II

(Muud kui seadusandlikud aktid)

OTSUSED

KOMISJONI RAKENDUSOTSUS (EL) 2020/1023,

15. juuli 2020,

millega muudetakse rakendusotsust (EL) 2019/1765 seoses COVID-19 pandeemia vastase võitluse eesmärgil toimuva piiriülese andmevahetusega riiklike kontakti tuvastamise ja sellest teavitamise mobiilirakenduste vahel

(EMPs kohaldatav tekst)

EUROOPA KOMISJON,

võttes arvesse Euroopa Liidu toimimise lepingut,

võttes arvesse Euroopa Parlamendi ja nõukogu 9. märtsi 2011. aasta direktiivi 2011/24/EL patsiendiõiguste kohaldamise kohta piiriüleses tervishoius, ([1]) eriti selle artikli 14 lõiget 3,

ning arvestades järgmist:

(1) Direktiivi 2011/24/EL artikliga 14 on liidule antud ülesanne toetada ja soodustada koostööd ja teabe vahetamist liikmesriikide vahel vabatahtlikus võrgustikus, mis ühendab liikmesriikide määratud riiklikke asutusi, kes vastutavad e-tervise eest (edaspidi „e-tervise võrgustik“).

(2) Komisjoni rakendusotsuses (EL) 2019/1765 ([2]) on sätestatud eeskirjad e-tervise eest vastutavate riiklike asutuste võrgustiku loomiseks, haldamiseks ja toimimiseks. Kõnealuse otsuse artikliga 4 usaldatakse e-tervise võrgustikule ülesanne hõlbustada info- ja kommunikatsioonitehnoloogia süsteemide suuremat koostalitlusvõimet ning elektrooniliste terviseandmete piiriülest ülekantavust piiriüleste tervishoiuteenuste puhul.

(3) COVID-19 pandeemia põhjustatud rahvatervisekriisi arvestades on mitu liikmesriiki välja töötanud mobiilirakendused, mis toetavad kontaktide tuvastamist ja võimaldavad selliste rakenduste kasutajaid teavitada, et nad võtaksid asjakohaseid meetmeid, nt laseksid ennast testida või jääksid eneseisolatsiooni, kui nad on viirusega tõenäoliselt kokku puutunud lähikontakti tõttu mõne teise sellise rakenduse kasutajaga, kes on teatanud positiivsest diagnoosist. Need rakendused kasutavad seadmete vahelise läheduse kindlakstegemiseks Bluetoothi tehnoloogiat. Kuna liikmesriikide vahelised reisipiirangud on alates 2020. aasta juunist kaotatud, tuleks liikmesriikidel e-tervise võrgustiku raames saavutada riiklike info- ja kommunikatsioonitehnoloogia süsteemide suurem koostalitlusvõime, rakendades digitaalset taristut, mis aitab tagada riiklike kontakti tuvastamist ja sellest teavitamist toetavate mobiilirakenduste koostalitlusvõime.

([1]) ELT L 88, 4.4.2011, lk 45.

([2]) Komisjoni 22. oktoobri 2019. aasta rakendusotsus (EL) 2019/1765, milles sätestatakse e-tervise eest vastutavate riiklike asutuste võrgustiku loomise, haldamise ja toimimise eeskirjad ning millega tunnistatakse kehtetuks rakendusotsus 2011/890/EL (ELT L 270, 24.10.2019, lk 83).

(4) Komisjon on liikmesriike eespool nimetatud mobiilirakenduste väljatöötamisel toetanud. 8. aprillil 2020 võttis komisjon vastu soovituse liidu ühise meetmekogumi kohta, mis võimaldab kasutada tehnoloogiat ja andmeid COVID-19 kriisi vastu võitlemiseks ja kriisist väljumiseks (edaspidi „komisjoni soovitus“), milles on eelkõige keskendutud mobiilirakendustele ja anonüümitud liikuvusandmete kasutamisele ([3]). E-tervise võrgustikku kuuluvad liikmesriigid võtsid komisjoni toetusel vastu liikmesriikide jaoks ette nähtud ELi ühise mobiilirakenduste meetmekogumi, mis võimaldab toetada kontaktide tuvastamist, ([4]) samuti koostalitlusvõime alased suunised ELis kontakti tuvastamiseks heaks kiidetud mobiilirakenduste kohta ([5]). Meetmekogumis selgitatakse riikide nõudeid riiklike kontakti tuvastamise ja sellest teavitamise mobiilirakenduste jaoks, eelkõige seda, et need peaksid olema vabatahtlikud, asjaomase riikliku tervishoiuasutuse poolt heaks kiidetud, privaatsust tagavad ja neist tuleks loobuda kohe, kui neid enam ei vajata. COVID-19 kriisi viimaseid arengusuundumusi jälgides on nii komisjon ([6]) kui ka Euroopa Andmekaitsenõukogu ([7]) andnud välja andmekaitsega seotud suunised mobiilirakenduste ja kontaktide tuvastamise vahendite kohta. Liikmesriikide mobiilirakenduste ja nende koostalitlusvõimet võimaldava digitaalse taristu lahendus põhineb ELi ühisel meetmekogumil, eespool nimetatud suunistel ja e-tervise võrgustikus kokku lepitud tehnilistel kirjeldustel.

