehtima üksnes olukordades ja kasutusjuhtudel, mil andmeid töödeldakse ja/või säilitatakse viisil, mille puhul on andmete parandamine tehniliselt võimalik ning eespool nimetatud kahjulikud mõjud tõenäolised.

39 Samuti leiab Euroopa Andmekaitsenõukogu, et enne kõnealuse vahendi kasutuselevõttu tuleb teha andmekaitsealane mõjuhinnang, kuna sedalaadi andmete töötlemist peetakse tõenäoliselt suurt ohtu kujutavaks (terviseandmed, eeldatav laialdane kasutuselevõtt, süstemaatiline seire, uue tehnoloogilise lahenduse kasutamine)[16]. Euroopa Andmekaitsenõukogu soovitab tungivalt andmekaitsealased mõjuhinnangud avaldada.

## 3.2 Soovitused ja funktsionaalsed nõuded

40 Lisaks muudele lõimitud andmekaitse ja vaikimisi andmekaitse meetmetele[17] peaks võimalikult väheste andmete kogumise põhimõtte kohaselt olema töödeldavate andmete maht rangelt minimaalne. Mobiilirakendusega ei tohiks koguda asjakohatut või mittevajalikku teavet, näiteks tsiviilõigusliku seisundi, side identifikaatorite, seadme kataloogiartiklite, sõnumite, kõneregistri, asukohaandmete, seadme identifikaatorite jms kohta.

41 Mobiilirakenduste kaudu edastatavad andmed võivad sisaldada vaid mõningaid kordumatuid ja pseudonüümitud identifikaatoreid, mille on loonud asjaomane mobiilirakendus ja mis on sellele eriomased. Neid identifikaatoreid tuleb uuendada korrapäraselt sagedusega, mis vastab viiruse leviku piiramise eesmärgile ning on piisav, et maandada üksikisikute tuvastamise ja füüsilise jälitamise riski.

42 Nakatunuga kokku puutunud isikute kindlakstegemise lahenduste puhul võidakse järgida tsentraliseeritud või detsentraliseeritud lähenemisviisi[18]. Kui paika on pandud piisavad turvameetmed, võiks mõlemat pidada toimivaks variandiks, sest kummalgi on oma tugevad ja nõrgad küljed. Seega peaks mobiilirakenduse väljatöötamise kontseptuaalses etapis alati põhjalikult kaaluma mõlemat lähenemisviisi, võttes igakülgselt arvesse kummagi mõju andmekaitsele/privaatsusele ja võimalikke tagajärgi üksikisikute õigustele.

43 Kõik nakatunuga kokku puutunud isikute kindlakstegemise süsteemi kaasatud serverid võivad koguda üksnes sellise kasutaja kokkupuudete ajalugu või pseudonüümitud identifikaatoreid, kes on tervishoiuasutuse nõuetekohase hindamise ja oma vabatahtliku toimingu tulemusena saanud nakkuse diagnoosi. Teise võimalusena säilitatakse serveris kas nakatunud kasutaja pseudonüümitud identifikaatoreid või tema kokkupuudete ajalugu üksnes seni, kuni võimalikke nakatunud kasutajaid teavitatakse nende kokkupuutest viirusega, ning serverid ei tohiks püüda võimalikke nakatunud kasutajaid tuvastada.

---

[16] Vt artikli 29 alusel asutatud andmekaitse töörühma suunised (vastu võtnud Euroopa Andmekaitsenõukogu), mis käsitlevad andmekaitsealast mõjuhinnangut ja selle kindlaksmääramist, kas isikuandmete töötlemise tulemusena „tekib tõenäoliselt suur oht“ vastavalt määrusele (EL) 2016/679.

[17] Vt Euroopa Andmekaitsenõukogu suunised 4/2019 artikli 25 lõimitud andmekaitse ja vaikimisi andmekaitse kohta.

[18] Üldjuhul on detsentraliseeritud lahendus paremini kooskõlas võimalikult väheste andmete kogumise põhimõttega.

44 Nakatunuga kokku puutunud isikute kindlakstegemise üleüldise metoodika (mis hõlmab nii mobiilirakendusi kui ka selliste isikute automatiseerimata väljaselgitamist) kehtestamisel võib teatud juhtudel olla vaja töödelda lisaandmeid. Sellised lisaandmed peaksid jääma kasutaja lõppseadmesse ning neid tuleks töödelda üksnes juhul, kui see on hädavajalik ja kasutaja on selleks eelnevalt andnud oma sõnaselge nõusoleku.

