

II

(Teatiseid)

EUROOPA LIIDU INSTITUTSIOONIDE, ORGANITE JA ASUTUSTE TEATISED

EUROOPA KOMISJON

KOMISJONI TEATIS

Andekaitsega seotud suunised COVID-19 pandeemia vastast võitlust toetavate mobiilirakenduste kohta

(2020/C 124 I/01)

1 TAUST

COVID-19 pandeemia on enneolematu väljakutse liidule ja liikmesriikidele, meie tervishoiusüsteemidele, eluviisile, majanduslikule stabiilsusele ja väärtustele. Digitehnoloogial ja -andmetel on COVID-19 kriisiga võitlemises väärtuslik roll. Liikmesriikide ja ELi tasandi rahvaterviseasutustel võib olla COVID-19 pandeemia leviku jälgimisel ja tõkestamisel abi eelkõige nutitelefonidele paigaldatud mobiilirakendustest ning need on eriti asjakohased pandeemia leviku tõkestamise meetmete kaotamise etapis. Mobiilirakenduste kaudu saab anda kodanikele vahetult suuniseid ja toetada kontaktide jälgimist. Nii ELis kui ka mujal maailmas on paljud riiklikud ja piirkondlikud ametiasutused või tarkvaraarendajad teatanud mitmesuguste funktsioonidega mobiilirakenduste loomisest, mille eesmärk on toetada võitlust viirusega.

8. aprillil 2020 võttis komisjon vastu soovituseliidu ühise meetmekogumi kohta, mis võimaldab kasutada tehnoloogiat ja andmeid COVID-19 kriisi vastu võitlemiseks ja kriisist väljumiseks, eelkõige seoses mobiilirakendustega ja anonüümsete liikuvusandmete kasutamisega (edaspidi „soovitus“) ⁽¹⁾. Soovituse eesmärk on muu hulgas välja kujundada Euroopa ühine lähenemisviis (meetmekogum) selliste ELi tasandil koordineeritavate mobiilirakenduste kasutamisele, mille abil saaksid kodanikud hoida tulemuslikult suhtlemisdistantsi ning mis võimaldavad hoiatada, ennetada ja kontakte jälgida, et piirata COVID-19 haiguse levikut. Soovitus on esitatud üldpõhimõtted, millest nimetatud meetmekogumi väljatöötamisel tuleks lähtuda, ja märgitud, et komisjon avaldab täpsemad suunised, mis käsitlevad muu hulgas seda, milline on sellealaste mobiilirakenduste kasutamise mõju andmekaitsele ja eraelu puutumatusele.

Euroopa ühises tegevuskavas COVID-19 leviku tõkestamiseks võetud meetmete lõpetamise suunas esitas komisjon koostöös Euroopa Ülemkogu eesistujaga hulga põhimõtteid, millest tuleks lähtuda COVID-19 puhangu leviku tõkestamise meetmete järkjärgulisel kaotamisel. Selles võib olla tähtis roll mobiilirakendustel, sealhulgas sellistel mobiilirakendustel, millel on kontaktide jälgimise funktsioon. Olenevalt nende omadustest ja sellest, mil määral elanikkond neid kasutab, võivad mobiilirakendused oluliselt mõjutada COVID-19 haiguse diagnoosimist, ravi ja ohjamist nii haiglakeskkonnas kui ka väljaspool seda. Need on eriti olulised siis, kui viiruse leviku tõkestamise meetmed lõpetatakse ja nakkusoht suureneb, sest üha rohkem inimesi puutub üksteisega kokku. Sellise rakendused võivad aidata katkestada nakkusahelaid kiiremini ja tulemuslikumalt kui üldised viiruse leviku tõkestamise meetmed ning märkimisväärselt vähendada viiruse edasikandumise ohtu. Seega peaksid need olema kriisist väljumise strateegia oluline osa, täiendades muid meetmeid, nagu suurem testimisvõimekus ⁽²⁾. Selleks et sellised mobiilirakendused välja töötataks ning et inimesed neid aktsepteeriks ja need kasutusele võtaksid, on tähtis tagada usaldus. Inimesed peavad olema kindlad, et on tagatud mobiilirakenduste kooskõla põhiõigustega, et neid ei kasutata massiliseks jälgimiseks, vaid ainult täpselt kindlaks määratud eesmärgil ning et igaühele jääb kontroll oma andmete üle. Sellest aluspõhimõttest sõltub mobiilirakenduste täpsus ja tulemuslikkus viiruse leviku

⁽¹⁾ Soovitus C(2020) 2296 final, 8. aprill 2020 https://ec.europa.eu/info/sites/info/files/recommendation_on_apps_for_contact_tracing_4.pdf,

⁽²⁾ https://ec.europa.eu/info/sites/info/files/communication_-_a_european_roadmap_to_lifting_coronavirus_containment_measures_0.pdf

tõkestamisel. Seepärast on väga oluline määrata kindlaks lahendused, millega sekkutakse kõige vähem ning mis vastavad täielikult ELi õiguses sätestatud isikuandmete kaitse ja eraelu puutumatuse nõuetele. Mobiilirakendused tuleks desaktiveerida hiljemalt siis, kui teatatakse, et pandeemia on kontrolli alla saadud. Need peaksid hõlmama ka tippasemel infoturbevahendeid.

Käesolevates suunistes on võetud arvesse Euroopa Andmekaitsekoostöögrupi⁽³⁾ panust ning e-tervise võrgustiku raames toimunud arutelusid. Andmekaitsekoostöögrupp kavatses esitada lähipäevil suunised geolokaliseerimise ja muude jälgimisvahendite kohta COVID-19 puhangu puhul.

