

**Lietotnes “Apturi Covid”
novērtējums par ietekmi uz datu aizsardzību**

Novērtējuma tvērums

1.1. Šis novērtējums par ietekmi uz datu aizsardzību (turpmāk – Novērtējums) attiecas uz personas datu apstrādi kontekstā ar Lietotni “Apturi Covid” (turpmāk – Lietotne).

Uz personas datu apstrādi, ko kompetentās iestādes veic ārpus Lietotnes ietvara, ir piemērojami attiecīgie normatīvie akti un ar to saistītie personas datu aizsardzības nosacījumi un šajā Novērtējumā tie netiek ietverti un apskatīti.

1.2. Šis Novērtējums ir izstrādāts atbilstoši Vispārīgās datu aizsardzības regulas¹ (turpmāk – Datu regula) 35.panta 1.punktam, kas paredz, ka – “Ja apstrādes veids, jo īpaši, izmantojot jaunās tehnoloģijas un ņemot vērā apstrādes raksturu, apjomu, kontekstu un nolūkus, varētu radīt augstu risku fizisku personu tiesībām un brīvībām, pārzinis pirms apstrādes veic novērtējumu par to, kā plānotās apstrādes darbības ietekmēs personas datu aizsardzību. [..]”.

1.3. Lietotnes neatņemamas sastāvdaļas ir:

- [Lietotnes noteikumi](#);
- Lietotnes [Privātuma politika](#);

un Lietotnes tehniskā apraksta dokumentācija:

- Lietotnes procesa shēma;
- Lietotnes uzbūve (vispārējais kopskats)
- Lietotnes infrastruktūras diagramma (detalizēta fiziskās arhitektūras shēma);
- SPKC sistēmas skats attiecībā uz saņemto kontakttālruni;
- SPKC sistēmas skats attiecībā uz brīdinājuma paziņojuma aktivizācijas koda piešķiršanu;
- Lietotnes drošības apraksts (“Whitepaper”).

I. Personas datu apstrādes vispārīgs apraksts

Iestādes nosaukums	Lietotnes pārzinis ir Slimību profilakses un kontroles centrs (turpmāk – SPKC) - veselības ministra pakļautībā esoša tiešās pārvaldes iestāde
Kontaktinformācija	Tālrunis: +371 67501590 E-pasts: pasts@spkc.gov.lv Adrese: Dunties iela 22, k-5, Rīga, Latvija, LV 1005
Novērtētājs (vārds, uzvārds)	Ļubova Tihomirova Amats: Vecākais eksperts
Kontaktinformācija	Tālrunis: 67895816 E-pasta adrese: lubova.tihomirova@spkc.gov.lv
Novērtējuma veikšanas periods	20.04.2020. – 20.05.2020.
Vai novērtējuma par ietekmi uz datu aizsardzību veikšanas procesā iesaistīts datu aizsardzības speciālists?	Jā ☒ Nē ☐ SPKC personas datu aizsardzības speciālists E-pasta adrese: das@spkc.gov.lv
Vai novērtējuma par ietekmi uz datu aizsardzību veikšanas procesā ir pieprasīts datu	Jā ☒ Nē ☐

¹ Eiropas Parlamenta un Padomes Regula (ES) 2016/679 (2016. gada 27. aprīlis) par fizisku personu aizsardzību attiecībā uz personas datu apstrādi un šādu datu brīvu apriti un ar ko atceļ Direktīvu 95/46/EK (Vispārīgā datu aizsardzības regula), ELI: <http://data.europa.eu/eli/reg/2016/679/oj>

subjektu vai viņu pārstāvju viedoklis? Ja ir, tad kāds ir iegūtais viedoklis, ja nav, tad kāpēc viedoklis nav iegūts?	1. Lietotnes izstrāde ir tapusi, pateicoties sabiedrības brīvprātīgai iniciatīvai saskaņā ar 2020.gada 28.aprīļa Memorandu sabiedrības līdzdalībai COVID-19 ierobežošanā. Sākoties Covid-19 vīrusa izplatībai, virkne Latvijas komersanti saskārās ar situāciju, ka bija nepieciešams steidzami meklēt risinājumus, kā aizsargāt savus darbiniekus, klientus un sadarbības partnerus, kā arī šo cilvēku ģimenes locekļus no Covid-19 saslimšanas. Lietotnes ideja un izstrāde tapa, veidojot dažādas neformālas fokusgrupu diskusijas un uzklausot: - dažādu darbinieku kā potenciālo Lietotnes datu subjektu viedokli; - dažādu ekspertu kā potenciālo Lietotnes datu subjektu viedokli; un - dažādu sabiedrības pārstāvju kā potenciālo Lietotnes datu subjektu viedokli; kā arī - Lietotnes izstrādē tika iesaistīti vairāk kā 80 cilvēki (dažādu nozaru pārstāvji), kas izstrādes ietvaros puda savu kā potenciālo Lietotnes datu subjektu viedokli Lietotnes saturs un funkcionalitātes jautājumos. Datu subjektu viedoklis kopumā nav viennozīmīgs². Daļa datu subjektu pozitīvi vērtē Lietotni kā papildu iespēju aizsargāt sevi un sev tuvos no Covid-19 vīrusa ķēdes nekontrolētas izplatības, un redz to kā iespēju, lai ātrāk pilnvērtīgi atgrieztos sociālā un ekonomiskā dzīvē. Savukārt daļa datu subjektu Lietotnes ideju uztver piesardzīgi, pat noraidoši. Analizējot saņemtos viedokļus ir secināms, ka noraidošā attieksme ir pamatā saistīta, nevis ar pašu Lietotni kā tādu, bet ar bažām, ka ar laiku Lietotne no valsts puses varētu tikt izmantota citiem mērķiem, nekā tas ir sākotnēji plānots. Daļa minētās bažas ir saistītas arī ar to, ka šī ir jauna pieeja un konkrētās Lietotnes izstrādes brīdī informācija par Lietotnes saturu nebija vēl daudz pieejama un līdz šim arī lietotnes tehnoloģiski risinājumi nav izmantoti vispār valsts sektorā un attiecīgi lietotājiem ar to nav pietiekamas pieredzes. Lietotāju viedokli daļēji ietekmē arī pasaulē paralēlie notikumi, kur atsevišķas ārpus Eiropas Savienības esošas valstis Covid-19 krīzes ietvaros ir pastiprinājušas vispārējo valsts varu pār personu privātumu. Izpratni par Lietotnes būtību lielā mērā ietekmē tas, cik plaša ir lietotājiem pieejamā informācija par lietotnē izmantotajiem tehnoloģiskajiem risinājumiem. Lietotnes viens no pamatprincipiem ir atklātība – datu subjekta iespēja pirms Lietotnes uzsākšanas iepazīties ar Lietotnes noteikumiem un Privātuma politiku un datu subjekta izvēles brīvība - iespēja brīvprātīgi uzsākt un jebkurā laikā brīvprātīgi pārtraukt Lietotnes izmantošanu, tādējādi dodot iespēju katram Lietotājam pašam pārliecināties par Lietotnes darbību un datu aizsardzību. 2. Eiropas Datu aizsardzības kolēģija (angļu val. - European Data Protection Board), (turpmāk – Kolēģija), kas Eiropas Savienības ietvaros nodrošina Datu regulas pareizu piemērošanu, ir paudusi atbalstošu nostāju tehnoloģisko risinājumu (lietotņu) izstrādei, lai aizsargātu sabiedrības veselību pret Covid-19. Vienlaikus Kolēģija ir norādījusi uz vairākiem datu aizsardzības kritērijiem, kas ir jāņem vērā šādu tehnoloģisko risinājumu izstrādei, lai tas aizsargātu datu subjektu tiesības uz privātumu. Skat., piemēram: - Kolēģijas 2020.gada 14.aprīļa vēstuli OUT2020-0028 un 2020.gada 23.aprīļa vēstule OUT2020-0030; - Kolēģijas 2020.gada 21.aprīļa Pamatnostādnes 04/2020³. Lietotnes izstrādē ņemtas vērā iepriekš minētās pamatnostādnes.
--	--

