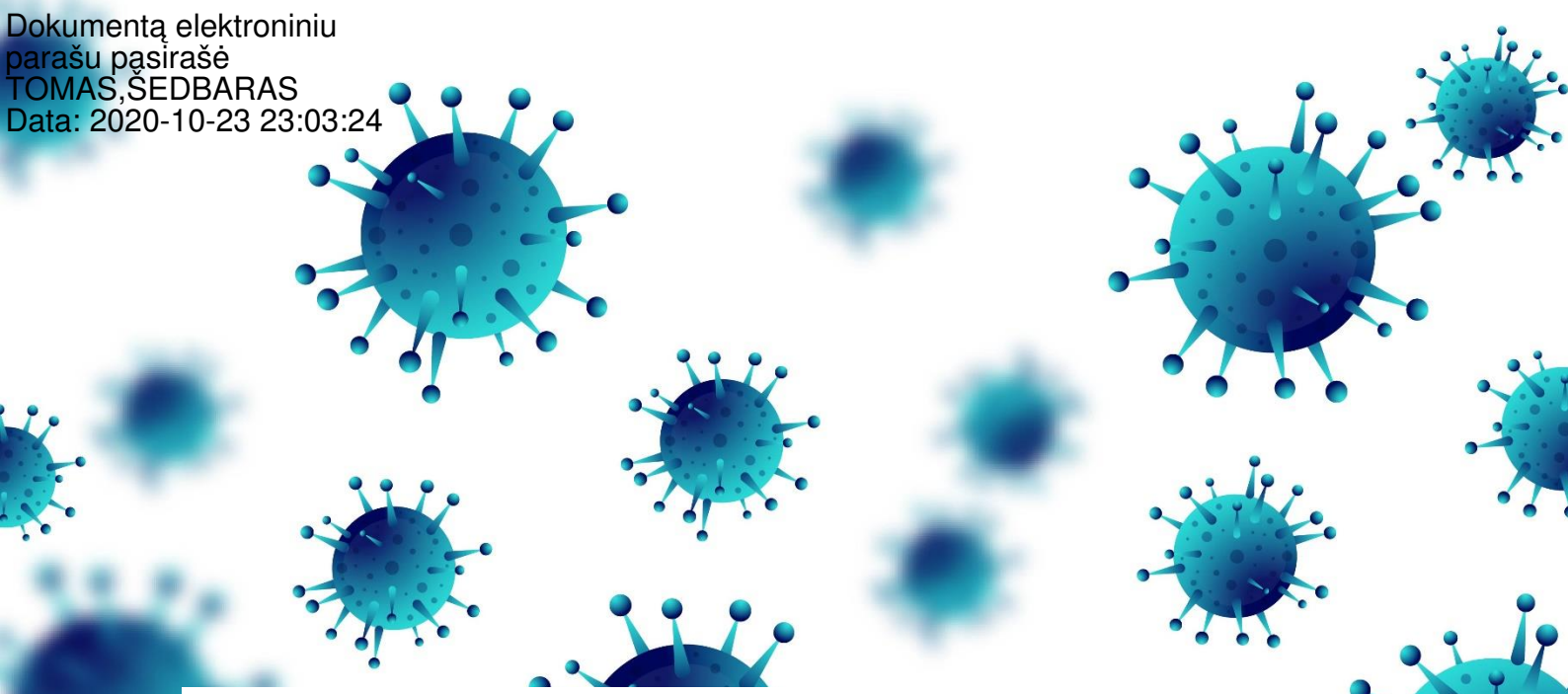


POVEIKIO DUOMENŲ APSAUGAI VERTINIMAS

Programėlė „Korona Stop LT“

SPALIO 23 D.

ŠEDBARO ADVOKATŲ PROFESINĖ BENDRIJA
Advokatas Tomas Šedbaras

TURINYS

TRUMPINIAI

APK – Užsikrėtimo Covid-19 infekcija atvejo patvirtinimo kodas
BDAR – 2016 m. balandžio 27 d. Europos Parlamento ir Tarybos reglamentas (ES) 2016/679 dėl fizinių asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo ir kuriuo panaikinama Direktyva 95/46/EB (Bendrasis duomenų apsaugos reglamentas)
BLE - mažai energijos naudojantis „Bluetooth“ (*angl. Bluetooth Low Energy)*
Covid-19 / koronavirusas - SARS-CoV-2 virusas.
ENF - Google ir Apple parengta pranešimo apie poveikį sistema (angl. Exposure Notification Framework)
ES – Europos Sąjunga
ESPBI IS - Elektroninės sveikatos paslaugų ir bendradarbiavimo infrastruktūros informacinė sistema
IVPK – Informacinės visuomenės plėtros komitetas
NKSC – Nacionalinis kibernetinio saugumo centras prie Krašto apsaugos ministerijos
NVSC – Nacionalinis visuomenės sveikatos centras prie Sveikatos apsaugos ministerijos
PDAV – BDAR 35 straipsnyje nustatyta poveikio duomenų apsaugai vertinimo sąvoka, kuri taip pat įtvirtinta Direktyvoje 2016/6803.
SAM – Sveikatos apsaugos ministerija
STS – Europos Komisijos sietinis tinklų sietuvas
TCP/UDP – duomenų perdavimo protokolai (angl. Transmission Control Protocol/User Datagram Protocol)
ULSKIS - Užkrečiamųjų ligų, galinčių išplisti ir kelti grėsmę, stebėsenos ir kontrolės informacinė sistema
VDAI – Valstybinė duomenų apsaugos inspekcija.

ĮŽANGA

Nuo to laiko, kai 2020 m. pradžioje SARS-CoV-2 virusas pradėjo plisti visoje Europoje, viešose ir politinėse diskusijose vis daugiau dėmesio buvo skiriama šios aktualiausios problemos technologiniam sprendimui. Ar pandemija gali būti sustabdyta naudojant kiekvieno asmens išmaniajame telefone esančias sekimo programas? Šios sistemos automatiškai užregistruotų visų programėlių naudotojų tarpusavio kontaktus ir taip leistų greitai atsekti viruso plitimo grandines. Tada potencialiai paveiktus asmenis būtų galima efektyviai nustatyti, norint juos izoliuoti ankstyvoje viruso stadijoje.

Programėlių funkcijos gali turėti skirtingą poveikį įvairioms ES pagrindinių teisių chartijoje įtvirtintoms teisėms, pavyzdžiui, žmogaus orumui, teisei į privatų ir šeimos gyvenimą, asmens duomenų apsaugai, judėjimo laisvei, nediskriminavimui, laisvei užsiimti verslu, susirinkimų ir asociacijų laisvei. Privatumo ir teisės į asmens duomenų apsaugą suvaržymas gali būti ypač svarbus atsižvelgiant į tai, kad kai kurios funkcijos grindžiamos daug duomenų reikalaujančiu modeliu.[1]

Tokios valstybės kaip Singapūras, Pietų Korėja ir Izraelis pasirinko radikalesnį požiūrį, strategiją, kuri Europos teisinės sistemos požiūriu reiškia neproporcingą pagrindinių teisių pažeidimą. Lietuvoje taip pat buvo bandymų kurti pandemijos sustabdymui skirtas programėles. Valstybinė duomenų apsaugos inspekcija (VDAI) vykdė programėlės „Karantinas“ stebėseną dėl asmens duomenų tvarkymo. Stebėsenos veiksmų priežiūros institucija ėmėsi įgyvendindama Bendrąjį duomenų apsaugos reglamentą (BDAR) ir reaguodama į žiniasklaidoje pasirodžiusią informaciją, susijusią su asmens duomenų tvarkymu programėle mobiliesiems įrenginiams „Karantinas“. VDAI įvertino stebėsenos metu surinktą informaciją ir nustatė, kad tvarkant asmens duomenis šia programėle gali būti pažeidžiamas BDAR 5 straipsnio 2 dalyje įtvirtintas atskaitomybės principas, kuris yra pagrindas vertinant asmens duomenų tvarkymo atitiktį kitiems BDAR 5 straipsnio 1 dalyje numatytiems asmens duomenų tvarkymo principams. Asmens duomenų tvarkymas nesilaikant minėtų principų sukelia potencialią grėsmę, kad duomenų subjekto teisės nebus tinkamai įgyvendinamos. Atsižvelgdama į stebėsenos rezultatus VDAI savo iniciatyva pradėjo tikrinimą ir priėmė sprendimą laikinai sustabdyti minėta programėle atliekamą asmens duomenų tvarkymą[2]. Programėlės veiklos stabdymai buvo vykdomi ne tik Lietuvoje. Norvegija 2020 m. birželio mėn. sustabdė programėlę išmaniesiems telefonams, skirtą stebėti ir sekti užsikrėtimo koronavirusu atvejus, kilus viešam ginčui tarp sveikatos apsaugos tarnybų ir duomenų apsaugos priežiūros institucijos. Norvegijos programėlė kėlė daugiausiai klausimų dėl jos „tiesioginio arba beveik tiesioginio programėlės naudotojų buvimo vietos sekimo“. Kitos šalys, pavyzdžiui, Vokietija, Italija, Šveicarija ir Latvija, naudoja „decentralizuotą“ modelį, pasitelkdamos „Android“ ir „Apple“ operacinių sistemų sąsajas. Pasak ekspertų, privatumo atžvilgiu tokios programėlės geresnės, nes duomenis jos saugo įrenginiuose[3]. Taigi, šiuo metu yra kuriamos artumo nustatymo sistemos, kurios yra palyginti palankesnės duomenų apsaugai nei kitos, net ir Europoje.

BDAR reikalauja, kad tais atvejais, kai dėl duomenų tvarkymo rūšies, visų pirma, kai naudojamos naujos technologijos, ir atsižvelgiant į duomenų tvarkymo pobūdį, aprėptį, kontekstą ir tikslus, fizinių asmenų teisėms bei laisvėms gali kilti didelis pavojus, duomenų valdytojas, prieš pradėdamas tvarkyti duomenis, atlieka numatytų duomenų tvarkymo operacijų poveikio asmens duomenų apsaugai vertinimą (PDAV)[4]. Programėlė „Korona Stop LT“ patenka į šią kategoriją. PDAV – tai procesas, skirtas duomenų tvarkymui aprašyti ir tokio tvarkymo reikalingumui ir proporcingumui įvertinti, padedantis valdyti pavojų, kuris fizinių asmenų teisėms ir laisvėms kyla dėl asmens duomenų tvarkymo, jį įvertinant ir nustatant šio pavojaus pašalinimo priemones. PDAV yra svarbi atskaitomybės priemonė, nes padeda duomenų valdytojams ne tik laikytis BDAR, bet ir įrodyti, kad, siekiant užtikrinti atitiktį Reglamentui, buvo imtasi tinkamų priemonių[5].

Taigi siekiama parengti BDAR 35 straipsnį atitinkantį PDAV, kad asmenų sąlyčio kontaktiniai (artumo) duomenys būtų apdorojami naudojant išmaniojo telefono programėlę. Tam gali prireikti artumo duomenų. Artumą ir artimą sąlytį tiksliau išmatuoti galima naudojantis mažai energijos naudojančią BLE technologiją turinčių prietaisų pranešimais. BLE leidžia nenaudoti sekimo funkcijos (priešingai nei naudojant geografinės vietos nustatymo duomenis).

Pagal duomenų tvarkymo apimtis programėlės gali būti skirstomos į tokius tipus:

---

[1] https://www.pepp-pt.org/content

[2] https://vdai.lrv.lt/lt/naujienos/nurodyta-laikinai-sustabdyti-programele-karantinas-del-galimai-netinkamo-asmens-duomenu-tvarkymo

[3] Skaitykite daugiau: https://www.delfi.lt/news/daily/world/norvegija-nebenaudos-covid-19-sekimo-programeles-kilus-susirupinimui-del-duomenu-saugumo.d?id=84543175

[4] BDAR 35 str. 1 dalis.

[5] Taip pat žr. BDAR 35 str. ir 84 konstatuojamoji dalis.

1) vietos duomenų (GNSS/GPS arba korinio ryšio prietaisų vietos nustatymo, mobiliojo telefono metaduomenų) apdorojimas;
2) judėjimo duomenų (suvestinių GPS, mobiliųjų telefonų metaduomenų) apdorojimas;
3) kontaktinių/artumo duomenų apdorojimas (artimos aplinkos jutikliai, pvz., BLE) ir įspėjimas apie galimą užsikrėtimo riziką.
3 tipo programėlę pagal duomenų saugojimo vietą galima būtų skirti į tokius potipius:
1) „centralizuotas“: serveris gauna visus užsikrėtusių naudotojų kontaktinius/artumo duomenis (įskaitant informaciją apie sąlytį turėjusių asmenų tapatybę), serveris informuoja naudotojus, kuriems gresia pavojus;
2) „decentralizuotas + epidemiologinis“: serveris gauna (matematiškai susijusius) užkrėstų asmenų raktus, išmaniajame telefone apskaičiuojama rizika ir naudotojas informuojamas vietoje. Sistema turi duomenų donorystės/pateikimo funkciją, kuria naudodamiesi naudotojai gali pateikti savo artumo istoriją epidemiologiniams tyrimams atlikti - šiais atvejais artumo duomenys yra atskleidžiami duomenų valdytojui ir institucijoms;
3) „visiškai decentralizuotas“: serveris gauna užkrėstų asmenų (matematiškai nepriklausomus) raktus, išmaniajame telefone apskaičiuojama rizika ir informuojamas naudotojas vietoje. Epidemiologiniams tyrimams programėlė institucijoms artumo duomenų neteikia.
PDAV atliekamas programėlei, kurioje duomenų tvarkymas vykdomas „visiškai decentralizuotai“. Pagrindinis duomenų tvarkymo operacijos tikslas sąlytį turėjusių asmenų išaiškinimas ir įspėjimas apie galimą užsikrėtimo pavojų. Naudotojų programėlių sugeneruoti laikini raktai perduodami per BLE ir tampa sveikatos duomenis generuojančiais raktais, jei bus pasidalinta duomenimis apie užsikrėtimą Covid-19. Po to Covid-19 infekcija užsikrėtęs asmuo juos siunčia į serverį, kur jie yra nuasmeninami taikant saugią atskyrimo procedūrą, užtikrinamą derinant teisines, organizacines ir technines priemones. Vėliau šiuos neidentifikuojančius infekciją rodančius duomenis gali atsisiųsti visi programėlės naudotojai. Tai leidžia kitiems naudotojams apskaičiuoti galimą užsikrėtimo riziką pagal kontaktinius/artumo duomenis, t. y. gautus „svetimus“ raktus, įskaitant trukmę ir signalo stiprumą.
Pasak WP 248[6], „PDAV turėtų būti pradėtas kuo anksčiau ir kai tai praktiškai įmanoma pritaikant duomenų tvarkymo operaciją, net jeigu tam tikros duomenų tvarkymo operacijos dar nėra žinomos. PDAV atnaujinimas projekto gyvavimo metu padės užtikrinti, kad būtų paisoma duomenų apsaugos ir privatumo ir paskatins kurti sprendimo būdus, padedančius laikytis reikalavimų. Progresuojant kūrimo procesui, taip pat gali prireikti pakartoti atskirus vertinimo etapus, nes tam tikrų techninių ar organizacinių priemonių pasirinkimas gali daryti poveikį duomenų tvarkymo keliamų pavojų rimtumui ar tikimybei.“ Todėl PDAV projektas vykdomas kartu su paslaugų teikėjų kuriama „Korona Stop LT“ programėle.
Siekdamos palengvinti nacionalinių kontaktų atsekimo ir įspėjimo programėlių sąveiką, e. sveikatos tinkle dalyvaujančios valstybės narės, kurios nusprendė savanoriškai aktyviau bendradarbiauti šioje srityje, padedamos Europos Komisijos sukūrė skaitmeninę infrastruktūrą kaip IT priemonę keitimuisi duomenimis. Ši skaitmeninė infrastruktūra vadinama sietiniu tinklų sietuvu[7]. Šiame PDAV nebus nagrinėjamas duomenų tvarkymas, susijęs su Europos Komisijos tvarkomu nacionalinių kontaktų atsekimo ir įspėjimo programėlių sąveiką užtikrinančiu sietiniu tinklų sietuvu. Šios duomenų tvarkymo operacijos PDAV projektą visoms šalims ruošia Europos Komisija.

[6] 29 straipsnio duomenų apsaugos darbo grupė (2017 m.). Poveikio duomenų apsaugai vertinimo (PDAV) gairės, kuriomis Reglamento 2016/679 taikymo tikslais nurodoma, kaip nustatyti, ar duomenų tvarkymo operacijos gali sukelti didelį pavojų. Paskutinį kartą peržiūrėtą ir priimtą 2017 m. Spalio 4 d. WP 248
[7] 2020 m. liepos 15 d. Komisijos įgyvendinimo sprendimas (ES) 2020/1023, kuriuo dėl nacionalinių kontaktų atsekimo ir įspėjimo programėlių tarpvalstybinio keitimosi duomenimis kovojant su Covid-19 pandemija iš dalies keičiamas Įgyvendinimo sprendimas (ES) 2019/1765

NAUDOTI DOKUMENTAI, KURIŲ PAGRINDU ATLIKTAS PDAV

Norėdami metodiškai atlikti šį PDAV pagal BDAR 35 straipsnį, rėmėmės šiais dokumentais:

- 29 straipsnio duomenų apsaugos darbo grupė (2013 m.). *Nuomonė Nr. 03/2013 dėl tikslo ribojimo*. WP 203
- 29 straipsnio duomenų apsaugos darbo grupė (2017 m.). *Poveikio duomenų apsaugai vertinimo (PDAV) gairės, kuriomis Reglamento 2016/679 taikymo tikslais nurodoma, kaip nustatyti, ar duomenų tvarkymo operacijos gali sukelti didelį pavojų.* Paskutinį kartą peržiūrėtą ir priimtą 2017 m. Spalio 4 d. WP 248
- 29 straipsnio duomenų apsaugos darbo grupė (2017 m.). *Gairės dėl sutikimo pagal Reglamentą 2016/679* Paskutinį kartą peržiūrėta ir priimta 2018 m. balandžio 10 d. (WP 259)
- The methodology of the French Data Protection Authority (CNIL) (2018 m.). *Privacy Impact Assessment (PIA) Methodology*
- Valstybinė duomenų apsaugos inspekcija (2018 m.). *Rekomendacija smulkiajam ir vidutiniams verslui dėl Bendrojo duomenų apsaugos reglamento taikymo*
- Valstybinė duomenų apsaugos inspekcija (2020 m.). *Tvarkomų asmens duomenų saugumo priemonių ir rizikos įvertinimo gairės duomenų valdytojams ir duomenų tvarkytojams* (3 versija, 2020-06-18)
- Europos Sąjunga (2016 m.) (BDAR). *2016 m. balandžio 27 d. Europos Parlamento ir Tarybos reglamentas (ES) 2016/679 dėl fizinių asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo ir kuriuo panaikinama Direktyva 95/46/EB (Bendrasis duomenų apsaugos reglamentas)*, OL L 119, 2016 5 4, 1–88
- Europos Sąjunga (2020 m.). Europos Komisijos komunikatas „*Duomenų apsaugos gairės dėl kovai su Covid-19 pandemija naudojamų programėlių*“ (2020/C 124 I/01)
- Europos Sąjunga (2020 m.). *Europos Komisijos 2020 m. liepos 15 d. įgyvendinimo sprendimas (ES) 2020/1023, kuriuo dėl nacionalinių kontaktų atsekimo ir įspėjimo programėlių tarpvalstybinio keitimosi duomenimis kovojant su COVID-19 pandemija iš dalies keičiamas Įgyvendinimo sprendimas (ES) 2019/1765*
- Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung (2020 m.). *Data Protection Impact Assessment for the Corona App*
- EDAV ir EDAPP (2019 m.). *Bendra EDAV ir EDAPP nuomonė Nr. 1/2019 dėl pacientų duomenų tvarkymo ir dėl Europos Komisijos vaidmens e. sveikatos skaitmeninių paslaugų infrastruktūroje (eHDSI)*
- Valstybinė duomenų apsaugos inspekcija*. Duomenų tvarkymo operacijų, kurioms taikomas reikalavimas atlikti poveikio duomenų apsaugai vertinimą, sąrašas patvirtintas Valstybinės duomenų apsaugos inspekcijos direktoriaus 2019 m. kovo 14 d. įsakymu Nr. 1T- 35 (1.12.E).*
- European Centre for Disease Prevention and Control*. Mobile applications in support of contact tracing for COVID-19 – A guidance for EU/EEA Member States, 10 June 2020. Stockholm: ECDC; 2020.*

1 KONTEKSTAS

1.1 DUOMENŲ TVARKYMO OPERACIJOS APŽVALGA

Programos naudojimas bus visiškai savanoriškas ir ją bus galima nemokamai atsisiųsti iš „Apple App Store“ ir „Google Play“ parduotuvės. Jis veiks „iPhone“, palaikančiuose „iOS 13.5“ (ar naujesnę) ir „Android“ telefonuose, kuriuose veikia 6.0 ir naujesnės versijos „Android“.