Suuniste kohaldamisala

Selleks et tagada kogu ELis sidus lähenemisviis ning anda liikmesriikidele ja mobiilirakenduste arendajatele juhiseid, esitatakse käesolevates suunistes omadused ja nõuded, millele mobiilirakendused peaksid vastama, et tagada nende kooskõla eraelu puutumatust ja isikundmete kaitset käsitlevate ELi õigusaktidega, eriti isikuandmete kaitse üldmääruse⁽⁴⁾ ja e-privaatsuse direktiiviga⁽⁵⁾. Suunistes ei käsitleta lisatingimusi, sealhulgas liikmesriikide õiguses sisalduda võivaid piiranguid seoses terviseandmete töötlemisega.

Käesolevad suunised ei ole õiguslikult siduvad. See ei piira Euroopa Liidu Kohtu rolli, mis on ainus institutsioon, mis saab autoriteetselt tõlgendada ELi õigust.

Käesolevates suunistes käsitletakse ainult vabatahtlikke COVID-19 pandeemia vastast võitlust toetavaid mobiilirakendusi (mille allalaadimine, paigaldamine ja kasutamine on inimestele vabatahtlik), mis täidavad ühte või mitut järgmistest funktsioonidest:

- anda inimestele täpset teavet COVID-19 pandeemia kohta;
- pakkuda inimestele küsimustikke, mida saab kasutada enesehindamiseks ja suunistena (sümptomikontrolli funktsioon)⁽⁶⁾;
- hoiatada inimesi, kes on teatava aja jooksul viibinud nakatunu läheduses, et anda teavet selle kohta, kas nad peaksid karantiini minema või end testida laskma (kontaktide jälgimise ja hoiatamise funktsioon);
- looma patsientide ja arstide vahelise teabevahetusfoorumi, mida saaks kasutada eneseisolatsiooni korral, et täpsustada diagnoosi ja pakkuda ravialast nõu (telemeditsiini ulatuslikum kasutamine).

E-privaatsuse direktiivi kohaselt saab sellise mobiilirakenduse kasutamise, mis on seotud direktiivi artiklis 5 sätestatud side konfidentsiaalsuse õigusega, muuta kohustuslikuks ainult seadusega, mis on vajalik, asjakohane ja proportsionaalne teatava konkreetse eesmärgi kaitsmiseks. Kuna selline lähenemisviis on väga sekkuv ja toob kaasa raskusi, sealhulgas seoses asjakohaste kaitsemeetmete kehtestamisega, leiab komisjon, et selle kasutamisele peaks eelnema hoolikas analüüs. Sellepärast soovib komisjon kasutada vabatahtlikke mobiilirakendusi.

Käesolevates suunistes ei käsitleta mobiilirakendusi, mille ülesanne on tagada karantiininõuete täitmine (sealhulgas selliseid kohustuslikke mobiilirakendusi).

2 MOBIILIRAKENDUSTE PANUS COVID-19 VASTASESSE VÕITLUSSE

Sümptomikontrolli funktsioon on vahend, mis võimaldab rahvaterviseasutustel juhendada oma kodanikke seoses COVID-19 testi tegemisega ning anda teavet eneseisolatsiooni ja selle kohta, kuidas vältida teiste inimeste nakatamist ja millal pöörduda arsti poole. See võib samuti täiendada esmatasandi arstiabi seiret ja parandada teavet elanikkonna nakatumiskordaja kohta COVID-19 puhul.

⁽³⁾ https://edpb.europa.eu/sites/edpb/files/files/file1/edpbletterecadvisecodiv-appguidance_final.pdf

⁽⁴⁾ Euroopa Parlamendi ja nõukogu 27. aprilli 2016. aasta määrus (EL) 2016/679 füüsiliste isikute kaitse kohta isikuandmete töötlemisel ja selliste andmete vaba liikumise ning direktiivi 95/46/EÜ kehtetuks tunnistamise kohta (isikuandmete kaitse üldmäärus) (ELT L 119, 4.5.2016, lk 1).

⁽⁵⁾ Euroopa Parlamendi ja nõukogu 12. juuli 2002. aasta direktiiv 2002/58/EÜ, milles käsitletakse isikuandmete töötlemist ja eraelu puutumatuse kaitset elektroonilise side sektoris (eraelu puutumatust ja elektroonilist sidet käsitlev direktiiv) (EÜT L 201, 31.7.2002, lk 37).

⁽⁶⁾ Kui mobiilirakendused annavad teavet diagnoosimise, ennetamise, seire või prognoosimise kohta, tuleks hinnata, kas need rakendused kvalifitseeruvad meditsiiniseadmeteks vastavalt meditsiiniseadmete õigusraamistikule. Vt seoses selle raamistikuga nõukogu 14. juuni 1993. aasta direktiiv 93/42/EMÜ meditsiiniseadmete kohta (EÜT L 169, 12.7.1993, lk 1) ja Euroopa Parlamendi ja nõukogu 5. aprilli 2017. aasta määrus (EL) 2017/745, milles käsitletakse meditsiiniseadmeid (ELT L 117, 5.5.2017, lk 1).