45 Serverites ja mobiilirakendustes salvestatud andmete ning mobiilirakenduste ja eemalasuva serveri vahelise andmevahetuse turvalisuse tagamiseks tuleb kasutada tehnika tasemele vastavaid krüptomeetodeid. Samuti peab mobiilirakenduse ja serveri vahel toimuma vastastikune autentimine.

46 Kasutajatest kui SARS-CoV-2 viirusesse nakatunutest teavitamine mobiilirakenduse kaudu peab toimuma nõuetekohase autoriseerimisega, näiteks ühekordselt kasutatava koodiga, mis on seotud nakatunu pseudonüümitud isikuga ja ühendatud testimiskoha või tervishoiutöötajaga. Kui kinnitust ei ole võimalik saada turvaliselt, ei tohiks toimuda niisugust andmetöötlust, mille puhul eeldatakse kasutaja seisundi kehtivust.

47 Vastutav töötleja koostöös avaliku sektori asutustega peab selgelt ja otsesõnu teavitama lingist, mille kaudu saab alla laadida nakatunuga kokku puutunud isikute kindlakstegemist võimaldava ametliku riikliku mobiilirakenduse, eesmärgiga vähendada riski, et inimesed kasutavad kolmandate isikute loodud mobiilirakendusi.

# 4 KOKKUVÕTE

48 Maailm seisab silmitsi märkimisväärse rahvatervise kriisiga, mis nõuab kindlat ja praegusest eriolukorrast kaugemale ulatuvate tagajärgedega tegutsemist. Andmete automatiseeritud töötlemine ja digitehnoloogiad võivad olla COVID-19 haiguse vastu võitlemisel äärmiselt olulised. Siiski tuleb olla valvas, et nende rakendamine ei oleks pöördumatu. Meie kohustus on tagada, et kõik selles erandlikus olukorras võetud meetmed on vajalikud, ajutised ja võimalikult väikese ulatusega, et neid vaadatakse korrapäraselt ja reaalselt üle ning neile antakse teaduslik hinnang.

49 Euroopa Andmekaitsenõukogu toonitab, et ei ole vaja valida kriisile tõhusa reageerimise ja põhiõiguste kaitse vahel: mõlema saavutamine on võimalik ning andmekaitse põhimõtetel võib viirusevastases võitluses olla väga oluline roll. Euroopa andmekaitseõigus võimaldab isikuandmete vastutustundlikku kasutamist tervisekorralduslikel eesmärkidel, tagades ühtlasi, et selle käigus ei kahjustata üksikisikute õigusi ega vabadusi.

Euroopa Andmekaitsenõukogu nimel

eesistuja

(Andrea Jelinek)

# LISA – NAKATUNUGA KOKKU PUUTUNUD ISIKUTE KINDLAKSTEGEMIST VÕIMALDAVAD MOBIILIRAKENDUSED ANALÜÜSIJUHEND

## 0. Märkus

Juhend ei ole ei normatiivne ega ammendav ning selle ainus eesmärk on anda nakatunuga kokku puutunud isikute kindlakstegemist võimaldavate mobiilirakenduste väljatöötajatele ja kasutusse võtjatele üldisi juhiseid. Kasutada võib ka muid lahendusi peale siinkirjeldatute ning need võivad olla seaduslikud, kui need on kooskõlas asjakohase õigusraamistikuga (s.t isikuandmete kaitse üldmääruse ja e-privaatsuse direktiiviga).

Samuti tuleb märkida, et käesolev juhend on oma laadilt üldine. Seetõttu ei tohi selles dokumendis sisalduvaid soovitusi ja kohustusi käsitada ammendavatena. Igasugune hindamine peab olema juhtumipõhine ning konkreetsete mobiilirakenduste puhul võib osutuda vajalikuks käesolevas juhendis käsitlemata lisameetmete võtmine.

## 1. Ülevaade

Paljudes liikmesriikides kaaluvad sidusrühmad *nakatunuga kokku puutunud isikute kindlakstegemist* võimaldavate mobiilirakenduste kasutamist, et võimaldada inimestel saada teada oma kokkupuutest SARS-CoV-2 viirusesse nakatunud inimesega.