NAGRINĖJAMOS DUOMENŲ TVARKYMO OPERACIJOS APRAŠYMAS

Trumpas duomenų tvarkymo operacijos aprašymas (pobūdis, apimtis, kontekstas)	Šiame PDAV aptariamas tik savanoriškos kovoti su Covid-19 pandemija padedančios programėlės (asmenų savanoriškai atsisiunčiamos, įdiegiamos ir naudojamos programėlės), turinčios įspėti asmenis, kurie tam tikrą laiką buvo netoli užkrėsto asmens, kad galėtų pateikti informaciją, pvz., apie tai, ar jiems taikoma saviizoliacija ir kur vykti atlikti tyrimo. Duomenys tvarkomi dideliu mastu, nes programėlė skirta visiems Lietuvos Respublikos gyventojams nuo 16 metų. Lietuvai prisijungus prie Europos sietinio tinklų sietuvo duomenimis bus keičiamasi tarp ES šalių narių. Duomenų tvarkymo kontekstas tikrai unikalus. Visos pasaulio šalys susidūrė su situacija, kurioje daugiau klausimų nei atsakymų ir duomenų tvarkymo operacijos nėra išbandytos. Duomenų tvarkymo operacijos vertinimo sudėtingumą lemia tai, jog tvarkant užsikrėtimo COVID-19 rizikos duomenis yra tvarkomi ir sveikatos duomenys.
Duomenų tvarkymo tikslas	Nustatyti Covid-19 infekcijos plitimo grandines ir jas nutraukti, t. y. nustatyti programėlę naudojančių asmenų, kurie turėjo sąlytį su Covid-19 užsikrėtusiu asmeniu, artumo duomenis, kad būtų galima įspėti užsikrėsti galėjusiu asmenis ir informuoti juos dėl tolesnių tinkamų veiksmų.
Duomenų tvarkymo nauda (įstaigai, duomenų subjektams, apskritai visuomenei)?	Sąlytį turėjusių asmenų išaiškinimo ir įspėjimo funkcijos yra priemonės, skirtos nustatyti asmenis, kurie turėjo sąlytį su Covid-19 užsikrėtusiu asmeniu, ir informuoti juos dėl tolesnių tinkamų veiksmų, kaip antai, saviizoliacijos, tyrimų, ar konsultuoti juos dėl to, ką daryti, jei pasireiškia simptomai. Todėl ši funkcija yra naudinga ir asmenims, ir visuomenės sveikatos institucijoms. Ji taip pat gali atlikti svarbų vaidmenį valdant izoliavimo priemones vykdant plitimo priemonių atšaukimo strategiją. Jų poveikis gali būti stipresnis taikant strategiją, kuria remiamas platesnio masto asmenų, kuriems pasireiškia lengvi simptomai, tyrimas. Kontaktų atsekimas yra patikrintas metodas, padedantis sustabdyti viruso plitimą. Siekiama kuo greičiau informuoti atitinkamus užkrėstų atvejų kontaktus apie užsikrėtimo galimybę, kad būtų galima laiku imtis tinkamų priemonių. Covid-19 atveju didelė perdavimų dalis vyksta per lašelius, kurie pasklinda tik tam tikru atstumu (apie 2 metrus). Taigi „kontaktai“ yra žmonės, kurie galėjo būti paveikti viruso tokiu būdu, per fizinį artumą.
Duomenų valdytojas	SAM
Duomenų tvarkytojai	NVSC

DUOMENŲ TVARKYMUI TAIKOMI STANDARTAI

Duomenų tvarkymui taikomi teisės aktai ir standartai
Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatymas
Lietuvos Respublikos kibernetinio saugumo įstatymas
Bendrųjų elektroninės informacijos saugos reikalavimų apraše, patvirtintame Lietuvos Respublikos Vyriausybės 2013 m. liepos 24 d. nutarimu Nr. 716 „Dėl Bendrųjų elektroninės informacijos saugos reikalavimų aprašo, Saugos dokumentų turinio gairių aprašo ir Elektroninės informacijos, sudarančios valstybės informacinius išteklius, svarbos įvertinimo ir valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo gairių aprašo patvirtinimo“
Organizacinių ir techninių kibernetinio saugumo reikalavimų, taikomų kibernetinio saugumo subjektams, aprašas, patvirtintas Lietuvos Respublikos Vyriausybės 2018 m. rugpjūčio 13 d. nutarimu Nr. 818 „Dėl Lietuvos Respublikos kibernetinio saugumo įstatymo įgyvendinimo“
Lietuvos standartuose LST ISO/IEC 27001 „Informacinės technologijos. Saugumo metodai. Informacijos saugumo valdymo sistemos. Reikalavimai“
LST ISO/IEC 27002 „Informacinės technologijos. Saugumo metodai. Informacijos saugumo kontrolės priemonių praktikos nuostatai“
Užkrečiamųjų ligų, galinčių išplisti ir kelti grėsmę, stebėsenos ir kontrolės informacinės sistemos duomenų saugos nuostatai, patvirtinti Lietuvos Respublikos sveikatos apsaugos ministro 2020 m. gegužės 5 d. įsakymu Nr. V-1067 „Dėl Užkrečiamųjų ligų, galinčių išplisti ir kelti grėsmę, stebėsenos ir kontrolės informacinės sistemos steigimo ir jos nuostatų bei duomenų saugos nuostatų patvirtinimo“

1.2 DUOMENYS, PROCESAI IR PAGALBINĖS PRIEMONĖS

DUOMENŲ APRAŠYMAS, GAVĖJAI IR SAUGOJIMO TRUKMĖ

Šiame dokumento skyriuje aprašomi duomenys, kurie bus tvarkomi, kiek duomenų surenkama ir naudojama, kaip dažnai jie bus tvarkomi, kiek laiko jie bus saugomi ir su kuo duomenys yra susiję.

Siūlomas duomenų tvarkymas susijęs su visais šalies gyventojais, kurie turi išmanųjį telefoną, atitinkantį nustatytus ENF reikalavimus ir kurie pasirenka atsisiųsti ir įdiegti programėlę.

Telefonai su aktyvia ENF nuolat ieškos kitų netoliese esančių telefonų, kuriuose aktyvus ENF. Tai atsitinka neatsižvelgiant į tai, kuri nacionalinė artumo registravimo programėlė yra įdiegta telefone, jei telefone veikia naujausia „Apple“ ir „Google“ operacinė sistema, įtraukianti ENF paslaugą. ENF neveikia telefonuose, kuriuose nėra įdiegta nacionalinė kontaktų paieškos programėlė.

Įvairiems tvarkomų duomenų tipams taikomi įvairūs saugojimo apribojimai, kurie lentelės forma išdėstyti žemiau šiame dokumento skyriuje. Visuotinė duomenų, susijusių su programėle, saugojimo politika yra ta, kad jokie asmens duomenys nebus tvarkomi po pandemijos laikotarpio[8], vadovaujantis naujausiomis Europos duomenų apsaugos valdybos gairėmis dėl tokių programėlių įvedimo. Panaikinimas apims tokias priemones kaip aiškių programėlės ištrynimo gairių pateikimas, programos pašalinimas iš programėlių parduotuvių, saugus visų asmeninių duomenų ir užsikrėtimo raktų naikinimas iš Programėlės serverio ir visų programėlės funkcijų išjungimas.

Programos naudotojai turi teisę būti pamiršti. Pasirinkus funkciją „Atkurti programėlę“, bus pašalinti visi programėlės turimi duomenys. Ištrynę programėlę iš telefono, taip pat pašalinsite visus programėlės duomenis iš telefono. Visus programėlės duomenis galima pašalinti bet kuriuo metu, o NVSC niekaip negali žinoti, kas pasirenka atkurti programėlę ar pašalinti ją.

Asmens duomenys	**Asmenys, turintys teisę tvarkyti**	**Saugojimo terminas**
Artumo raktas (pseudoniminis) Informaciniame modelyje artumo raktas atvaizduoja laikinai ribotą programėlės naudotojo buvimą šalia. Šiame artumo rakte nėra jokios informacijos apie	Šios informacijos gavėjai yra kiti programėlės naudotojai, esantys BLE diapazone.	14 kalendorinių dienų

[8] Tai numatyta ir Užkrečiamųjų ligų, galinčių išplisti ir kelti grėsmę, stebėsenos ir kontrolės informacinės sistemos nuostatų, patvirtintų Lietuvos Respublikos sveikatos apsaugos ministro 2020 m. gegužės 5 d. įsakymu Nr. V-1067 „Dėl Užkrečiamųjų ligų, galinčių išplisti ir kelti grėsmę, stebėsenos ir kontrolės informacinės sistemos steigimo ir jos nuostatų bei duomenų saugos nuostatų patvirtinimo“ 35 punkte.

vietą, laiką ar asmenį, tačiau jis yra asmeninis, jei jis yra asmens, siunčiančiojo ar priimančiojo išmaniajame telefone. Ši informacija keičiama reguliariais intervalais, pavyzdžiui, kas 5, 10, 15 ar 30 minučių.		
Atstumas Atstumas yra numatomas atstumas tarp dviejų išmaniųjų telefonų, esančių fiziniame diapazone. Jį nustato jutikliai, naudojant gaunamų artumo raktų BLE signalo stiprumą. Tačiau sukurtas signalo stiprumo ir atstumo ryšys pagrįstas skirtingomis prielaidomis apie fizinę ir techninę situaciją. Pavyzdžiui, viena prielaida yra ta, kad išmaniojo telefono vieta yra identiška programėlės naudotojo vietai trimatėje erdvėje. Kita prielaida yra ta, kad kontaktiniame lauke nėra erdvę dalijančių elementų (pavyzdžiui, stiklinės sienos).	Atitinkami duomenys saugomi kartu su gaunamu svetimu artumo raktu naudotojo telefone ir prieinami tik naudotojui.	14 kalendorinių dienų
Trukmė Trukmė nurodo registruotą identiškų artumo raktų skaičių laiko atžvilgiu.	Duomenys saugomi programėlės naudotojo išmaniajame telefone kartu su gaunamu svetimu artumo raktu ir prieinami tik naudotojui.	14 kalendorinių dienų
Programėlės naudotojo užsikrėtimo atvejis Infekcijos būsena turi keletą programėlės būsenų: neužkrėsta, užkrėsta. Pirmoji būsena yra numatytoji būsena. Antroji būsena atsiranda dėl sąlyčio atvejų su užkrėstais asmenimis. Jei infekcijos būsena yra „užkrėsta“, ši informacija perduodama programėlės serveriui perduodant užsikrėtusiųjų raktus. Po nuasmeninimo serveryje yra tik anoniminiai užsikrėtimo atvejį nurodantys duomenys (užsikrėtimo raktai).	Anoniminiai užsikrėtimo atvejį nurodantys duomenys (užsikrėtimo raktai) saugomi programėlės serveryje ir teikiami kitiems programėlės naudotojams.	14 kalendorinių dienų
Rizikos balas Jei sutampa gauti artumo raktai ir iš serverio gauti anoniminiai užsikrėtimo atvejį nurodantys duomenys (užsikrėtimo raktai), individualus rizikos balas apskaičiuojamas pagal sąlyčio atvejus naudojant statistinio skaičiavimo taisykles, vertinant kontakto trukmę ir atstumą. Jei šis balas viršija nustatytą ribinę vertę, suaktyvinamas naudotojo pranešimas.	Rizikos balas saugomas tik naudotojo išmaniajame telefone ir prieinamas tik naudotojui.	14 kalendorinių dienų
IP adresai IP adresas yra būtinas bendravimui internete (maršruto parinkimas, adresavimas). Dėl interneto architektūros šių duomenų gavėjai pirmiausia yra serverių operatoriai, antra, interneto paslaugų teikėjai. IP adresas yra būtinas bent trimis skirtingais programėlės naudojimo atvejais: (a) gaunant programą iš diegimo šaltinio internete, (b) iš serverio gaunant anoniminius užsikrėtimo atvejį nurodančius duomenis (užsikrėtimo raktus), ir (c) pranešant serveriui savo užsikrėtimo raktus, jei naudotojui nustatytas Covid-19 atvejis.	Programėlės serveris, interneto ryšio paslaugų teikėjai. Šis duomuo tvarkomas tik tiek, kiek naudojantis programėle yra naudojamas internetas, tačiau su kitais programėlėje tvarkomais duomenimis nėra siejamas ir nesaugomas.	Nesaugomas
Laiko specifikacija Laiko specifikacijoje nurodoma kontakto data.	Ši data kartu su gautu svetimu artumo raktu yra saugoma programėlės naudotojo	14 kalendorinių dienų

	išmaniajame telefone ir yra prieinama tik naudotojui.	
APK (atvejo patvirtinimo kodas) APK generuoja NVSC ir pateikia asmeniui, kuriam nustatytas Covid-19 atvejis. Šis APK reguliuoja prieigos kontrolę serveryje ir leidžia asmeniui ir tik asmeniui perduoti savo užsikrėtimo raktą į serverį.	NVSC darbuotojas, turintis prieigą prie ULSKIS ir programėlės naudotojas.	21 kalendorinė diena
Mobilaus telefono ryšio numeris Nustačius Covid-19 atvejį, NVSC susisiekia su asmeniu, jei asmuo yra programėlės naudotojas ir nusprendžia įkelti savo užsikrėtimo raktus, jis patvirtina savo mobiliojo telefono numerį, į kurį SMS žinute siunčiamas APK leidžiantis įkelti užsikrėtimo raktus. Programėlės serveris naudotojui SMS žinute siunčia APK, leidžiantį įkelti užsikrėtimo raktus, APK naudotojas gali įvesti į programėlę. Kadangi šie duomenys tvarkomi tik užsikrėtimo atveju, jie laikomi sveikatos duomenimis.	NVSC darbuotojas, turinis prieigą prie ULSKIS, ir aktyvuojantis APK siuntimą programėlės naudotojui SMS žinute.	Kai tik išsiunčiama SMS žinutė, telefono numeris ištrinamas ir išsaugomas tik kodas su simptomo data.

Nagrinėjamu atveju svarbu įvertinti, ar duomenų tvarkymo operacijos metu yra tvarkomi asmens duomenys, todėl žemiau pateikiame lentelėje nurodytų duomenų paaiškinimą šiuo aspektu.
Asmens duomenų ir duomenų tvarkymo sąvokos yra apibrėžtos BDAR 4 straipsnio 1 ir 2 punktuose.
Programėlėje renkami artumo duomenys nėra aiškiai apibrėžti BDAR. Artumo duomenys nustatomi lyginant artumo raktus. Jie sugeneruojami asmens išmaniajame telefone ir yra susiję su asmeniu tol, kol jie yra saugomi išmaniajame telefone.
Programėlėje yra tvarkomi ir sveikatos duomenys, kurių sąvoka apibrėžta BDAR 4 str. 15 punkte. Jei asmeniui nustatomas Covid-19 atvejis, NVSC duomenų subjektui išsiunčia atvejo patvirtinimo kodą (APK), o tai reiškia, kad pateikia sveikatos duomenis; tas pats pasakytina apie užsikrėtusių asmenų, gavusių APK, užsikrėtimo raktą. Jei sveikatos duomenys perduodami į serverį (-ius) ir jei valdytojas įgyvendina veiksmingą nuasmeninimo procedūrą, gauti duomenys yra anoniminiai užsikrėtimo atvejį nurodantys duomenys.
Atsižvelgiant į tai, galima teikti, kad šiai duomenų tvarkymo operacijai taikomos BDAR nuostatos.
Dar vienas svarbus aspektas šifruotų ir pseudoniminių duomenų tvarkymas. Asmens duomenų šifravimas ar pseudonimizavimas neturi reikšmės vertinant, ar asmens duomenys yra tvarkomi (žr. EDAV ir EDAPP 2019, 8 dalį[9]). Norint patvirtinti asmens duomenų tvarkymą, pakanka, kad artumo raktai buvo sugeneruoti naudotojo galinėje įrangoje. Tai, kad artumo raktų žymenys siunčiami šifruota forma per saugų tinklą, nekeičia asmeninio šių žymenų pobūdžio. Net ir tvarkant šifruotus asmens duomenis, duomenų susiejimas su asmeniu vis tiek lieka.
Šiomis aplinkybėmis yra tikslinga manyti, kad vienintelis asmens duomuo, kuris tvarkomas programėlės serveryje yra mobilaus telefono ryšio numeris, kurį NVSC naudoja siunčiant SMS APK, leidžiantį atsitiktinius užsikrėtimo raktus įkelti į Programėlės serverį, kai nustatytas užsikrėtimas Covid-19 infekcija. Naudotojai turi galimybę neįkelti šių užsikrėtimo raktų.
Tačiau, šis PDAV laikosi konservatyvaus požiūrio ir laiko IP adresą asmens duomenimis, kurie veikia kaip asmens identifikatorius. Visi asmens duomenys, perduodami į Programėlės serverį ir iš jo, kol jie yra susieti su IP adresu, nors ir labai trumpu laikotarpiu, yra susiję su asmeniu ir laikomi asmens duomenimis.

Šiame PDAV nustatyta, kad visi į Programėlės serverį įkelti duomenys naudojami be IP adresų ir IP adresai toliau nenaudojami. Tvarkant asmens duomenis laikomasi griežto duomenų mažinimo metodo ir bus tvarkomi tik tie asmens duomenys, kurie būtini tinkamam programėlės veikimui.

[9] https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_edps_joint_opinion_201901_ehdsi_lt.pdf

PROCESŲ IR PAGALBINIŲ PRIEMONIŲ APRAŠYMAS

NVSC specialistai šiuo metu atlieka rankinį kontaktų sekimą. Tai procesas, kai asmuo, užkrėstas COVID-19, apklausiamas siekiant nustatyti žmones, su kuriais jis artimai bendravo ir kuriuos galėjo užkrėsti COVID-19 infekcija. NVSC specialistai poto skambinama šiems artimiems kontaktams ir jiems patariama apriboti jų judėjimą pagal visuomenės sveikatos politiką, taip apribojant viruso plitimą. Programėlė atlieka analogišką funkciją rankiniam kontaktų atsekimui, tik vykdo tai automatiniu būdu. Programėlė naudodama ENF ir BLE nustato programėlės naudotojo atrimus kontaktus su kitais asmenimis naudojančiais tokias pačias programėlės ar analogiškas naudojančias ENF ir BLE technologijas. Programėlės nustatomas artimas kontaktas apima tuos atvejus, kai programėlės naudotojai praleidžia daugiau nei 15 minučių arčiau nei 2 metrų atstumu vienas nuo kito. Ši programėlės funkcija artimiems kontaktams registruoti vadinama „Artumo registravimo“ funkcija ir ji skirta išplėsti dabartinę rankinio kontakto sekimo operaciją NVSC.
Programėlės naudojimas bus visiškai savanoriškas ir ją bus galima nemokamai atsisiųsti iš „Apple App Store“ ir „Google Play“ parduotuvės. Ji veiks „iPhone“, palaikančiuose „iOS 13.5“ (ar naujesnę) ir „Android“ telefonuose, kuriuose veikia 6.0 ir naujesnės versijos „Android“.