(5) Selleks et hõlbustada riiklike kontakti tuvastamise ja sellest teavitamise mobiilirakenduste koostalitlusvõimet, töötasid e-tervise võrgustikus osalevad liikmesriigid, kes otsustasid edendada oma sellealast koostööd vabatahtlikkuse alusel, komisjoni toetusel andmevahetuse IT-vahendina välja digitaalse taristu. Seda digitaalset taristut nimetatakse födereeritud väravaks.

(6) Käesoleva otsusega kehtestatakse sätted osalevate liikmesriikide ja komisjoni rolli kohta riiklike kontakti tuvastamise ja sellest teavitamise mobiilirakenduste piiriülese koostalitlusvõime jaoks loodava födereeritud värava toimimises.

(7) Riiklike kontakti tuvastamise ja sellest teavitamise mobiilirakenduste kasutajate isikuandmete töötlemine, mis toimub liikmesriikide või nende muude avalik-õiguslike organisatsioonide või ametiasutuste vastutusel, peaks toimuma kooskõlas Euroopa Parlamendi ja nõukogu määrusega (EL) 2016/679 ([8]) (edaspidi „isikuandmete kaitse üldmäärus“) ning Euroopa Parlamendi ja nõukogu direktiiviga 2002/58/EÜ ([9]). Komisjoni vastutusel toimuv isikuandmete töötlemine, mille eesmärk on hallata födereeritud väravat ja tagada selle turvalisus, peaks toimuma kooskõlas Euroopa Parlamendi ja nõukogu määrusega (EL) 2018/1725 ([10]).

(8) Födereeritud värav peaks olema turvaline IT-taristu ühise liidesega, mille kaudu määratud riiklikud asutused või ametiasutused saavad vahetada miinimumandmeid kontaktide kohta SARS-CoV-2ga nakatunud isikutega, et teavitada teisi nende võimalikust kokkupuutest kõnealuse nakkusega ja edendada toimivat tervishoiualast koostööd liikmesriikide vahel, hõlbustades asjakohase teabe vahetamist.

(9) Käesolevas otsuses tuleks seepärast sätestada ELis määratud riiklike asutuste või ametiasutuste vahel födereeritud värava kaudu toimuva piiriülese andmevahetuse kord.

([3]) Komisjoni 8. aprilli 2020. aasta soovitus (EL) 2020/518 liidu ühise meetmekogumi kohta, mis võimaldab kasutada tehnoloogiat ja andmeid COVID-19 kriisi vastu võitlemiseks ja kriisist väljumiseks, eelkõige seoses mobiilirakendustega ja anonüümitud liikuvusandmete kasutamisega (ELT L 114, 14.4.2020, lk 7).

([4]) https://ec.europa.eu/health/sites/health/files/ehealth/docs/covid-19_apps_en.pdf

([5]) https://ec.europa.eu/health/sites/health/files/ehealth/docs/contacttracing_mobileapps_guidelines_en.pdf

([6]) Komisjoni teatis „Andmekaitsega seotud suunised COVID-19 pandeemia vastast võitlust toetavate mobiilirakenduste kohta“ (ELT C 124I, 17.4.2020, lk 1).

([7]) Suunised 04/2020 asukohaandmete ja kontaktide tuvastamise vahendite kasutamise kohta COVID-19 pandeemia kontekstis ja Euroopa Andmekaitsenõukogu 16. juuni 2020. aasta avaldus kontakti tuvastamise rakenduste vahelise koostalitlusvõime mõju kohta andmekaitsele; mõlemad on kättesaadavad aadressil: https://edpb.europa.eu.

([8]) 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).

([9]) 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).

([10]) Euroopa Parlamendi ja nõukogu 23. oktoobri 2018. aasta määrus (EL) 2018/1725, mis käsitleb füüsiliste isikute kaitset isikuandmete töötlemisel liidu institutsioonides, organites ja asutustes ning isikuandmete vaba liikumist, ning millega tunnistatakse kehtetuks määrus (EÜ) nr 45/2001 ja otsus nr 1247/2002/EÜ (ELT L 295, 21.11.2018, lk 39).