² Latvijas sabiedrības neviennozīmīgo attieksme pret pašu Covid-19 slimību kā tādu parāda arī SKDS veiktā aptauja. Neskatoties uz pasaulē lielo upuru skaitu, ko prasījis Covid-19, Latvijā šo vīrusu nopietni uztver tikai 52,4% iedzīvotāju. Skat. 9.05.2020. "Aptauja: Covid-19 nopietni uztver 52,4% sabiedrības". <https://www.lsm.lv/raksts/zinas/latvija/aptauja-covid-19-nopietni-uztver-524-sabiedribas.a359144/>

³https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_20200420_contact_tracing_covid_with_annex_en.pdf

IEROBEŽOTAS PIEEJAMĪBAS INFORMĀCIJA

Kāds ir personas datu apstrādes mērķis*? <i>*Ar mērķi saprotam konkrēti definētu rezultātu, kas sasniedzams ar plānoto personas datu apstrādi (piemēram,</i>	Lietotnes personas datu apstrādes mērķis ir sniegt Latvijas iedzīvotājiem un atbildīgajām institūcijām atbalstu vīrusa Covid-19 ierobežošanā. Lietotne daļēji papildinās SPKC līdzšinēji manuāli veikto inficētās personas iespējamo kontaktpersonu noskaidrošanu, noteikšanu, apziņošanu un brīdināšanu. Lietotne palīdzēs Latvijas iedzīvotājiem, kas lieto Lietotni: 1. Laikus uzzināt par iespējamo Covid-19 saskares risku, tādējādi dodot iespēju nekavējoties uzsākt piesardzības pasākumus (t.sk., piemēram, ierobežot saskarsmi ar citiem), un nepieciešamības gadījumā, ja ir parādījušies simptomi, laikus vērsties pēc medicīniskās palīdzības, kas tiek nodrošināta atbilstoši esošam regulējumam ārpus Lietotnes ietvara. Tas palīdzēs pārraut Covid-19 vīrusa izplatības ķēdi un attiecīgi sargāt katra Latvijas iedzīvotāja, kas lieto Lietotni, paša veselību, kā arī aizsargāt savu ģimeni, draugus, kolēģus un citus sev tuvumā esošos cilvēkus, tostarp nejauši sastaptus svešus cilvēkus cīņā ar Covid-19 izplatību. 2. Laikus informēt citus lietotājus, kas izmanto Lietotni, ja lietotājam ir apstiprināta Covid-19 saslimšana. Lietotne papildus SPKC esošajam manuālam kontaktu apzināšanas procesam, dos iespēju informēt tos lietotājus, ar ko ir bijusi saslimušajam lietotājam saskare pēdējo 14 dienu laikā, kas ir fiksēta starp tuvumā esošu lietotāju galiekārtām, kurās ir lejupielādēta Lietotne. Tas dos iespēju informēt arī tos lietotājus, ar kuriem kontakts var rasties neapzināti vai nejauši, piemēram, sabiedriskā vietā vai publiskā pasākumā, un ko citādi būtu sarežģīti apzināt un informēt, ja šāda Lietotne netiktu izstrādāta. 3. Sekot līdzi aktuālajai Covid-19 izplatības situācijai. Lietotnē ērtā veidā Lietotājam informatīvi būs pieejama statistiskā informācija, piemēram, par Covid-19 saslimušo personu skaitu kopumā Latvijā un tml., kā arī citas ar Covid-19 svarīgas aktualitātes. Šī Lietotnes funkcionalitāte - aktuālās informācijas pieejamībai - neparedz lietotāju personas datu apstrādi un šajā Novērtējumā to nav nepieciešams detalizētāk izvērtēt no personas datu apstrādes viedokļa. 4. Dot iespēju lietotājiem Lietotnē aizpildīt simptomu pašpārbaudes informāciju, lai lietotājam būtu iespēja pievērst uzmanību tiem simptomiem, kas var liecināt par Covid-19 saslimšanu. Tāpat tas dos iespēju SPKC uzzināt par Covid-19 simptomu attīstību un tendenci, piemēram, ja tiek konstatēti jauni simptomi vai to atšķirīgi paveidi salīdzinājumā ar līdzšinējo pieredzi. Šī Lietotnes funkcionalitāte simptomu pašpārbaudei neparedz personas datu apstrādi, kas dotu iespēju identificēt konkrētu lietotāju kā datu subjektu un šajā Novērtējumā to nav nepieciešams detalizētāk izvērtēt no personas datu apstrādes viedokļa. Atkārtots izvērtējums par šo funkcionalitāti tiks veikts Lietotnes 2.kārtas ietvaros, nepieciešamības gadījumā veicot Novērtējumu, ja tas būs attiecīgi piemērojams.
Kāds ir personas datu apstrādes nolūks*? <i>*Ar nolūku saprotam veidu kā tiek plānots iepriekš norādīto mērķi sasniegt (piemēram,</i>	1. Lietotnes ietvaros datu apstrādes virsmērķis (nolūks) ir epidemioloģiskā drošība sabiedrības veselības aizsardzībai pret Covid-19 un ar to saistītie zemāk norādītie mērķi (nolūki): 1.1. Covid-19 gadījumu ātrā atklāšana un piesardzības pasākumu veikšana; 1.2. Covid-19 epidemioloģiskā uzraudzība, tostarp Covid-19 epidemioloģiskās izpētes veikšana, kas skar Covid-19 izplatīšanos laikā, teritorijā un veidā un kas dod iespēju izziņāt un savlaicīgi veikt nepieciešamos profilakses un pretepidēmijas pasākumus, vienlaikus izvērtējot to efektivitāti; 1.3. sabiedrības informēšana par Covid-19 un izglītošana par Covid-19 profilaktiskajiem jautājumiem.