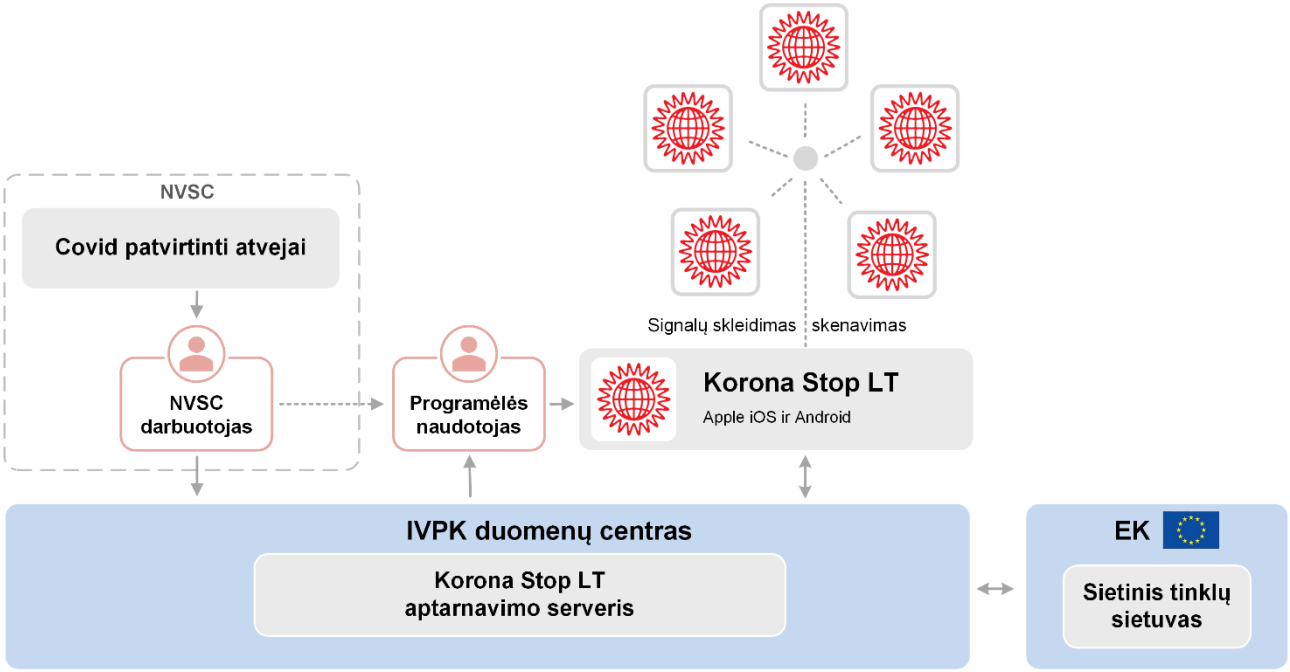
Procesas	Detalus proceso aprašymas	Priemonės
Artumo registravimas ir dalinimasis anoniminiu identifikatoriumi	Kiekvienas telefonas trumpu atstumu transliuoja laikinai galiojantį, patvirtintą ir anoniminį raktą, kurio negalima susieti su naudotoju. Kitų naudotojų telefonų atstumas įvertinamas matuojant radijo signalus (BLE ir kt.), naudojant gerai patikrintus ir kalibruotus algoritmus. Kai telefonas A yra epidemiologiniu požiūriu pakankamai arti telefono B epidemiologiškai pakankamu laikotarpiu, kaip nustatyta matavimuose, anoniminis telefono B raktas įrašomas į šifruotą artumo registrą, saugomą pačiame telefone A (ir atvirkščiai). Nebūna registruojama jokia geografinė padėtis, jokia asmeninė informacija ar kiti duomenys, kurie leistų identifikuoti naudotoją. Šios anoniminės artumo istorijos negali peržiūrėti niekas, net telefono A naudotojas. Senesni įvykiai artumo registre ištrinami, kai jie tampa epidemiologiškai nesvarbūs. Lietuvos gyventojų naudojamuose išmaniuosiuose telefonuose turėtų būti įdiegta programėlė „Korona Stop LT“, kuri naudoja BLE technologiją, kad išsiųstų atsitiktinę simbolių eilutę (atsitiktinį raktą) reguliariais laiko tarpais, atsitiktinis raktas reguliariai keičiasi per dieną, pavyzdžiui, kas 5, 10, 15 ar 30 minučių. Jei išmanusis telefonas A su įdiegta programėle gauna tam tikro stiprumo signalą iš išmaniojo telefono B (taip pat su įdiegta programėle), apskaičiuojamas atstumas tarp išmaniųjų telefonų. Kuo stipresnis signalas tarp išmaniųjų telefonų, tuo mažesnis atstumas tarp žmonių. Jei atstumas tarp asmenų yra pakankamai mažas, abi programėlės sugeneruoja atsitiktinius raktus ir jais keičiasi. Artumo registre saugomi duomenys yra susiję su asmeniu, nes jie yra saugomi išmaniajame telefone (programėlėje), kuris yra priskirtas asmeniui. Kai asmuo atsisiunčia programėlę, jis gali pasirinktinai įjungti jos artumo registravimo funkciją. Jei jis pasirinks tai padaryti, asmuo bus paprašytas įjungti telefono pranešimo apie poveikį sistemą. ENF yra nauja funkcija, kurią „Apple“ ir „Google“ mobilių telefonų operacinė sistema vykdo, kad palaikytų kontaktų paiešką, naudojant privatumo išsaugojimo būdus naudojant „iPhone“ ir „Android“ telefonus.	ULSKIS (Programėlės serveris), Apple (iOS) ar Google (Android), BLE

	Nuolatinis nuskaitymas - telefonai, kuriuose aktyvus ENF, nuolat ieškos kitų netoliese esančių telefonų, kuriuose aktyvus ENF. Tai atsitinka neatsižvelgiant į tai, kuri programėlė („Apple“ ar „Google“) yra įdiegta telefone, jei telefone veikia naujausia „Apple“ ir „Google“ operacinė sistema, įtraukianti ENF paslaugą. ENF neveikia telefonuose, kuriuose nėra įdiegta programėlė. Telefonai nuolat ieškos kitų netoliese esančių telefonų, kai aktyvus ENF. Aptikus artumą, telefonai tai įrašo siunčiant vienas kitam artumo raktus, nereikalaujant jokių naudotojo veiksmų, ir pateikia informaciją apie BLE signalo stiprumą, kuris vėliau bus naudojamas atstumui įvertinti. 14 dienų trukmės artumo raktai ir pridedama informacija, kurioje užfiksuoti paskutiniai žmogaus susitikimai, saugiai saugomi naudotojo telefone. Šių artumo raktų neįmanoma panaudoti naudotojo tapatybei nustatyti, nes jie kuriami atsitiktinių raktų generavimo principu. Be to, bet kada galima išjungti ir įjungti ENF, taigi artumo registravimas nepriklauso nuo kitų programėlės funkcijų.	
Artumo registro naudojimas: du veikimo režimai.	1 režimas Jei naudotojui nėra nustatyta Covid-19 infekcija, anoniminiai artumo registro duomenys lieka užšifruoti naudotojo telefone ir jų niekas negali peržiūrėti ar perduoti. Bet kuriuo laiko momentu išsaugomi tik artumo duomenys, kurie gali būti svarbūs viruso perdavimui, o ankstesni duomenys registre nuolat ištrinami. 2 režimas Jei bus patvirtinta, kad telefono A naudotojas yra užsikrėtęs Covid-19 infekcija, NVSC pagal dabartinius kontaktų paieškos procesus atlikdama epidemiologinę diagnostiką, susisieks su naudotoju A. Skambučio metu jo bus klausiama, ar jis yra programėlės naudotojas ir ar jis nori įkelti savo atsitiktinius artumo raktus į Programėlės serverį. Jei jis pasirenka skleisti savo atsitiktinius artumo raktus, jo prašoma nurodyti savo mobiliojo telefono numerį, į kurį SMS žinute siunčiamas APK. Kai APK įvedamas į programėlę, tai leidžia įkelti jo artumo raktus į Programėlės serverį. Paskelbti atsitiktiniai artumo raktai tolesniuose procesuose vadinami „užsikrėtimo raktais“. Atsižvelgdami į savanorišką programėlės pobūdį, naudotojai neprivalo įkelti savo raktų, tačiau to pasekoje jų artimi kontaktai nebus įspėti. Pranešimas apie poveikį - visos programėlės periodiškai (bent kartą per dieną) iš programėlės serverio atsisiunčia visus naujus užsikrėtimo raktus ir palygina su telefone įrašytais artumo raktais. Remiantis Europos ligų prevencijos ir kontrolės centro rekomendacijomis, kai artimas kontaktas yra 2 metrų atstumu 15 ar daugiau minučių, telefonas įspėja naudotoją, kad jis buvo susidūręs su asmeniu, kuriam nustatytas užsikrėtimas COVID-19 infekcija. Programėlė rodo naujausią artumo buvimo datą ir pateikia rekomendacijas. Įspėjimas apie artimą kontaktą su Covid-19 užsikėtusiu asmeniu programėlėje rodomi už paskutines 14 dienų. Naudotojai per nustatymus gali bet kada išvalyti pranešimus apie artimo kontakto riziką iš savo programėlės. Jei naudotojas gauna kelis pranešimus apie užsikrėtimo riziką, susijusią su įvairiais artimais kontaktais, jis gauna naują įspėjimą tik tuo atveju, jei pranešimas apie poveikį yra susijęs su naujesniu poveikio įvykiu.	ULSKIS, Programėlės serveris, Apple (iOS), Google (Android)

	Naudotojas naudoja APK norėdamas savanoriškai teikti informaciją programėlės serverių sistemai, kuri leidžia pranešti naudotojų B programėlėms, įrašytoms į naudotojo A artumo registrą, kad naudotojui B pranešti apie galimą užsikrėtimo riziką. Kadangi artumo registre yra tvarkomi anoniminiai identifikatoriai, nė vienas asmuo negali žinoti apie kito tapatybę. Darant prielaidą, kad išmaniojo telefono naudotojui A nustatomas užsikrėtimas Covid-19 infekcija ir jis gauna NVSC APK, kuriuo jis pasinaudoja, atsitiktiniai raktai, pranešimo apie užsikrėtimą metu tampa užsikrėtimo raktais ir yra įkeliami į Programėlės serverį. Po įkėlimo duomenys nuasmeninami teisinėmis, organizacinėmis ir techninėmis veiksmingomis priemonėmis, o anoniminiai užsikrėtimo atvejį nurodantys duomenys saugomi serveryje kaip centrinė užkarda. Visi kiti išmaniųjų telefonų naudotojai reguliariai atsisiunčia paskelbtus anoniminius užsikrėtimo atvejį nurodančius duomenis į savo programėlę. Šiuose raktuose nėra jokių duomenų apie ryšį su nustatytu ar atpažįstamu fiziniu asmeniu. Tuo pačiu metu jie turi informacinę vertę tik tiems asmenims, kurie turėjo kontaktą su užkrėstais asmenimis tam tikroje rizikos zonoje. Palyginus serveryje paskelbtus anoniminius užsikrėtimo atvejį nurodančius duomenis su išmaniuosiuose telefonuose lokaliai saugomais atsitiktiniais raktais, galima nustatyti, ar šis naudotojas per tam tikrą laiką turėjo kontaktą su tariamai užsikrėtusiu asmeniu. Tačiau iš duomenų negalima spręsti, ar kontaktas buvo su vienu užsikrėtusiu asmeniu ilgesnį laiką, ar tai buvo keli trumpi kontaktiniai įvykiai su daugybe skirtingų žmonių. Tokių detalių negalima atkurti iš duomenų. Naudojant užprogramuotą skaičiavimo taisyklę, iš kontaktinių įvykių apskaičiuojamas rizikos balas. Programėlės serveryje nėra duomenų apie tai, kurie žmonės yra užkrėsti, kur jie buvo ir kada, ar kuriuos žmones jie sutiko.	
Keitimasis artumo istorija tarp ES šalių[10]	Atsitiktiniai anoniminiai raktai yra užšifruoti mechanizmai, skirti nustatyti kiekvienos programos, naudojančios programėlę, šalį. Naudojant šią informaciją, anoniminiai raktai tvarkomi konkrečiai šaliai: 1 režimas Jei abu anoniminiai telefono A ir B raktai yra iš tos pačios šalies, gali būti pažymėtas anoniminis potencialiai užkrėstos šalies raktas, kad šios šalies programai teiraujantis apie jo ar jos būseną, programa būtų informuota apie galimą poveikį. 2 režimas Jei nustatoma, kad anoniminis telefono B raktas yra susijęs su kita šalimi, ne telefonu A, informacija, susieta su anoniminiu telefono B raktu, perduodama kitos šalies Programėlės serverių sistemai. Šis perdavimas yra visiškai užšifruotas ir pasirašytas skaitmeniniu būdu. Tolesnį tvarkymą vykdo šalies gavėjos duomenų valdytojas.	Europos Komisijos sietinis tinklų sietuvas

[10] Ši duomenų tvarkymo operacija dar nėra įdiegta kuriamoje programėlėje, todėl toliau nenagrinėjama. PDAV šiai duomenų tvarkymo operacijai pagal Europos Komisijos patvirtintą projektą turės būti atliktas atskirai.

Sveikatos priežiūros procesai po pranešimo apie galimą užkratą[11]	Naudotojas gavęs pranešimą apie artimą kontaktą nukreipiamas į NVSC interneto svetainę, kurioje jau nebe programėlės funkcionalumų pagalba jei pageidauja pateikia visą NVSC epidemiologinei diagnostikai atlikti reikiamą informaciją.	NVSC interneto svetainė



pav. 1 Programėlės "Korona Stop LT" komponentų ir srautų schema

Žemiau visi procesai aprašomi smulkiau išskiriant duomenų, programinės įrangos ir IT paslaugų bei priemonių lygmenis:

Duomenų tvarkymo veikla „Artumo registravimas ir dalinimasis anoniminiu identifikatoriumi programėlėje“:

Duomenų lygmuo:

Nr.	Procedūra	Rolės	Duomenys
0	Programėlės diegimas ir paleidimas	Programėlės naudotojas	Naudojimo duomenys, įrenginio duomenys
1	Savų artumo raktų generavimas		Artumo raktai
2	Savų artumo raktų išsaugojimas		Artumo raktai
3	Dalinimasis savo artumo raktais		Artumo raktai
4	Svetimų artumo raktų gavimas per BLE		Svetimų artumo raktų žymės
5	Kontaktų/sąlyčio atvejų išsaugojimas		Svetimi artumo raktai, trukmė, laikas

Programinės įrangos lygmuo:

Nr.	Veiksmas	Naudojama programinė įranga
1	Savų artumo raktų generavimas	Programėlė
2	Savų artumo raktų išsaugojimas	Programėlė
3	Dalinimasis savo artumo raktais	Programėlė
4	Svetimų artumo raktų gavimas per BLE	Programėlė
5	Kontaktų/sąlyčio atvejų išsaugojimas	Programėlė

[11] Ši duomenų tvarkymo operacija yra NVSC vykdomos epidemiologinės diagnostikos dalis, todėl toliau šiame PDAV nėra nagrinėjama.

IT paslaugų ir priemonių lygmuo:

Nr.	Programinė įranga	IT paslaugos / priemonės	Veiksmas	Rolė
1	Korona Stop LT	Išmanusis telefonas, BLE paslauga	Gyvavimo ciklo priežiūra	Programėlės naudotojas

Ryšiai ir sąsajos:

Nr.	Šaltinis	Gavėjas	Sąsaja	Tikslas
1	Programėlė 1	Programėlė 2	BLE	Artumo rakto perdavimas iš programėlės 1
2	Programėlė 2	Programėlė 1	BLE	Artumo rakto perdavimas iš programėlės 2

Duomenų tvarkymo veikla „Artumo registro naudojimas: Leidimas įkelti, nuasmeninti, laikinai išsaugoti ir platinti užsikrėtimo Covid-19 būseną“:

Duomenų lygmuo:

Nr.	Procedūra	Rolės	Duomenys
1	Covid-19 atvejo patvirtinimas ir APK kodo išsiuntimas	NVSC, programėlės naudotojas	APK
2	Autorizuotas programėlė naudotojų užsikrėtimo raktų perdavimas į serverį	Programėlės naudotojas	APK, Užsikrėtimo raktas
3	Užsikrėtimo rakto serveryje nuasmeninimas	Programėlės serverio administratorius	Užsikrėtimo raktas, anoniminiai užsikrėtimo atvejį nurodantys duomenys
4	Anoniminių užsikrėtimo atvejį nurodančių duomenų saugojimas	Programėlės serverio administratorius	anoniminiai užsikrėtimo atvejį nurodantys duomenys
5	Anoniminių užsikrėtimo atvejį nurodančių duomenų ištrynimas iš serverio praėjus 14 dienų po epidemiologiškai nustatyto laiko	Programėlės serverio administratorius	anoniminiai užsikrėtimo atvejį nurodantys duomenys

Programinės įrangos lygmuo:

Nr.	Duomenų tvarkymo veiksmas	Programinė įranga
1	Covid-19 atvejo patvirtinimas ir APK kodo išsiuntimas	ULSKIS, Programėlės serveris
2	Autorizuotas programėlė naudotojų užsikrėtimo raktų perdavimas į serverį	Programėlė
3	Užsikrėtimo rakto serveryje nuasmeninimas	Programėlės serveris
4	Anoniminių užsikrėtimo atvejį nurodančių duomenų saugojimas	Programėlės serveris
5	Anoniminių užsikrėtimo atvejį nurodančių duomenų ištrynimas iš serverio praėjus 14 dienų po epidemiologiškai nustatyto laiko	Programėlės serveris

IT paslaugų ir priemonių lygmuo:

Nr.	Programinė įranga	IT paslaugos / priemonės	Veiksmas	Rolė
1	ULSKIS, programėlės serveris	Interneto ir GSM ryšys	APK administravimas	NVSC darbuotojas
2	Programėlė	Išmanusis telefonas, internetas	Gyvavimo ciklo priežiūra	Programėlės naudotojas
3	Programėlės serveris, duomenų bazės	Duomenų centras, internetas	Serverio administravimas,	Serverio administratorius

	serveris, operacinės sistemos serveris		duomenų centro tvarkymas	

Ryšiai ir sąsajos:

Nr.	Šaltinis	Gavėjas	Sąsaja	Tikslas
1	Programėlė	Programėlės serveris	TCP/UDP	Užsikrėtimo rakto perdavimas
2	Programėlės serveris	Programėlė	TCP/UDP	Anoniminių užsikrėtimo atvejų nurodančių duomenų paieška

Duomenų tvarkymo veikla „Artumo registro naudojimas: Decentralizuotas kontaktų/sąlyčių nustatymas“:

Duomenų lygmuo

Nr.	Procedūra	Rolės	Duomenys
1	Kitų programėlės naudotojų anoniminių užsikrėtimo atvejį nurodančių duomenų serveryje užklausos	Programėlė naudotojas	Anoniminių užsikrėtimo atvejį nurodančių duomenų sąrašas
2	Anoniminių užsikrėtimo atvejį nurodančių duomenų palyginimas su artumo raktais, gautais per BLE išmaniajame telefone		Artumo raktų ir anoniminių užsikrėtimo atvejį nurodančių duomenų sutapimų sąrašas
3	Sutapimų sąrašo naudojimas užsikrėtimo rizikai nustatyti ir tolimesnėms elgesio rekomendacijoms pateikti		Sutapimai
4	Programėlės naudotojui nusprendus, atliekami rekomenduojami veiksmai, susisiekiama su NVSC		Dokumentai, tekstas, paveiksliukai, nuorodos, sąveika

Programinės įrangos lygmuo:

Nr.	Duomenų tvarkymo veiksmas	Programinė įranga
1	Kitų programėlės naudotojų anoniminių užsikrėtimo atvejį nurodančių duomenų serveryje užklausos	Programėlė, programėlės serveris
2	Anoniminių užsikrėtimo atvejį nurodančių duomenų palyginimas su artumo raktais, gautais per BLE“ išmaniajame telefone	Programėlė
3	Sutapimų sąrašo naudojimas užsikrėtimo rizikai nustatyti ir tolimesnėms elgesio rekomendacijoms pateikti	Programėlė
4	Programėlės naudotojui pageidaujant, atliekami rekomenduojami veiksmai, susisiekiama su NVSC	Programėlė, NVSC interneto svetainė

IT paslaugų ir priemonių lygmuo:

Nr.	Programinė įranga	IT paslaugos / priemonės	Veiksmas	Rolė
1	Programėlė	Išmanusis telefonas, internetas	Gyvavimo ciklo priežiūra	Programėlės naudotojas
2	Programėlės serveris	Duomenų bazės serveris, duomenų centras, internetas	Serverio administravimas	Serverio administratorius

Ryšiai ir sąsajos:

Nr.	Šaltinis	Gavėjas	Sąsaja	Tikslas
1	Programėlės serveris	Programėlė	TCP / UDP	Anoniminių užsikrėtimo atvejį nurodančių duomenų perdavimas į programėlę sulyginimui.

Programėlių keitimosi duomenimis tarp šalių funkcinis aprašymas (Žr. pav.2)

Dauguma ES šalių naudoja kontaktų atsekimo programėles, kurios veikia naudodamos Google ir Apple parengtą pranešimo apie poveikį sistemą (toliau - ENF). Skirtingų šalių programėlių naudojami artumo nustatymo principai yra suderinami, tačiau programėlių serveriai neturi priemonių kaip bendrauti vienam su kitu. ES šalys siekdamos palengvinti nacionalinių kontaktų atsekimo ir įspėjimo programėlių sąveiką, padedamos Komisijos sukūrė skaitmeninę infrastruktūrą kaip IT priemonę keitimuisi duomenimis. Ši skaitmeninė infrastruktūra vadinama sietiniu tinklų sietuvu (toliau STS). STS įgalina šalių programėlių serverius keistis duomenimis.

Toliau aprašyti du naudojimo atvejai aprašo ir pagrindžia STS naudojamą architektūrą.

Pirmas atveju programėlės naudotojas gyvenantis šalyje A keliauja į šalį B. Vėliau programėlės naudotojas užsikrečia Covid-19 infekcija ir nori apie tai įspėti šalies B gyventojus. Tam programėlės naudotojas persiųsdamas užsikrėtimo raktus per nacionalinę programėlę savo noru prideda „susijusią šalį“ B. Susijusi šalis B yra pridedama prie skelbiamų programėlės naudotojo užsikrėtimo raktų ir perduodami nacionalinės šalies A programėlės serveriui. Šalies A programėlės serveris prie gautų duomenų prideda „raktų kilmės šalies“ atributą ir persiunčia STS. STS visoms prisijungusioms šalims teikia 14-kos dienų užsikrėtusių raktus. Šalies B programėlės serveris iš STS gaudamas užsikrėtusių raktus, pagal atributą „susijusi šalis“ įvertina, kad šie raktai turi būti pateikti visiems B šalies programėlės naudotojams. Tuo atveju šie užsikrėtusių raktai kartu su šalyje B surinktais užsikrėtusių raktais yra pasiekiami visiems šalies B programėlės naudotojams. Visos šalys užsikrėtusių raktus grupuoja pagal atributą „raktų kilmės šalis“ ir teikia šių šalių programėlių naudotojams. Šiuo atveju šalių programėlės kitų šalių užsikrėtusių raktus naudoja pagal poreikį, kuris pateiktas kitame pavyzdyje.

