

Vabariigi Valitsuse 1. detsembri 2016. a määruse nr 138 „Tervise infosüsteemi põhimäärus“ muutmise määruse eelnõu seletuskiri

1. Sissejuhatus

1.1. Sisukokkuvõte

Eelnõuga muudetakse Vabariigi Valitsuse 1. detsembri 2016. a määrust nr 138 „[Tervise infosüsteemi põhimäärus](#)“, mis on kehtestatud tervishoiuteenuste korraldamise seaduse § 59¹ lõike 3 alusel.

Eelnõu on seotud riikliku nakkushaiguse levikut tõkestava rakenduse (edaspidi *rakendus*) kasutuselevõtuga riikliku asutuse poolt, mis eeldab nakkuse diagnoosi kinnitamist tervise infosüsteemis (edaspidi *TIS*), et vältida rakenduse väärkasutust. Rakendus ise ei hakka töötleva isikuandmeid. Määruse muudatusena lisatakse TIS-i andmeandjana rakendus ning sätestatakse andmesubjektile võimalus teha tahteavaldus nakatumist kinnitava isikustamata koodi edastamiseks nimetatud rakendusele. Rakenduse kasutamise vajaduse otsustab nakkushaiguste ennetamise ja tõrje eest vastutav pädev asutus. Rakendus teavitab vaid eriti ohtlikest nakkushaigustest või uudest ohtlikust nakkushaigusest, sest just nendel juhtudel on tegemist haigusega, mis levib kiiresti ja ulatuslikult või mille kulg on raske või eluohtlik.

1.2. Eelnõu ettevalmistaja

Eelnõu ja seletuskirja on koostanud Sotsiaalministeeriumi nutika arengu toetamise osakonna nõunik Kristel Niidas (kristel.niidas@sm.ee, tel 626 9137) ja e-teenuste asekancleri nõunik Priit Tohver (priit.tohver@sm.ee, tel 626 9134). Eelnõu juriidilise ekspertiisi on teinud Sotsiaalministeeriumi õigusosakonna õigusnõunik Nele Nisu (nele.nisu@sm.ee).

Eelnõu ja seletuskirja ettevalmistamisse kaasati Tervise ja Heaolu Infosüsteemide Keskus.

Eelnõu on keeleteoimetanud Rahandusministeeriumi ühisosakonna dokumendihaldustalituse keeleteoimetaja Virge Tammaru (virge.tammaru@fin.ee, tel 626 9320).

1.3. Märkused

Eelnõu on seotud isikuandmete töötlemisega isikuandmete kaitse üldmääruse¹ tähenduses ning selle kohta on koostatud täpsem mõjuanalüüs käesoleva eelnõu seletuskirja 4. punktis.

2. Eelnõu sisu ja võrdlev analüüs

Punktiga 1 sätestatakse, et TIS-i volitatud töötlejal on kohustus tagada andmevahetus riikliku rakendusega olukorras, kus nakkushaiguste ennetamise ja tõrje seaduses nimetatud pädev asutus (Terviseamet) on otsustanud, et rakendus aitab kaasa rahva tervise kaitsele. Pädeva asutuse otsus on vajalik selleks, et rakendust saaks kasutada üksnes nendes olukordades, kus on vaja hoiatada isikuid kokkupuutest nakkushaigust põdeva isikuga. Tegemist ei ole isikustatud andmetel põhineva rakendusega. On oluline selgitada, et nakkuse leviku tõkestamiseks on sarnaste rakenduste kasutamise (sh isikustatud andmetega) heaks kiitnud ka Euroopa Komisjon oma suunises (vt selle kohta selgitusi järgnevatel punktides) ja seda juhul, kui sellel on rahva tervise kaitse eesmärk ja kui vastutus on riiklikul asutusel.