(10) Osalevad liikmesriigid, keda esindavad määratud riiklikud asutused või ametiasutused, määravad koos kindlaks födereeritud värava kaudu toimuva isikuandmete töötlemise eesmärgi ja vahendid ning on seega kaasvastutavad töötlejad. Isikuandmete kaitse üldmääruse artiklis 26 on sätestatud isikuandmete töötlemise eest kaasvastutavate töötlejate kohustus määrata läbipaistval viisil kindlaks nende vastavad vastutusvaldkonnad kõnealuse määruse kohaste kohustuste täitmisel. Samuti on ette nähtud võimalus, et need ülesanded võib kindlaks määrata vastutava töötleja suhtes kohaldatavas liidu või liikmesriigi õiguses. Iga vastutav töötleja peaks tagama, et tema riigis on olemas õiguslik alus andmete töötlemiseks födereeritud värava kaudu.

(11) Komisjon kui födereeritud värava tehniliste ja organisatsiooniliste lahenduste pakkuja töötleb födereeritud väravas kaasvastutavate töötlejatena osalevate liikmesriikide nimel pseudonüümitud isikuandmeid ja on seega volitatud töötleja. Isikuandmete kaitse üldmääruse artiklis 28 ja määruse (EL) 2018/1725 artiklis 29 on sätestatud, et volitatud töötleja töötleb andmeid volitatud töötlejat ja vastutavat töötlejat omavahel siduva lepingu või liidu või liikmesriigi õiguse kohase siduva õigusakti alusel, milles täpsustatakse töötlemist. Käesoleva otsusega kehtestatakse eeskirjad, millega reguleeritakse andmete töötlemist komisjoni kui volitatud töötleja poolt.

(12) Isikuandmete töötlemisel födereeritud värava kaudu peab komisjon järgima komisjoni otsust (EL, Euratom) 2017/46 ([11]).

(13) Võttes arvesse seda, et eesmärgi jaoks, milleks vastutavad töötlejad riiklikes kontakti tuvastamise ja sellest teavitamise mobiilirakendustes isikuandmeid töötlevad, ei ole ilmtingimata vaja andmesubjekti tuvastamist, ei pruugi vastutavatel töötlejatel olla alati võimalik tagada andmesubjektide õiguste kohaldamist. Isikuandmete kaitse üldmääruse artiklites 15–20 osutatud õigusi ei pruugita seega kohaldada, kui kõnealuse määruse artikli 11 kohased tingimused on täidetud.

(14) Rakendusotsuse (EL) 2019/1765 kehtiv lisa tuleb kahe uue lisa lisamise tõttu ümber nummerdada.

(15) Seepärast tuleks rakendusotsust (EL) 2019/1765 vastavalt muuta.

(16) Võttes arvesse COVID-19 pandeemiaga seotud olukorra kiireloomulisust, tuleks käesolevat otsust kohaldada alates järgmisest päevast pärast selle avaldamist *Euroopa Liidu Teatajas*.

(17) Kooskõlas määruse (EL) 2018/1725 artikli 42 lõikega 1 konsulteeriti Euroopa Andmekaitseinspektoriga, kes esitas oma arvamuse 9. juulil 2020.

(18) Käesoleva otsusega ettenähtud meetmed on kooskõlas direktiivi 2011/24/EL artikli 16 kohaselt asutatud komitee arvamusega,

ON VASTU VÕTNUD KÄESOLEVA OTSUSE:

Artikkel 1

Rakendusotsust (EL) 2019/1765muudetakse järgmiselt:

1) artikli 2 lõikele 1 lisatakse punktid g, h, i, j, k, l, m, n ja o:

„g) „rakenduse kasutaja“ – isik, kelle valduses on nutiseade ja kes on alla laadinud kontakti tuvastamiseks ja sellest teavitamiseks kasutatava heakskiidetud mobiilirakenduse ning kasutab seda;

h) „kontakti tuvastamine“ – meetmed, mida rakendatakse eesmärgiga selgitada välja isikud, kes on kokku puutunud tõsise piiriülese terviseohu allikaga Euroopa Parlamendi ja nõukogu otsuse nr 1082/2013/EL (*) artikli 3 punkti c tähenduses;

([11]) Komisjoni 10. jaanuari 2017. aasta otsus (EL, Euratom) 2017/46 Euroopa Komisjoni side- ja infosüsteemide turvalisuse kohta (ELT L 6, 11.1.2017, lk 40). Komisjon avaldab lisateavet kõigi Euroopa Komisjoni infosüsteemide suhtes kohaldatavate turvastandardite kohta aadressil https://ec.europa.eu/info/publications/security-standards-applying-all-european-commission-information-systems_en.