Antru atveju šalies B programėlės naudotojas visą laiką lieka šalyje B. Programėlės naudotojas gyvena dideliame mieste, kurį lanko daug užsienio turistų, ir jis yra susirūpinęs, kad gali sutikti užsienio turistus, kurie nenaudoja šalies B nacionalinės programėlės, bet naudoja užsienio šalies iš yra atvykę programėles. Šalies B programėlės naudotojas tuomet savo programėlėje pažymi, kurių šalių kaip kilmės šalių užkrėtusių raktus turi tikrinti naudojama programėlė. Programėlė tuomet prisijungia prie programėlės serverio ir atsisiunčia naudotojo nurodytų šalių užsikrėtusių raktus. Atsisiuntusi raktus programėlė patikrina užsikrėtusių raktus su naudotojo programėlėje užregistruotais kontaktais.

STS architektūroje numatyta, kad visos STS naudojančios šalys gali atsisiųsti visus užsikrėtusiųjų raktus.

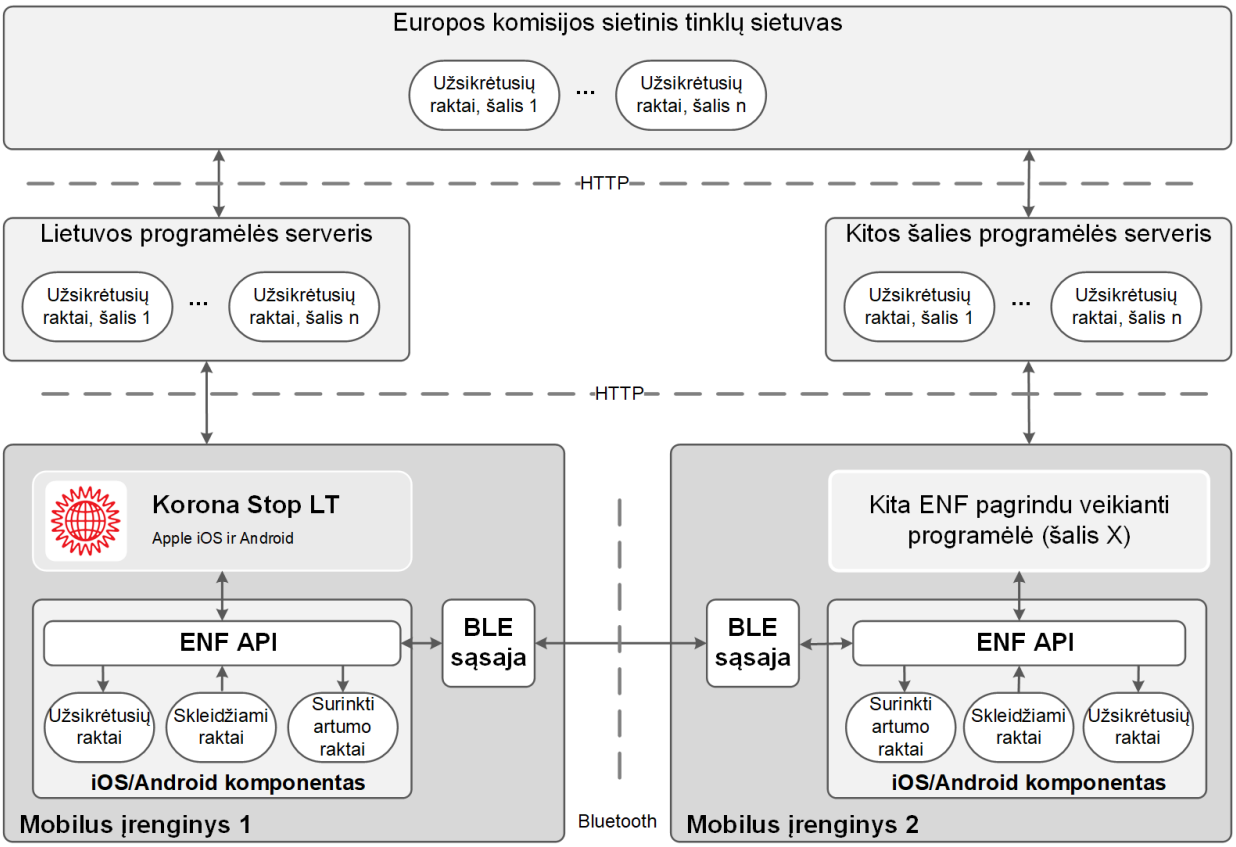
STS architektūra taip pat įgalina, kad šalių programėlių serveriams reikia bendrauti su STS, ir taip išvengiama poreikio tiesioginiam bendravimo tarp programėlių serverių.

Google ir Apple nustatė užsikrėtusių raktų eksporto failo formatą. Šalių programėlių serveriai gali keistis šiais užsikrėtusių raktų failais pridedant raktų kilmės šalį atributą ir susijusias šalis.

Dviejų programėlių bendravimo proceso aprašymas

Susitikus dviejų programėlių naudotojams abi programėlės renka kitos programėlės skleidžiamus artumo raktus (angl. RPI - Rotating Proximity Identifiers). Raktai tarp programėlės mobilių įrenginių skleidžiami ir renkami naudojant BLE. Užsikrėtusių raktai bus pasiekiami kitai programėlei tik tuo atveju, jei programėlės naudotojai pasidalins užsikrėtusių raktais pasidalindami užsikrėtimo faktu ir jie pateks į programėlės serverį bei per STS bus pasiekiami kitos šalies programėlės serveriui ir tuomet kitos šalies programėlės naudotojui.

Toliau pateiktame piešinuke pavaizduota panaudojant STS užsikrėtusių raktai pasiekiami kitos šalies programėlei ir suderinamos programėlės (naudojančios ENF ir STS) perduodą Covid-19 infekcijos užsikrėtimo rizikos duomenis. Tuo metu kai programėlės naudotojas paskelbia apie užsikrėtimo faktą, programėlės iki tol 14-kos dienų skleisti raktai perduodami programėlės serveriui, tuo metu jie virsta perduodamais užsikrėtusio raktais. Per STS užsikrėtusių raktai pasiekią kitos šalies programėlės serverį.



pav. 2 Europos komisijos sietinio tinklų sietuvo srautų schema

2 PAGRINDINIAI PRINCIPAI

Kuriant ir naudojant programėlę, užtikrinama, kad būtų laikomasi žemiau išvardintų projektavimo principų:

- Programėlė yra visiškai savanoriška naudoti;
- Programėlė naudojama išplėsti esamą rankinio kontaktų nustatymo procesą;
- Programėlė naudojama PDAV nustatytais tikslais ir tik esant COVID-19 pandemijai;
- Pasibaigus COVID-19 pandemijai, programėlės naudojimas bus nutrauktas;
- Programėlė tvarko duomenis, kaip nustatyta PDAV;
- Programėlė nenaudoja vietos nustatymo paslaugų naudotojų buvimo vietai stebėti ar jokiu kitu tikslu;
- Programėlė neatskleidžia ir niekada neatskleidžia asmens, užsikrėtusio COVID-19, tapatybės;
- Programėlė turi veikti, kol ekranas užrakintas.

2.1. DUOMENŲ TVARKYMO BŪTINUMO IR PROPORCINGUMO VERTINIMASTIKSLŲ PAAIŠKINIMAS IR PAGRINDIMAS

Tikslai	**Teisėtumas**
Nustatyti Covid-19 infekcijos plitimo grandines ir jas nutraukti, t. y. nustatyti programėlę naudojančių asmenų, kurie turėjo sąlytį su Covid-19 užsikrėtusiu asmeniu, artumo duomenis, kad būtų galima įspėti užsikrėsti galėjusius asmenis ir informuoti juos dėl tolesnių tinkamų veiksmų.	Infekcijos plitimo grandinių nutraukimas įspėjant žmones, kurie gali būti užkrėsti, yra ne tik teisėtas, bet ir būtinas labai užkrečiamos, o blogiausiu atveju - mirtinos ligos atveju. Asmenys negali savarankiškai siekti šio tikslo, todėl tai yra teisėtas tikslas. Duomenų tvarkymo operacijos tikslas apibrėžtas kaip galima siauriau, kad būtų išlaikytas balansas ir duomenų tvarkymo operacija nepažeistų pagrindinių teisių ir laisvių.

TEISĖTUMO PAAIŠKINIMAS IR PAGRINDIMAS

Teisinis programėlės duomenų tvarkymo pagrindas yra sutikimas. Tvarkymas apima tiek įprastas, tiek specialias duomenų kategorijas, todėl taikomas ir BDAR 6 straipsnio 1 dalies a) punktas ir 9 straipsnio 2 dalies a) punktas. Kiekvienai toliau pateiktoje lentelėje nurodytai asmens duomenų tvarkymo veiklai reikalingas aiškus, suprantama ir lengvai prieinama forma pateiktas sutikimas. Atsižvelgiant į visiškai savanorišką ir diskrecinį programos atsisiuntimo pobūdį ir pažymint, kad SAM ir NVSC negali nustatyti, ar asmuo įdiegė programėlę, ar ne, nelaikoma, kad atsiranda „jėgos disbalansas“ (BDAR preambulės 43 dalis). Daugiau informacijos apie sutikimo sąlygas, nustatytas BDAR 7 straipsnyje, pateikiama PDAV 2.2 dalyje.

Šiuo metu NVSC vykdo rankinę kontaktų atsekimo operaciją, su kuria programėlė sąveikaus nustatytais būdais. Šis PDAV aiškiai nurodo šiuos sąveikos taškus, kokius programėlės ir programinės įrangos apdorotus duomenis NVSC gali tvarkyti, kokiais atvejais ir kokiais tikslais, ir patvirtina, kad naudotojas yra tinkamai informuotas. Šis vertinimas neapima NVSC veiklos įvertinimo, išskyrus ką tik pateiktą atvejį.

Teisėto tvarkymo kriterijai	**Taikoma**	**Pagrindimas**
Duomenų subjektas davė sutikimą, kad jo asmens duomenys būtų tvarkomi vienu ar keliais konkrečiais tikslais [12]	Taip*	Programėlė įrenginyje įdiegiama savanoriškai ir nekelia jokių neigiamų pasekmių asmeniui, kuris nuspręstų jos neatsisiųsti arba nenaudoti. Sutikimas naudoti programėlę ir sutinkančių asmenų asmens duomenų tvarkymas automatiškai nereiškia sutikimo (visai) procedūrai. Sutikimas naudoti programėlę atskirtas nuo sutikimo perduoti APK, t. y. patvirtinti užsikrėtimo atvejį ir į serverį perduoti užsikrėtimo raktą. Šis reikalavimas netrukdo naudotojui sujungti įvairių programėlės funkcijų, tai naudotojui siūloma kaip opcija**. Jei naudojami artumo duomenys (duomenys, gaunami keičiantis mažai energijos naudojančią BLE technologiją turinčių prietaisų signalais, kai

[12] Apie duomenų subjekto sutikimo gavimą ir pastarojo informavimą žr. 2.2 skyrių.

		išlaikomas epidemiologiškai tinkamas atstumas ir epidemiologiškai tinkamas laikas), jie turėtų būti saugomi asmens prietaise. Yra būtinas sutikimo valdymas.

* Pagal E. privatumo direktyvą[13] (5 straipsnį) saugoti informaciją naudotojo įrenginyje arba gauti prieigą prie jau saugomos informacijos leidžiama tik tuo atveju, jei i) naudotojas davė sutikimą arba ii) ją saugoti ir (arba) suteikti prieigą tikrai būtina tam, kad būtų suteikta informacinės visuomenės paslauga (pvz., programėlė), kurios naudotojas aiškiai paprašė (t. y. įdiegė ir aktyvavo).
Tam, kad programėlės veiktų, paprastai būtina, kad būtų išsaugoma informacija apie asmens prietaisą ir gaunama prieiga prie jame jau saugomos informacijos. Be to, kad būtų įmanoma naudotis sąlytį turėjusių asmenų išaiškinimo ir įspėjimo funkcija, būtina, kad naudotojo įrenginyje būtų išsaugoma tam tikra papildoma informacija (pvz., trumpalaikiai, periodiškai keičiami šios artumo funkcijos naudotojų raktai). Be to, tam, kad būtų įmanoma naudotis šia funkcija, gali prireikti, kad (užsikrėtęs arba potencialiai užsikrėtęs) naudotojas įkeltų artumo duomenis. Tam, kad veiktų pati programėlė, tokių duomenų įkelti nebūtina. Todėl nesilaikoma ankstesnės dalies ii) punkte nurodytų reikalavimų. Taigi sutikimas (galimybė, nurodyta i) punkte) lieka tinkamiausiu pagrindu imtis susijusių veiksmų. Kaip apibrėžta BDAR, šis sutikimas turėtų būti „suteiktas laisva valia“, „konkretus“, „vienareikšmis“ ir „informacija pagrįstas“. Jis turėtų būti išreikštas aiškiais patvirtinamaisiais asmens veiksmais; nepriimtinas tylus sutikimas (pvz., tylėjimas; neveikimas)[14].
Jei sutikimas duodamas valstybinei institucijai, paprastai daroma prielaida, kad jis nėra duotas savanoriškai (įrodinėjimo pareiga savanoriškumo nenaudai, BDAR preambulės 43 p.). Šiuo atveju reikia įrodyti, kad disbalansas, kuris paprastai egzistuoja tam tikroje situacijoje, netaikomas. Todėl suteikiant sutikimą institucijai turi būti keliami specialūs reikalavimai. Šį disbalansą reikia atsverti tuo, kad programėlės naudojimas nėra privalomas ir nesukelia jokių standartizuotų, tiesioginių teisinių pasekmių.
** Norint naudoti programėlę, atskirtos dvi apdorojimo veiklos. Pirma, keitimasis artumo raktais tarp programėlių ir, antra, APK ir užsikrėtimo raktų perdavimas į serverį patvirtintos Covid-19 infekcijos atveju. Sutikimo davimo tikslas ir forma yra lemiami, jei naudotojas neperduoda informacijos serveriui. Jei naudotojas nepateikia APK, jis (ji) nesutinka dėl tolesnio informacijos, susijusios su užsikrėtimu, apdorojimo. Abi veiklos yra aktyvuotos naudotojo veiksmais. Jei keitimasis artumo raktais suprantamas kaip būtina sąlyga norint būti informuotam apie kontaktą su užsikrėtusiu asmeniu, sutikimas gali būti susijęs su abiem veiksmais. Programėlės naudotojui suteikta galimybė laisvai nuspręsti, ar perduoti informaciją apie užsikrėtimą Covid-19 infekcija, šis pasirinkimas taip pat turėtų būti aiškiai išreikštas informuoto sutikimo formoje.
Toliau pateikiami šiame PDAV nurodytų asmens duomenų tvarkymo teisiniai pagrindai. Trumpai nurodyta duomenų tvarkymo veikla, kad būtų aiškiau.

Duomenys	**Veikla**	**Teisinis pagrindas**
Tvarkomi duomenys: **- Artumo raktas (pseudoniminis)** **- atstumas** **- trukmė** **- programėlės naudotojo užsikrėtimo atvejis** **- anoniminiai užsikrėtimo atvejį nurodantys duomenys (užsikrėtimo raktai)** **- rizikos balas** **- laiko specifikacija**	Naudotojas savanoriškai atsisiunčia programėlę. Pradėjęs naudoti programėlę naudotojas gali sutikti skleisti savo artumo raktus. Esant užsikrėtimo Covid-19 infekcija atvejui, naudotojas gali duoti leidimą bendrinti savo užsikrėtimo raktus Programėlės serveryje. Užsikrėtimo raktus atsisiunčia visos programėlės, kad atsektų kontaktus su Covid-19	Užsikrėtimo raktai rodo asmens sveikatos būklę. Prieš tvarkant prašoma leidimo. Teisinis pagrindas yra sutikimas - BDAR 6 straipsnio 1 dalies A punktas ir 9 straipsnio 2 dalies a punktas. Įkeliant į Programėlės serverį, IP adresas panaikinamas. Tai daroma prieš užsikrėtimo raktų saugojimą ir viešą prieinamumą Programėlės serveryje ir prieš paskirstant kitoms programė-

[13] 2002 m. liepos 12 d. Europos Parlamento ir Tarybos direktyva 2002/58/EB dėl asmens duomenų tvarkymo ir privatumo apsaugos elektroninių ryšių sektoriuje (Direktyva dėl privatumo ir elektroninių ryšių) (OL L 201, 2002 7 31, p. 37).
[14] Žr. Europos duomenų apsaugos valdybos gaires dėl sutikimo: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=623051

	užsikrėtusiais asmenimis ir pateiktų šio įvertinimo riziką	lėms. Taigi šiame etape duomenys laikomi anoniminiais.
Mobilaus telefono ryšio numeris	Kontaktinė informacija, įskaitant mobiliojo telefono numerį, yra renkama kaip esamos kontaktų atsekimo operacijos dalis, kai asmeniui nustatoma užsikrėtimas Covid-19 infekcija. Šie duomenys, gavus asmens sutikimą, yra toliau tvarkomi, kad programėlės serveris galėtų išsiųsti SMS kodą, leidžiantį įkelti APK; ir išfiltruoti atitinkamą užsikrėtimo raktų rinkinį, kurį galima platinti per Programėlės serverį.	Šie duomenys rodo asmens sveikatos būklę. Prieš tvarkymą prašoma leidimo. Teisinis pagrindas yra sutikimas - BDAR 6 straipsnio 1 dalies A punktas ir 9 straipsnio 2 dalies a punktas.
APK	APK kodas gaunamas SMS žinute, po to, kai NVSC, atlikdama kontaktų atsekimo operaciją sužino apie asmens ketinimą paskelbti apie užsikrėtimą, siekiant įspėti kitus programėlės naudotojus.	Šie duomenys rodo asmens sveikatos būklę. Prieš tvarkymą prašoma leidimo. Teisinis pagrindas yra sutikimas - BDAR 6 straipsnio 1 dalies A punktas ir 9 straipsnio 2 dalies a punktas.
IP adresai	Šie duomenys yra viso Programėlės serverio tinklo srauto dalis.	Šie duomenys tvarkomi pagalbiniu tinklo ir informacijos saugumo užtikrinimo tikslu. Prieš apdorojant prašoma leidimo. Teisinis pagrindas yra sutikimas - BDAR 6 straipsnio 1 dalies a punktas.

DUOMENŲ KIEKIO MAŽINIMO PAAIŠKINIMAS IR PAGRINDIMAS

Išsami informacija apie tvarkomus duomenis	**Duomenų kategorijos**	**Duomenų poreikio ir tinkamumo pagrindimas**	**Sumažinimo kontrolė**
Informavimo funkcija.	Jeigu programėlė turi tik šią funkciją, nereikės tvarkyti jokių duomenų apie asmenų sveikatą. Programėlė jiems teiks tik informaciją. Siekiant laikytis šio reikalavimo, galiniuose įrenginiuose gali būti tvarkoma tik ta saugoma ir prieinama informacija, kuri reikalinga informavimo tikslais.	-	-

Sąlytį turėjusių asmenų išaiškinimo ir įspėjimo funkcijos	Artumo duomenys Užsikrėtimo duomenys	Dauguma Covid-19 infekcijų perduodamos lašeliniu būdu per mažą atstumą. Siekiant nutraukti infekcijos grandinę, labai svarbu kuo greičiau nustatyti asmenis, kurie buvo arti užkrėstojo. Artumo nustatymas priklauso nuo kontaktavimo atstumo ir trukmės ir turėtų būti nustatomas įvertinus epidemiologinius aspektus. Nutraukti infekcijos grandinę itin svarbu tada, kai krizės įveikimo stadijoje siekiama išvengti infekcijos pasikartojimo. Atsižvelgiant į tai, būtina išsaugoti duomenis apie sąlyčio dieną, kad būtų galima išsiaiškinti, ar sąlytis įvyko tada, kai asmeniui pasireiškė simptomai, ir patarti, kokių tolesnių veiksmų imtis, pavyzdžiui, kiek laiko taikyti saviizoliaciją. Artumo duomenys renkami ir tvarkomi tik tuo atveju, jei užsikrėtimo rizika yra reali (priklauso nuo sąlyčio artumo ir trukmės). Įspėjimą programėlė automatiškai perduoda artimai bendraujantiems asmenims, kai naudotojas, naudodamasis programėle, praneša (gavęs NVSC patvirtinimą, pvz., APK), kad jis užsikrėtė infekcija (decentralizuotas tvarkymas). Svarstant duomenų tvarkymo būtinybę, reikia atsižvelgti į techninį aspektą. Jei tikslą taip pat galima pasiekti „švelnesnėmis“ techninėmis priemonėmis. Mažo nuotolio technologijų, tokių kaip BLE, naudojimas reikalingas, kad NVSC užduotis greitai ir efektyviai aptikti infekcijos grandines galėtų būti įvykdyta daug greičiau ir tiksliau naudojant programėlę, nei naudojant klausimynus ir telefonų skambučius.	BLE technologija, kuri generuoja pranešimų duomenis. Pseudonimų suteikimas bei nuasmeninimas*.