Kontaktide jälgimise ja hoiatamise funktsioon on vahend, mis võimaldab teha kindlaks COVID-19sse nakatunuga kokku puutunud isikuid ning anda neile teavet sel juhul võetavate meetmete, näiteks karantiini minemise ja testi tegemise või selle kohta, mida teha sümptomite korral. Sellest funktsioonist on seega kasu nii üksikisikutele kui ka rahvaterviseasutustele. Sellel võib olla ka tähtis roll viiruse leviku tõkestamise meetmete haldamisel meetmete kaotamise korral. Selle funktsiooni mõju saab tugevdada kergete sümptomitega inimeste ulatuslikuma testimise strateegia kaudu.

Mõlemad funktsioonid võivad samuti kujutada endast olulist andmeallikat rahvaterviseasutuste jaoks ning hõlbustada selliste andmete edastamist riiklikele epidemioloogiaasutustele ja Haiguste Ennetamise ja Tõrje Euroopa Keskusele (ECDC). See aitaks mõista nakatumismustreid ja testimistulemustega kombineerimise korral hinnata hindamisteede sümptomite positiivset ennustuväärtust teatava kogukonna puhul ning anda teavet viiruse levikutaseme kohta.

Hinnangute usaldusväärsus on otseselt seotud edastatud andmete hulga ja usaldusväärsusega.

Kui kombineerida sümptomikontrolli ja kontaktide jälgimise funktsioon asjakohaste testimisstrateegiatega, võivad need anda teavet viiruse levikutaseme kohta ning aidata hinnata suhtlemisdistantsi hoidmise ja liikumispääsude mõju. Nagu on märgitud soovitusel, tuleks tagada eri liikmesriikide IT-lahenduste koostalitlusvõime, et oleks võimalik teha piiriülest koostööd ja tagada kontaktide avastamine eri mobiilirakendusi kasutavate inimeste vahel (see on eriti oluline kodanike piiriülese liikumise korral). Kui nakatunu puutub kokku teise liikmesriigi mobiilirakenduse kasutajaga, peaks juhul, kui see on vajalik, olema võimalik edastada kasutaja isikuandmed piiriülelt tema liikmesriigi tervishoiuasutustele. Selle küsimusega on kavas tegeleda soovitusel teatatud meetmekogumi raames. Koostalitlusvõime tagamiseks tuleks kehtestada tehnilised nõuded ning parandada riiklike tervishoiuasutuste vahelist teabevahetust ja koostööd. COVID-19 pandeemia ajal kontaktide jälgimiseks kasutatavate mobiilirakenduste juhtimisraamistikuna võiks kasutada ka piiritletud koostöö mudelit ⁽⁷⁾.

3 RAKENDUSTE USALDUSVÄÄRSE JA VASTUTUSTUNDLIKU KASUTAMISE ELEMENTID

Rakendustes sisalduvad funktsioonid võivad mitmel viisil mõjutada paljusid ELi põhiõiguste hartas sätestatud õigusi, nagu inimväärikus, era- ja perekonnaelu austamine, isikuandmete kaitse, liikumisvabadus, mittediskrimineerimine, ettevõtlusvabadus ning kogunemis- ja ühinemisvabadus. Nende hulgas võivad eriti olulised olla eraelu austamine ja õigus isikuandmete kaitsele, arvestades, et mõned funktsioonid põhinevad andmemahukal mudelil.

Allpool esitatud elementide eesmärk on anda suuniseid selle kohta, kuidas piirata rakenduse funktsioonide liigset tungimist eraellu, et tagada vastavus isikuandmete kaitset ja eraelu puutumatust käsitlevatele ELi õigusaktidele.

3.1 Riiklikud tervishoiuasutused (või avalikes huvides tegutsevad tervishoiuvaldkonna üksused) vastutava töötlejana

Isikuandmete töötlemise vahendite ja eesmärkide üle otsustava isiku (vastutava töötleja) kindlaksmääramine on väga oluline, et oleks selge, kes vastutab ELi isikuandmete kaitse eeskirjade järgimise eest, ning eelkõige, kes peaks andma rakendust alla laadivatele üksikisikutele teavet selle kohta, milleks nende isikuandmeid (mis on juba olemas või mis luuakse seadme, näiteks nutitelefoniga kaudu, kuhu rakendus on paigaldatud) kasutatakse, millised on nende õigused, kes vastutab andmetega seotud rikkumiste eest jne.

Võttes arvesse asjaomaste isikuandmete tundlikkust ja allpool kirjeldatud andmetöötluse eesmärki, on komisjon seisukohal, et rakendused peaksid olema kavandatud nii, et vastutavaks töötlejaks oleksid riiklikud tervishoiuasutused (või avalikes huvides tegutsevad tervishoiuvaldkonna üksused) ⁽⁸⁾. Vastutavad töötlejad vastutavad isikuandmete kaitse üldmääruse järgimise eest (vastutuse põhimõte). Andmetele juurdepääsu ulatus peaks olema piiratud punktis 3.5 kirjeldatud põhimõtete kohaselt.

⁽⁷⁾ Selline koostöö toimub juba projekti MyHealth@EU puhul patsiendi koondandmete ja digireseptide vahetamiseks Vt ka komisjoni rakendusotsuse 2019/1765 artikli 5 lõige 5 ja põhjendus 17.

⁽⁸⁾ Vt isikuandmete kaitse üldmääruse põhjendus 45.

See suurendab ka inimeste usaldust ja seega rakenduste (ja neis nakkusahelate kohta kasutatavate infosüsteemide) ühiskondlikku heakskiitmist ning tagab, et need täidaksid rahvatervise kaitse eesmärki. Vastutavad riiklikud tervishoiuasutused peaksid andmetöötlemise aluseks olevad põhimõtted, nõuded ja järelevalvemenetlused ühtlustama ja rakendama neid kooskõlastatult.