Veel ei ole kehtestatud tingimusi, mille alusel sedalaadi mobiilirakendused saaks aidata tõhusalt kaasa pandeemia ohjeldamisele. Need tingimused tuleks kehtestada enne niisuguse mobiilirakenduse kasutuselevõttu. Sellele vaatamata tuleb rakenduste arendamisega tegelevatele töörühmadele anda asjakohast teavet sisaldavaid suuniseid, et isikuandmete kaitse oleks tagatud alates varajasest väljatöötamisetapist.

Juhime tähelepanu, et käesolev juhend on oma laadilt üldine. Seetõttu ei tohi käsitada selles dokumendis sisalduvaid soovitusi ja kohustusi ammendavatena. Igasugune hindamine peab olema juhtumipõhine ning konkreetsete mobiilirakenduste puhul võib osutuda vajalikuks käesolevas juhendis käsitlemata lisameetmete võtmine. Juhendi eesmärk on anda nakatunuga kokku puutunud isikute kindlakstegemist võimaldavate mobiilirakenduste väljatöötajatele ja kasutusse võtjatele üldisi suuniseid.

Mõned kriteeriumid võivad olla rangemad kui andmekaitseraamistikust tulenevad nõuded. Nende eesmärk on tagada suurim läbipaistvus, et soodustada nakatunuga kokku puutunud isikute kindlakstegemist võimaldavate mobiilirakenduste ühiskondlikku vastuvõetavust.

Selleks peaks nakatunuga kokku puutunud isikute kindlakstegemist võimaldavate mobiilirakenduste omanikud arvestama alljärgnevate tingimustega.

- Sedalaadi mobiilirakenduse kasutamine peab olema rangelt vabatahtlik. See ei tohi olla õigusaktidega tagatud õiguste kasutamise tingimuseks. Üksikisikule peab alati jääma täielik kontroll oma andmete üle ja tal peaks olema võimalik vabalt valida, kas mobiilirakendust kasutada.

- Nakatunuga kokku puutunud isikute kindlakstegemist võimaldavate mobiilirakendustega tekib tõenäoliselt suur oht füüsiliste isikute õigustele ja vabadustele ning see nõuab andmekaitsealase mõjuhinnangu koostamist enne rakenduse kasutuselevõttu.
- Teavet mobiilirakenduse kasutajate vahelise vahemaa kohta saab hankida ilma kasutajate asukohta tuvastamata. Niisuguse mobiilirakenduse tarbeks ei ole vaja asukohaandmeid ja seega ei tohiks neid rakenduses ka kasutada.
- Kui kasutajal diagnoositakse SARS-CoV-2 nakkus, tuleks teavitada üksnes isikuid, kellega asjaomane kasutaja on olnud lähikontaktis nakatunuga kokku puutunud isikute kindlakstegemist võimaldavate andmete epidemioloogiliselt asjakohase säilitamisperioodi jooksul.
- Sõltuvalt mobiilirakenduseks valitud arhitektuurist võib selle toimimiseks olla vajalik keskserveri kasutamine. Sellisel juhul peab keskserveris töödeldavate andmete maht piirduma rangelt minimaalsega kooskõlas võimalikult väheste andmete kogumise ja lõimitud andmekaitse põhimõtetega.
    - Kui kasutajal diagnoositakse nakkus, võib teavet tema varasemate lähikontaktide või kasutaja mobiilirakenduse kaudu edastatud identifikaatorite kohta koguda üksnes kasutaja nõusolekul. Ette peab olema nähtud kontrollimeetod, mis võimaldab isiku nakatumist kinnitada ilma kasutajat tuvastamata. Tehniliselt oleks see võimalik, kui nakatunuga kokku puutunud isikuid teavitatakse alles pärast tervishoiutöötaja sekkumist, näiteks spetsiaalse ühekordselt kasutatava koodi abil.
    - Keskserverisse salvestatud teave ei tohiks võimaldada vastutaval töötlejal tuvastada kasutajaid, kes on saanud nakkuse diagnoosi või on olnud niisuguste kasutajatega lähikontaktis, ega teha järeldusi selliste kokkupuutemustrite kohta, mida ei ole vaja asjakohaste kontaktide kindlakstegemiseks.
- Niisuguste mobiilirakenduste toimimiseks on vaja edastada andmeid, mida loevad teiste kasutajate seadmed, ja neid vastu võtta.
    - Piisab, kui kasutajate mobiilsete seadmete (arvutite, tahvelarvutite, andmesideühendusega kellade jne) vahel vahetatakse pseudonüümitud identifikaatoreid, edastades neid näiteks väikese energiatarbega Bluetoothi tehnoloogia abil.
    - Identifikaatorid tuleb luua tehnika tasemele vastavate krüptomeetoditega.
    - Identifikaatoreid tuleb korrapäraselt uuendada, et vähendada füüsilise jälitamise ja andmete seostamise ohtu.
- Niisugune mobiilirakendus peab ohutu tehnilise toimimise tagamiseks olema turvatud. Eelkõige tuleb silmas pidada järgmist.
    - Mobiilirakendusega ei tohiks edastada kasutajatele teavet, mis võimaldab neil järeldada teiste kasutajate isikusamasust või diagnoosi. Keskserver ei tohi kasutajaid tuvastada ega tuletada teavet nende kohta.