IEROBEŽOTAS PĪEEJAMĪBAS INFORMĀCIJA

	2. Attiecībā uz datiem, kas tiek apstrādāti Lietotnes tehniskā risinājuma ietvaros – mērķis (nolūks) ir Lietotnes datu drošība un aizsardzība pret trešajām personām, tostarp Lietotnes konfidencialitāte un integritāte.
Kāds ir plānotās personas datu apstrādes raksturs?	Lietotnes ietvaros tiek veikta šāda datu apstrāde: – datu apstrāde, uzsākot Lietotnes lietošanu; – datu apstrāde, lietojot Lietotni; – datu apstrāde, ko Lietotājs pats izvēlas sniegt SPKC. Detalizēts apstrādes rakstura apraksts ietverts Lietotnes Privātuma politikas 5.1., 5.2. un 5.3.punktā.
Tai skaitā kādā veidā notiek personas datu apstrāde – manuāli vai automatizēti?	Datu apstrāde Lietotnes ietvaros notiek gan manuāli, gan automatizēti. Lietotnes tehniskie dati tiek apstrādāti automātiski, savukārt Lietotnes konkrēto funkciju aktivizēšanu lietotājs izdara manuālā veidā ar aktīvu darbību. Piemēram, ieslēdzot Bluetooth Low Energy (turpmāk – bluetooth) funkciju vai to izslēdzot, norādot ar SPKC saziņai paredzēto kontakttālruni vai to izdzēšot (vai arī to nomainot uz citu). Tāpat lietotājs, kam ir konstatēta saslimšana ar Covid-19, veic manuāli aktīvu darbību – aktivizē SPKC saņemto kodu, lai izsūtītu tālāk jau automātiski paziņojumus tiem lietotājiem, kas ir bijuši pēdējo 14 dienu laiku saskarē ar šo lietotāju. Lietotājam pēc izvēles ir iespēja izmantot automātisko saņemto koda “ielasīšanu”, ja lietotāja galiekārta piedāvā šādu iespēju. SPKC ietvaros kontakttālruni saziņai ar personu, kam ir noticis potenciālais kontakts ar Covid-19 saslimušo personu, saņem tikai tad, ja pats lietotājs, uzstādot lietotni, ir norādījis savu kontakttālruni, un savā galiekārtā saņem automātisko paziņojumu ar brīdinājumu, ka ir konstatēta iespējamā saskare ar Covid-19. Šajā brīdī kontakttālrunis tiek automātiski nosūtīts no Lietotnes uz SPKC sistēmu, lietotājam papildus nekas nav jādara. Turpmākā saziņa ar potenciālo kontaktu, kas savā lietotnē pirms tam ir norādījis kontakttālruni saziņai ar SPKC, norisinās manuālā veidā – SPKC attiecīgi zvina uz saņemto kontakttālruni un ārpus Lietotnes veic turpmāko sarunu saskaņā ar spēkā esošo regulējumu – personu atzīstot par kontaktpersonu un piešķirot personai šo statusu, vai arī neatzīstot personu par kontaktpersonu, piemēram, ja kontakts ir fiksēts laikā, kad lietotājs nav faktiski lietojis Lietotni.
Sniedziet plānotās personas datu apstrādes funkcionālu aprakstu.	Lietotnes izmantošana ir brīvprātīga un bez maksas. Lai lietotu Lietotni, lietotājam ir nepieciešama galiekārta (piemēram, mobilais telefons), kas piemērota Lietotnes darbībai, un datu pārraides pieejamība, kas dod iespēju lejupielādēt un lietot Lietotni. Izvēli par bluetooth aktivizāciju (ieslēgšanu un izslēgšanu) kontaktu fiksēšanai starp tuvumā esošām galiekārtām, kurās ir lejupielādēta Lietotne, izdara pats lietotājs. Ja lietotājs ir izvēlējis neaktivizēt bluetooth – kontakti šajā laikā netiek fiksēti un lietotājam attiecīgi netiek sūtīts (nav iespējams nosūtīt) brīdinājuma paziņojumu, ja kāds no kontaktiem tajā laikā intervālā, kad nebija aktivizēts bluetooth, ir bijis ar Covid-19 saslimušo personu. Lietotnes fiksētie saskares kontakti ar citu lietotāju galiekārtām tiek glabāti katras attiecīgās Lietotnes galiekārtā – netiek veidots centralizēts datu glabāšanas mehānisms. Lietotnē norādītais lietotāja kontakttālrunis tiek glabāts Lietotnē – SPKC to saņem tikai tad, ja ir iestājies lietotāja potenciālais kontakts ar Covid-19 saslimušo personu. Lai nodrošinātu kontakttālruna precizitāti un citu lietotāju datu drošību (lai netiktu nepamatoti norādīts citu personu kontakttālrunis) – lietotājam uz norādīto kontakttālruni tiek nosūtīts kods, ko lietotājs ievada kontakttālruna apstiprināšanai. Lai SPKC būtu iespēja ātrāk sazināties ar lietotāju – lietotājam Lietotnē pēc izvēles ir iespēja ielikt norādi (bez papildu datiem), ja konkrētais kontakttālrunis