3.2 Üksikisikul peab säilima kontroll oma andmete üle

Otsustav tegur, mis võimaldab üksikisikul rakendusi usaldada, on võimalus veenduda, et ta säilitab kontrolli oma isikuandmete üle. Komisjon leiab, et selle tagamiseks peaksid olema täidetud eelkõige järgmised tingimused:

- rakenduse paigaldamine seadmesse peaks olema vabatahtlik ja sellel ei tohiks olla mingeid negatiivseid tagajärgi üksikisikule, kes otsustab rakendust mitte alla laadida või mitte kasutada;
- rakenduse erinevaid funktsioone (nt teave, sümptomikontroll, kontaktide jälgimise ja hoiatamise funktsioonid) ei tohiks kokku liita, et üksikisik saaks anda oma nõusoleku eraldi iga funktsiooni jaoks. See ei tohiks takistada kasutajal rakenduse eri funktsioone kombineerida, kui teenusepakkuja pakub seda valikuvõimalusena;
- kui kasutatakse lähedusandmeid (andmed, mis on saadud BLE tehnoloogia (väikese energiatarbega Bluetooth) signaalide vahetamisel seadmete vahel, mis on üksteisest epidemioloogiliselt asjakohases kauguses epidemioloogiliselt asjakohase aja jooksul), tuleks need salvestada üksikisiku seadmesse. Kui neid andmeid tuleb jagada tervishoiuasutustega, tuleks seda teha alles pärast kinnituse saamist selle kohta, et asjaomane isik on nakatunud COVID-19 viirusega, ja tingimusel, et ta otsustab neid andmeid jagada;
- tervishoiuasutused peaksid andma üksikisikutele kogu vajaliku teabe, mis on seotud nende isikuandmete töötlemisega (kooskõlas isikuandmete kaitse üldmääruse artiklitega 12 ja 13 ning e-privatsuse direktiivi artikliga 5);
- isikul peaks olema võimalik kasutada oma isikuandmete kaitse üldmäärusest tulenevaid õigusi (eelkõige oma andmetega tutvuda, neid parandada ja kustutada). Isikuandmete kaitse üldmäärusest ja e-privatsuse direktiivist tulenevate õiguste mis tahes piiramine peaks olema kooskõlas nende õigusaktidega ning vajalik, proportsionaalne ja sätestatud õigusaktides;
- rakendused tuleks desaktiveerida hiljemalt siis, kui pandeemia on kuulutatud kontrolli all olevaks; desaktiveerimine ei tohiks sõltuda sellest, kas kasutaja kõrvaldab rakenduse oma seadmest.

3.3 Isikuandmete töötlemise õiguslik alus

Rakenduste paigaldamine ja teabe salvestamine kasutaja seadmesse

Nagu eespool märgitud, on e-privatsuse direktiivi (artikkel 5) kohaselt teabe salvestamine kasutaja seadmesse või juba salvestatud teabe juurdepääsu saamine lubatud üksnes juhul, kui i) kasutaja on andnud selleks nõusoleku või ii) salvestamine ja/või juurdepääs on rangelt vajalik infoühiskonna teenuse (nt rakenduse) jaoks, mida kasutaja on sõnaselgelt taotlenud (st seadmesse paigaldanud ja aktiveerinud).

Teabe salvestamine üksikisiku seadmesse ja juurdepääs selles seadmes juba salvestatud teabele on rakenduste toimimiseks tavaliselt vajalik. Peale selle eeldab kontaktide jälgimise ja hoiatamise funktsioon, et kasutaja seadmesse salvestatakse ka muud teavet (näiteks selle funktsiooni teiste läheduses viibivate kasutajate ajutised, korrapäraselt muutuvad kasutajanimed). Samuti võib see funktsioon nõuda (nakatunud või tõenäoliselt nakatunud) kasutajalt lähedusandmete üleslaadimist. Nende üleslaadimine ei ole aga rakenduse kui sellise toimimiseks otseselt vajalik. Seega ei ole eelmises lõigus nimetatud variandi ii) tingimused täidetud. Järelikult jääb asjaomase tegevuse kõige sobivamaks aluseks nõusolek (eespool nimetatud variant i)). Selline nõusolek peaks olema vabatahtlik, konkreetne, selgesõnaline ja teadlik isikuandmete kaitse üldmääruse tähenduses. See peaks väljenduma üksikisiku selges kinnitavas tegevuses; see ei hõlma vaikiva nõusoleku vorme (nt vaikimine või tegevusetus) (⁹).

(⁹) Vt Euroopa Andmekaitseõukogu suunised nõusoleku kohta: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=623051

Riiklikes tervishoiuasutustes andmete töötlemise õiguslik alus – liidu või liikmesriigi õigus

Riiklikud tervishoiuasutused töötlevad isikuandmeid üldjuhul siis, kui ELi või liikmesriigi õiguses on sätestatud juriidiline kohustus, mis näeb ette sellise töötlemise ja vastab isikuandmete kaitse üldmääruse artikli 6 lõike 1 punktis c ja artikli 9 lõike 2 punktis i sätestatud tingimustele, või kui selline töötlemine on vajalik ELi või liikmesriigi õiguses sätestatud avaliku huvi edendamiseks ⁽¹⁰⁾.

Mis tahes siseriiklikus õigusaktis peavad olema sätestatud konkreetsed ja sobivad meetmed andmesubjektide õiguste ja vabaduste kaitsmiseks. Üldiselt, mida suurem on mõju üksikisikute vabadustele, seda tugevamad kaitsemeetmed peaksid olema sätestatud asjaomastes õigusaktides.