i) „riiklik kontakti tuvastamise ja sellest teavitamise mobiilirakendus“ – nutiseadmetes, eelkõige nutitelefonides, käitatav riiklikul tasandil heaks kiidetud tarkvaraline rakendus, mis on tavaliselt projekteeritud ulatuslikult ja sihipäraselt veebiressursse kasutama, mis suudab töödelda lähedusandmeid ja iga nutiseadme paljude andurite kogutavat muud kontekstiteavet, selleks et tuvastada SARS-CoV-2ga nakatunutega toimunud kontaktid ja hoiatada isikuid, kes võivad olla SARS-CoV-2ga kokku puutunud. Nende mobiilirakenduste abil on võimalik tuvastada teiste Bluetoothi tehnoloogiat kasutavate seadmete olemasolu ja vahetada internetti kasutades teavet põhiserveritega;

j) „födereeritud värav“ – võrguvärav, mida haldab komisjon turvalise IT-vahendi kaudu ning mis võtab vastu, säilitab ja teeb liikmesriikide põhiserverite vahel kättesaadavaks minimaalse isikuandmete kogumi, et tagada riiklike kontakti tuvastamise ja sellest teavitamise mobiilirakenduste koostalitlusvõime;

k) „võti“ – kordumatu ajutine identifikaator, mis on seotud rakenduse kasutajaga, kes on teatanud SARS-CoV-2ga nakatumisest või kes võib olla SARS-CoV-2ga kokku puutunud;

l) „nakatumise kinnitus“ – meetod, mida kasutati SARS-CoV-2 nakkuse kinnitamiseks, see tähendab, et kas rakenduse kasutaja teatas sellest ise või tulenes see riikliku tervishoiuasutuse kinnitusest või laboratoorsest uuringust;

m) „huvialused riigid“ – liikmesriik või liikmesriigid, kus rakenduse kasutaja on 14 päeva jooksul enne võtmete üleslaadimise kuupäeva viibinud ja kus ta on riikliku kontakti tuvastamise ja sellest teavitamise heakskiidetud mobiilirakenduse alla laadinud ja/või kus ta on reisinud;

n) „võtmete päritoluriik“ – liikmesriik, kus asub võtmed födereeritud väravasse üles laadinud põhiserver;

o) „logiandmed“ – födereeritud värava kaudu töödeldavate andmete vahetamise ja neile juurdepääsuga seotud tegevuse automaatne salvestus, mis näitab eelkõige töötlemistoimingu liiki, töötlemistoimingu kuupäeva ja kellaaega ning andmeid töötleva isiku tunnust.

(*) Euroopa Parlamendi ja nõukogu 22. oktoobri 2013. aasta otsus nr 1082/2013/EL tõsiste piiriüleste terviseohtude kohta ja millega tunnistatakse kehtetuks otsus nr 2119/98/EÜ (ELT L 293, 5.11.2013, lk 1).“;

2) artikli 4 lõikele 1 lisatakse punkt h:

„h) anda liikmesriikidele suuniseid riiklike kontakti tuvastamise ja sellest teavitamise mobiilirakenduste vahel födereeritud värava kaudu toimuva isikuandmete piiriülese vahetamise kohta.“;

3) artikli 6 lõikele 1 lisatakse punktid f ja g:

„f) töötab välja, rakendab ja haldab asjakohaseid tehnilisi ja organisatsioonilisi meetmeid, mis on seotud isikuandmete edastamise ja säilitamise turvalisusega födereeritud väravas, et tagada riiklike kontakti tuvastamise ja sellest teavitamise mobiilirakenduste koostalitlusvõime;

g) toetab e-tervise võrgustikku, et leppida kokku riiklike asutuste tehnilises ja organisatsioonilises vastavuses födereeritud värava kaudu toimuva isikuandmete piiriülese vahetamise nõuetele, pakkudes ja viies läbi vajalikke teste ja auditeid. Komisjoni audiitoreid võivad abistada liikmesriikide eksperdid.“;

4) artiklit 7 muudetakse järgmiselt:

a) pealkiri asendatakse järgmisega: „E-tervise digiteenuste taristu kaudu töödeldavate isikuandmete kaitse“;

b) lõikes 2 asendatakse sõna „lisas“ tekstiga „I lisas“;

5) lisatakse artikkel 7a:

„*Artikkel 7a*

Riiklike kontakti tuvastamise ja sellest teavitamise mobiilirakenduste vahel födereeritud värava kaudu toimuv piiriülene andmete vahetamine

1. Kui isikuandmeid vahetatakse födereeritud värava kaudu, piirdub töötlemine eesmärgiga hõlbustada riiklike kontakti tuvastamise ja sellest teavitamise mobiilirakenduste koostalitlusvõimet födereeritud väravas ning kontaktide tuvastamise järjepidevusega piiriüleses kontekstis.