* Pagrindinės priemonės, kuriomis užtikrinamas duomenų tvarkymo operacijos apribojimas yra pseudonimų ir nuasmenintų duomenų naudojimas, kai informacija, susijusi su fiziniu asmeniu, kiek įmanoma pašalinama arba kai papildoma informacija, naudojama priskiriant asmens duomenis konkrečiam duomenų subjektui, būtų laikoma atskirai.

Pagal šią procedūrą tai reiškia, kad artumo rakte nėra asmens duomenų, bet yra unikalūs atsitiktiniai skaičiai. Be sąlyginių aplinkybių jie neturėtų daryti tiesiogiai sietis su asmeniu, vieta, laiku ir socialinėmis aplinkybėmis. Norint užtikrinti išmaniojo telefono tikslo ribojimą, programėlė turi būti paleista talpykloje. Talpykla turėtų apsaugoti nuo kitų programėlių ar operacinės sistemos prieigos. Be to, artumo duomenų žymių sąsajai, taip pat anoniminių užsikrėtimo atvejį nurodančių duomenų atsisiuntimui ir užsikrėtimo rakto įkėlimui į serverį turi būti taikoma speciali apsauga naudojant autentifikavimą ir šifravimą. Šie įvykiai taip pat turi būti registruojami.

Labai svarbią informaciją apie identifikuotą ar atpažįstamą fizinį asmenį sudaro duomenų tvarkymo veikla, kai NVSC darbuotojas perduoda APK, leidžiantį įkelti užsikrėtimo raktą į serverį. NVSC darbuotojo sukurtas ryšys tarp APK ir užsikrėtusio asmens yra griežtai konfidencialus ir turi būti apsaugotas tinkamomis saugumo priemonėmis, tokiomis kaip gavimo, įvedimo ir prieigos kontrolė, autorizacijos valdymas, atsarginės kopijos, šifravimas, vientisumo apsaugos priemonės, ištrynimas ir registravimas, įskaitant brandų duomenų apsaugos valdymą.
Kita priemonė, susijusi su tikslo ribojimu ir nesusiejimu, yra automatinis duomenų ištrynimas.
Programėlė turi veikti taip, kad kuo labiau sumažintų tvarkomų asmens duomenų kiekį, kad būtų pasiekti jos apibrėžti tikslai. Toliau pateikiami projektavimo metodai, pabrėžiantys duomenų minimizavimo principo įgyvendinimą:
• Sąlytį turėjusio asmens įspėjimai veikia taip, kad juos būtų galima sugeneruoti nerenkant asmens telefono numerio skambučiui.
• Naudojant „decentralizuotą“ modelį artumo registravimo funkcijai, telefonai gali apdoroti duomenis telefone, kad vietoje sukurtų glaudžius sąlyčio įspėjimus, nereikalaujant įkelti visus telefonui žinomus artumo duomenis į centralizuotą serverį.
• Siunčiant APK į mobilų telefoną, taip leidžiant programėlės naudotojui paskelbti užsikrėtimo raktus, mobiliojo telefono numeris, kuriuo naudojamasi siųsti SMS, iš karto ištrinamas iš programėlės serverio iki to kai užsikrėtimo raktai įkeliami į programėlės serverį. Tai leidžia išvengti netyčinio ar kitokio užsikrėtimo raktų derinimo su mobiliojo telefono numeriu.
• IP adreso duomenys, įtraukti į visą interneto srautą tarp programėlės ir programėlės serverio, nėra registruojami nei programėlėje nei programėlės serveryje.
• Visų asmens duomenų saugojimo laikotarpis yra įvertintas ir taikomas toks, kokio reikia jo saugojimo ir tvarkymo tikslui pasiekti.
• Kiekviena iš programėlės funkcijų gali būti naudojama nenaudojant kitų.
• Kai tikslui pasiekti pakanka nuasmenintų asmens duomenų, tvarkomi tik nuasmeninti anoniminiai arba pseudoniminiai duomenys. Toliau pateikiama išsami informacija apie minėtą nuasmeninimą.
Užsikrėtimo raktai – įkeliant užsikrėtimo raktus nenaudojami jokie asmens duomenys. Raktai sukuriami programėlėje naudojant atsitiktinių raktų generavimo priemones, nenaudojant jokių asmens duomenų. Šie „atsitiktiniai raktai“ yra saugomi programėlėje. Raktus galima įkelti į programėlės serverį, kai asmuo gauna APK. Šį kodą SMS žinute perduoda NVSC, kai asmeniui nustatomas Covid-19 atvejis.
Vien raktai negali identifikuoti asmens, tačiau reikia užtikrinti, kad jokie asmens duomenys nebūtų susieti su užsikrėtimo raktais saugomais programėlės serveryje. Tai yra užtikrinama taip: 1) IP adresas matomas programėlės serverio, užsikrėtimo raktų gavimo metu, nėra saugojamas programėlės serveryje, todėl IP adreso jo negalima vėliau sieti su paskelbtais užsikrėtimo raktais; 2) Mobilaus telefono numeris, naudojamas APK siųsti SMS žinute, pašalinamas iškart, kai tik išsiunčiama SMS žinutė, taip užkertant kelią telefono numerį vėliau susieti su programėlės naudotojo užsikrėtimo raktais; 3) Vieninteliai duomenys, kurie skelbiami programėlės serveryje, yra užsikrėtimo raktai, neturintys jokių asmens duomenų, ar tai būtų IP adresai / telefono numeris, ar kiti asmens duomenys. Užsikrėtimo raktus periodiškai atsisiunčia visos programėlės, ir „Google“ ir „Apple“ ENF riboja, kaip raktus galima naudoti tikrinant, ar nėra atitikimo, kad visuomenės sveikatos institucijos negalėtų piktnaudžiauti ir atskleisti užsikrėtusio asmens tapatybę. Atsižvelgiant į tai, kas išdėstyta, laikoma, kad nėra pagrįstos tikimybės, kad asmenį galima atpažinti naudojant užsikrėtimo raktus.

DUOMENŲ KOKYBĖS PAAIŠKINIMAS IR PAGRINDIMAS

Duomenų kokybės kontrolė	**Pagrindimas**
BLE technologija, kuri generuoja pranešimų duomenis	Naudojant šią technologija fiksuojamas kontaktas, sąlytis asmenų tam tikru atstumu, tam tikra trukme. Tokiu būtu fiksuojami asmenys ne tiesiog esantys tam tikroje vienoje vietoje vienu metu, tačiau įvertinamo epidemiologiškai svarbios aplinkybės (atstumas ir trukmė).
APK kodas, kuris leidžia paskelbti apie užsikrėtimą Covid-19 infekcija	APK kodas leidžia užtikrinti, kad apie užsikrėtimą galėtų paskelbti tik tas asmuo, kuris iš tiesių yra užsikrėtęs ir jo Covid-19 atvejis iš ties yra

	patvirtintas oficialios institucijos – NVSC. Tai užtikrina, jog bus keičiamas užsikrėtimo raktais tik tų asmenų, kurie tikrai užsikrėtė. APK kodas yra tikrinamas Programėlės serveryje. Antrą kartą panaudoti to paties kodo negalima. APK kodas galioja 24 val.

SAUGOJIMO TRUKMĖS PAAIŠKINIMAS IR PAGRINDIMAS

Šioje lentelėje pateikiama išsami informacija apie kiekvieno asmens duomenų lauko išsaugojimo pagrindimą ir priemones, skirtas užtikrinti, kad būtų laikomasi saugojimo politikos.

Duomenų kategorijos	**Saugojimo trukmė**	**Saugojimo trukmės pagrindimas**	**Ištrynimo mechanizmas pasibaigus saugojimo trukmei**
Tvarkomi duomenys: **- Artumo raktas (pseudoniminis)** **- atstumas** **- trukmė** **- programėlės naudotojo užsikrėtimo atvejis** **- anoniminiai užsikrėtimo atvejį nurodantys duomenys (užsikrėtimo raktai)** **- rizikos balas** - laiko specifikacija	Telefonai, generuojantys atsitiktinius artumo raktus, saugo duomenis 14 dienų, nebent naudotojas ištrina ENF duomenis naudodamas telefono nustatymus. Programėlės serveris saugo raktus 14 dienų. Programėlės atsisiunčia ir apdoroja užsikrėtimo raktus, kad patikrintų, ar nebuvo artimo kontakto su užsikrėtusiu asmeniu.	Kiekviename telefone yra iki 14 kasdienių atsitiktinių artumo raktų, kuriuos galima įkelti ir paskelbti programėlės serveryje, kad kiti programos naudotojai galėtų patikrinti, ar jie artimai bendravo per pastarąsias 14 dienų. 14 dienų laikoma epidemiologinės reikšmės laikotarpiu, kuris paprastai apima viruso perdavimo potencialą. Programėlės serveris dėl pirmiau nurodytos priežasties saugo raktus iki 14 dienų. Raktai yra atsisiunčiami siekiant patikrinti artimą kontaktą.	Telefonai automatiškai ištrina sugeneruotus atsitiktinius artumo raktus po 14 dienų. Po 14 dienų Programėlės serveris automatiškai ištrina atsitiktinius raktus. Atsisiųsti užsikrėtimo raktai ištrinami patikrinus juos su anksčiau išsaugotais artumo raktais.
Mobilaus telefono ryšio numeris	Kai tik išsiunčiama SMS žinutė, telefono numeris ištrinamas ir išsaugomas tik APK su pranešimo data. Programėlės serveris niekaip negali žinoti asmens, kuris arba įkelia raktus, arba nusprendžia jų neįkelti, telefono numerio.	Mobiliojo telefono numerio išsaugojimo nurodytu laikotarpiu pagrindimas yra SMS siuntimas, kad naudotojas galėtų įkelti užsikrėtimo raktus. APK saugomas siekiant įgalinti užsikrėtimo raktų įkėlimą, kad užsikrėtimo raktų registras programėlės serveryje nebūtų užterštas padirbtais pateikimais.	Mobiliojo telefono numeris automatiškai trinamas.

APK	APK tvarkomas pakankamai ilgai (21 kalendorinę dieną), kad būtų leista įkelti užsikrėtimo raktus, kad būtų nustatytas tinkamas užsikrėtimo raktų laikotarpis, kurį reikia įkelti į registrą. Jis ištrinamas, kai bus pasiekti šie tikslai.	APK saugomas siekiant užtikrinti įkėlimą, kad Programėlės serveris nebūtų užterštas padirbtais užsikrėtimo raktų pateikimais. APK turi būti ištrinamas iš naudotojo išmaniojo telefono iš karto, kai jis yra panaudojamas, tačiau Programėlės serveryje jis yra saugomas siekiant užtikrinti NVSC darbuotojų APK kodo siuntimo kontrolę.	APK trinami automatiškai.
IP adresai	IP adresas yra tvarkomas interneto tinkle, tačiau nesaugomas nei programėlėje, nei programėlės serveryje.	IP adresas yra būtinas bendravimui internete (maršruto parinkimas, adresavimas), tačiau siekiant neidentifikuoti naudotoją nėra saugomas Programėlės serveryje.	Šie duomenys saugomi tol, kol jų reikia interneto tinklo ryšio tikslais.
Archyvuoti duomenys (anoniminiai užsikrėtimo atvejį nurodantys duomenys)	Saugomi 14 paskutinių kalendorinių dienų duomenys	Programėlės serveryje duomenys saugomi atsarginėje kopijoje siekiant atkurti sistemą.	Periodinis automatinis duomenų kopijų trynimas

PRIEMONIŲ VERTINIMAS

Jei reikia tvarkyti duomenis, būtina, kad naudojamos priemonės būtų veiksmingos siekiamam tikslui pasiekti ir būtinos palyginti su kitomis galimybėmis pasiekti tą patį tikslą. Duomenų tvarkymo proporcingumas reikalauja, kad siūlomo tvarkymo pranašumai nebūtų atsverti trūkumais, kuriuos priemonės gali sukelti asmens teisėms, todėl turi būti išlaikyta pusiausvyra tarp naudojamų priemonių ir numatyto tikslo.

Būtinumas ir kontaktų atsekimas - poreikis naudoti kontaktų atsekimo formą COVID-19 pandemijos metu nekelia abejonių. Pagrindinis veikimo principas yra tas, kad diagnozuojant asmeniui Covid-19 užsikrėtimą, nustatomi glaudūs to asmens kontaktai, paprastai atliekant apklausas, ir imamasi atitinkamų priemonių taip identifikuotų asmenų atžvilgiu, siekiant kontroliuoti užsikrėtimų plitimą. Tai veiksminga intervencija į kovą su Covid-19 ir naudojama visame pasaulyje. Tačiau rankiniu būdu atliekant kontaktų sekimą yra būdingi iššūkiai. Infekcinės ligos, kurios ilgas inkubacinis laikotarpis, atveju sumažėja gebėjimas prisiminti su kuo buvo bendrauta ir padidėja tikimybė, kad užsikrėtimas išplis už žinomų ir įprastų kontaktų ribų. Be to, rankinis kontaktų sekimas taip pat reikalauja didelių žmogiškųjų išteklių. Rankinio kontakto atsekimo procedūros yra per lėtos, trūksta efektyvumo ir vyksta per mažu mastu, kad būtų galima suvaldyti Covid-19. Lietuvoje ir kitose šalyse buvo įvestos papildomos priemonės, padedančios kontroliuoti virusą, pavyzdžiui, labai apribotas asmenų judėjimas, darbo įpročiai ir bendra kasdienė veikla.

Pagrindiniai efektyvaus kontaktų atsekamumo rodikliai yra glaudaus kontakto identifikavimo išsamumas, artimo kontakto identifikavimo greitis ir tolesni veiksmai, siekiant greitai ir žymiai sumažinti viruso perdavimo potencialą. Tikslas yra naudoti mobiliąja programėle pagrįstą kontaktų atsekimo sprendimą kaip priedą prie esamo rankinio kontaktų atsekimo, t. y. padidinti nustatytų artimų kontaktų išsamumą ir padidinti tų artimų kontaktų nustatymo greitį ir riboti Covid-19 plitimą.

Neseniai, nuo 2020 birželio mėn. buvo pristatytos ES šalių mobiliosios programėlės. Beveik visos ES valstybės narės dar neįdiegusios programėlės, nurodė planus ateityje įdiegti tokias programėles. Jau programėles įdiegusiose šalyse, jų naudojamumas yra nuo 10 iki 40 proc. ES šalių gyventojų. Nors nedidelis įsisavinimas

gali turėti įtakos Covid-19 plitimo mažinimui, akivaizdu, kad kuo didesnis naudojimas, tuo didesnis teigiamas priemonės potencialas.
Lietuva ketina pristatyti programėlę, pagrįstą „Apple“ ir „Google“ ENF paslauga.
Iki šiol kitose šalyse 2020m. kovo-gegužės mėn. pristatytos programėlės nebuvo tokios sėkmingos, nes nebuvo ENF ir turėjo didelių funkcinių sunkumų, būtent neveikė arba labai trukdė mobiliems telefonams, akumuliatoriaus veikimo trukmei. Be to, šios programėlės paprastai buvo pagrįstos „centralizuotu“ veikimo modeliu, kai visuomenės sveikatos priežiūros institucijos gaudavo prieigas prie daugybės užsikrėtimo ir artimų kontaktų atsekimo duomenų.
Naudojant ENF siekiama išspręsti minėtus klausimus, susijusius su artumo registravimo funkcionalumu. Be to Lietuviškos programėlės veikimas grindžiamas decentralizuotu modeliu, pašalinant poreikį dalytis artumo duomenimis su centrine institucija. Taip pat tikimasi, kad vis daugiau ir daugiau šalių naudodamosi ENF paslauga, kuriai visoje ES tenka nemažas impulsas ir palaikymas, bus sustiprinta Covid-19 kovoje taikomų priemonių patikimumas. Alternatyvūs būdai, kaip pasiekti pirmiau nurodytus tikslus, buvo centralizuoto modelio naudojimas ir GPS / vietos stebėjimas.
Atsižvelgiant į siekiamus programėlės tikslus, šių tikslų pagrindimą ir kontekstą, lūkesčius, kad siūloma kontaktų atsekimo funkcija bus veiksminga ir žmonėms pritaikyta atsižvelgiant į pasirinktą privatumo išsaugojimo decentralizuotą modelį ir pasirinktą ENF technologiją, nurodytą palaikymą įdiegiant tokią programėlės funkciją, ši funkcija laikoma mažiausiai įsibraunančia priemone norint pasiekti nurodytus tikslus, manoma, kad siūlomas duomenų apdorojimas programėlės artumo registravimo funkcijoje yra būtinas.
Proporcingumas ir kontaktų atsekimas - yra aiškus ir neatidėliotinas socialinis poreikis atlikti greitą ir veiksmingą kontaktų atsekimo operaciją, kuri yra vienas iš pagrindinių ramsčių kontroliuojant viruso plitimą. Pagrįstai tikimasi, kad programėlės „Artumo registravimo“ funkcija atitiks poreikį padidinti glaudaus kontakto identifikavimo ir tolesnių veiksmų išsamumą ir greitį, kai bus naudojama kartu su šiuo metu NVSC veikiančiu rankiniu kontaktų atsekimu. Ypatingas rūpestis kelia iššūkius, susijusius su artimo kontakto nustatymo ir tolesnių veiksmų išsamumu ir savalaikiškumu, ypač palengvinant judėjimo, socialinius ir su darbu susijusius apribojimus. Tikimasi, kad įvedus programos „Artumo registravimo“ funkciją bus galima sušvelninti šias problemas, nes didėja žmonių tarpusavio sąveika, ypač sąveika, kai žmonės vieni kitiems nėra žinomi arba apie juos paprastai nepranešama rankinio kontaktų atsekimo metu.
Apsaugos priemonės, skirtos apriboti kišimosi į duomenų apsaugą ir teisių į privatumą mastą, yra nustatomos užtikrinant, kad duomenys būtų tvarkomi laikantis tvarkymo tikslo ir BDAR principų, įskaitant visišką duomenų tvarkymo nutraukimą, kai baigsis COVID-19 pandemija, ir nuolatinis programos efektyvumo stebėjimas. Sukūrus ir įgyvendinant artumo registravimo funkciją, šios teisės yra dar labiau apsaugotos užtikrinant, kad duomenų tvarkymas yra visiškai savanoriškas, kad naudotojų prašoma aiškaus sutikimo, jei jie nori įjungti ENF, teikia tolesnius leidimus, atsiųsti APK ir paskalbti programėlės naudotojo jų užsikrėtimo raktus. Svarbu tai, kad jei naudotojai nenori, jie gali nepranešti apie užsikrėtimą ar programėlės naudojimą apskritai.
Vietos nustatymo paslaugos naudojamos naudotojų vietai stebėti, o vietoj to BLE naudojamas aptikti artumą be jokių vietos duomenų, taip sumažinant tvarkomus duomenis ir naudojant tik būtinus duomenis tikslui pasiekti. Sutikimą dėl bet kokio kontaktų atsekimo duomenų tvarkymo galima atšaukti bet kuriuo metu ir jį galima ištrinti kontroliuojant duomenų subjektui, nepriklausomai ir be NVSC žinios. Programėlės nenaudojimas neturi jokių pasekmių, nes NVSC negali pasakyti, kas turi ir kas neįdiegė programėlės. Atsižvelgiant į aukščiau išdėstytą būtinybę ir ribotą kišimąsi į duomenų subjektų teises, siūlomas apdorojimas pagal programos funkciją „Artumo registravimas“ laikomas būtinu ir proporcingu.