ELi ja liikmesriikide õigusakte, mis kehtisid enne COVID-19 puhangut, ja õigusakte, millega liikmesriigid konkreetselt võitlevad epideemia leviku vastu, võib põhimõtteliselt kasutada õigusliku alusena üksikisikute andmete töötlemisel, kui nendega nähakse ette epideemia seiret võimaldavad meetmed ja kui need õigusaktid vastavad isikuandmete kaitse üldmääruse artikli 6 lõikes 3 sätestatud täiendavatele nõuetele.

Arvestades asjaomaste isikuandmete laadi (eelkõige terviseandmed kui isikuandmete eriliik) ja praeguse COVID-19 pandeemia asjaolusid, aitaks õigusakti valimine õiguslikuks aluseks suurendada õiguskindlust, kuna see võimaldaks i) sätestada üksikasjalikult konkreetsete terviseandmete töötlemise ja täpsustada selgelt töötlemise eesmärgid; ii) määrata üheselt kindlaks, kes on vastutav töötleja, st andmeid töötlev üksus, ja kellel peale vastutava töötleja on veel juurdepääs kõnealustele andmetele; iii) välistada võimaluse töödelda selliseid andmeid muudel kui õigusaktides loetletud eesmärkidel ja iv) sätestada konkreetsed kaitsemeetmed. Selleks et mitte kahjustada rakenduste üldist kasulikkust ja ühiskondlikku heakskiitu, peaksid riiklikud seadusandjad pöörama erilist tähelepanu sellele, et valitud lahendus oleks kodanike suhtes võimalikult kaasav.

Andmete töötlemine tervishoiuasutustes õigusaktide alusel ei muuda asjaolu, et üksikisikutel on õigus otsustada, kas rakendust paigaldada või mitte ning kas jagada oma andmeid tervishoiuasutustega. Seega ei tohiks rakenduse paigaldamata jätmine tuua kasutajale kaasa kahjulikke tagajärgi.

Kontaktide jälgimise ja hoiatamise rakendused võimaldavad üksikisikuid hoiatada. Kui see hoiatus esitatakse vahetult rakenduse kaudu, juhib komisjon tähelepanu keelule kohaldada üksikisikute suhtes otsust, mis põhineb üksnes automatiseeritud töötlemisel, millel on õiguslikke tagajärgi või sarnane märkimisväärne mõju (isikuandmete kaitse üldmääruse artikkel 22).

3.4 Võimalikult väheste andmete kogumine

Seadmete kaudu kogutud ja juba varem neis seadmetes salvestatud andmeid kaitstakse järgmiselt:

- „Isikuandmeid“, st mis tahes teavet tuvastatud või tuvastatava füüsilise isiku kohta (isikuandmete kaitse üldmääruse artikli 4 lõige 1), kaitstakse isikuandmete kaitse üldmääruse alusel. Terviseandmete suhtes kohaldatakse täiendavat kaitset (isikuandmete kaitse üldmääruse artikkel 9).
- „Asukohaandmeid“, st elektroonilises sidevõrgus või elektroonilise sideteenuse kaudu töödeldavaid andmeid, mis näitavad kasutaja lõppseadme geograafilist asukohta, kaitstakse e-privatsuse direktiivi alusel (artikli 5 lõige 1 ning artiklid 6 ja 9) ⁽¹¹⁾.
- Kasutaja lõppseadmesse salvestatud ja sealt saadud teavet kaitstakse vastavalt e-privatsuse direktiivi artikli 5 lõikele 3.

Isikustamata andmeid (nt pöördumatult anonüümitud andmed) isikuandmete kaitse üldmääruse alusel ei kaitsta.

Komisjon tuletab meelde, et võimalikult väheste andmete kogumise põhimõtte kohaselt võib töödelda ainult selliseid isikuandmeid, mis on piisavad, asjakohased ja piirduvad eesmärgi saavutamiseks vajalikuga ⁽¹²⁾. Isikuandmete töötlemise vajadust ja selliste isikuandmete asjakohasust tuleks hinnata taotletava eesmärgi (taotletavate eesmärkide) seisukohast.

Komisjon tõdeb näiteks, et kui funktsiooni eesmärk on sümptomite kontrollimine või telemeditsiin, ei nõua need eesmärgid juurdepääsu seadme omaniku kontaktide nimekirjale.

⁽¹⁰⁾ Isikuandmete kaitse üldmääruse artikli 6 lõike 1 punkt e.

⁽¹¹⁾ Elektroonilise side seadustikus on sätestatud, et see hõlmab ka samaväärsete funktsioonidega elektroonilise side teenuseid.

⁽¹²⁾ Võimalikult väheste andmete kogumise põhimõte.

Vähemate andmete kogumine ja töötlemine vähendab turvariske. Seetõttu on võimalikult väheste andmete kogumise meetmete järgimine ühtlasi turvameede.

— Teabefunktsioon:

Üksnes selle funktsiooniga rakenduses ei pea töötleva üksikisikute terviseandmeid. See annab neile üksnes teavet. Selle eesmärgi täitmiseks ei tohi lõppseadmesse salvestatud ja sealt saadud teavet töödelda muul otstarbel kui see, mis on vajalik teabe andmiseks.

— Sümptomikontrolli ja telemeditsiini funktsioon

Kui rakendusel on üks või kaks neist funktsioonidest, töödeldakse selles terviseandmeid. Seetõttu tuleks tervishoiuasutuste suhtes kohaldatavates alusõigusaktides sätestada, milliseid andmeid võib töödelda.