**Märkus.** Eespool toodud põhimõtted on seotud üksnes *nakatunuga kokku puutunud isikute kindlakstegemist* võimaldavate mobiilirakenduste väidetava eesmärgiga, milleks on vaid viirusega potentsiaalselt kokku puutunud inimeste automaatne teavitamine (ilma neid tuvastamata).

Mobiilirakenduse operaatoreid ja selle taristut võib kontrollida pädev järelevalveasutus. Nende suuniste täielikust või osalisest järgimisest ei pruugi piisata andmekaitseraamistikuga täieliku kooskõla tagamiseks.

## 2. Mõisted

| | |
|---|---|
| **Nakatunuga kokku puutunud isik** | Nakatunuga kokku puutunud isikute kindlakstegemist võimaldava mobiilirakenduse tähenduses on nakatunuga kokku puutunud isik kasutaja, kes on suhelnud kinnitatult viirusekandjaks osutunud kasutajaga ning kelle kokkupuute kestus ja kaugus on tekitanud olulise viirusesse nakatumise ohu. Inimestevahelise kokkupuute kestuse ja kauguse näitajaid peavad hindama tervishoiuasutused ning need võib määrata mobiilirakenduses. |
| **Asukohaandmed** | Kõik andmed, mida töödeldakse elektroonilise side võrgus või elektroonilise side teenuse abil ning mis näitavad üldkasutatavate elektrooniliste sideteenuste (e-privaatsuse direktiivi tähenduses) kasutaja lõppseadme geograafilist asukohta, samuti võimalikest muudest allikatest pärit andmed, mis puudutavad:<br>– lõppseadme asukoha laiuskraadi, pikkuskraadi või kõrgust merepinnast;<br>– kasutaja teekonna suunda või<br>– asukohaandmete salvestamise aega. |
| **Suhtlus** | Nakatunuga kokku puutunud isikute kindlakstegemist võimaldava mobiilirakenduse tähenduses on suhtlus kahe teineteise vahetus läheduses (ruumiliselt ja ajaliselt) asuva seadme vaheline kasutatava sidetehnoloogia (nt Bluetooth) ulatuses toimuv teabevahetus. See määratlus ei hõlma nende kahe suhtluses osaleva kasutaja asukohta. |
| **Viirusekandja** | Selles dokumendis käsitatakse viirusekandjana kasutajaid, kelle viiruseanalüüs on osutunud positiivseks ja kes on saanud arstilt või tervishoiuasutuselt ametliku diagnoosi. |
| **Nakatunuga kokku puutunud isikute kindlakstegemine** | Inimestel, kes on lähedalt kokku puutunud (vastavalt epidemioloogide määratavatele kriteeriumitele) viirusesse nakatunud inimesega, on tõsine oht samuti nakatuda ja omakorda teisi nakatada.<br>Nakatunuga kokku puutunud isikute kindlakstegemine on haigustõrje metoodika, mille raames koostatakse loetelu kõikidest inimestest, kes on olnud viirusekandja vahetus läheduses, eesmärgiga kontrollida, kas neil on oht nakatuda, ning võtta nende suhtes asjakohaseid sanitaarmeetmeid. |