2. Lõikes 3 osutatud isikuandmed edastatakse födereeritud väravasse pseudonüümitud kujul.

3. Födereeritud värava kaudu vahetatavad ja seal töödeldavad pseudonüümitud isikuandmed sisaldavad üksnes järgmist teavet:

a) riiklike kontakti tuvastamise ja sellest teavitamise mobiilirakenduste poolt kuni 14 päeva enne võtmete üleslaadimise kuupäeva edastatud võtmed;

b) võtmetega seotud logiandmed kooskõlas võtmete päritoluriigis kasutatava tehnilise kirjelduse protokolliga;

c) nakatumise kinnitus;

d) huvialused riigid ja võtmete päritoluriik.

4. Födereeritud väravas isikuandmeid töötlevad määratud riiklikud asutused või ametiasutused tegutsevad födereeritud väravas töödeldavate andmete kaasvastutavate töötlejatena. Kaasvastutavate töötlejate vastavad kohustused jaotatakse vastavalt II lisale. Iga liikmesriik, kes soovib osaleda riiklike kontakti tuvastamise ja sellest teavitamise mobiilirakenduste vahelises piiriüleses andmete vahetamises, teatab enne ühinemist komisjonile oma kavatsusest ja märgib riikliku asutuse või ametiasutuse, mis on määratud vastutavaks töötlejaks.

5. Komisjon on födereeritud väravas töödeldavate isikuandmete volitatud töötleja. Volitatud töötlejana tagab komisjon isikuandmete töötlemise, sealhulgas edastamise ja majutamise turvalisuse födereeritud väravas ning täidab volitatud töötleja kohustusi, mis on sätestatud III lisas.

6. Komisjon ja födereeritud väravale juurdepääsu omavad riiklikud asutused kontrollivad ja hindavad födereeritud väravas toimuva isikuandmete töötlemise turvalisuse tagamiseks võetavate tehniliste ja organisatsiooniliste meetmete tulemuslikkust korrapäraselt.

7. Ilma et see piiraks kaasvastutavate töötlejate otsust lõpetada töötlemine födereeritud väravas, lõpetatakse födereeritud värava käitamine hiljemalt 14 päeva pärast seda, kui kõik ühendatud riiklikud kontakti tuvastamise ja sellest teavitamise mobiilirakendused lõpetavad võtmete edastamise födereeritud värava kaudu.“;

6) lisa muudetakse I lisaks;

7) lisatakse II ja III lisa, mille tekst on esitatud käesoleva otsuse lisas.

Artikkel 2

Käesolev otsus jõustub järgmisel päeval pärast selle avaldamist *Euroopa Liidu Teatajas*.

Brüssel, 15. juuli 2020

Komisjoni nimel
eesistuja
Ursula VON DER LEYEN

LISA

Rakendusotsusele (EL) 2019/1765 lisatakse II ja III lisa:

„II LISA

OSALEVATE LIIKMESRIIKIDE ÜLESANDED KAASVASTUTAVATE TÖÖTLEJATENA RIIKLIKE KONTAKTI TUVASTAMISE JA SELLEST TEAVITAMISE MOBIILIRAKENDUSTE VAHELISEKS PIIRIÜLESEKS ANDMETÖÖTLUSEKS ETTE NÄHTUD FÖDEREERITUD VÄRAVA PUHUL

1. JAGU

1. alajagu

Vastutusalade jaotus

1) Kaasvastutavad töötlejad töötlevad isikuandmeid födereeritud värava kaudu vastavalt e-tervise võrgustiku tehnilisele kirjeldusele ([1]).

2) Iga vastutav töötleja vastutab isikuandmete töötlemise eest födereeritud väravas kooskõlas isikuandmete kaitse üldmäärusega ja direktiiviga 2002/58/EÜ.

3) Iga vastutav töötleja loob üldpostkastiga varustatud kontaktpunkti, mida kasutatakse teabe vahetamiseks nii kaasvastutavate töötlejate vahel kui ka kaasvastutavate töötlejate ja volitatud töötleja vahel.

4) E-tervise võrgustiku poolt artikli 5 lõike 4 kohaselt loodud ajutisele allrühmale tehakse ülesandeks uurida kõiki probleeme, mis on seotud riiklike kontakti tuvastamise ja sellest teavitamise mobiilirakenduste koostalitlusvõimega ning asjaomaste isikuandmete töötlemisega kaasvastutavate töötlejate poolt, ning hõlbustada kooskõlastatud juhiste andmist komisjonile kui volitatud töötlejale. Muu hulgas võivad vastutavad töötlejad eespool nimetatud ajutise allrühma tegevuse käigus välja töötada ühise lähenemisviisi andmete säilitamiseks oma riiklikes põhiserverites, võttes arvesse födereeritud värava puhul kindlaks määratud säilitamistähtaega.

5) Juhiseid volitatud töötlejale tuleb saata kaasvastutavate töötlejate kontaktpunktide kaudu kokkuleppel teiste kaasvastutavate töötlejatega, kes kuuluvad eespool osutatud allrühma.