Priemonės, užtikrinančios duomenų tvarkymo proporcingumą ir būtinumą	**Priimtina / galima patobulinti?**	**Taisomoji priemonė**
Tikslai: konkretūs, aiškūs ir teisėti	Priimtina	
Pagrindas: duomenų tvarkymo teisėtumas, piktnaudžiavimo draudimas	Priimtina	

Duomenų mažinimas: tinkamas ir ribotas	Priimtina	
Duomenų kokybė: tiksli ir nuolat atnaujinama	Priimtina	
Laikymo trukmė: ribota	Priimtina	

2.2 DUOMENŲ SUBJEKTŲ TEISĖMS APSAUGOTI SKIRTŲ PRIEMONIŲ VERTINIMAS

DUOMENŲ SUBJEKTŲ INFORMAVIMO PRIEMONIŲ NUSTATYMAS IR APRAŠYMAS

Teisės į informaciją įgyvendinimo priemonės	**Įgyvendinimas**	**Įgyvendinimo pagrindimas arba pagrindimas, kodėl ne**
Duomenų naudojimo / konfidencialumo sąlygų pristatymas	Taip	Informacija pateikiama Privatumo politikoje, su kuria supažindinamas programėlės naudotojas
Galimybė susipažinti su naudojimo / konfidencialumo sąlygomis	Taip	Informacija pateikiama Privatumo politikoje, su kuria supažindinamas programėlės naudotojas
Pateikiama glausta, skaidria, suprantama ir lengvai prieinama forma, aiškia ir paprasta kalba, ypač jei informacija yra konkrečiai skirta vaikui	Taip	Informacija pateikiama Privatumo politikoje, su kuria supažindinamas programėlės naudotojas
Išsamus duomenų tvarkymo tikslų pristatymas (nurodyti tikslai, duomenų suderinimas, jei taikoma, ir kt.)	Taip	Informacija pateikiama Privatumo politikoje, su kuria supažindinamas programėlės naudotojas
Išsamus surinktų asmens duomenų pristatymas	Taip	Informacija pateikiama Privatumo politikoje, su kuria supažindinamas programėlės naudotojas
Bet kokios prieigos prie įrenginio, išmaniojo telefono / planšetinio kompiuterio ar kompiuterio identifikatorių pateikimas nurodant, ar šie identifikatoriai perduodami trečiosioms šalims	Taip	Informacija pateikiama Privatumo politikoje, su kuria supažindinamas programėlės naudotojas
Naudotojo teisių pristatymas (sutikimo atšaukimas, duomenų ištrynimas ir kt.)	Iš dalies	Informacija pateikiama Privatumo politikoje, su kuria supažindinamas programėlės naudotojas
Informacija apie saugų duomenų saugojimą (metodus)	Taip	Informacija pateikiama Privatumo politikoje, su kuria supažindinamas programėlės naudotojas
Susisiekimo (duomenų valdytojo, tvarkytojo įvardinimas ir kontaktiniai duomenys) konfidencialumo klausimais tvarka	Taip	Informacija pateikiama Privatumo politikoje, su kuria supažindinamas programėlės naudotojas
Dėl duomenų perdavimo trečiosioms šalims:		
- išsamus perdavimo trečiosioms šalims tikslų pristatymas	Ne	Duomenys į trečiąsias šalis neteikiami
- išsamus perduotų asmens duomenų pristatymas	Ne	Duomenys į trečiąsias šalis neteikiami
- trečiųjų šalių įstaigų tapatybės nurodymas	Ne	Duomenys į trečiąsias šalis neteikiami

PRIEMONIŲ, LEIDŽIANČIŲ GAUTI SUTIKIMĄ, NUSTATYMAS IR APRAŠYMAS

Kaip išdėstyta PDAV dokumente, programėlės naudojimas yra visiškai savanoriškas ir bus toks. Valdytojas neturi jokių priemonių aptikti programėlės naudojimą ar jos nenaudojimą bet kurio identifikuojamo asmens mobiliame telefone. BDAR 7 straipsnyje nustatyta keletas sąlygų, kai asmens duomenys tvarkomi remiantis sutikimu. Šių sąlygų įvertinimas išdėstytas taip.

Sutikimo gavimo priemonės	**Įgyvendinimas**	**Įgyvendinimo pagrindimas arba pagrindimas, kodėl ne**
Sutikimo pareiškimas prieš duomenų tvarkymo operaciją	Taip	Programėlės naudotojas duoda sutikimą: atsisiųsdamas programėlę; sutikdamas naudoti artumo registravimo funkciją ir sutikdamas dalinti užsikrėtimo Covid-19 infekcija atveju, suvesdamas APK.
Sutikimas segmentuotas pagal duomenų kategoriją arba tvarkymo tipą	Taip	Sutinkama prieš pradedant naudotis programėle, prieš pradedant naudoti artumo registravimo funkciją ar norint pranešti apie užsikrėtimą.
Sutikimo išreiškimas prieš duomenų teikimą kitiems naudotojams	Ne	Kitiems naudotojams nėra teikiami duomenys, iš kurių kiti naudotojai gali tiesiogiai ar netiesiogiai nustatyti programėlės naudotoją.
Sutikimas pateikiamas glausta, skaidria, suprantama ir lengvai prieinama forma, aiškia ir paprasta kalba, ypač jei informacija yra konkrečiai skirta vaikui.	Taip	Kad atsakomybė už pasirinkimo galimybių įvertinimą ir visiškai rizikos vertinimą nebūtų perkelta duomenų subjektui, duomenų subjekto pagrindinių teisių rizika turėtų būti pateikiama aiškia ir paprasta kalba, pradedant nuo procedūros aprašymo, kad duomenų subjektas galėtų pasverti pagrindinių teisių riziką ir siekiamą tikslą. Toks pateikimas aiškia ir paprasta kalba vargu ar yra įmanomas, atsižvelgiant į procedūros sudėtingumą ir programėlės naudojimo padarinius. Tačiau privatumo politikoje pateikiama informacija, su kuria susipažįsta programėlės naudotojas prieš pradėdamas naudotis programėle, labai stipriai supaprastina ir pateikta aiškia paprasta, suprantama kalba, nenaudojant daug techninių detalių.
Tėvų sutikimo gavimas nepilnamečiams iki 14 metų	Ne	Programėlės naudojimas yra numatytas tik nuo 16 metų.[15]
Sutikimas gaunamas iš kiekvieno naujo naudotojo	Taip	Sutikimas gaunamas kiekvienos įdiegtos programėlės naujam naudotojui atveju.
Kai naudotojas sutiko tvarkyti specialių kategorijų duomenis (pvz., Jo / jos sveikatos duomenis), aiškiai nurodoma, kad minėtas tvarkymas vyksta (piktograma ar lemputė)	Taip	Privatumo politikoje, su kuria naudotojas susipažįsta prieš pradėdamas naudoti programėlę, turi būti aiškiai išskirtas sveikatos duomenų tvarkymas..

[15] Šešiolika yra sveiktos duomenų tvarkymo sutikimo amžius Lietuvoje. Dėl šios priežasties būsimų programėlės naudotojų bus paprašyta patvirtinti, kad atsisiuntimo metu jie yra 16 metų ar vyresni. Programėlių parduotuvės valdikliai bus įdiegti siekiant apriboti programos prieinamumą tiek, kiek įmanoma. „Google Play“ parduotuvė gali apriboti 16 ir daugiau; o „Apple“ programėlių parduotuvė gali apriboti nuo 12 ir daugiau - šie nustatymai bus taikomi. Manoma, kad tai didelis iššūkis patikimai prašyti tėvų sutikimo, kad būtų palaikomi jaunesni programėlės naudotojai šiame etape. Šiuo metu nėra aišku, kaip tai galima pasiekti praktiniu būdu, kuris galėtų išplėsti mastą. Be to, nėra aišku, ar tikslinga perspėti jaunus žmones pranešant apie poveikį, nes jie tuo metu gali nebūti globėjo akivaizdoje.

Kai vartotojas keičia įrenginį, išmanųjį telefoną ar kompiuterį, iš naujo įdiegia programą mobiliesiems arba ištrina slapukus, išlaikomi su jo sutikimu susiję nustatymai	Ne	Įdiegus programėlę iš naujo naudotojas yra fiksuojamas, kaip naujas, todėl sutikimas turi būti duodamas iš naujo.
Sutikimo atšaukimas	Taip	Bet kuriuo metu galima atšaukti bet kurį Programėlės nustatymuose pateiktą sutikimą. Norint atšaukti artumo registravimo funkciją, galima išjungti šią funkciją Programėlės nustatymuose arba ištrinant Programėlę. Norėdami atšaukti sutikimą dėl pasidalinimo Covid-19 atveju, reikia ištrinti Programėlę. Šiuo atveju bus sunaikinti visi artumo raktai, saugomi Programėlėje, o pastaroji nebebus siejama su naudotojo išmaniuoju telefonu. Perduotų anoniminių užsikrėtimo atvejį nurodančių raktų iš serveryje saugomo sąrašo ir iš kitų naudotojų išmaniųjų telefonų Programėlės valdytojas panaikinti negali, nes jie nėra siejami su konkrečiu naudotoju. Ši informacija turi būti pateikta privatumo politikoje.

Duomenys	**Sutikimo demonstravimas**	**Aiškiai atskirtas**	**Teisė atšaukti**	**Sąlyginis / laisvai duotas**
Tvarkomi duomenys: **- Artumo raktas (pseudoniminis)** **- atstumas** **- trukmė** **- programėlės naudotojo užsikrėtimo atvejis** **- anoniminiai užsikrėtimo atvejį nurodantys duomenys (užsikrėtimo raktai)** **- rizikos balas** **- laiko specifikacija**	Telefono nustatymai saugo įrašą, kad asmuo sutiko telefone įjungti arba išjungti artumo duomenų registravimo paslaugas. Įjungus šią paslaugą, artumo raktai bus saugomi telefone. Be to, prieš įkeliant užsikrėtimo raktus, naudotojo prašoma sutikimo, o po raktų įkėlimo programa pateikia naudotojui patvirtinimą apie įkėlimą.	Telefono nustatymų ekranus, susijusius su užsikrėtimo klavišais, teikia „Apple“ ir „Google“ ir jie yra atskirai nuo programėlės ekranų. Nustatymų ekranai yra susiję tik su konkrečiu pranešimo apie poveikį tikslu. Prieš įkeldama užsikrėtimo raktus, telefonas prašo naudotojo leisti programai pasiekti užsikrėtimo raktus.	Telefono nustatymuose naudotojas gali bet kada įjungti ir išjungti artumo registravimo paslaugas, taip pat bet kuriuo metu ištrinti visus ENF duomenis atkurdamas programėlę nustatymuose. NVSC turimi užsikrėtimo raktai nėra susiję su jokiu konkrečiu asmeniu, todėl jų pašalinti negalima.	Užsikrėtimo raktų tvarkymas yra neprivalomas ir nepriklauso artumo registravimo funkcijos. Be to, nėra jokios priklausomybės nuo šių duomenų tvarkymo ar su jomis susijusių sąlygų, išskyrus konkretų jų apdorojimo tikslą - pranešimą apie poveikį. Užsikrėtimo raktai negali būti naudojami asmeniui identifikuoti, todėl kontrolieriai neturi jokių priemonių ir nesiekia nustatyti, ar konkretus asmuo turi užsikrėtimo raktų.
Mobilaus telefono ryšio numeris	Kai NVSC surinktas mobiliojo telefono numeris	Asmeniui paskambinus NVSC nustatomas Covid-	Mobiliojo telefono tvarkymas yra	Tai neprivalomas žingsnis, o rankinis kontaktų sekimo

	tvarkomas siekiant išsiųsti APK, NVSC saugo įrašą, kurį asmuo sutiko atlikti.	19 atvejis ir atskirai ir aiškiai telefonu klausiama, ar jis yra programėlės naudotojas ir ar jis sutinka dalytis savo užsikrėtimo raktais.	laikinas. Kai mobiliojo telefono numeris buvo panaudotas siųsti SMS, jis iš programėlės serverio nedelsiant ištrinamas.	interviu tęsiasi kaip įprasta. Be to, nėra jokio priklausomybės nuo šių duomenų tvarkymo ar su jais susijusių sąlygų, išskyrus konkretų jų apdorojimo tikslą - užsikrėtimo raktų paskelbimą programėlės serveryje, kad būtų įgalintas pranešimas apie poveikį.
APK	Sutikimas gauti APK duodamas bendraujant užsikrėtusiam asmeniui su NVSC specialistu vykdančių rankinį kontaktų atsekimą	Asmeniui paskambinus NVSC nustatomas Covid-19 atvejis ir atskirai ir aiškiai telefonu klausiama, ar jis yra programėlės naudotojas ir ar jis sutinka dalytis savo užsikrėtimo raktais bei gauti tam reikalingą APK.	Gavęs APK naudotojas gali jo nenaudoti.	APK gavimas telefone neprivalomas žingsnis ir atsiunčiamas taip sutarus rankinio kontaktų atsekimo interviu metu.
IP adresai	Programa yra prijungta prie interneto, todėl tinklo maršrutas ir saugos žymės yra apdorojami kaip įprasta. Programėlės buvimas naudotojo įrenginyje laikomas įrodymu, kad sutikimas buvo gautas.	Laikoma, kad atsisiuntimo ir diegimo veiksmas yra aiškiai atskiriamas pagal internetą naudojančių programėlių normą.	IP adresai nėra saugomi programėlėje ar jos serveryje, todėl jų negalima pašalinti.	Programėlė yra visiškai savanoriška, o dalyvavimas artumo registravime nėra sąlyginis programos naudojimas. Be to, nėra jokios priklausomybės nuo šių duomenų tvarkymo ar sąlygų, susijusių su konkrečiu pačios programos tikslu.

PRIEIGOS TEISIŲ, DUOMENŲ PERKELIAMUMO IR TEISĖS IŠTAISYTI PRIEMONIŲ NUSTATYMAS IR APRAŠYMAS

Šios duomenų subjekto teisės gali būti įgyvendinamos, kai yra galimybė vienareikšmiškai nustatyti asmens tapatybę, tuo tarpu programėlėje naudojamos technologijos yra sukurtos taip, kad asmens duomenų būtų tvarkoma kaip galima mažiau arba visai netvarkoma, tai yra tvarkomi anoniminiai raktai, todėl duomenų subjekto teisės gauti prieigą, taisymą, ištrynimą, tvarkymo apribojimą, prieštaravimą tvarkymui ir duomenų perkeliamumą nėra taikomos dėl to, kad neįmanoma jų įvykdyti nerenkant perteklinių duomenų apie asmenį. Nei „Google“, nei „Apple“, nei kiti naudotojai negali matyti programėlės naudotojo tapatybės. Pranešimų apie galimą kontaktą su užsikrėtusiu asmeniu sistema duomenų derinimas atliekamas naudotojo įrenginyje.

Tai reiškia, kad tik naudotojas ir programa žino, ar pranešta, kad naudotojas užsikrėtė Covid-19, ir ar kontaktavo su kuo nors, kas pranešė apie užsikrėtimą Covid-19. Naudotojo tapatybė nebendrinama nei su kitais naudotojais, nei su „Apple“ ar „Google“.

TEISĖS IŠTRINTI PRIEMONIŲ NUSTATYMAS IR APRAŠYMAS

Ši duomenų subjekto teisė gali būti įgyvendinama, kai yra galimybė vienareikšmiškai nustatyti asmens tapatybę, tuo tarpu programėlėje naudojamos technologijos yra sukurto taip, kad asmens duomenų būtų tvarkoma kaip galima mažiau arba visai netvarkoma, tai yra tvarkomi anoniminiai raktai, todėl duomenų subjekto teisės gauti prieigą, taisymą, ištrynimą, tvarkymo apribojimą, prieštaravimą tvarkymui ir duomenų perkeliamumą nėra taikomos dėl to, kad neįmanoma jų įvykdyti nerenkant perteklinių duomenų apie asmenį. Nei naudotojas, nei duomenų valdytojas ar tvarkytojas neturi galimybės ištrinti savo skleistų atsitiktinių artumo raktų, kurie yra saugomi kito naudotojo įrenginyje. Anoniminiai užsikrėtimo atvejį nurodantys duomenys, kurie saugomi Programėlės serveryje, negali būti ištrinti, nes nėra galimybės nustatyti šių duomenų asmens tapatybės. Artumo raktai, kurie yra saugomi naudotojo įrenginyje gali būti ištrinti atkūrus programėlės gamyklinius parametrus programėlės nustatymuose.

TEISIŲ Į DUOMENŲ TVARKYMO APRIBOJIMĄ IR PRIEŠTARAVIMĄ PRIEMONIŲ NUSTATYMAS IR APRAŠYMAS

Teisių į apribojimą ir prieštaravimą įgyvendinimo priemonės	**Įrenginyje tvarkomi duomenys**	**Kito naudojo įrenginyje ir programėlės serveryje tvarkomi duomenys**	**Pagrindimas**
„Privatumo“ nustatymų buvimas	Taip	Taip	Programėlė sukurta taip, kad ji nėra siejama su konkretaus asmens tapatybę ir nesaugo nei telefono numerio, nei IP adreso ar kt. asmenį identifikuojančių duomenų, tačiau naudotojas gali valdyti programėlės naudojamus leidimus ir funkcijas.
„Privatumo“ nustatymai pasiekiami registracijos metu	Taip	Taip	Naudotojas turi galimybę pasirinkti, kokias programėles funkcijas naudos ir kokius leidimus suteiks.
„Privatumo“ nustatymai pasiekiami po registracijos	Taip	Taip	Programėlės naudotojas gali bet kuriuo metu pasiekti privatumo nustatymus ir išjungti leidimus, bei atkurti programėlės pradinius parametrus.
Tėvų kontrolės sistemos egzistavimas vaikams iki 14 metų	Ne	Ne	Programėlė taikoma asmenims nuo 16 metų.
Atitikimas stebėjimo atžvilgiu (slapukai, reklama ir kt.)	Ne	Ne	Programėlės naudotojai nėra stebimi ir slapukai, ar reklama nėra taikomi.
Vaikų iki 14 metų neįtraukimas į automatinį profiliavimą	Taip	Taip	Programėlė platinama asmenims nuo 16 metų.
Faktinis naudotojo duomenų tvarkymo pašalinimas, jei	Taip	Ne	Programėlėje pašalinami artumo duomenys, kai nustatymuose atkuriami gamykliniai parametrai arba

sutikimas yra panaikinamas			programėlė ištrinama. Programėlės serveryje tvarkomi anoniminiai duomenys, todėl nebegali būti ištrinti.

TVARKYTOJAMS TAIKOMŲ ĮSIPAREIGOJIMŲ NUSTATYMAS IR APRAŠYMAS

Tvarkytojo pavadinimas	Tikslas	Apimtis	Sutarties nuoroda	Atitiktis BDAR 28 str.
NVSC	ULSKIS nuostatuose numatytu funkcijų ir pareigų įgyvendinimas.	Fiksuoja Covid-19 užsikrėtimo atvejį ULSKIS, generuoja APK ir pateikia jį naudotojui, duomenų valdytojo vardu įgyvendina duomenų subjektų teises, vykdo kitas ULSKIS numatytas funkcijas ir pareigas.	ULSKIS nuostatai	Atitinka
IVPK	Prižiūri Programėlės Techninę infrastruktūros dalį (serverių sistemą)	Duomenų mainų tarp programėlės naudotojų per programėlės serverį užtikrinimas.	Sutartis	Atitinka
EK	Europos Komisijos sietinio tinklų sietuvo techninė priežiūra.	Duomenų mainų tarp ES šalių užtikrinimas. Europos Komisija vykdo konkrečius įpareigojimus, nustatytus jai, kaip duomenų valdytojų duomenų tvarkytojui, pagal Įgyvendinimo sprendimo (ES) 2019/1765 III priedą.	Sutartis dar nėra sudaryta ir programėlė su EK dar neintegruota.	

DUOMENŲ PERDAVIMO UŽ EUROPOS SĄJUNGOS RIBŲ PRIEMONIŲ NUSTATYMAS IR APRAŠYMAS

Programėlėje kaupiami duomenys gali būti naudojami tik Lietuvos, ES arba EEB valstybių serveriuose.

PRIEMONIŲ VERTINIMAS

Vartotojai pagal BDAR turi teises, kai jų asmens duomenis tvarko duomenų valdytojai. Reikėtų atkreipti dėmesį į šias aplinkybes. IP adresai nėra saugomi nei programėlėje, nei jos serveryje, o tvarkomi laikino tinklo nukreipimo ir tinklo saugumo tikslais. Užsikrėtimo raktų negalima susieti su asmeniu, nes jie nėra susiejami pagal programėlės architektūrą. Mobilaus telefono numeris, jei jis pateiktas, ir naudojant kurį SMS žinute siunčiamas APK, yra laikinai apdorojamas ir nedelsiant ištrinamas išsiuntus SMS.

Teisė į informaciją - duomenų apsaugos informacinis pranešimas pateikiamas pačioje programėlėje tuose puslapiuose, kuriuose reikalaujama informacijos, taip pat programėlės informacijoje. Pranešime pateikiama informacija, nustatyta BDAR 13 ir 14 straipsniuose.

Prieigos teisė - naudotojas gali pats pasiekti duomenis per programėlę ir taip pat pateikti duomenų subjekto prieigos užklausą NVSC.

Teisė į taisymą - naudotojas turi teisę ištaisyti netikslius asmens duomenis ir gali prašyti, kad jų duomenys būtų pataisyti NVSC dėl telefone neapdorotų duomenų, ir gali atnaujinti duomenis naudodamasis programėlės nustatymais.

Teisė ištrinti - naudotojas gali pasirinkti funkciją „Atkurti programėlę“, bet kada ištrinti programėlę ir ištrinti ENF duomenis per įrenginio nustatymus - ištrinti visus telefone tvarkomus duomenis. Daugiau prašymų ištrinti galima siųsti NVSC.

Teisė į apribojimą - naudotojas gali atšaukti savo ENF leidimą, nuspręsti nekelti raktų. Galiausiai naudotojas gali nuspręsti ištrinti programėlę iš savo įrenginio.