Punktidega 2 ja 5 sätestatakse andmeandja ning isiku võimalus nõusoleku alusel rakendusele andmeid edastada ehk veel üks tahteavalduse võimalus teiste seas. Rakenduse andmeandjana sätestamise vajadus tuleneb sellest, et rakendus edastab TIS-i nakkushaiguse diagnoosi fakti

¹ Euroopa Parlamendi ja nõukogu 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, 04.05.2016, lk 1–88).

kinnitamiseks tuvastuskoodi (rakenduse jaoks isikustamata). Isikul on võimalik TIS-i patsiendiportaali sisenedes kinnitada nakkuse olemasolu ja lubada TIS-il edastada rakendusele andmesubjekti nõusoleku alusel anonüümne kood. Ei rakenduse poolt edastatav tuvastuskood ega TIS-i poolt edastatav kinnituskood sisalda isikuandmeid ning selle põhjal ei saa koodi edastanud isikut tuvastada ei rakenduse teised kasutajad ega Terviseamet. Samas loob see suurema läbipaistvuse ning isikul säilib võimalus ise oma nakatumise kinnitus anda või mitte anda. Rakenduse eesmärk on hoiatada isikut kokkupuutumisest isikuga, kes on põdenud eriti ohtlikku või uudset nakkushaigust (just need haigused levivad kiiresti ja ulatuslikult või on nende kulg raske või lausa eluohtlik). Täpsem kirjeldus on esitatud seletuskirja punktis 4.

Punktiga 3 sätestatakse erand üldisest andmevahetusest ning selle kohaselt hakkavad TIS ja rakendus eelmises punktis nimetatud koode vahendama krüpteeritud andmevahetuskanali vahendusel. Selline andmete vahetamise viis on heaks kiidetud ka Euroopa Komisjoni 16.04.2020 teatises „Andekaitsega seotud suunised COVID-19 pandeemia vastast võitlust toetavate mobiilirakenduste kohta“.² Kuna ka meditsiinilisi ülesvõtteid vahetatakse krüpteeritud andmevahetuskanali, mitte X-tee kaudu, siis on sõnastus selles osas ühtlustatud.

Punktiga 4 lisatakse autentimisvahendite loetellu smart-ID või muu samaväärne autentimisvahend. Tegemist on näidisloeteluga, kuid see on vajalik, et määrata teatud turvaline autentimisvahendite aste, mis on piisavalt usaldusväärne.

3. Eelnõu vastavus Euroopa Liidu õigusele

Eelnõu vastab Euroopa Liidu õigusele.

4. Määruse mõjud

Määruse muudatuste tulemusena on võimalik turvaliselt ja isikuandmeid edastamata kinnitada nakatunud isiku kinnitatud diagnoos (nakkushaigusesse nakatunud) ning edasi on rakendusel võimalik teavitada isikuid, kes on viibinud nakatunud isikuga lähikontaktis, et anda esmased käitumissuunised ning edasised sammud enda ja teiste tervise kaitseks. Ka Euroopa Komisjon on oma suunistes välja toonud, et rakendus on vahend, mis võimaldab teha kindlaks COVID-19-sse nakatunuga kokku puutunud isikuid ja anda neile teavet võimalike meetmete kohta (näiteks karantiini minemise ja testi tegemise võimalused) või selle kohta, mis vaid selgitab seda, mida teha avalduvate sümptomite korral. Suunistes rõhutatakse, et sellistest funktsioonidest on kasu nii üksikisikutele kui ka rahvaterviseasutustele³. Rakendus on seda mõjusam, mida rohkem inimesi seda kasutab.

Mõju seoses rakenduse kasutuselevõttuga:

- **Patsiendi** jaoks kiireneb info liikumine võimaliku nakatunuga lähikontaktis olemise kohta. Praegu võtab Terviseamet oma ülesannete täimisel nakatunuga ühendust, selgitab välja võimalikud lähikontaktid ning võtab omakorda lähikontaktsetega ühendust suuniste andmiseks. Rakendus muudab lähikontaktsete teavitamise kiiremaks ning suurendab ka teavitatud inimeste hulka. Nakatunu suudab reeglina meenutada lähikontaktsetena neid isikuid, kes on talle tuttavad, kuid rakenduse kaudu on võimalik teavitada ka neid, keda nakatunu ei mäleta või ei tunne (näiteks bussis tema kõrval istunud isikut), ning seda kõike isikuandmeid töötlemata.
- **Tervishoiuteenuse** osutajate jaoks väheneb eeldatavalt nakatunud ja ravivajavate isikute arv. Rakenduse kasutamine võimaldab isikutel vältida nakkusohtlikul perioodil kontakti teiste isikutega ning seetõttu väheneb ka haigestunud ja ravi vajavate isikute arv.
- **Eesti Haigekassa** eelarve kasutamine muutub efektiivsemaks, sest rakenduse kasutamine võimaldab isikutel ennetavalt võtta kasutusele meetmeid enda ja ka teiste isikute kaitseks, sest nakkusahelate läbilõikamisel väheneb nende inimeste arv, kes on nakatunud COVID-19-sse.