Lisaks võib tervishoiuasutustel olla vaja sümptomikontrolli rakendust kasutanud ja tulemusi üles laadinud isikute telefoninumbreid. Lõppseadmesse salvestatud ja sealt saadud teavet võib töödelda ainult niivõrd, kui see on vajalik selleks, et rakendus saaks täita oma eesmärgi ja toimida.

— Kontaktide jälgimine ja hoiatusfunktsioon:

COVID-19 nakkus levib enamasti piiratud vahemaal edasikanduvate piiskade kaudu. Nakkusahela katkestamise üheks kõige olulisemaks teguriks on nakatunud isiku läheduses viibinud isikute võimalikult kiire tuvastamine. Läheduse määramine sõltub kokkupuute kaugusest ja kestusest ning selle aluseks peaksid olema epidemioloogilised kaalutlused. Nakkusahela katkestamine on eriti oluline selleks, et vältida nakkuse taaslevikut kriisist väljumise etapis.

Selleks võivad olla vajalikud lähedusandmed. Läheduse ja lähikontaktide mõõtmiseks näib seadmete vahel BLE tehnoloogia (väikese energiatarbega Bluetooth) kasutamine olevat täpsem ja seega asjakohasem kui asukohatuvastuse andmete (GNSS/GPS või mobiiltelefoni asukohaandmed) kasutamine. BLE tehnoloogia kasutamisel ei ole andmeid võimalik jälgida (erinevalt geograafilise asukoha andmetest). Seepärast soovib komisjon kasutada läheduse kindlakstegemiseks BLE sideandmeid (või samaväärse tehnoloogia abil loodud andmeid).

Asukohaandmed ei ole kontaktide jälgimise funktsiooni seisukohast vajalikud, kuna nende eesmärk ei ole jälgida üksikisikute liikumist ega täita ettekirjutusi. Lisaks oleks asukohaandmete töötlemist kontaktide jälgimise kontekstis võimalikult väheste andmete kogumise põhimõtet silmas pidades raske põhjendada ning see võib tekitada probleeme turvalisuse ja eraelu puutumatuse seisukohast. Seetõttu soovib komisjon asukohaandmeid selles kontekstis mitte kasutada.

Olenemata läheduse kindlaksmääramiseks kasutatavatest tehnilistest vahenditest ei tundu olevat vajalik salvestada kontakti toimumise täpset aega ega kohta (kui need andmed on olemas). Siiski võib olla kasulik salvestada kontakti toimumise päev, et teada, kas kontakt toimus siis, kui isikul olid tekkinud sümptomid (või 48 tundi varem ⁽¹³⁾), ning saata seejärel sõnum suunistega vabatahtliku isolatsiooni kestuse kohta.

Lähedusandmeid tuleks koguda ja töödelda üksnes juhul, kui on olemas tegelik nakkusoht (sõltuvalt kokkupuute läheduses ja kestusest).

Tuleb pöörata tähelepanu sellele, et andmete kogumise vajalikkus ja proportsionaalsus sõltub seega muu hulgas sellest, kui kättesaadavad on testimiseseadmed, eelkõige juhul, kui sellised meetmed nagu karantiin on juba ette nähtud. Nakatunud isikuga lähedalt kokku puutunud isikuid saab hoiatada kahel viisil:

Esimene võimalus on saata lähikontaktidele rakenduse kaudu automaatselt hoiatus, kui kasutaja on teatanud rakendusele – tervishoiuasutuse heakskiidul või kinnitusel, näiteks QR- või TAN-koodi abil –, et ta on saanud positiivse testitulemuse (detsentraliseeritud töötlemine). Hoiatusteate sisu peaks eelistatavalt kindlaks määrama tervishoiuasutus. Teine võimalus on salvestada teatavad ajutised identifikaatorid tervishoiuasutuse põhiserverisse (põhiserveri lahendus). Kasutajaid ei saa nende andmete kaudu otseselt tuvastada. Identifikaatorite alusel saavad kasutajad, kes on olnud lähikontaktis positiivse testitulemuse saanud kasutajaga, oma seadmesse hoiatuse. Kui tervishoiuasutused soovivad võtta ühendust kasutajatega, kes on olnud lähikontaktis nakatunud isikuga, ka telefoni või SMS-i teel, on neil telefoninumbrite edastamiseks vaja asjaomaste kasutajate nõusolekut.

⁽¹³⁾ Nakatunud isik on nakkav 48 tundi enne sümptomite ilmnemist.

3.5 Andmete avaldamise/juurdepääsetavuse piiramine

— Teabefunktsioon:

Lõppseadmesse salvestatud ja sealt saadud teavet ei või tervishoiuasutustega jagada, välja arvatud juhul, kui see on vajalik teabefunktsiooni tagamiseks. Kuna see funktsioon kujutab endast ainult sidevahendit, ei saa tervishoiuasutus juurdepääsu muudele andmetele.

— Sümptomikontrolli ja telemeditsiini funktsioon

Sümptomikontrolli funktsioon võib olla liikmesriikidele kasulik, et anda kodanikele juhiseid selle kohta, kas nad peaksid laskma ennast testida, anda teavet isoleerumise kohta ning selle kohta, millal ja kuidas saavad eelkõige riskirühmad juurdepääsu tervishoiuteenustele. See funktsioon võib ka täiendada esmatasandi arstiabis rakendatavat seiret ja aidata aru saada, milline on COVID-19 nakkuse määra elanikkonna hulgas. Seetõttu võib otsustada, et vastutavad tervishoiuasutused ja riiklikud epidemioloogilised asutused peaksid saama juurdepääsu patsiendi esitatud teabele. Haiguste Ennetamise ja Tõrje Euroopa Keskus võiks saada riiklikelt asutustelt epidemioloogilise seire otstarbel koondandmeid.