## 3. Üldteave

| | |
|---|---|
| GEN-1 | Mobiilirakendus peab täiendama traditsioonilisi nakatunuga kokku puutunud isikute kindlakstegemise meetodeid (eelkõige nakatunute küsitlemist), s.t moodustama osa laiaulatuslikumast rahvatervise programmist. Seda tohib kasutada üksnes hetkeni, mil uute nakatumiste hulka arvestades tullakse nakatunuga kokku puutunud isikute kindlakstegemisel toime vaid automatiseerimata meetoditega. |
| GEN-2 | Hiljemalt siis, kui pädevad ametiasutused otsustavad taastada n-ö normaalse olukorra, tuleb paika panna kord identifikaatorite kogumise lõpetamiseks (mobiilirakenduse üldine deaktiveerimine, juhised mobiilirakenduse desinstallimiseks, automaatne desinstallimine jne) ning mis tahes andmebaasidest (mobiilirakendused ja serverid) kõikide kogutud andmete kustutamise alustamiseks. |
| GEN-3 | Mobiilirakenduse ja selle tagasüsteemi lähtekood peavad olema avatud ning tehniline spetsifikatsioon peab olema avalik, et kõik huvitatud isikud saaksid koodi kontrollida ning vajaduse korral aidata kaasa koodi täiustamisele, võimalike programmivigade parandamisele ja isikuandmete töötlemise läbipaistvuse tagamisele. |
| GEN-4 | Mobiilirakenduse kasutuselevõtu etapid peavad võimaldama järk-järgult kinnitada selle tõhusust rahvatervise seisukohalt. Sel eesmärgil peab varajases etapis olema koostatud hindamiseeskiri, mis sisaldab rakenduse tõhusust mõõta võimaldavaid näitajaid. |

## 4. Eesmärgid

| | |
|---|---|
| PUR-1 | Mobiilirakenduse ainus eesmärk peab olema nakatunuga kokku puutunud isikute kindlakstegemine, et inimesi, kes võivad olla kokku puutunud SARS-CoV-2 viirusega, saaks sellest teavitada ja nende eest oleks võimalik hoolt kanda. Seda ei tohi kasutada muul eesmärgil. |
| PUR-2 | Mobiilirakenduse esmasest kasutuseesmärgist ei tohi kõrvale kalduda, et jälgida karantiinimeetmetest või liikumispiirangust ja/või suhtlemisdistantsi nõudest kinnipidamist. |
| PUR-3 | Mobiilirakendust ei tohi kasutada selleks, et teha järeldusi kasutajate asukoha kohta, lähtudes suhtlusest ja/või muudest alustest. |

## 5. Funktsionaalsed kaalutlused

| | |
|---|---|
| FUNC-1 | Mobiilirakendus peab võimaldama kasutajaid teavitada asjaolust, et nad võivad olla kokku puutunud viirusega, kusjuures see teave põhineb tõigal, et nad on olnud nakatunud kasutaja läheduses X päeva enne positiivse analüüsitulemuse saamist (X-i väärtuse määravad tervishoiuasutused). |

| | |
|---|---|
| FUNC-2 | Mobiilirakendus peaks andma soovitusi kasutajatele, kelle puhul on tuvastatud võimalik kokkupuude viirusega. See peaks edastama juhiseid meetmete kohta, mida need kasutajad peaksid võtma, ning võimaldama kasutajal nõu küsida. Sellistel juhtudel oleks inimese sekkumine kohustuslik. |
| FUNC-3 | Algoritm, mis mõõdab nakatumise ohtu, võttes arvesse vahemaad ja aega ning tehes seejärel otsuse, millal tuleb kokkupuude kanda nakatunuga kokku puutunud isikute nimekirja, peab olema turvaliselt kohandatav, et arvesse saaks võtta kõige värskemaid teadmisi viiruse levimise kohta. |
| FUNC-4 | **Kasutajaid tuleb viiruse peiteaja jooksul teavitada, kui nad on viirusega kokku puutunud**, või nad peavad saama korrapäraselt teavet selle kohta, kas nad on viirusega kokku puutunud. |
| FUNC-5 | Mobiilirakendus peaks olema teistes liikmesriikides väljatöötatud mobiilirakendustega koostalitlusvõimeline, et eri liikmesriikides reisivaid kasutajaid saaks tõhusalt teavitada. |