	ir lietotāja pārstāvja kontakttālrunis (piemēram, ja lietotājs ir jaunāks par 13 gadiem – šādā gadījumā ir būtiski, ka SPKC sazinās caur vecāku vai citu tiesisko pārstāvi). Atrašanās vietas dati Lietotnes ietvaros netiek fiksēti un glabāti un SPKC tie nav pieejami ne par lietotāju, ne arī par citiem lietotājiem (kontaktiem), ar ko ir bijusi saskare. Izvēli par citu lietotāju informēšanu – izdara pats lietotājs, kam ir konstatēta Covid-19 saslimšana. Lai aktivizētu automātiski izsūtāmu brīdinājuma paziņojumu, lietotājam, kam ir apstiprināts Covid-19, nepieciešams aktivizēt no SPKC saņemtu kodu. Lietotājam ir iespēja izvēlēties neaktivizēt kodu. Kods ir izmantojams vienai reizei un derīgs 30 minūtes. Lietotājam netiek sniegta informācija par kontaktiem, kas ir saņēmuši brīdinājuma paziņojumu. Lietotājiem, kas saņem brīdinājumu, netiek sniegta informācija par lietotāju, kam ir konstatēts Covid-19 un kas ir attiecīgi aktivizējis brīdinājuma izsūtīšanu. Informācija par katru saskari Lietotnes vēsturē tiek dzēsta, kad ir pagājušas 14 dienas pēc atbilstošas saskares. Kontakttālrunis Lietotnē tiek dzēsts pēc lietotāja izvēles. Visi dati Lietotnē tiek dzēsti, kad lietotājs nolemj dzēst Lietotni. Kontakttālrunis, kas tiek saņemts SPKC – tiek apstrādāts uz saziņai nepieciešamo laiku, vai attiecīgi ilgāk, ja tas nepieciešams SPKC pienākumu izpildei saskaņā ar normatīvajiem aktiem epidemioloģiskās drošības jomā. Detalizēts Lietotnes funkcionālais apraksts ir ietverts Lietotnes noteikumu 3. un 4.punktā un Lietotnes Privātuma politikas 5. un 7.punktā.
Kāpēc šāda rakstura apstrāde svarīga konkrēto nolūku sasniegšanai?	Lietotne kā tehnoloģiskais risinājums darbojas kā SPKC papildu rīks, lai sniegtu sabiedrībai atbalstu cīņā ar Covid-19. Lietotne dod iespēju vieglāk apzināt tos lietotājus, kas ir nonākuši saskarē ar Covid-19 saslimušo lietotāju. Bez Lietotnes SPKC veic manuālu potenciālo kontaktu apzināšanu un tas var neaptvert visus potenciālos kontaktus. Īpaši, ja kontakti ir radušies nejauši vai nepazināti, piemēram, publiskā vietā vai plaši apmeklētā pasākumā vai arī, ja saslimušai personai nav iespēja atcerēties visas personas, ar ko pēdējo dienu laikā ir bijis kontakts. Kopējā cīņā pret Covid-19 Eiropas Komisijas ir norādījusi, ka <i>“Digitālajām tehnoloģijām un datiem ir liela nozīme Covid-19 krīzes apkarošanā, ņemot vērā, ka daudzu cilvēku mobilās ierīces Eiropā ir pieslēgtas internetam. Šīs tehnoloģijas un dati var būt svarīgs instruments, ar kuru informēt sabiedrību un palīdzēt attiecīgajām valsts iestādēm to centienos ierobežot vīrusa izplatīšanos [..]”</i>⁴. Eiropas Savienības ietvaros izstrādātajā dokumentā (pieejams angļu valodā - eHealth Network - <i>Mobile applications to support contact tracing in the EU's fight against COVID-19</i> - Common EU Toolbox for Member States Version 1.0 15.04.2020⁵) ir norādīts uz divām iespējamām datu apstrādes pieejām: decentralizētā datu glabāšana (kontakta fiksēšana lietotnes galiekārtā) un centralizētā (angļu valodā – Backend server solution), kad fiksētie kontaktu dati tiek glabāti kompetentās iestādes sistēmā. Lai aizsargātu lietotāju tiesības un brīvības attiecībā uz datu drošību – SPKC Lietotnē ir izmantots <u>decentralizētais risinājums</u>. SPKC Lietotnes risinājums paredz, ka fiksētie kontakti tiek glabāti lietotnes galiekārtā šifrētā veidā un ne lietotājam, ne SPKC un trešajām personām nav pieejami. Izvēlētais risinājums dod priekšroku lietotāja aizsardzībai. Risinājuma zināms trūkums ir tas, ka SPKC nav iespēja redzēt kopējo situāciju, piemēram, to, cik daudz ir kopumā fiksēto kontaktu ar Lietotnes palīdzību. Šāda informācija dotu plašāku epidemioloģiskās drošības pārraudzību.