6) Juurdepääs kasutajate isikuandmetele, mida vahetatakse födereeritud värava kaudu, on ainult määratud riiklike asutuste või ametiasutuste volitatud isikutel.

7) Iga määratud riigiasutus või ametiasutus lakkab olemast kaasvastutav töötleja alates kuupäevast, mil ta födereeritud väravas osalemisest loobub. Ta jääb siiski vastutavaks selle töötlemise eest, mis toimus födereeritud väravas enne, kui osalemisest loobuti.

2. alajagu

Andmesubjektide taotluste käsitlemise ja teavitamisega seotud ülesanded ja vastutusvaldkonnad

1) Iga vastutav töötleja annab oma riikliku kontakti tuvastamise ja sellest teavitamise mobiilirakenduse kasutajatele (edaspidi „andmesubjektid“) teavet nende isikuandmete töötlemise kohta födereeritud väravas riiklike kontakti tuvastamise ja sellest teavitamise mobiilirakenduste piiriülese koostalitlusvõime eesmärgil kooskõlas isikuandmete kaitse üldmääruse artiklitega 13 ja 14.

2) Iga vastutav töötleja tegutseb riikliku kontakti tuvastamise ja sellest teavitamise mobiilirakenduse kasutajate kontaktpunktina ning käsitleb selliste kasutajate või nende esindajate poolt andmesubjektide õiguste kasutamiseks esitatud taotlusi kooskõlas isikuandmete kaitse üldmäärusega. Iga vastutav töötleja määrab andmesubjektidelt saadud taotlustega tegelemiseks sihtotstarbelise kontaktpunkti. Kui kaasvastutav töötleja saab andmesubjektilt taotluse, mis ei kuulu tema vastutusalasse, edastab ta selle viivitamata vastutavale kaasvastutavale töötlejale. Taotluse korral abistavad kaasvastutavad töötlejad üksteist andmesubjektide taotluste käsitlemisel ning vastavad üksteisele põhjendamatu viivituseta ja hiljemalt 15 päeva jooksul alates abitaotluse saamisest.

([1]) Eelkõige 16. juuni 2020. aasta koostalitlusvõime spetsifikatsioonid heakskiidetud rakenduste vaheliste piiriüleste ülekandeahelate kohta, mis on kättesaadavad aadressil: https://ec.europa.eu/health/ehealth/key_documents_en#anchor0.

3) Vastutav töötleja teeb andmesubjektidele kättesaadavaks käesoleva lisa sisu, sealhulgas punktides 1 ja 2 sätestatud korra.

2. JAGU

Turvaintsidentide, sealhulgas isikuandmetega seotud rikkumiste haldamine

1) Kaasvastutavad töötlejad abistavad üksteist födereeritud väravas töötlemisega seotud turvaintsidentide, sealhulgas isikuandmetega seotud rikkumiste kindlakstegemisel ja käsitlemisel.

2) Kaasvastutavad töötlejad teavitavad üksteist eelkõige järgmisest:

a) födereeritud väravas töödeldavate isikuandmete kättesaadavuse, konfidentsiaalsuse ja/või terviklusega seotud võimalikud või tegelikud ohud;

b) födereeritud värava töötlemistoimingutega seotud turvaintsidendid;

c) kõik isikuandmetega seotud rikkumised, isikuandmetega seotud rikkumise tõenäolised tagajärjed ja füüsiliste isikute õigusi ja vabadusi ähvardava ohu hindamine ning kõik meetmed, mis on võetud isikuandmetega seotud rikkumise käsitlemiseks ning füüsiliste isikute õigusi ja vabadusi ähvardava riski maandamiseks;

d) födereeritud värava töötlemistoimingutega seotud tehniliste ja/või organisatsiooniliste kaitsemeetmete rikkumine.

3) Kaasvastutavad töötlejad teavitavad komisjoni, pädevaid järelevalveasutusi ja vajaduse korral andmesubjekte kooskõlas määruse (EL) 2016/679 artiklitega 33 ja 34 või pärast komisjonilt teate saamist kõigist isikuandmetega seotud rikkumistest, mis leiavad aset födereeritud värava töötlemistoimingute käigus.

3. JAGU

Andmekaitsealane mõjuhinnang

Kui vastutav töötleja vajab isikuandmete kaitse üldmääruse artiklites 35 ja 36 sätestatud kohustuste täitmiseks teavet teiselt vastutavalt töötlejalt, saadab ta eritaotluse 1. jao 1. alajao punktis 3 osutatud üldpostkasti. Vastutav töötleja, kellele eritaotlus esitatakse, teeb asjaomase teabe andmiseks kõik endast oleneva.