## 6. Andmed

| | |
|---|---|
| DATA-1 | Mobiilirakendus peab suutma andmeid edastada ja vastu võtta lähisidetehnoloogia, näiteks väikese energiatarbega Bluetoothi tehnoloogia abil, et oleks võimalik nakatunuga kokku puutunud isikuid kindlaks teha. |
| DATA-2 | Edastatavad andmed peavad sisaldama tugevalt krüpteeritud pseudojuhuslikke identifikaatoreid, mille on loonud asjaomane mobiilirakendus ja mis on sellele eriomased. |
| DATA-3 | Pseudojuhuslike identifikaatorite kollisiooni oht peaks olema piisavalt väike. |
| DATA-4 | Pseudojuhuslikke identifikaatoreid tuleb korrapäraselt uuendada sagedusega, mis on küllaldane, maandamaks riski, et keegi, sealhulgas keskserveri pidaja, teised mobiilirakenduse kasutajad või pahatahtlikud kolmandad isikud saaksid üksikisikuid taasidentifitseerida, füüsiliselt jälitada või andmetega seostada. Kasutaja mobiilirakendus peab need identifikaatorid looma näiteks keskserveri antud lähteväärtuse põhjal. |
| DATA-5 | Võimalikult väheste andmete kogumise põhimõtte kohaselt ei tohi mobiilirakendus koguda muid andmeid peale nende, mis on hädavajalikud nakatunuga kokku puutunud isikute kindlakstegemiseks. |
| DATA-6 | Mobiilirakendus ei tohi koguda nakatunuga kokku puutunud isikute kindlakstegemiseks asukohaandmeid. Asukohaandmeid võib töödelda üksnes selleks, et võimaldada mobiilirakendusel suhelda samalaadsete mobiilirakendustega teistes riikides, ning nende täpsusaste peaks piirduma üksnes selle eesmärgi saavutamiseks hädavajalikuga. |
| DATA-7 | Mobiilirakendus ei tohiks koguda muid terviseandmeid peale nende, mis on rakenduse eesmärgi saavutamiseks hädavajalikud, välja arvatud vabatahtlikkuse alusel ja üksnes selleks, et aidata kaasa kasutaja teavitamise otsuse tegemisele. |

| | |
|---|---|
| DATA-8 | Kasutajaid peab teavitama kõikidest kogutavatest isikuandmetest. Neid andmeid võiks koguda üksnes kasutaja loal. |

## 7. Tehnilised omadused

| | |
|---|---|
| TECH-1 | Mobiilirakenduses tuleks rakenduse aktiveerinud seadme lähedal asuvate kasutajate avastamiseks kasutada olemasolevat tehnoloogiat, nagu lähisidetehnoloogia (nt väikese energiatarbega Bluetooth). |
| TECH-2 | Mobiilirakendus peaks säilitama seadmes kasutaja kokkupuudete ajalugu eelnevalt kindlaksmääratud ajavahemiku vältel. |
| TECH-3 | Mobiilirakendus võib mõningate oma funktsioonide rakendamisel tugineda keskserverile. |
| TECH-4 | Mobiilirakenduse arhitektuur peab tuginema võimalikult suures ulatuses kasutajate seadmetele. |
| TECH-5 | Kui kasutaja kohta on teatatud, et ta on viirusesse nakatunud, tuleks selle kasutaja algatusel ja pärast nõuetekohaselt sertifitseeritud tervishoiutöötaja sellekohast kinnitust saata kasutaja kokkupuudete ajalugu või tema identifikaatorid keskserverisse. |

## 8. Turvalisus

| | |
|---|---|
| SEC-1 | SARS-CoV-2 viirusesse nakatumisest teatanud kasutajate seisundit tuleb kontrollida, luues näiteks ühekordselt kasutatava koodi, mis on seotud testimiskoha või tervishoiutöötajaga. Kui kinnitust ei ole võimalik saada turvaliselt, ei tohi andmeid töödelda. |
| SEC-2 | Keskserverisse tuleb andmeid edastada turvalise kanali kaudu.<br>Operatsioonisüsteemi platvormide pakutavate teavitusteenuste kasutamist tuleks hoolikalt hinnata ning selle tulemusena ei tohiks kolmandatele isikutele avaldada mingeid andmeid. |
| SEC-3 | Päringud ei tohi olla pahatahtliku kasutaja manipulatsioonide suhtes kaitsetud. |
| SEC-4 | Mobiilirakenduse ja serveri vahelise ning rakendustevahelise teabevahetuse turvalisuse tagamiseks, samuti mobiilirakendustesse ja serverisse salvestatud teabe üldiseks kaitsmiseks tuleb kasutada tehnika tasemele vastavaid krüptomeetodeid. Näiteks võib kasutada: sümmeetrilist ja asümmeetrilist krüpteerimist, räsifunktsioone, privaatse liikmesuse testi (*private membership test*), hulkade ühisosa leidmist (*private set intersection*), Bloomi filtreid, teabe privaatset hankimist (*private information retrieval*), homomorfset krüpteerimist jne. |
| SEC-5 | Keskserver ei tohi säilitada ühegi kasutaja võrguühenduse identifikaatoreid (nt IP-aadresse), sealhulgas nende kasutajate võrguühenduse identifikaatoreid, kes on saanud viiruse diagnoosi ning kes on edastanud oma kokkupuudete ajaloo või oma identifikaatorid. |