⁴ Skat. preambulas 2.ievilkums - Komisijas lēmums (ES) 2020/518 (2020. gada 8. aprīlis) par vienotu Savienības rīkkopu tehnoloģiju un datu izmantošanai ar mērķi apkarot Covid-19 krīzi un iziet no tās, it īpaši attiecībā uz mobilajām lietotnēm un anonimizētu mobilitātes datu izmantošanu. ELI: <http://data.europa.eu/eli/reco/2020/518/oj>

⁵ https://ec.europa.eu/health/sites/health/files/ehealth/docs/covid-19_apps_en.pdf

	Kontaktu fiksēšanu tehnoloģiski ir iespēja veikt dažādos veidos – izmantojot bluetooth tehnoloģiju vai atrašanās vietas datu apstrādi. SPKC Lietotnes risinājumam ir izvēlēta <u>bluetooth tehnoloģija</u>, jo tā dod iespēju kontaktus fiksēt šifrētā veidā Lietotnes galiekārtā, neapstrādājot lietotāja atrašanās vietas datus. Šāds risinājums aizsargā lietotāja tiesības uz datu drošību un atbilst datu minimizācijas principam. Bluetooth tehnoloģiju kā piemērotu risinājumu kontaktu fiksēšanai ir atzinusi arī Kolēģija.⁶ Lietotnes ietvaros personas <u>datu apstrāde tiek veikta tikai minimāli nepieciešamā apjomā</u>. Lietotājam ir iespējanorādīt kontakttālruni saziņai ar SPKC gadījumā, ja lietotājs tiks konstatēts kā potenciālais Covid-19 saslimušās personas kontakts. Lietotājam ir tiesības arī nenorādīt kontakttālruni un pēc laika to dzēst, ja lietotājs pārdomā savu izvēli. Kontakttālrunis ir būtisks, lai SPKC būtu iespēja lietotājam sniegt atbalstu un ar lietotāju izrunātu turpmākos piesardzības soļus, ja lietotājs tiek atzīts par kontaktpersonu saskaņā ar normatīvajiem aktiem. Bez kontakttālruna norādīšanās lietotājam var paildzināties laiks, kamēr lietotājs pats sazinās ar SPKC, kā arī radīt lietotājam nevajadzīgas bažas un satraukumu, piemēram, ja lietotājs pats nesazinās ar SPKC un attiecīgi nesaņem atbalstu no SPKC. Iespēju paredzēt lietotāja izvēli norādīt kontakttālruni ir atzinusi arī Eiropas Komisija savā paziņojumā⁷. SPKC Lietotnes ietvaros personas identificējoši dati kā vārds, uzvārds un tml. netiek saņemti un apstrādāti. Šobrīd pasaulē un Eiropas Savienībā virkne valstis paralēli darbojas pie līdzīgu tehnoloģisko risinājumu izstrādes⁸. Atšķirības pieejā parāda, ka katrai valstij ir būtiski izvēlēties to pieeju, kas vislabāk atbilst konkrētās valsts specifikai, jo identiska pieeja, ņemot vērā valstīs esošo veselības procesu atšķirības, ne vienmēr var nodrošināt sabiedrības aizsardzībai nepieciešamo rezultātu.
Vai personas datu apstrādes mērķi nosaka normatīvie akti? Ja atbilde ir "jā", norādiet normatīvos aktus, kas paredz datu apstrādi	Jā ☒ Nē ☐ Attiecībā uz Lietotnes virsmērķi – epidemioloģiskā drošība un ar to saistītajiem augstāk minētajiem mērķiem – SPKC pienākumus nosaka normatīvie akti veselības, tostarp epidemioloģiskās drošības jomā. Piemēram: – Epidemioloģiskās drošības likums un tam pakārtotie Ministru kabineta noteikumi; – Ministru kabineta 2012.gada 3.aprīļa noteikumi Nr.241 "Slimību profilakses un kontroles centra nolikums"; – Ministru kabineta 2020. gada 12. marta rīkojums Nr. 103 "Par ārkārtējās situācijas izsludināšanu". Saskaņā ar Ministru kabineta 2020.gada 28.aprīļa sēdes protokola⁹ Nr. 28, 51.8 "Krīzes vadības padomes sagatavotais informatīvais ziņojums" 5.punktu Ministru kabinets ir nolēmis "Atbalstīt Slimību profilakses un kontroles centra vispārējās kapacitātes attīstīšanu un kontaktpersonu identificēšanas un informēšanas tehnoloģiskā risinājuma ieviešanu [...]". Attiecībā uz Lietotnes tehnoloģiskā risinājuma drošību SPKC pienākumus nosaka normatīvie akti informācijas tehnoloģiju drošībā. Piemēram: – Informācijas tehnoloģiju drošības likums; – Ministru kabineta 2015.gada 28.jūlija noteikumi Nr. 442 "Kārtība, kādā tiek nodrošināta informācijas un komunikācijas tehnoloģiju sistēmu atbilstība minimālajām drošības prasībām";

⁶ Skat. Kolēģijas 2020.gada 21.aprīļa Pamatnostādnes 04/2020 https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_20200420_contact_tracing_covid_with_annex_en.pdf

⁷ Skat. 3.4.punkts Komisijas Paziņojums Norādījumi par lietotnēm, kas sniedz atbalstu cīņā pret Covid-19 pandēmiju saistībā ar datu aizsardzību 020/C 124 I/01 <https://eur-lex.europa.eu/legal-content/LV/TXT/?uri=CELEX%3A52020XC0417%2808%29>

⁸ Skat. Eiropas Padomes apkopojumu - "Contact Tracing Apps" <https://www.coe.int/en/web/data-protection/contact-tracing-apps>