III LISA

KOMISJONI ÜLESANDED ISIKUANDMETE VOLITATUD TÖÖTLEJANA RIIKLIKE KONTAKTI TUVASTAMISE JA SELLEST TEAVITAMISE MOBIILIRAKENDUSTE VAHELISEKS PIIRIÜLESEKS ANDMETÖÖTLUSEKS ETTE NÄHTUD FÖDEREERITUD VÄRAVA PUHUL

Komisjon teeb järgmist.

1) Loob ja tagab turvalise ja usaldusväärse sidetaristu, mis ühendab födereeritud väravas osalevate liikmesriikide riiklikke kontakti tuvastamise ja sellest teavitamise mobiilirakendusi. Oma kohustuste täitmiseks födereeritud värava volitatud töötlejana võib komisjon kaasata alamtöötlejatena kolmandaid isikuid; komisjon teavitab kaasvastutavaid töötlejaid kõigist alamtöötlejate lisamise või asendamisega seotud kavandatavatest muudatustest, andes seeläbi vastutavatele töötlejatele võimaluse esitada selliste muudatuste suhtes ühine vastuväide vastavalt II lisa 1. jao 1. alajao punktile 4. Komisjon tagab, et nende alamtöötlejate suhtes kohaldatakse samu andmekaitsekohustusi, mis on sätestatud käesolevas otsuses.

2) Töötleb isikuandmeid üksnes vastutavate töötlejate dokumenteeritud juhiste alusel, välja arvatud juhul, kui nõutakse töötlemist liidu või liikmesriigi õiguse alusel; sel juhul teatab komisjon sellest õiguslikust nõudest enne isikuandmete töötlemist vastutavatele töötlejatele, kui selline teatamine ei ole olulise avaliku huvi tõttu kõnealuse õigusega keelatud.

3) Andmete töötlemine komisjoni poolt hõlmab järgmist:

a) riiklike põhiserverite autentimine riiklike põhiserverite sertifikaatide alusel;

b) käesoleva rakendusotsuse artikli 7a lõikes 3 osutatud ja riiklike põhiserverite poolt üles laaditud andmete vastuvõtmine, pakkudes rakendusliidest, mis võimaldab riiklikel põhiserveritel asjaomaseid andmeid üles laadida;

c) riiklikest põhiserveritest saadud andmete säilitamine födereeritud väravas;

d) andmete allalaadimiseks kättesaadavaks tegemine riiklikele põhiserveritele;

e) andmete kustutamine, kui kõik osalevad põhiserverid on need alla laadinud või 14 päeva pärast asjaomaste andmete vastuvõtmist, olenevalt sellest, kumb kuupäev on varasem;

f) pärast teenuse osutamise lõppu kustutatakse kõik allesjäänud andmed, välja arvatud juhul, kui liidu või liikmesriigi õigusega nõutakse isikuandmete säilitamist.

Volitatud töötleja võtab töödeldavate andmete tervikluse säilitamiseks vajalikud meetmed.

4) Võtab födereeritud värava haldamiseks kõik organisatsioonilised, füüsilised ja loogilised turvameetmed, mida tehnika tase võimaldab. Sel eesmärgil teeb komisjon järgmist:

a) määrab födereeritud värava tasandil turbehalduse eest vastutava üksuse, edastab vastutavatele töötlejatele selle kontaktandmed ja tagab, et üksus on turvaohtudele reageerimiseks kättesaadav;

b) vastutab födereeritud värava turvalisuse eest;

c) tagab, et kõikide isikute suhtes, kellele antakse födereeritud väravale juurdepääs, kehtib lepinguline, ametialane või seadusjärgne konfidentsiaalsuskohustus.

5) Võtab kõik vajalikud turvameetmed, et mitte ohustada riiklike põhiserverite tõrgeteta toimimist. Selleks kehtestab komisjon erimenetlused, mis on seotud ühenduse loomisega riiklike põhiserverite ja födereeritud värava vahel. See hõlmab järgmist:

a) riskihindamismenetlus, et teha kindlaks süsteemi võimalikud ohud ja neid hinnata;

b) auditeerimis- ja läbivaatamismenetlus, et:

   i. kontrollida rakendatud turvameetmete ja kohaldatava turbepoliitika vastavust;

   ii. korrapäraselt kontrollida süsteemifailide, turvaparameetrite ja antud lubade terviklust;

   iii. teostada jälgimist, et avastada turvarikkumisi ja sissetunge;

   iv. teha muudatusi, et vältida olemasolevaid turvapuudusi, ning

   v. anda luba, sealhulgas vastutavate töötlejate taotluse korral, korraldada sõltumatuid auditeid, sealhulgas kontrolle, ja vaadata läbi julgeolekumeetmed, tingimusel et järgitakse Euroopa Liidu toimimise lepingu protokolli (nr 7) Euroopa Liidu privileegide ja immuniteetide kohta; ([2])