² Euroopa Komisjoni (EK) suunis [https://eur-lex.europa.eu/legal-content/ET/TXT/PDF/?uri=CELEX:52020XC0417\(08\)&from=ET](https://eur-lex.europa.eu/legal-content/ET/TXT/PDF/?uri=CELEX:52020XC0417(08)&from=ET) (17.4.2020, C 124/1-9).

³ EK suunis, p 3

- **Eesti majandus** saab rakendusest kasu efektiivsema kontaktteavitamise kaudu. Kontaktteavitus on üks meetmetest, mis aitab ohjata nakkushaiguste levikut pärast liikumiskiirangute leevendamist. Efektiivne kontaktteavitus aitab vältida vajadust suurt osa riigist sulgeda ning võimaldab majandustegevusel taastuda.

Andmekaitsealane mõjuhinna

Euroopa Komisjon on andnud välja andmekaitsega seotud suunised COVID-19 pandeemia vastast võitlust toetavate mobiilirakenduste kohta, milles on välja toodud, et liikmesriikide ja Euroopa Liidu (EL) 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. Selleks, et sellised mobiilirakendused välja töötataks ning et inimesed neid aktsepteeriks ja need kasutusele võtaksid, on tähtis tagada rakenduse usaldus. Inimesed peavad olema kindlad, et tagatud on mobiilirakenduste kooskõla põhiõigustega, et neid ei kasutata massiliseks jälgimiseks, vaid ainult täpselt kindlaks määratud eesmärgil ning et igaühele jääb kontroll oma andmete üle. Seepärast on väga oluline määrata kindlaks lahendused, millega sekkutakse kõige vähem isikute eraellu ning mis vastavad täielikult EL-i õiguses sätestatud isikuandmete kaitse ja eraelu puutumatuse nõuetele⁴.

Suunises käsitletakse ainult vabatahtlikke mobiilirakendusi, mis aitaksid kuidagi võidelda COVID-19 pandeemia vastu. See tähendab, et isik saab valida, kas laadida see endale telefoni või mitte. Komisjoni suunises on esitatud nõuded, mis tagavad isiku kontrolli oma andmete üle: rakendus peab olema vabatahtlik, rakenduse erinevaid funktsioone (teave, sümptomikontroll, kontaktide jälgimise ja hoiatamise funktsioonid) ei tohi kokku liita ning lähedusandmed tuleks salvestada üksikisiku seadmesse⁵. Eestis kasutatava rakenduse puhul on need nõuded täidetud. Näiteks saavad isikud teha sümptomite kontrolli koroonatesti veebilehe⁶ kaudu ning see ei ole rakendusega seotud.

Suunised ei käsitle olukorda, kus riik sekkuks isikute privaatsusesse n-ö jõuga (nt rakendused, mille ülesanne oleks tagada karantiin nõuete täitmine ehk isiku liikumine oleks jälgitav). Vabatahtliku valikuna tuuakse näidetena kolm rakendust:

- juhiste jagamiseks ehk **teabefunktsioon** ja isikuandmeid ei töödelda (millised on sümptomid; mida teha, kui need avalduvad; milline on COVID-19 nakkuse määr elanikkonnas jne);
- sümptomikontroll ja **telemeditsiin** ehk rakendus, mis töötleks terviseandmeid (nt antakse ette küsimustik, mis lubab eeldada, et tal on COVID-19 või nt antakse konkreetset meditsiinilist nõu, saab vastused oma muredele);
- haigetega **kokkupuutest teavitamiseks** (jälgitakse kontakte ja hoiatatakse rakenduse kasutajaid; võimaldab tuvastada, kas isik on teatud perioodil nakatunuga kokku puutunud ning kui on, siis võimaldab sel isikul jääda karantiini või otsustada minna testile).