| | |
|---|---|
| SEC-6 | Selleks, et vältida teise isikuna esinemist või võltskasutajate loomist, peab server mobiilirakenduse autentima. |
| SEC-7 | Mobiilirakendus peab autentima keskserveri. |
| SEC-8 | Serveri funktsioonid peavad olema kaitstud kordusrünnete eest. |
| SEC-9 | Keskserveri edastatud teave peab olema allkirjastatud, et oleks võimalik tuvastada selle päritolu ja usaldusväärsust. |
| SEC-10 | Kõikidele keskserverisse salvestatud andmetele, mis ei ole avalikult kättesaadavad, peab olema juurdepääs üksnes volitatud isikutel. |
| SEC-11 | Operatsioonisüsteemi tasandil võib seadme loahaldur taotleda üksnes selliseid lube, mis on tarvilikud vajaduse korral sidemoodulitele ligipääsuks ja nende kasutamiseks, andmete lõppseadmesse salvestamiseks ning teabevahetuseks keskserveriga. |

## 9. Füüsiliste isikute isikuandmete ja privaatsuse kaitse

*Meeldetuletus. Suunised puudutavad mobiilirakendust, mille ainus eesmärk on nakatunuga kokku puutunud isikute kindlakstegemine.*

| | |
|---|---|
| PRIV-1 | Andmevahetuse käigus tuleb austada kasutajate privaatsust (eelkõige järgida võimalikult väheste andmete kogumise põhimõtet). |
| PRIV-2 | Mobiilirakendus ei tohi võimaldada selle kasutamise käigus kasutajaid otseselt tuvastada. |
| PRIV-3 | Mobiilirakendus ei tohi võimaldada jälgida kasutajate liikumist. |
| PRIV-4 | Mobiilirakenduse kasutamine ei tohiks võimaldada kasutajatel saada mingit teavet teiste kasutajate kohta (eelkõige seda, kas teine kasutaja on viirusekandja). |
| PRIV-5 | Usaldus keskserveri vastu peab olema piiratud. Keskserveri haldajad peavad järgima selgelt määratletud juhtimiseeskirju ja võtma kõiki vajalikke meetmeid serveri turvalisuse tagamiseks. Keskserveri asukoht peaks võimaldama pädevatel järelevalveasutustel teha tõhusat järelevalvet. |
| PRIV-6 | Koostada tuleb andmekaitsealane mõjuhinnang ja see tuleks avalikustada. |
| PRIV-7 | Mobiilirakendus peaks kasutajale avaldama üksnes selle, kas ta on viirusega kokku puutunud, ning kokkupuudete arvu ja kuupäevad, kui see on võimalik ilma teiste kasutajate kohta andmeid avaldamata. |
| PRIV-8 | Mobiilirakenduse edastatav teave ei tohi võimaldada kasutajatel tuvastada viirusekandjatest kasutajaid ega nende liikumist. |
| PRIV-9 | Mobiilirakenduse edastatav teave ei tohi võimaldada tervishoiuasutustel tuvastada kasutajaid, kes võivad olla viirusega kokku puutunud, ilma nende nõusolekuta. |
| PRIV-10 | Päringud, mida mobiilirakendus keskserverile saadab, ei tohi avaldada mingeid andmeid viirusekandja kohta. |
| PRIV-11 | Päringud, mida mobiilirakendus keskserverile saadab, ei tohi avaldada mittevajalikke andmeid kasutaja kohta, välja arvatud võib-olla ja üksnes vajaduse korral tema pseudonüümitud identifikaatorid ja kokkupuudete nimekiri. |
| PRIV-12 | Andmete seostamise ründed ei tohi olla võimalikud. |
| PRIV-13 | Kasutajatel peab olema võimalik kasutada oma õigusi mobiilirakenduse kaudu. |
| PRIV-14 | Mobiilirakenduse kustutamise tulemusena peavad kustuma kõik kohapeal kogutud andmed. |
| PRIV-15 | Mobiilirakendus peaks koguma üksnes andmeid, mille on edastanud see mobiilirakendus või samaväärsed koostalitlevad mobiilirakendused. Koguda ei tohi andmeid, mis on seotud teiste mobiilirakendustega ja/või lähisideseadmetega. |
| PRIV-16 | Selleks, et välistada taasidentifitseerimine keskserveris, tuleks kasutada vaheservereid. Nende *läbipaistvate serverite* eesmärk on segada omavahel ära mitme kasutaja (nii viirusekandjate kui ka päringu esitajate) identifikaatorid enne |