Teisė į perkeliamumą - naudotojai negali perkelti savo raktų, pavyzdžiui, iš vieno įrenginio į kitą įrenginį, nes naudotojai neturi prieigos prie tokių raktų savo įrenginyje (išskyrus, kad juos ištrintų) ir Programėlės serveryje, NVSC negali nustatyti, kurie raktai priklauso kuriam naudotojui.
Teisė prieštarauti - naudotojas gali ištrinti programėlę iš savo įrenginio.
Teisė netaikyti tik automatizuoto sprendimų priėmimo, įskaitant profiliavimą - jei ENF aptinka suderinamumą tarp programoje esančio artumo rakto ir iš Programėlės serverio atsisiųsto užsikrėtimo rakto, priimamas sprendimas, kad buvo užmegztas artimas kontaktas. Šis sprendimas yra pagrįstas tik automatizuotu identifikatorių ir raktų apdorojimu ir daro didelę įtaką naudotojams. Tačiau šis tvarkymas grindžiamas aiškiu naudotojo sutikimu, kai jis įgalino paslaugą savo telefone. Programėlė nepriima automatinio sprendimo dėl to, ar asmuo turi COVID-19, bet, atsižvelgdamas į artimą kontaktą, pateikia galimos užsikrėtimo rizikos vertinimą.

Duomenų subjektų teisių įgyvendinimo priemonės	**Priimtina / galima patobulinti?**	**Taisomoji priemonė**
Informacija duomenų subjektams (sąžiningas ir skaidrus tvarkymas)	Galima patobulinti	Papildyti Privatumo politikoje pateikiamą informacija apie duomenų subjektų teises. Nurodyti, kad informaciją, kad duomenų subjekto teisės gauti prieigą, ištaisyti, ištrinti, apriboti tvarkymą, prieštarauti tvarkymui ir duomenų perkeliamumui nėra taikomos arba netaikomos tam tikriems duomenims dėl to, kad neįmanoma įvykdyti; informacija, kad duomenų subjekto teisė bet kuriuo metu atšaukti sutikimą yra apribota reikalaujant, kad programėlė nutrauktų tolesnį asmens duomenų tvarkymą, kai neįmanoma nustatyti naudotojo santykių turint tokius asmens duomenis, todėl jau pateikti asmens duomenys vis tiek bus tvarkomi.
Sutikimo gavimas	Priimtina	
Naudojimasis prieigos ir duomenų perkeliamumo teisėmis	Priimtina	
Teisių į ištaisymą ir ištrynimą įgyvendinimas	Priimtina	
Naudojimasis teisėmis į duomenų tvarkymo apribojimą ir prieštaravimą	Priimtina	
Tvarkytojai: nustatyti ir valdomi pagal sutartį arba teisės aktu	Priimtina	
Duomenų perdavimas: duomenų perdavimo už Europos Sąjungos ribų įsipareigojimų vykdymas	Šis funkcionalumas dar neįdiegtas	

3 RIZIKŲ DUOMENŲ APSAUGAI VERTINIMAS

Ar būtina programėlės vykdomai duomenų tvarkymo operacijai atlikti PDAV?

Žemiau pateiktos analizės tikslas yra nustatyti duomenų subjektų duomenų tvarkymo veiklos rizikos lygį. Kai dėl duomenų tvarkymo rūšies, ypač kai naudojamos inovatyvios technologijos, ir atsižvelgiant į duomenų tvarkymo pobūdį, aprėptį, kontekstą ir tikslus, fizinių asmenų teisėms bei laisvėms gali kilti didelis pavojus, BDAR 35 str. numato, kad duomenų valdytojas turi atlikti PDAV.

BDAR išskiria du rizikos lygius, t. y. žemą / įprastą ir aukštą. Atsižvelgiant į rizikos lygį, tvarkymas turi būti: a) ypač kruopščiai suprojektuotas atsižvelgiant į poveikį pagrindinėms teisėms ir laisvėms, ir b) turi būti kruopščiai atrinktos ir įgyvendintos sustiprintos veiksmingos apsaugos priemonės, kurias galima patikrinti ir kontroliuoti. Kadangi vien tik asmens duomenų tvarkymo faktas paprastai kelia žemą / įprastą riziką duomenų subjektams, todėl bet kokiu atveju tvarkant asmens duomenis reikia imtis apsaugos priemonių. Šios priemonės turi užtikrinti, kad būtų vykdomi duomenų tvarkymo veiklos reikalavimai pagal BDAR 5, 24, 25 ir 32 straipsnius.

Norint nustatyti atitinkamos duomenų tvarkymo veiklos rizikos lygį, naudojami trys kriterijų rinkiniai: a) BDAR 9 str. 1 d.; b) BDAR 25 str. ir c) 29 straipsnio duomenų apsaugos darbo grupės 248 darbo dokumento sąrašas.

A) Apdorojant specialių kategorijų duomenis, o programėlės atveju – **sveikatos duomenis**, kyla didelė rizika. Programėlė renka tik atstumo duomenis tarp išmaniųjų telefonų. Kol asmeniui nebuvo diagnozuotas užsikrėtimas ir jam nebuvo išduotas APK, tai nėra duomenys apie sveikatą. Gavus APK, programoje esantis artumo raktas tampa sveikatos duomenimis, kurie turi būti ypač saugomi.

b) BDAR 25 str. pateikiami keli kriterijai, pagal kuriuos nustatoma rizika, kurią kelia pati duomenų tvarkymo veikla, o ne tvarkomi duomenys. Šie kriterijai apima duomenų tvarkymo pobūdį, apimtį, aplinkybes ir tikslus, taip pat rizikos tikimybę ir rimtumą fizinių asmenų teisėms ir laisvėms.

Nagrinėjamu atveju kontaktiniai/sąlyčio atvejai apskaičiuojami iš didelio nuotolio duomenų kiekio, remiantis euristika, kuriai priskiriamas poveikio **pobūdis**, tai sukelia rimtų teisinių ir faktinių pasekmių atitinkamiems asmenims, pavyzdžiui, pareigą saviizoliacijai.

Duomenų tvarkymo sritis susijusi su bet kuriuo asmeniu, turinčiu išmanųjį telefoną su įdiegta programa. Atsižvelgiant į lūkesčius, kad bent 60% gyventojų dalyvaus šiame procese, kad jis turėtų epidemiologinį apsauginį poveikį, ir į socialinį spaudimą jį naudoti, galima manyti, kad šis duomenų tvarkymas **paveiks daugelį Lietuvos gyventojų**.

Aplinkybės priklauso nuo duomenų tvarkymo **konteksto**. Toks duomenų tvarkymas greičiausiai diskriminuos asmenis, turinčius tam tikrų savybių, pavyzdžiui, dėl to, kad jie yra užkrėsti Covid-19 infekcija. Taip pat galima įsivaizduoti, kad atsakingas asmuo, proceso vykdytojas ar politinė vadovybė vėliau gali nustatyti papildomus kriterijus, pagal kuriuos kitų tipų asmenys bus „filtruojami“, tada kontroliuojami ar valdomi. Programėlėje atliekamo duomenų tvarkymo **tikslas** yra identifikuoti ir atskirti asmenis, kad galima būtų paveikti jų elgesį.

Tikimybė, kad asmenys bus rasti taikant šią procedūrą, yra didelė, ir šio duomenų tvarkymo **tikslas** yra surasti tam tikrų tipų asmenis. Be to, yra didelė rizika ar tikimybė, kad procedūra išfiltruos asmenis, kurie nėra užsikrėtę Covi-19 infekcija, bet kurie vis dėlto turi bent laikinai patirti rimtą kišimąsi į savo pagrindines teises ir laisves.

c) kaip trečiasis rizikos lygio nustatymo kriterijus yra naudojamos 29 straipsnio darbo grupės „Duomenų apsaugos poveikio vertinimo gairės“. Šiose rekomendacijose išvardinti devyni skirtingi kriterijai, kad būtų nustatytas rizikos lygis. Duomenų apsaugos institucijos ES sutarė, kad „tikėtina, jog didelės rizikos“ situacija yra, jei tenkinami bent du šio sąrašo kriterijai:

1. „Vertinimas arba balų skyrimas, įskaitant profiliavimą ir prognozavimą …“,
2. „Automatizuotas sprendimų, sukeliančių teisinį arba panašų rimtą poveikį, priėmimas …“,
3. „Sisteminga stebėsena: duomenų tvarkymas, naudojamas duomenų subjektų stebėsenos arba kontrolės tikslais...“,
4. „Neskelbtini duomenys arba labai asmeniški duomenys …“,
5. „Didelio masto duomenų tvarkymas ...“,
6. „Duomenų rinkinių siejimas ir derinimas...“,
7. „Su pažeidžiamais duomenų subjektais susiję duomenys…“,
8. „Naujoviškas naudojimas arba naujų technologinių ar organizacinių sprendimo būdų taikymas…“,
9. „Atvejis, kai dėl paties duomenų tvarkymo „duomenų subjektams užkertamas kelias naudotis savo teisėmis, paslaugomis arba sudaryti sutartis“ (22 straipsnis ir 91 konstatuojamoji dalis)…“.

Ankstesniuose skyriuose išanalizavę programėlės duomenų tvarkymo veiklas, matome, jog šiai procedūrai taikomi paskutiniai septyni šio sąrašo kriterijai, kaip trumpai išdėstyta aukščiau.
Atsižvelgiant į tai, darytina išvada, kad nagrinėjamai duomenų tvarkymo veiklai dėl didelės rizikos duomenų subjektams PDAV pagal BDAR 35 str. būtina atlikti.

3.1. DUOMENŲ APSAUGOS PRIEMONIŲ VERTINIMAS

LOGINĖS DUOMENŲ APSAUGOS PRIEMONĖS

Loginės priemonės skirtos duomenų tvarkymui	**Įgyvendinimas arba pagrindimas, kodėl gi ne**	**Priimtina/galima patobulinti**	**Korekcinės priemonės**
Šifravimas	• Artumo duomenys saugomi užšifruoti mobilaus įrenginio ENF komponente ir programėlei pasiekiami tik per ENF sąsajas (ENF API). • Duomenys saugomi programėlės serveryje yra saugojami užkoduota forma. • Duomenys perduodami elektroniniu būdu yra šifruojami.	Priimtina	
Nuasmeninimas	Užsikrėtusiųjų raktai yra sukurti kaip atsitiktiniai raktai ir pagal jų kūrimo principą nėra išvestinis duomuo iš programėlės naudotojo kitų duomenų. Paskelbti užsikrėtusiųjų raktai perdavimo iš programėlės į programėlės serverį metu yra atsiejami nuo programėlės naudotoją galinčių identifikuoti duomenų tokių kaip IP adresas. Toliau programėlės serveryje saugomi tik paskelbti užsikrėtusių raktai. Paskelbti raktai jau yra nuasmeninti ir nesusiejami su jais sukūrusiomis konkrečių naudotojų programėlėmis.	Priimtina	
Duomenų skaidymas (likusios informacinės sistemos atžvilgiu)	• Programėlės ENF komponento skleidžiamų raktų generavimui naudojami kodai atsinaujina kas dieną, taip įgalinant duomenų skaidymą pagal dienas. • Naudojamas duomenų skaidymas pagal skirtingas veiklas vykdančius procesus. Tokiu būdu programėlės serveris turi kelias logines dalis. Vienoje programėlės serverio dalyje vykdomi verifikavimo procesai susiję su APK sukūrimu ir išsiuntimu naudotojams, bei APK patikrinimu kuomet vykdomas užsikrėtimo raktų pateikimas iš programėlės į programėlės serverį, o kita programėlės serverio dalis skirta užsikrėtusių raktų tvarkymui (saugojimas, keitimasis su kitais serveriais, šalinimas) ir platinimui. Abi dalys programėlės serverio kūrimo metu turėtų būti realizuotos kaip atskiri fiziniai komponentai ir diegiami atskiruose virtualiuose serveriuose.	Priimtina	
Loginė prieigos kontrolė	• ULSKIS naudotojų siunčiančių APK programėlės naudotojams prieigos teisės yra valdomos pagal aprašytas roles.	Priimtina	

	• Prisijungimo slaptažodžių sudėtingumui naudojamos slaptažodžio sudėtingumo taisyklės. • Klaidingi prisijungimai numatytam laikui blokuoja atitinkamo naudotojo prisijungimą, taip įgalinat apsisaugoti nuo įsilaužimų atspėjant naudotojo slaptažodį.		
Veiksmų registravimas	Programėlės serverio naudotojų prisijungimų žurnalas, APK siuntimo žurnalas. Registruoti veiksmai turi būti periodiškai analizuojami siekiant pastebėti nesankcionuotas prieigas ar darbą su sukurta sistema.	Priimtina	
Vientisumo stebėjimas	• Atsiunčiant duomenų paketus iš programėlės serverio į programėlę, programėlė patikrina ar duomenys yra skaitmeniniu būdu pasirašyti programėlės serverio. • Užsikrėtusių raktų pateikimui į serverį yra vykdoma kontrolė, kad duomenys būtų pateikiami tik su galiojančiais APK. • Programėlė periodiškai atsisiunčia užsikrėtimo rizikos vertinimo skaičiavimo parametrus iš programėlės serverio taip užtikrinant numatytą rizikos paskaičiavimo metodikos naudojimą.	Priimtina	
Archyvavimas	• Duomenų kopijų darymo procese užtikrinamas principas, kad archyvuojami užsikrėtusių raktai ne senesni kaip 14 dienų. • Saugomose duomenų kopijose neturi būti tokių saugomų kopijų, kuriose būtų senesni kaip 14 dienų raktai. Tam vykdomas savalaikis duomenų kopijų šalinimas.	Priimtina	
Popierinių dokumentų apsauga	Popierinių dokumentų tvarkymas nėra vykdomas	Netaikoma	

FIZINĖS (TECHNINĖS) APSAUGOS PRIEMONĖS

Sistemos, kurioje vykdomas tvarkymas, fizinės (techninės) apsaugos priemonės	**Įgyvendinimas arba pagrindimas, kodėl gi ne**	**Priimtina/galima patobulinti**	**Korekcinės priemonės**
Eksploatavimo sauga	Eksploatuojant programėlės sprendimą laikomasi ULSKIS duomenų saugos nuostatuose nustatytų reikalavimų. Periodiškai diegiami programinės įrangos ir operacinių sistemų atnaujinimai.	Priimtina	
Kenkėjiškų programų prevencija	Kenkėjiškų programų prevencija vykdoma ULSKIS naudotojų darbo vietose ir ULSKIS serveriuose. Reikalavimai kenkėjiškų programų prevencijai nustatyti ULSKIS duomenų saugos nuostatuose ir su juo susijusiuose saugos dokumentuose	Priimtina	

Personalinių kompiuterių administravimas	ULSKIS naudotojų darbo kompiuteriuose taikoma automatinio užrakto priemonė, vykdomas periodinis programinės įrangos atnaujinimas.	Priimtina	
Interneto svetainių sauga	Programėlės duomenys nėra tvarkomi interneto svetainėje. Interneto svetainėje pateikiami tik su programėle susijusi informacija, dažnai užduodami klausimai.	Priimtina	
Atsarginės kopijos	Atsarginės serverio kopijos ir duomenų kopijos užtikrina programėlės veikimo atstatymą įvykus duomenų praradimui ar atstatant sistemos veikimą. Atsarginės kopijos daromos ir saugomos saugioje vietoje, pasiekiamoje tik sistemos administratoriams. Programėlės serverio atsarginės kopijos kuriamos ir saugojamos IVPK duomenų centre. Už atsarginių kopijų darymą atsakinga NVSC ir jos įgaliotas IT administratorius, pagal aplinkybes remiamasi IVPK paslaugomis arba samdomais IT sistemų administravimo paslaugų teikėjais.	Priimtina	
Palaikymas	Techninės įrangos palaikymą vykdo IVPK. Programėlės serverio programinės įrangos nuotolinį palaikymą vykdo NVSC ir pagal NVSC įgaliojimą paslaugų teikimo įmonė įdiegusi programėlę.	Priimtina	
Tinklo saugumas	Tinklo ir komunikacijos sauga yra ypač svarbi, siekiant užtikrinti asmens duomenų saugą. Informacinės sistemos tinklas atskirtas nuo kitų duomenų valdytojo tinklų. Prieiga prie IT sistemos atliekama tik iš patvirtintų įrenginių.	Priimtina	
Stebėjimas	Duomenų judėjimui stebėti diegiamos ugniasienės ir įsibrovimo aptikimo ir prevencijos sistema.	Priimtina	
Fizinė praėjimo kontrolė	APK kodo išsiuntimas vykdomas NVSC specialistų darbo vietose. Darbo vietų saugai užtikrinti galioja ne silpnesni reikalavimai nei numatyti ULSKIS duomenų saugos nuostatuose.	Priimtina	
Techninės įrangos sauga	Techninė įranga, kurioje veikia programėlės serveris ir jam reikalinga infrastruktūra saugoma IVPK duomenų centre. Fizinė prieiga prie techninės įrangos leidžiama IVPK specialistams ir IVPK samdomiems paslaugų teikėjams.	Priimtina	
Rizikos šaltinių užkardymas	ULSKIS serverių komponentai ir duomenys saugomi Lietuvoje IVPK duomenų centre arba kitose ES šalyse, kurios užtikrina asmens duomenų apsaugą	Priimtina	
Apsauga nuo ne nuo žmogaus priklausančių rizikų	Taikomos saugos priemonės dėl nuo žmogaus elgesio nepriklausančių rizikų: gaisras, užliejimas, kita. Šios saugos priemonės taikomos IVPK duomenų centre, kuriame veikia programėlės serveris ir susijusi tinklo infrastruktūra.	Priimtina	

ORGANIZACINĖS APSAUGOS PRIEMONĖS

Organizacinės apsaugos priemonės	Įgyvendinimas arba pagrindimas, kodėl gi ne	Priimtina/galima patobulinti	Korekcinės priemonės
Duomenų apsaugos organizavimas	Už duomenų apsaugos organizavimą yra atsakinga NVSC, kuri paskiria ULSKIS saugos įgaliotinį ir duomenų apsaugos pareigūną. Šios dvi pareigybės atskirtos. Saugos specialisto uždaviniai nustatyti ULSKIS duomenų saugos nuostatuose ir kituose saugos dokumentuose.	Priimtina	
Tvarkos	NVSC nustatyta pranešimo apie asmens duomenų saugumo pažeidimus kompetentingoms institucijoms ir duomenų subjektams tvarka, parengta programėlės privatumo politika, duomenų saugos dokumentai (duomenų saugos nuostatai, naudotojų administravimo taisyklės, veiklos tęstinumo valdymo planas, elektroninės informacijos tvarkymo taisyklės).	Priimtina	
Rizikų valdymas	Rizikų valdymui naudojamos valdymo priemonės, kuriomis valdomos nustatytos rizikos, vykdomas rizikų stebėjimas, periodiškai įvertinamos naujos galimos rizikos ir skirtos priemonės jų valdymui.	Priimtina	
Projekto valdymas	Vykdant programėlės projektą kūrimo ir eksploatacijos metu aiškiai įvardintos funkcijos, specialistai ir jų rolės projekte. Taip pat aiškiai įvardintos programėlės kūrime ir eksploatacijoje dalyvaujantys paslaugų teikėjai ir jų sutartiniai įsipareigojimai.	Priimtina	
Duomenų apsaugos pažeidimų valdymas	NVSC nustatytas reagavimo į saugumo incidentus planas, užtikrinantis veiksmingą incidentų, susijusių su asmens duomenų saugumu, valdymą. Asmens duomenų saugumo pažeidimai fiksuojami (dokumentuojami). Apie juos nedelsiant pranešama vadovybei ir kitoms atsakingoms ar susijusioms institucijoms.	Priimtina	
Personalo valdymas	NVSC užtikrinta, kad visi darbuotojai dirbantys su ULSKIS suprastų savo atsakomybes ir įsipareigojimus, susijusius su asmens duomenų tvarkymu. Vaidmenys ir atsakomybės yra aiškiai išdėstytos darbuotojui prieš pradedant vykdyti jam paskirtas funkcijas ir darbus. Darbuotojai, prieš pradėdami eiti savo pareigas, pasirašytinai supažindinami su organizacijos saugumo politika, taip pat pasirašo atitinkamus informacijos konfidencialumo ir neatskleidimo susitarimus.	Priimtina	

	Darbuotojai, atsakingi už aukštos rizikos asmens duomenų tvarkymo operacijas, laikosi konkrečių jiems taikomų konfidencialumo sąlygų (pagal jų darbo sutartį ar kitą teisės aktą).		
Santykiai su trečiosiomis šalimis	Programėlės kūrimo ir eksploatacijos metu sudaromos paslaugų sutartys, su paslaugų teikėjais: programėlės kūrėjais, duomenų centro paslaugų teikėju ir kitais susijusiais paslaugų teikėjais. Sutartyse be kitų susitarimų numatytos ir duomenų subtvarkymo sąlygos.	Priimtina	
Duomenų apsaugos priemonių stebėjimas	Duomenų saugos įgaliotinis kartu su duomenų apsaugos pareigūnu stebi, kaip laikomasi duomenų saugos principų ir vertina kiek veiksmingos yra įdiegtos priemonės. Pastebėjus trūkumus, įvedamos naujos priemonės ar tikslinamos esamos.	Priimtina	

3.2 RIZIKŲ VERTINIMAS: GALIMI DUOMENŲ APSAUGOS PAŽEIDIMAI

Rizikų vertinime naudojamos skalės:
Sunkumas: 1-žemas, 2-vidutinis, 3-aukštas.
Tikimybė: 1-žema, 2-vidutinė, 3-aukšta.