Eestis võetakse kasutusele rakendus, mis on kooskõlas põhiõigustega ja isikuandmete kaitse põhimõtetega ning rakenduse kasutajaid ei ole võimalik jälgida (täpsem selgitus on rakenduse e-poes). Rakenduse enda kasutamisega ei selgu seda kasutavate isikute isikuandmed ega haigestunute isikuandmed ning rakenduse eesmärk on hoiatada isikuid eespool viidatud nakkushaigust põdenud isikutega kokkupuutumisest.

Rakendus töötab kasutajate telefonide poolt edastatud lähedusandmetel. Lähedusandmed on andmed, mis on saadud BLE tehnoloogia (väikese energiatarbega Bluetooth) kasutamisel ning BLE tehnoloogia kasutamisel ei ole andmeid võimalik jälgida (erinevalt geograafilise asukoha andmetest). Asukohaandmed ei ole kontaktide jälgimise funktsiooni seisukohast vajalikud, kuna

⁴ EK suunis, p 1

⁵ EK suunis, p 3.2

⁶ www.koroonatest.ee

⁶ EK suunis, p 3.4

nende eesmärk ei ole jälgida üksikisikute liikumist ega täita ettekirjutusi. Ka Euroopa Komisjon soovib kasutada läheduse kindlakstegemiseks BLE sideandmeid.⁷ Vastavalt Bluetooth'i signaali tugevusele registreerivad telefonid ära, kas kokkupuude teise inimesega oli lähikontakt. Lähikontakti tuvastamiseks vajalikud parameetrid on Terviseamet rakendusele ette määranud, lähtudes rahvusvahelistest soovitustest. Traditsiooniliselt loetakse lähikontaktiks kokkupuudet vähem kui 2 meetri kauguselt vähemalt 15 minuti jooksul nakatunu nakkusohtlikul perioodil.

Kasutusele võetav rakendus toimib nii, et kui rakendus on lähikontakti tuvastanud, talletub isiku telefonis lähikontakti anonüümne kood. Kui isik on saanud teada, et ta on nakatunud, on tal võimalik oma nakatumisest teada anda kinnituskoodi edastamisega. Nakkuse kinnitamine toimub TIS-i vahendusel. Selleks peab isik ennast TIS-i veebikeskkonnas (edaspidi *patsiendiportaal*) autentima. Oluline on siinkohal see, et autentimine toimub patsiendiportaalis, mitte rakenduses, st rakendus ei tuvasta isikut. Juhul kui isik on TIS-is olevate andmete põhjal nakatunud, kinnitatakse rakendusest TIS-i edastatud tuvastuskood ning kinnitatud isikustamata kinnituskood edastatakse rakendusele (mõlemad on isikustamata andmestikud).

Eelviidatu on oluline, kuna nakatumise kinnitamise protseduuri puhul tuleb välistada, et rakendust saaks väärkasutada, nt isikul ennast pahatahtlikult nakatunuks määrata, teavitades nii isikuid lähikontaktist nakatunuga, mis tegelikult aset ei leidnud. Väärkasutusega oleks võimalik ühiskonnas palju segadust tekitada. Seetõttu on eriti oluline, et nakatumise kinnitamine toimuks usaldusväärse allika juures, milleks TIS kindlasti on. Nakkuse usaldusväärse kinnitamise vajaduse on välja toonud ka Euroopa Komisjon oma juhendis.⁸ Kuna nakkuse kinnitamiseks kasutatakse kood on ühekordne, 256 biti pikkune ja juhuslikult valitud, pole selle äraarvamine jõumeetodil võimalik. TIS kontrollib nakkusstaatust ning positiivse diagnoosi korral kinnitab seda, andes koodile lisaks oma digitaalallkirja, mida välised osapooled võltsida ei suuda. Terviseandmestik, mille alusel kinnituskood genereeritakse, põhineb infosüsteemis olemasolevatel andmetel (st käesoleva rakendusega infosüsteem ise uut teavet ei omanda – positiivne või negatiivne saatekirja vastus on infosüsteemis olemas).