⁹ <http://tap.mk.gov.lv/mk/mksedes/saraksts/protokols/?protokols=2020-04-28>

IEROBEŽOTAS PĪEEJAMĪBAS INFORMĀCIJA

	Attiecībā uz Lietotnes pieejamību un ērtumu SPKC pienākumus nosaka normatīvie akti, kas nosaka valsts pārvaldes darbības principus. Piemēram: - Valsts pārvaldes iekārtas likums. Attiecībā uz Lietotnes datu aizsardzību SPKC pienākumus nosaka normatīvie akti personas datu aizsardzības jomā. Piemēram: - Datu regula; - Fizisko personu datu apstrādes likums.
Kādus personas datus, (piemēram, vārds, uzvārds, personas kods) tiek plānots apstrādāt personas datu apstrādes mērķa sasniegšanai?	Lietotnes ietvaros pēc lietotāja izvēles tiek apstrādāts lietotāja <u>kontakttālrunis</u>. Citi identificējoši lietotāja dati (vārds, uzvārds un tml.) Lietotnes ietvaros netiek apstrādāti. Datus par lietotāju, kam ir apstiprināta Covid-19 saslimšana, SPKC iegūst normatīvo aktu ietvaros no ārstniecības iestādēm ārpus Lietotnes tvēruma. Lietotnes tehniskai funkcionalitātei tiek apstrādāti <u>tehniskie dati</u>, piemēram, Lietotnes paziņojumu attēlošana, kontakttālruna apstiprinājuma kods, Lietotnes valodas iestatījumi un tml. Kontaktu fiksēšana notiek Lietotāja galiekārtā un Lietotnē tiek apstrādāts: - <u>šifrēts ID</u>, kas regulāri tiek mainīts Lietotāja identitātes aizsardzībai – tas nepieciešams, lai Lietotne atšķirtu dažādas galiekārtas, kas sazinās savā starpā, un informētu tās galiekārtas ar Lietotnēm, kuru savstarpējais kontakts var radīt inficēšanās risku ar Covid-19; - kontakta ilgums nepieciešams, lai konstatētu kontaktus, kuru ilgums rada paaugstinātu inficēšanās risku ar Covid-19 (piemēram, ~ 15+ minūtes); - kontakta datums nepieciešams, lai konstatētu no Covid-19 slimības gaitas viedokļa aktuālus kontaktus (piemēram, kontaktus pēdējo 14 dienu laikā); - bluetooth signāla stiprums kontakta brīdī nepieciešams, lai konstatētu kontaktus, kuru attālums rada paaugstinātu inficēšanās risku ar Covid-19 (piemēram, tuvāk nekā 4 metri). SPKC sistēmā Lietotāja dati – kontakttālrunis, atzīme, ja tas ir lietotāja pārstāvja kontakttālrunis, <u>kontakta datums</u> un <u>ilgums</u>, un <u>bluetooth signāla stiprums</u> – tiek apstrādāti tikai no brīža, kad lietotājs ir fiksēts kā iespējamais Covid-19 kontakts, par ko lietotājs saņem Lietotnes paziņojumu. SPKC sistēmā tiek glabāta informācija par paziņojuma izsūtīšanas aktivizācijas kodu un atbildīgo SPKC darbinieku, kas ir izsniedzis šo kodu, un lietotāja SPKC piešķirts lietotāja ID - gadījuma numurs, kam ir apstiprināta Covid-19 saslimšana. Minētā informācija ir nepieciešama, lai nodrošinātu, ka kods tiek izmantots drošā veidā un tas nerada nesankcionētu citu lietotāju tiesību aizskārumu (nepamatotu ziņojumu izsūtīšanu). Aktivizācijas kodam tiek noteikts vienreizējs lietojums un 30 minūšu derīguma termiņš. SPKC sistēmā tiek veikti auditācijas pieraksti.
Ja tiek apstrādāti ģpašo kategoriju personas dati, norādiet tos	Tiešā veidā identificējami ģpašo kategoriju dati Lietotnes ietvaros netiek apstrādāti. Lietotājs, kas saņem paziņojumu par iespējamo kontaktu ar Covid-19, netiek automātiski uzskatīts par kontaktpersonu normatīvo aktu ietvaros. Šādu statusu

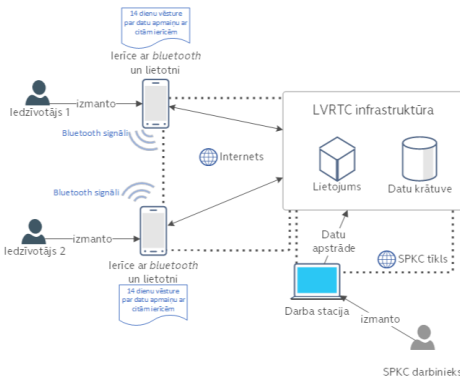
IEROBEŽOTAS PĪEEJAMĪBAS INFORMĀCIJA

	lietotājam piešķirt SPKC ārpus Lietotnes tvēruma saskaņā ar piemērojamiem normatīvajiem aktiem. Informāciju par lietotāju, kam ir apstiprināta Covid-19 saslimšana, SPKC saņem ārpus Lietotnes no ārstniecības iestādēm normatīvo aktu ietvaros. Attiecībā uz Lietotni – SPKC sistēmā saglabātie dati par Covid-19 saslimušam lietotājam izsniegto paziņojuma izsūtīšanas aktivizācijas kodu nedod iespēju šajā SPKC sistēmā tiešā veidā identificēt šo lietotāju – tiek saglabāts SPKC piešķirts lietotāja ID (gadījuma numurs). Ar Covid-19 saslimušā lietotāja identifikāciju kombinācijā ar citiem SPKC rīcībā esošiem datiem nosaka normatīvie akti ārpus Lietotnes tvēruma.		
Vai īpašo kategoriju personas datu apstrāde ir nodalīta no pārējo personas datu apstrādes? Ja atbilde ir "jā", raksturojiet procedūru, kā tas tiek nodrošināts. Ja atbilde ir "nē", norādiet iemeslus	Jā ☒ Nē ☐ Informācija par lietotāju (vārds, uzvārds un tml.), kam ir apstiprināta Covid-19 saslimšana, tiek saņemta ārpus Lietotnes tvēruma. Šī informācija tiek glabāta atsevišķi SPKC sistēmā un uz to netiek attiecināts Lietotnes tvērums.		
Vai personas datu apstrāde ir uzticēta personas datu apstrādātājam?	Jā ☒ Nē ☐ Lietotnes sistēmas uzturēšanai tiek piesaistīts VAS Latvijas Valsts radio un televīzijas centrs (turpmāk – LVRTC). LVRTC ir viens no vadošajiem pakalpojumu sniedzējiem Latvijā, kas nodrošina kvalitatīvus un drošus risinājumus arī valsts institūcijām.		
Vai ar personas datu apstrādātāju ir/tiks noslēgts rakstisks līgums?	Jā ☒ Nē ☐ Ar LVRTC ir noslēgts attiecīgs līgums.		
Vai līgumā ar personas datu apstrādes apstrādātāju ietverti Regulas 28.panta 3.punkta nosacījumi?	Jā ☒ Nē ☐ Sadarbības ietvaros ar LVRTC tiek ņemtas vērā SPKC saistošās normatīvo aktu prasības attiecībā uz informācijas tehnoloģiju drošību, tostarp Datu regulas 28.pantā apstrādātājam noteiktās prasības.		
Norādiet citas datu saņēmēju kategorijas, ja tādas ir.	Lietotnes ietvaros saņemtos personas datus nav paredzēts sniegt citām valsts iestādēm vai trešajām personām (citiem pārzinjiem). Uz datu apstrādi, kas tiek veikta ārpus Lietotnes tvēruma, tiek piemēroti attiecīgie normatīvie akti.		
Norādiet apstrādāt plānoto personas datu glabāšanas ilgumu?	Personas dati 1. Lietotnē <u>fiksētie kontakti</u>. Ja lietotājs atslēdz bluetooth funkciju – kontakti netiek fiksēti un paziņojumu par potenciālo kontaktu ar Covid-19 nav iespējams saņemt attiecībā uz laiku, kad	Glabāšanas ilgums 1. Lietotnē tiek glabāti 14 dienas, pēc tam tiek automātiski dzēsti	Apstrādes tiesiskais pamats 1. Datu regulas 5.panta princips - "glabāšanas ierobežojums" kopsakarā ar normatīvajiem aktiem epidemioloģiskās drošības jomā un šobrīd