Kui otsustatakse võtta ühendust tervishoiuametnikega, mitte ainult rakenduse kaudu, siis tuleb avaldada riiklikele tervishoiuasutustele ka rakenduse kasutaja telefoninumber.

— Kontaktide jälgimine ja hoiatusfunktsioon:

— Nakatunud isiku andmed

Rakendused genereerivad kasutaja telefoniga kontaktis olevate telefonide lühiajalisi pseudojuhuslikke ja perioodiliselt muutuvaid identifikaatoreid. Üks võimalus on salvestada need identifikaatorid kasutaja seadmesse (detsentraliseeritud töötlemine). Teise võimalusena võib need identifikaatorid salvestada serverisse, millele tervishoiuasutustel on juurdepääs (nn põhiserveri lahendus). Detsentraliseeritud lahendus on rohkem kooskõlas võimalikult väheste andmete kogumise põhimõttega. Tervishoiuasutustel peaks olema juurdepääs üksnes nakatunud isiku seadme lähedusandmetele, et ta saaks nakkusohus inimestega ühendust võtta.

Need andmed tehakse tervishoiuasutustele kättesaadavaks alles pärast seda, kui nakatunud isik on neid andmeid (pärast testimist) proaktiivselt nendega jaganud.

Nakatunud isikule ei tohiks edastada nende isikute andmeid, kellega tal võib olla olnud epidemioloogiliselt asjakohaseid kokkupuuteid ja keda hoiatatakse.

— Andmed isikute kohta, kes on nakatunud isikuga (epidemioloogiliselt) kokku puutunud

Nakatunud isiku andmeid ei tohiks avaldada isikutele, kellega ta on epidemioloogiliselt kokku puutunud. Piisab sellest, kui neile teatatakse, et nad on nakatunud isikuga viimase 16 päeva jooksul (epidemioloogiliselt) kokku puutunud. Nagu eespool märgitud, ei tohiks selliste kokkupuudete aega ja kohta käsitlevaid andmeid säilitada. Seepärast ei ole nende andmete edastamine vajalik ega võimalik.

Nakatunud e-rakenduse kasutaja epidemioloogiliste kontaktide jälgimiseks tuleks riiklikke tervishoiuasutusi teavitada üksnes selle isiku identifitseerimisandmetest, kellega nakatunud isik on epidemioloogiliselt kokku puutunud ajavahemikus 48 tundi enne sümptomite ilmnemist kuni 14 päeva pärast sümptomite ilmnemist, lähtudes kokkupuute lähedusest ja kestusest.

Haiguste Ennetamise ja Tõrje Euroopa Keskus võiks saada riiklikelt epidemioloogilise seire asutustelt koondandmeid koostöös liikmesriikidega kindlaks määratud näitajate kohta.

3.6 Andmete töötlemise täpne eesmärk

Õigusliku alusega (liidu või liikmesriigi õigus) tuleks ette näha andmete töötlemise täpne eesmärk. See eesmärk peaks olema selge ja konkreetne, et ei jääks mingit kahtlust, milliseid isikuandmeid on vaja soovitud tulemuse saavutamiseks töödelda.

Täpne eesmärk (täpsed eesmärgid) sõltub (sõltuvad) rakenduse funktsioonist. Rakenduse igal funktsioonil võib olla mitu eesmärki. Selleks et üksikisikul oleks oma andmete üle täielik kontroll, soovitab komisjon eri funktsioone mitte siduda. Igal juhul peaks üksikisikul olema võimalik valida eri funktsioonide vahel, millega taotletakse eri eesmärgi.

Komisjon ei soovita kasutada andmeid, mis on eespool nimetatud tingimustel kogutud muuks otstarbeks kui COVID-19 vastaseks võitluseks. Juhul kui osutub vajalikuks arvata eesmärkide hulka näiteks teadusuuringud ja statistika, tuleks need algsesse eesmärkide loetellu lisada ja neist kasutajatele selgelt teada anda.

— Teavitamise funktsioon

Selle funktsiooni eesmärk on anda kriisi tingimustes tervishoiuasutuste seisukohast olulist teavet.

— Sümptomikontrolli ja telemeditsiini funktsioon

Sümptomikontrolli funktsioon võib anda teavet selle kohta, kui suur osa COVID-19 sümptomitest teatanud isikutest on tõepoolest nakatunud (nt võidakse võtta kõigilt või osalt sümptomitega isikutelt ninaneelu proov või neid muul moel testida, kui see on võimalik). Selle eesmärgi puhul tuleks selgitada, et tervisealaseid isikuandmeid töödeldakse selleks, et i) anda isikule võimalus talle esitatavate küsimuste alusel oma seisundit ise hinnata, kui tal on tekkinud COVID-19 sümptomid, või ii) saada meditsiinilist nõu, kui tal on tekkinud COVID-19 sümptomid.

— Kontaktide jälgimise ja hoiatamise funktsioon

Pelgalt eesmärgile „uute COVID-19 nakkuste ennetamine“ osutamine ei ole piisavalt konkreetne. Siin soovib komisjon täpsustada eesmärki (eesmärke) suunal „rakendust kasutavate ja COVID-19 nakkusega kokku puutuda võinud isikute kontaktide säilitamine, et hoiatada isikuid, kes võivad olla nakatunud“.