([2]) Protokoll (nr 7) Euroopa Liidu privileegide ja immuniteetide kohta (ELT C 326, 26.10.2012, lk 266).

c) muudatuse haldamise menetlus, et dokumenteerida ja mõõta muudatuse mõju enne selle rakendamist ning teavitada vastutavaid töötlejaid kõigist muudatustest, mis võivad mõjutada teabevahetust teiste riiklike taristutega ja/või nende turvalisust;

d) hooldus- ja remondimenetluse kehtestamine, et täpsustada seadmete hoolduse ja/või remondi korral kohaldatavaid eeskirju ja tingimusi;

e) turvaintsidentide korral kasutatava menetluse kehtestamine, et määrata kindlaks aruandlus- ja eskalatsioonikava, teavitada viivitamata vastutavaid töötlejaid ja Euroopa Andmekaitseinspektorit igast isikuandmetega seotud rikkumisest ning määrata kindlaks distsiplinaarmenetlus turvarikkumistega tegelemiseks.

6) Rakendab tipptasemel füüsilisi ja/või loogilisi turvameetmeid ruumides, kus asuvad födereeritud värava seadmed, ning loogiliste andmete kontrolli ja juurdepääsukontrolli puhul. Sel eesmärgil teeb komisjon järgmist:

a) tagab füüsilise julgeoleku, määrates eraldavad turvaperimeetrid ja võimaldades rikkumiste avastamist;

b) kontrollib juurdepääsu ruumidele ja peab jälgimise eesmärgil külastajate registrit;

c) tagab, et väliseid isikuid, kellele on antud juurdepääs ruumidele, saadavad nõuetekohaselt volitatud töötajad;

d) tagab, et seadmeid ei saa lisada, asendada ega eemaldada ilma selleks määratud vastutavate asutuste eelneva loata;

e) kontrollib riiklike põhiserverite juurdepääsu födereeritud väravale ja födereeritud värava juurdepääsu riiklikele põhiserveritele;

f) tagab kesksele födereeritud väravale juurdepääsu omavate isikute identimise ja autentimise;

g) vaatab födereeritud väravat mõjutava turvanõuete rikkumise korral uuesti läbi sellele taristule juurdepääsuga seotud loa andmise õigused;

h) säilitab födereeritud värava kaudu edastatud teabe tervikluse;

i) rakendab tehnilisi ja organisatsioonilisi turvameetmeid, et hoida ära loata juurdepääs isikuandmetele;

j) rakendab vajaduse korral meetmeid, et blokeerida loata juurdepääs födereeritud väravale riiklike kontaktpunktide domeenist (st blokeerida asukoht/IP-aadress).

7) Võtab meetmeid (sealhulgas ühenduste katkestamine), et kaitsta oma domeeni olulise kõrvalekalde korral kvaliteedi- või turvapõhimõtetest ja -kontseptsioonidest.

8) Haldab oma vastutusalaga seotud riskijuhtimiskava.

9) Jälgib födereeritud värava teenuste kõigi teenusekomponentide toimimist reaalajas, koostab korrapäraselt statistikat ja registreerib toiminguid.

10) Pakub födereeritud värava kõigi teenuste puhul inglise keeles ööpäeva- ja nädalaringset tuge telefoni, posti või veebiportaali kaudu ning võtab vastu kõnesid selleks loa saanud helistajatelt, kes on födereeritud värava koordinaatorid ja nende vastava kasutajatoe töötajad, projektiametnikud ja komisjonist määratud isikud.

11) Abistab vastutavaid töötlejaid asjakohaste tehniliste ja organisatsiooniliste meetmetega, niivõrd kui see on võimalik, et nad saaksid täita vastutava töötleja kohustust vastata isikuandmete kaitse üldmääruse III peatükis sätestatud taotlustele andmesubjekti õiguste kasutamiseks.

12) Toetab vastutavaid töötlejaid, esitades födereeritud väravaga seotud teavet, et nad saaksid täita isikuandmete kaitse üldmääruse artiklites 32, 35 ja 36 sätestatud kohustusi.

13) Tagab, et födereeritud väravas töödeldavad andmed on loetamatud kõigile isikutele, kellel ei ole juurdepääsuõigust.

14) Võtab kõik asjakohased meetmed, et hoida ära födereeritud värava operaatorite loata juurdepääs edastatavatele andmetele.

15) Võtab meetmeid, et hõlbustada födereeritud värava jaoks määratud vastutavate töötlejate koostalitlust ja suhtlust.

16) Peab registrit vastutavate töötlejate nimel tehtud töötlemistoimingute kohta vastavalt määruse (EL) 2018/1725 artikli 31 lõikele 2.“