IEROBEŽOTAS PIEEJAMĪBAS INFORMĀCIJA

bluetooth ir bijis izslēgts. 2. Lietotāja norādītais <u>kontakttālrunis</u> 3. <u>Lietotnes tehniskie dati</u>, piemēram, valodas izvēle 4. <u>SPKC sistēmā apstrādātie dati</u>, piemēram, brīdinājuma paziņojuma aktivizācijai piešķirtais kods un ar to saistītā informācija, tostarp tā derīgums, atbildīgais SPKC darbinieks un tml.	2.1. Lietotnē glabā līdz lietotājs kontakttālruni dzēš vai maina vai arī dzēš visu Lietotni 2.2. SPKC kontakttālruni ar kontakta saskares informāciju (pazīmi, vai tas ir pārstāvja kontakttālrunis, kontakta datums, ilgums, signāla stiprums) sistēmā saņem, ja ir iestājies potenciālā kontakta gadījums – glabā uz saziņas laiku. Turpmākas kontakttālruņa apstrādes pamats ir normatīvie akti, kas regulē SPKC pienākumu veikšanu epidemioloģiskās drošības jomā. 3. Līdz brīdim, kad tiek dzēsta Lietotne 4. Uz laiku, kas nepieciešams SPKC pienākumu izpildei saskaņā ar normatīvajiem aktiem epidemioloģiskās drošības jomā	pieejamiem klīniskajiem secinājumiem, ka risks inficēties ir pirmās 14 dienas. 2.1. Datu regulas 7.pants par datu subjekta piekrišanu – spēkā līdz atsaukumam 2.2. Datu regulas 5.panta princips - “glabāšanas ierobežojums” kopsakarā ar Normatīvajiem aktiem epidemioloģiskās drošības jomā 3. Datu regulas 5.panta princips - “glabāšanas ierobežojums” 4. Normatīvajiem aktiem epidemioloģiskās drošības jomā
---	--	--

IEROBEŽOTAS PIEEJAMĪBAS INFORMĀCIJA

	5. SPKC <u>sistēmas tehniskie dati</u>, (pierakstu veidošana), piemēram, auditācijas pieraksti	5. 12 mēnešus vai uz ilgāku laiku, kas nepieciešams SPKC sistēmas drošības uzraudzības, tostarp auditu/pārbaužu īstenošanai	5. Normatīvie akti informācijas tehnoloģiju drošības jomā, tostarp Ministru kabineta 2015.gada 28.jūlija noteikumi Nr. 442 "Kārtība, kādā tiek nodrošināta informācijas un komunikācijas tehnoloģiju sistēmu atbilstība minimālajām drošības prasībām" un Fizisko personu datu apstrādes likuma 37.pants, kas paredz, ka auditācijas pieraksti "ir uzglabājami ne ilgāk kā vienu gadu pēc ieraksta izdarīšanas, ja normatīvie akti vai apstrādes raksturs nenosaka citādi."
Norādiet resursus, kas tiks izmantoti personas datu apstrādē. <i>*Ja apstrādē tiek plānots piesaistīt apstrādātājus, uzskaitē ir veicama sadarbībā ar operatoriem.</i>	Resursi: Lietotnes uzbūve (vispārējais kopskats): 	Apstrādes process kurā līdzeklis tiks izmantots: Detalizēta informācija par resursiem ir ietverta Lietotnes infrastruktūras diagrammā (detalizēta fiziskās arhitektūras shēmā).	
Vai apstrādes atbilstības nodrošināšanai tiks izmantots apstiprināts rīcības kodekss?	Jā ☐ Nē ☒ Šobrīd šāds rīcības kodekss nav. Lietotnes izstrādes ietvaros tiek sekots līdzi Eiropas Savienības ietvaros sniegtajām rekomendācijām un vadlīnijām šādu lietotņu izstrādei. Piemēram:		

	- (pieejams angļu valodā) - eHealth Network - <i>Mobile applications to support contact tracing in the EU's fight against COVID-19</i> - Common EU Toolbox for Member States Version 1.0 15.04.2020¹⁰; - Kolēģijas 2020.gada 21.aprīļa Pamatnostādnes 04/2020¹¹; - Komisijas 2020.gada 17.aprīļa Paziņojums Norādījumi par lietotnēm, kas sniedz atbalstu cīņā pret Covid-19 pandēmiju saistībā ar datu aizsardzību 2020/C 124 I/01¹².
Ja atbilde Jā, sniedziet sīkāku informāciju par rīcības kodeksu	Skat. iepriekš norādīto informāciju.