Kui isiku nakkus kinnitatakse, siis laetakse isiku nõusolekul (nõusolekut saab anda patsiendiportaalis) TIS-ist tema kinnituskood rakenduse kesksesse serverisse. Kinnituskoodi olemasolul teeb rakendus oma keskses serveris isiku anonüümse koodi kättesaadavaks, mille järel teise kasutaja telefonis olev rakenduse selle alla laeb. Anonüümse koodi põhjal ei ole kasutajatel võimalik inimest tuvastada. Kasutaja telefon võrdleb, kas nakatunu anonüümne kood ühtib mõne koodiga, mis on tema telefonisse talletunud või mitte. Kui jah, loetakse kasutaja lähikontaktseks ja ta saab vastava teavituse koos tegevusjuhistega. Kasutaja ei saa teada, kes oli see nakatunu, kellega ta kokku puutus, ega ka muud infot, mis võimaldaks nakatunut kaudselt tuvastada (kohtumise aeg jms).

Kontaktide jälgimise rakenduse kasutamise kohta on ka Euroopa Andmekaitse nõukogu (edaspidi *EDPB*) välja andnud juhised⁹, milles on rõhutatud, et andmekaitse õigusraamistik peab olema paindlik, et selle abil tõhusalt pandeemiat piirata, kaitstes samas ka inimõigusi ja vabadusi. Samuti on EDPB seisukohal, et rakenduse kasutamine peab olema vabatahtlik ning peaks toetuma lähedusandetele, mitte asukohaandmetele. EDPB juhis keskendub suures osas rakendustele, mis töötlevad isikuandmeid. Käesolev rakendus on aga loodud selliselt, et rakendus isikuandmeid ei töötle ning suur osa juhendis esitatud soovitusel ei olegi seetõttu asjakohased. Üritatud on rohkem, kui juhise järgi eeldatud.

Eestis arendatud rakendus on majutatud Eestis asuvas riigipilves ning tehnilist tuge sellele pakub Tervise ja Heaolu Infosüsteemide Keskus. Rakendus isikuandmeid ei töötle. Rakenduse kasutamise vajaduse otsustab nakkushaiguste ennetamise ja tõrje seaduses nimetatud pädev

⁷ EK suunis, p 3.4

⁸ EDPB juhis

https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_20200420_contact_tracing_covid_with_annex_en.pdf

asutus. Andmevahetus TIS-i ja rakenduse vahel ei toimu kogu aeg, vaid üksnes vastavalt vajadusele ja seda hindab Terviseamet, kellele kuulub ka rakendus.

Seega ei toimu rakenduses isikuandmete töötlemist ning andmed ei võimalda kasutajaid ja nakatunud isikuid tuvastada. Seetõttu on andmekaitsealne risk väga väike.

5. Määruse rakendamisega seotud tegevused, vajalikud kulud ja määruse rakendamise eeldatavad tulud

Rakenduse kasutuselevõtt on vabatahtlik, kaasnevad kulutused on Tervise ja Heaolu Infosüsteemide Keskusel. Nakatumise kinnitamise tehnilise lahenduse arendamise kulu on 42 000 eurot ning kuna tegemist on COVID-19 pandeemia levikut tõkestava IT arendusega, siis taotleme vahendeid arenduseks Vabariigi Valitsuse reservfondist. Kui täiendavaid vahendeid Vabariigi Valitsuse reservfondist ei eraldata, leitakse vahendid investeringuteks Sotsiaalministeeriumi valitsemisalast, vaadates üle olemasolevate IT-projektide tegevusplaanid. Projekti 2020. aasta halduskulud on TEHIK-ul olemas ning 2021. aasta halduskulud planeerib Sotsiaalministeerium 2021. aasta riigieelarve planeerimise käigus.

6. Määruse jõustumine

Määrus jõustub üldises korras.

7. Eelnõu kooskõlastamine, huvirühmade kaasamine ja avalik konsultatsioon

Eelnõu esitati eelnõude infosüsteemi EIS kaudu kooskõlastamiseks ministeeriumidele ning arvamuse avaldamiseks Tervise ja Heaolu Infosüsteemide Keskusele, Terviseametile ja Andmekaitse Inspeksioonile. Rahandusministeerium palus seletuskirja täiendada arendus- ja halduskulude osas, ametlikku kooskõlastuskirja ei esitatud. Eelnõu kohta esitas märkused Andmekaitse Inspeksioon, märkused on leitud seletuskirjale lisatud kooskõlastuse märkuste tabelist ning selgitused on omavahelisel kohtumisel läbi arutatud.