RIZIKŲ DUOMENŲ APSAUGAI ANALIZĖ IR VERTINIMAS

Rizika	Pagrindinis rizikos šaltinis	Pagrindinės grėsmės	Pagrindinis galimas poveikis	Pagrindinės priemonės mažinančios sunkumą ir tikimybę	Sun-kumas	Tiki-mybė
Sutikimas duotas ne laisva valia	Programėlės naudotojas	Apsimestinis programėlės naudojimas, neduodantis planuoto efekto, asmens teisių ir laisvių ribojimas.	Asmens teisės rinktis suvaržymas	Teisingos informacijos apie programėlę pristatymas	3	1
Netinkamas naudotojo sutikimas dėl neaiškiai pateiktos informacijos	Programėlės naudotojas	Galimas duomenų integralumo sumažėjimas	Galimas duomenų integralumo sumažėjimas	Saugos ir naudojimo informacijos pateikimas paprasta kalba	3	2
Asmenų iki 16 m. programėlės naudojimas	Programėlės naudotojas	Neužtikrinamas teisėtas duomenų tvarkymas	Pažeistos naudotojų laisvės ir teisės	Informacijos apie programėlę pristatymas, aiškūs programėlės tekstai, tėvų sutikimo rinkimas nėra galimas nes	3	1

				didintų duomenų tvarkymą, veikia saugos tvarkos Google Play Store ir Apple Store, mobiliuose įrenginiuose vaikų tėvai gali įdiegti priemones, kurios draustų Korona Stop LT programėlės įdiegimą		
Neteisėtas APK gavimas per pagalbos liniją	NVSC darbuotojas	Pažeistas duomenų vientisumas	Kiti programėlės naudotojai gaus klaidingus įspėjimus	NVSC pagalbos linijos darbuotojai taiko būtinas ir iš anksto tvarkose numatytas priemones skambinančiųjų identifikavimui. Covid-19 užsikrėtusio identifikavimą užtikrina ir tai kad NVSC pati susisiekia su užsikrėtusiu asmeniu vykdydama klasikinį kontaktų atsekimą	2	1
Brute-force ataka APK nustatymui	Įsilaužėlis	Netikro užsikrėtimo publikavimas, naudotojų pasitikėjimo programėle praradimas, pažeistas duomenų vientisumas	Bus pažeistos asmenų teisės, nes gaus klaidingus įspėjimus apie galimą užsikrėtimą.	APK kodų ribota galiojimo trukmė, APK kodos ilgumas, tipinės priemonės prieš brute force atakas stabdančios brute force užklausas	3	1
Duomenų tvarkymas po programėlės pašalinimo	Programėlės naudotojas	Žala programėlės saugumui ir reputacijai,	Pažeistos duomenų subjektų teisės ir laisvės	Panaudotos programinės įrangos pastebėtų spragų sekimas	3	1

		nenumatytas duomenų tvarkymas		ir versijų periodinis atnaujinimas		
Klaidingi teigiami rezultatai	NVSC, laboratorijos, sveikatos priežiūros įstaigos	Automatiškai primestos saviizoliacijos skaidrumas ir patrauklumas	Naudotojai bus neteisingai izoliuoti, galbūt kelis kartus iš eilės, turėdami didelių ekonominių ir socialinių padarinių.	Galimybė kreiptis į NVSC, siekiant įvertinti užsikrėtimo riziką ne automati-zuotomis priemonėmis.	3	1
Priklausomybė nuo išorinių paslaugų teikėjų Google/Apple	Google/Appl e	Nenumatytas duomenų tvarkymas	Nenumatytas duomenų tvarkymas	Mobilių įrenginių naudotojai naudodami iOS/Android jau yra išreiškę sutikimą naudoti šių gamintojų išmanius telefonus	3	1
Nepakankami sutartiniai susitarimai su paslaugų teikėju IVPK dėl duomenų centro paslaugų	Paslaugų teikėjas IVPK	Su paslaugų teikėju nepilnai suderinta duomenų subtvarkytojo role ir iš to galimi saugos pažeidimai	Paslaugų teikėjo neprisiimti būtini įsipareigojimai	Pakankami ir aiškūs sutartiniai įsipareigojimai dėl duomenų subtvarkymo ir paslaugų teikimo	2	1
Trečių šalių programinės įrangos naudojimo rizika *(Dėl nenumatytų savybių naudojant atviro kodo ar nemokamą programinę įrangą)*		Žala programėlės saugumui ir reputacijai, nenumatytas duomenų tvarkymas	Pažeistos duomenų subjektų teisės ir laisvės	Tikrinti naudojamų programinių paketų pažeidžiamumus, diegti atnaujinimus	2	1
Perteklinių duomenų tvarkymas ir saugojimas Apple/Google *(ENF veikia pagal*	Apple/ Google	Nenumatytas duomenų tvarkymas	Nenumatytas duomenų tvarkymas	Riziką švelninanti priemonė yra tai, kad mobilių įrenginių naudotojai naudodami	3	1

deklaruotą Apple/Google modelį, bet nėra pilnų garantijų ir įsipareigojimų iš Apple/Google)				iOS/Android jau yra išreiškę sutikimą naudoti šių gamintojų išmanius telefonus, vadinai yra išreiškė pasitikėjimą šiuo gamintoju.		
Artumo nustatymo netikslumas	Programėlė	Netikslus artumo su kito mobiliu įrengiu nustatymas	Netikslus ar įspėjimas programėlės naudotojui apie turėtą sąlytį su užsikrėtusiu asmeniu	Naudotojo informavimas programėlės veikimo aprašyme apie galimus netikslumus	3	1
Sąmoningas BLE skleidimas prieš APK suvedimą, siekiant išprovokuoti norimą reakciją *(pvz.: mokyklos uždarymą, t.y. progr. naudotojas žino, kad yra užsikrėtęs ir turi teisę gauti APK, ir prieš APK gavimą aktyviai kontaktuoja su kitais asmenimis)*	Programėlės naudotojas (nusiženginat is tvarkai)	Naudojimasis programėle neigiamais tikslais	Norimos reakcijos išprovokavima s nors sąlytis galėjo būti ir neužkrečiantis	NVSC darbuotojų informavimas apie galimus neigiamą poveikį keliančius programėlės naudojimo scenarijus	2	1
Apsaugos spragų ir duomenų apsaugos incidentų atsiradimas programų operatoriui ir (arba) serverio operatoriui	Programėlės ir programėlės serveris		Visuomenės pasitikėjimo programėle praradimas	NVSC ir susijusių paslaugos teikėjų saugos incidentų valdymas, programėlės saugos monitoringas, programėlės techninis saugos auditas	3	1
Funkcionalumo pažeidimas dėl neteisingų	Programėlės naudotojas	Programėlės naudojimo pažeidimai	Klaidingai pateikti programėlės	Aiškus programėlės naudojimo	3	1

nustatymų (BLE“ įjungimas / išjungimas) ir naudojimo (įrenginys fiziškai atskirtas nuo asmens)		sukuriantis neteisingus rezultatus	įspėjimai apie turėtą sąlytį	aprašymas, patogus artumo fiksavimo įjungimas/išjungimas, priminimai telefone apie išjungtą sąlyčio fiksavimą		
Teisės į duomenų ištrynimą neįgyvendinimas	ULSKIS tvarkytojas	Teisė į duomenų ištrynimą neįgyvendinimas	Teisė į duomenų ištrynimą neįgyvendinimas	Su programėlės serveryje tvarkomais duomenimis negalima nustatyti naudotojų, todėl jų pašalinimas nėra vykdomas. Programėlės naudotojai gali pilnai ištrinti programėlę su jos duomenimis išmaniame įrenginyje	3	1
Teisės į duomenų perkeliamumą neįgyvendinimas	ULSKIS tvarkytojas	Teisės į duomenų perkeliamumą neįgyvendinimas	Teisės į duomenų perkeliamumą neįgyvendinimas	Duomenys serveryje nėra susieiti su juos paskelbusiu naudotoju, todėl jų perkėlimas nėra galimas.	1	1
Konfidencialumo pažeidimas (Stebint ryšio kanalą nustatyti užsikrėtimą paskelbusį asmenį)	Hakeris	Konfidencialumo pažeidimas	Konfidencialumo pažeidimas	Tik būtinų duomenų naudojimas programėlėje ir keitimasis su ENF, fiktyvių užsikrėtimų paskelbimo naudojimas	3	1

RIZIKOS VERTINIMAS

Rizikos	Priimtina/galima patobulinti	Korekcinės priemonės	Liekamasis sunkumas	Likusi tikimybė
Sutikimas duotas ne laisva valia	Priimtina		1	1
Netinkamas naudotojo sutikimas dėl neaiškiai pateiktos informacijos	Priimtina		1	1
Asmenų iki 16 m. programėlės naudojimas	Priimtina		1	1
Neteisėtas APK gavimas per pagalbos liniją	Priimtina		1	1
Brute-force ataka APK nustatymui	Priimtina		1	1

Duomenų tvarkymas po programėlės pašalinimo	Priimtina		1	1
Klaidingi teigiami rezultatai	Priimtina		1	1
Priklausomybė nuo išorinių paslaugų teikėjų Google/Apple	Priimtina		1	1
Nepakankami sutartiniai susitarimai su paslaugų teikėju IVPK dėl duomenų centro paslaugų	Priimtina		1	1
Trečių šalių programinės įrangos naudojimo rizika	Priimtina		1	1
Perteklinių duomenų tvarkymas ir saugojimas Apple/Google	Priimtina		1	1
Artumo nustatymo netikslumas	Priimtina		1	1
Sąmoningas BLE skleidimas prieš APK suvedimą, siekiant išprovokuoti norimą reakciją (pvz.: mokyklos uždarymą)	Priimtina		1	1
Apsaugos spragų ir duomenų apsaugos incidentų atsiradimas programų operatoriui ir (arba) serverio operatoriui	Priimtina		1	1
Funkcionalumo pažeidimas dėl neteisingų nustatymų (BLE įjungimas / išjungimas) ir naudojimo (įrenginys fiziškai atskirtas nuo asmens)	Priimtina		1	1
Teisė į duomenų ištrynimą neįgyvendinimas	Priimtina		1	1
Teisės į duomenų perkeliamumą neįgyvendinimas	Priimtina		1	1
Konfidencialumo pažeidimas	Priimtina		1	1

NVSC DAP komentaras:
Manytina, kad šioje dalyje turėjo būti suformuluotos PDAV išvados. Deja bet išvadų šiame dokumente iš viso nėra.

4 PDAV PATVIRTINIMAS:

4.1 PATVIRTINIMUI REIKALINGOS MEDŽIAGOS PARUOŠIMAS

Priemonių įvertinimui naudojamos reikšmės:

- Netaikoma
- Nepriimtina
- Planuojamas tobulinimas
- Priimtina

SUVESTINĖ DĖL PASIRINKTŲ PRIEMONIŲ, UŽTIKRINANČIŲ ATITIKIMĄ PAGRINDINIAMS BDAR ĮTVIRTINTIEMS PRINCIPAMS

Pasirinktų priemonių suderinamumas su pagrindiniais principais	**Įvertinimas**
Priemonės įgalinančios tvarkymo proporcingumą ir būtinumą	
Tikslas (ai): konkretus, aiškus ir teisėtas	Priimtina
Pagrindas: duomenų tvarkymo teisėtumas, piktnaudžiavimo draudimas	Priimtina
Asmens duomenų apimties mažinimas: tinkamas, aktualus ir ribotas	Priimtina
Asmens duomenų kokybė: tikslūs ir prireikus atnaujinami	Priimtina
Saugojimo trukmė: ribota	Priimtina
Duomenų subjektų teisėms apsaugoti skirtos priemonės	
Duomenų subjektų informavimas (teisingas ir skaidrus apdorojimas)	Planuojamas tobulinimas
Sutikimo gavimas	Priimtina
Teisė susipažinti ir teisė į duomenų perkeliamumą	Priimtina
Teisės reikalauti ištaisyti ir teisė ištrinti duomenis	Priimtina
Teisė apriboti duomenų tvarkymą ir teisė nesutikti	Priimtina
Tvarkytojai: nustatyti ir reglamentuojami sutartimi	Priimtina
Duomenų perdavimas: duomenų perdavimo už Europos Sąjungos ribų įsipareigojimų vykdymas	Priimtina

SUVESTINĖ DĖL PASIRINKTŲ PRIEMONIŲ SKIRTŲ RIZIKŲ VALDYMUI DĖL DUOMENŲ APSAUGOS SUDERINAMUMO SU GEROSIOMIS SAUGOS PRAKTIKOMIS

Įdiegtos priemonės duomenų apsaugos rizikų valdymui	**Įvertinimas**
Priemonės skirtos duomenų tvarkymui	
Šifravimas	Priimtina
Nuasmeninimas	Priimtina
Duomenų skaidymas (likusios informacinės sistemos atžvilgiu)	Priimtina
Loginė prieigos kontrolė	Priimtina
Veiksmų registravimas	Priimtina
Vientisumo stebėjimas	Priimtina
Archyvavimas	Priimtina
Popierinių dokumentų apsauga	Netaikoma
Bendrosios apsaugos priemonės sistemai, kurioje vyksta tvarkymas	
Eksploatavimo sauga	Priimtina
Kenkėjiškų programų prevencija	Priimtina
Personalinių kompiuterių administravimas	Priimtina
Interneto svetainių sauga	Priimtina
Atsarginės kopijos	Priimtina
Palaikymas	Priimtina
Tinklo saugumas	Priimtina
Stebėjimas	Priimtina
Fizinė praėjimo kontrolė	Priimtina
Techninės įrangos sauga	Priimtina
Rizikos šaltinių užkardymas	Priimtina

Apsauga nuo ne nuo žmogaus priklausančių rizikų	Priimtina
Organizacinės apsaugos priemonės (valdymas)	
Duomenų apsaugos organizavimas	Priimtina
Tvarkos	Priimtina
Rizikų valdymas	Priimtina
Projekto valdymas	Priimtina
Duomenų apsaugos pažeidimų valdymas	Priimtina
Personalo valdymas	Priimtina
Santykiai su trečiosiomis šalimis	Priimtina
Privatumo valdymo veiksmingumo stebėjimas	Priimtina

SU DUOMENŲ SAUGUMU SUSIJUSIOS RIZIKOS NUSTATYMAS IR REKOMENDACIJOS

Kad būtų įvykdyti BDAR reikalavimai, programėlės valdytojui ir pagrindiniam tvarkytojui rekomenduojama imtis šių apsaugos priemonių, kad būtų galima nustatyti užsikrėtimo rizikoje esančius kontaktus su Covid-19 infekcija užsikrėtusiais asmenimis:

1. Turi būti nustatytas tinkamas teisinis pagrindas ir šiuo atžvilgiu turi būti apibrėžta atsakomybė. Duomenų tvarkymas turi būti „savanoriškas“ ir vykdomas sutikimo pagrindu, kuris privalo atitikti teisės aktuose, reglamentuojančius asmens duomenų apsaugą, nustatytus reikalavimus, ypač todėl, kad kyla abejonių dėl naudotojo valios ir sąmoningumo išraiškos. Siekiant patenkinti šiuos reikalavimus, turi būti sukurta teisinė bazė, visų pirma susijusi su tikslo ribojimu, nuasmeninimu, ištrynimo samprata ir duomenų apsaugos valdymu. Čia labai svarbu atkreipti dėmesį ne tik į technines programos specifikacijas, bet ir į visą apdorojimo procedūrą, įskaitant jos sąsajas, pavyzdžiui, integravimą į planuojamą SMS pranešimo siuntimo procedūrą. Taip pat reikia atsižvelgti į nepageidaujamus techninius ir socialinius šalutinius poveikius, darančius įtaką pagrindinių teisių įgyvendinimui. Šie šalutiniai poveikiai taip pat netiesiogiai daro įtaką duomenų tvarkymo procedūros pripažinimui. Taigi turi būti užtikrinta, kad tretieji asmenys neturėtų prieigos prie programėlės ir jos išvesties naudotojų išmaniuosiuose telefonuose. Teisės aktus priimantys subjektai turi priimti turi priimti teisės aktą, kuriame būtų nustatyti techniniai reikalavimai, atitinkantys duomenų apsaugą, tai gali būti ir informacinės sistemos saugos nuostatai.

2. Fizinio asmens, kurio tapatybė nustatyta, ar gali būti nustatyta atžvilgiu ypač jautrios yra dvi situacijos visoje proceso grandinėje; būtent artumo rakto sukūrimas ir saugojimas bei programėlės užkrėstų asmenų užsikrėtimo raktų įkėlimas į serverį ir jų saugojimas kaip anoniminių užsikrėtimo atvejį nurodančių duomenų. Šios operacijos turi būti suprojektuotos taip:

a. Kuriant artumo raktus programėlėje, reikia įsitikinti, kad tarp su artumo raktais nėra jokio ryšio ir jo niekada negali būti įmanoma sukurti. Todėl konkretus artumo raktas neturi būti gaunamas nei iš ankstesnio, nei iš paprastos sekos. Artumo raktai turi būti saugomi programėlėje taip, kad būtų neįmanoma retrospektyviai nustatyti, kokia tvarka jie buvo sukurti ir išsaugoti.

b. Programėlės serverio (-ių) sprendimas turi naudoti veiksmingą atskyrimo metodą, kuris užsikrėtimo raktus iš Covid-19 infekuotų asmenų programėlių paverčia anoniminiais užsikrėtimo atvejį nurodančiais duomenimis serveryje. Tai turi būti užtikrinama teisinėmis, organizacinėmis ir techninėmis priemonėmis. ULSKIS pagrindinis tvarkytojas privalo turėti duomenų apsaugos valdymą, kuris leistų veiksmingai vykdyti ir išlaikyti patikrinamą atskyrimą. Techniškai ULSKIS pagrindinis tvarkytojas ar įgaliotas subtvarkytojas turi nustatyti atskyrimo procesą taip, kad užsikrėtimo raktų įkėlimai nebūtų registruojami nei serveryje, nei serverio infrastruktūroje. Be to, užsikrėtimų raktų įkėlimas tarp programėlių ir serverių turi būti visiškai užšifruotas ir apsaugotas nuo tarpininkų, per kuriuos šie duomenys siunčiami. Siekdama kontroliuoti duomenų apsaugą, atsakinga duomenų apsaugos institucija turi nuolat tikrinti atskyrimo metodą.

Visų IT komponentų, naudojamų visoje proceso grandinėje, saugumas turi atitikti atitinkamo lygio informacinėms sistemoms taikomą teisės aktuose numatytą duomenų apsaugos lygį.

3. Kartu su programėlės publikavimu turi būti užtikrinta teisės aktais ir faktiškai, kad naudotojai neprivalo trečiosioms šalims atskleisti nei programėlės statuso, nei egzistavimo pačiame išmaniajame įrenginyje. NVSC galėtų būti taikoma išimtis vykdant izoliavimą, o darbdaviams taikant nuotolinį darbą. Šių taisyklių tikslas yra užtikrinti programos paskirties apribojimą. Turi būti užkirstas kelias viešųjų ir privačių pastatų, universitetų, mokyklų, transporto priemonių, viešojo administravimo įstaigų, policijos nuovadų ir pan. kontrolei, remiantis programėlės būsenos atskleidimu.

4. Papildyti privatumo politikoje pateikiamą informacija apie duomenų subjektų teises. Nurodyti, kad informaciją, kad duomenų subjekto teisės gauti prieigą, ištaisyti, ištrinti, apriboti tvarkymą, prieštarauti tvarkymui ir duomenų perkeliamumui nėra taikomos arba netaikomos tam tikriems duomenims dėl to, kad neįmanoma įvykdyti; informacija, kad duomenų subjekto teisė bet kuriuo metu atšaukti sutikimą yra apribota reikalaujant, kad programėlė nutrauktų tolesnį asmens duomenų tvarkymą, kai neįmanoma nustatyti vartotojo santykių turint tokius asmens duomenis, todėl jau pateikti asmens duomenys vis tiek bus tvarkomi.

5. Prieš paskelbiant programėlę, nepriklausoma įstaiga turi atlikti išsamų programinės įrangos ir visos sistemos tyrimą (pvz., NKSC). Ypatingas dėmesys turi būti skiriamas rizikai, kylančiai dėl sąveikos su operacinės sistemos komponentais, kurie gali būti svarbūs ir ne programėlės naudotojams. Šis punktas gali nepavykti, jei didelės platformų įmonės („Google“, „Apple“) nenori bendradarbiauti arba jei teisinės ar faktinės kliūtys trukdo užtikrinti duomenų apsaugos reikalavimus. Pavyzdžiui, jei negalima atmesti galimybės,

kad tokios platformos gali fiksuoti kontaktus ir atlikti atitikimo nustatymą su užkrėstais asmenimis, tinkama priemonė būtų stabdyti tokios programėlės veikimą.