| | |
|---|---|
| | nende jagamist keskserveriga, et vältida olukorda, kus keskserver teab kasutajate identifikaatoreid (nt IP-aadresse). |
| PRIV-17 | Mobiilirakendus ja server on vaja hoolikalt välja arendada ning konfigureerida, et ei kogutaks tarbetuid andmeid (nt serveri logifailides ei tohiks sisalduda ühtegi identifikaatorit jne) ja oleks välistatud võimalus, et kolmanda isiku tarkvaraarenduskomplektiga kogutakse andmeid muul eesmärgil. |

Suurem osa praegu arutluse all olevatest nakatunuga kokku puutunud isikute kindlakstegemist võimaldavatest mobiilirakendustest kasutab põhimõtteliselt kahte lahendust, kui kasutaja tunnistatakse nakatunuks: need võivad saata serverisse kogutud lähikokkupuudete ajaloo või oma identifikaatorite nimekirja. Alljärgnevad põhimõtted on esitatud vastavalt nendele kahele lahendusele. Ehkki käesolevas dokumendis on käsitletud neid lahendusi, ei tähenda see, et muud variandid ei oleks võimalikud või isegi paremad, näiteks mingit laadi otspunktkrüpteerimist või muid turvalisust või privaatsust suurendavaid tehnoloogiaid kasutavad lahendused.

### 9.1. Põhimõtted, mis kehtivad üksnes juhul, kui mobiilirakendus saadab serverisse kokkupuudete nimekirja

| | |
|---|---|
| CON-1 | Keskserver peab koguma SARS-CoV-2 viirusesse nakatunud kasutajate kokkupuudete ajalugusid asjaomaste kasutajate vabatahtliku toimingu tulemusena. |
| CON-2 | Keskserver ei tohi säilitada ega levitada viirusekandjatest kasutajate pseudonüümitud identifikaatorite nimekirja. |
| CON-3 | Keskserveris salvestatud kokkupuudete ajalugu tuleb kustutada kohe, kui kasutajaid on teavitatud lähikokkupuutest haiguse diagnoosi saanud isikuga. |
| CON-4 | Kasutaja seadmest võib andmeid välja saata üksnes juhul, kui haiguse diagnoosi saanud kasutaja jagab oma kokkupuudete ajalugu keskserveriga või kui kasutaja esitab serverile päringu eesmärgiga selgitada välja oma võimalik kokkupuude viirusega. |
| CON-5 | Kõik kohalike andmete ajaloos sisalduvad identifikaatorid tuleb kustutada X päeva möödumisel nende kogumisest (X-i väärtuse määravad tervishoiuasutused). |
| CON-6 | Kasutajate esitatud kokkupuudete ajalugu ei tohiks täiendavalt töödelda, näiteks viia korrelatsiooni, et luua üldisi lähikokkupuudete kaarte. |
| CON-7 | Serveri logifailides peab sisalduma võimalikult vähe andmeid ja logifailide puhul tuleb täita andmekaitsenõudeid. |

### 9.2. Põhimõtted, mis kehtivad üksnes juhul, kui mobiilirakendus saadab serverisse oma identifikaatorite nimekirja

| | |
|---|---|
| ID-1 | Keskserver peab koguma SARS-CoV-2 viirusesse nakatunud kasutajate mobiilirakenduse edastatud identifikaatoreid asjaomaste kasutajate vabatahtliku toimingu tulemusena. |
| ID-2 | Keskserver ei tohi säilitada ega levitada viirusekandjatest kasutajate kokkupuudete ajalugu. |
| ID-3 | Keskserverisse salvestatud identifikaatorid tuleb kustutada kohe pärast nende edastamist teistele mobiilirakendustele. |
| ID-4 | Kasutaja seadmest võib andmeid välja saata üksnes juhul, kui haiguse diagnoosi saanud kasutaja jagab oma identifikaatoreid keskserveriga või kui kasutaja esitab serverile päringu eesmärgiga selgitada välja oma võimalik kokkupuude viirusega. |
| ID-5 | Serveri logifailides peab sisalduma võimalikult vähe andmeid ja logifailide puhul tuleb täita andmekaitsenõudeid. |