3.7 Ranged piirangud andmete säilitamisele

Andmete säilitamise piirangu põhimõtte kohaselt ei tohi isikuandmeid säilitada kauem kui vajalik. Ajalised piirangud tuleks kehtestada meditsiinilise vajaduse põhjal (sõltuvalt rakenduse eesmärgist: peiteaeg jms). Kehtestada tuleks ka realistlikud tähtajad seoses haldusmeetmetega, mida võib olla tarvis võtta.

— Teavitamise funktsioon

Juhul kui selle funktsiooni paigaldamise ajal on kogutud mis tahes andmeid, tuleks need viivitamata kustutada. Selliste andmete hoidmine ei ole põhjendatud.

— Sümptomikontrolli ja telemeditsiini funktsioon

Tervishoiuasutused peaksid need andmed kustutama hiljemalt ühe kuu möödudes (peiteaeg pluss varu) või juhul, kui isikut testiti ja tulemus oli negatiivne. Tervishoiuasutused võivad säilitada andmeid pikema aja jooksul järelevalve ja uuringute eesmärgil, eeldusel et andmed anonüümitakse.

— Kontaktide jälgimise ja hoiatamise funktsioon

Lähedusandmed tuleks kustutada niipea, kui neid ei ole isikute hoiatamiseks enam tarvis ehk hiljemalt ühe kuu möödudes (peiteaeg pluss varu) või juhul, kui isikut testiti ja tulemus oli negatiivne. Tervishoiuasutused võivad säilitada lähedusandmeid pikema aja jooksul järelevalve ja uuringute eesmärgil, eeldusel et andmed anonüümitakse.

Andmed tuleks salvestada kasutaja seadmesse. Tervishoiuasutustele ligipääsetavas serverisse tuleks üles laadida ainult need andmed, mille kasutajad on sinna edastanud ja mis on eesmärgi saavutamiseks vajalikud, juhul kui nad on selle valikuvariandi valinud (s.t serverisse laaditakse üles üksnes andmed positiivse COVID-19 testitulemusega isiku lähedaste kontaktide kohta).

3.8 Andmete kaitse tagamine

Komisjon soovib salvestada andmed isiku lõppseadmesse krüptitud kujul. Krüptimiseks tuleks kasutada ajakohaseid krüptomeetodeid. Juhul kui andmeid säilitatakse keskserversis, tuleks neile juurde pääsemiseks (ka halduseesmärgil) end sisse logida.

Lähedusandmeid tuleks genereerida ja säilitada ainult isiku lõppseadmes krüptitud ja pseudonüümitud kujul. Selleks et kaitsta andmeid kolmandate osapoolte jälitustegevuse eest, tuleks võimaldada aktiveerida Bluetooth, ilma et oleks tarvis aktiveerida muid asukoha määramise teenuseid.

Lähedusandmete kogumisel väikese energiatarbega Bluetoothi (BLE) kaudu on soovitatav luua ja salvestada ajutisi kasutajatunnuseid, mis korrapäraselt muutuvad, selle asemel et salvestada seadme tegelik tunnus. See meede pakub täiendavat kaitset häkkerite poolse pealtkuulamise ja jälgimise eest ning raskendab seega isikute tuvastamist.

Komisjon soovib rakenduse lähtekoodi avalikustada ja teha see läbivaatamise eesmärgil kättesaadavaks.

Töödeldavate andmete kaitsmiseks võib ette näha veel muid meetmeid, näiteks andmete automaatse kustutamise või nende anonüümimise teatava aja möödudes. Üldiselt peaks kaitse tase olema proportsionaalne töödeldavate isikuandmete hulga ja tundlikkusega.

Kogu andmeedastus isiku seadmest riigi tervishoiuasutustele peaks toimuma krüptitult.

Juhul kui siseriiklike õigusaktidega on ette nähtud, et kogutud isikuandmeid võib töödelda ka teadusuuringute eesmärgil, tuleks andmed põhimõtteliselt pseudonüümida.

3.9 Andmete täpsuse tagamine

Töödeldavate isikuandmete täpsuse tagamine ei ole mitte ainult rakenduse tõhusa toimimise eeltingimus, vaid ka isikuandmete kaitse õigusaktides sätestatud nõue.

Seetõttu on valepositiivsete tulemuste saamise ohu minimeerimiseks väga oluline tagada, et teave nakatunud isikuga aset leidnud kontaktide kohta (epidemioloogiline distants ja kestus) on täpne. See peaks hõlmama olukordi, kus kaks rakenduse kasutajat on puutunud kokku tänaval, ühissõidukis või mõnes hoones. Mobiilsidevõrkudest saadavate asukohaandmete kasutamine sel eesmärgil ei ole tõenäoliselt piisavalt täpne.

Seepärast soovitatakse tugineda tehnoloogiale, mis võimaldab kontakte üksikasjalikumalt hinnata (nt Bluetooth).

3.10 Andmekaitseasutuste kaasamine

Rakenduse väljatöötamisse tuleks täies ulatuses kaasata andmekaitseasutused, kellega tuleks konsulteerida ja kes peaksid rakenduse kasutamist kontrollima. Arvestades, et andmete töötlemine rakenduse raames kvalifitseerub andmete eriliikide (terviseandmed) ulatuslikuks töötlemiseks, juhib komisjon tähelepanu isikuandmete kaitse üldmääruse artiklile 35, milles käsitletakse andmekaitsealast mõjuhinnangut.