II. Nepieciešamības un samērīguma novērtējums

1. Atbilstība datu aizsardzības principiem	
Vai apstrāde tiek veikta konkrētos, skaidros un leģitīmos nolūkos (atbilstoši Regulas 5.panta 1.punkta b)apakšpunktam)?	Jā ☒ Nē ☐ Lietotnes datu apstrādes mērķi un nolūku skat. augstāk. Lietotnes pārzinis ir publiskās pārvaldes iestāde, tas nozīmē, ka lietotnes pārzinis lietotnes ietvaros veikto informācijas apstrādi var izmantot tikai savu normatīvajos aktos noteikto funkciju sasniegšanai. Iegūtās informācijas izmantošana ārpus iepriekš norādītajiem datu apstrādes mērķiem nav funkcionāli paredzēta, tāpat publiskās pārvaldes iestādes datu apstrādes darbības ierobežo normatīvajos aktos noteiktais deleģējums.
Kāds ir plānotās personas datu apstrādes tiesiskais pamats atbilstoši Regulas 6.pantam	Lietotnes datu apstrādes tiesiskais pamats: Sabiedrības interesēs, izpildot normatīvo aktu prasības – SPKC darbojas saskaņā ar normatīvajiem aktiem veselības jomā, tostarp epidemioloģiskās drošības jomā un atbilstoši Ministru kabineta 2012.gada 3.aprīļa noteikumiem Nr.241 "Slimību profilakses un kontroles centra nolikums", kas nosaka SPKC uzdevumus, funkcijas un tiesības. Vienlaikus SPKC savā darbībā ievēro citus saistošos normatīvos aktus, tostarp normatīvos aktus personas datu aizsardzības jomā un informācijas tehnoloģiju drošībā. Lietotnes funkcionalitātē ir ņemti vērā arī normatīvie akti, kas nosaka valsts pārvaldes darbības principus, lai Lietotne būtu Lietotājam saprotamā un ērti pieejamā veidā. Lietotāja piekrišana – Lietotnes ietvaros Lietotājs piekrišanu sniedz ar savu aktīvu darbību, gan izmantojot Lietotni, gan arī brīvprātīgi ievadot Lietotnē informāciju, kuras ievadīšana Lietotnē ir funkcionāli iespējama.
Ja tiek veikta īpašo kategoriju datu apstrāde norādiet plānotās personas datu apstrādes tiesisko pamatu atbilstoši Regulas 9.pantam.	Lietotnes ietvaros tiešā veidā īpašo kategoriju datu apstrāde nav paredzēta. Īpašo kategoriju datu apstrādes pamatu, ko SPKC veic ārpus Lietotnes, piemēram, saņemot informāciju par personu, kam ir apstiprināta Covid-19 saslimšana, nosaka normatīvie akti epidemioloģiskās drošības jomā.
Vai personas datu apstrādes mērķi var sasniegt, vispār neapstrādājot personas datus vai apstrādājot mazākā apjomā? Pamatojiet	Var ☐ Nevar ☒ Lietotnes tehniskais risinājums ir izstrādāts veidā, kas dod iespēju lietotājam izmantot tikai daļu no Lietotnes funkcionalitātēm, piemēram, apskatot tikai aktuālās informācijas sadaļu. Šādā gadījumā lietotājam nav nepieciešams aktivizēt kontaktu fiksēšanu un norādīt kontakttālruni. Tomēr šāda Lietotnes izmantošana tikai daļēji sasniedz Lietotnes mērķi (attiecībā uz lietotāja

¹⁰ https://ec.europa.eu/health/sites/health/files/ehealth/docs/covid-19_apps_en.pdf

¹¹ https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_20200420_contact_tracing_covid_with_annex_en.pdf

¹² <https://eur-lex.europa.eu/legal-content/LV/TXT/?uri=CELEX%3A52020XC0417%2808%29>

IEROBEŽOTAS PIEEJAMĪBAS INFORMĀCIJA

	informēšanu un izglītošanu) un nedod iespēju sniegt atbalstu lietotājam epidemioloģiskās drošības jomā, ja lietotājam ir bijis kontakts ar Covid-19 saslimušu personu. Lai varētu fiksēt kontaktus – lietotājam ir jāaktivizē bluetooth funkcionalitāte. Tas nedod iespēju identificēt lietotāju, bet bez šīs funkcijas aktivizācijas lietotājam nebūtu iespēja fiksēt kontaktus un saņemt ziņu, ja ir bijusi saskare ar Covid-19 saslimušu lietotāju. Ja Lietotājs vēlas, lai potenciālā kontakta gadījumā varētu saņemt zvanu no SPKC – Lietotājam ir iespēja norādīt kontakttālruni. Citi dati (vārds, uzvārds un tml.) netiek prasīti. Bez kontakttālruna nebūtu iespēja citādākā veidā ar Lietotāju sazināties. Lietotājs savu izvēli var mainīt – piemēram, dzēšot norādīto kontakttālruni. Pats kontakttālrunis nedod iespēju tiešā veidā identificēt konkrēto personu. Identificējoša informācija (vārds, uzvārds un tml.), ja tas nepieciešams SPKC pienākumu veikšanai – tiek īstenots ārpus Lietotnes ietvara – atbilstoši normatīvajiem aktiem, SPKC veicot epidemioloģiskās drošības pasākumus un uz to tiek attiecināts cits datu apstrādes process, kas nav saistīts ar Lietotnes ietvaru.
Vai visi apstrādājamie dati ir nepieciešami personas datu apstrādes mērķa sasniegšanai? Ja atbilde ir "jā", uzskaitiet šos datus, norādot, kādēļ tie nepieciešami personas datu apstrādes mērķa sasniegšanai. Ja atbilde ir "nē", norādiet iemeslus	Jā ☒ Nē ☐ Kontaktu fiksēšana Lietotnes galiekārtā (pēc lietotāja izvēles) ir nepieciešama, lai varētu informēt lietotāju, ja ir bijusi saskare ar Covid-19 saslimušu lietotāju. Bez kontakta fiksēšanas to nebūtu iespējams izdarīt. Kontakttālruna norāde (pēc lietotāja izvēles) un kontakta saskares informācija (ilgums, datums, signāla stiprums un tml.) ir nepieciešama, lai lietotājs saņemtu brīdinājumu tad, kad iespējamais risks ir pietiekami augsts (attiecīgi, lai lietotājs netiktu traucēts par kontaktiem, kas nerada inficēšanās risku) un lai potenciālā kontakta gadījumā SPKC varētu ar lietotāju sazināties. Kontakttālruna apstiprinājuma kods ir nepieciešams, lai lietotājs varētu pārliecināties par Lietotnē ievadītā kontakttālruna pareizību un lai tiktu aizsargātas citas personas (nepamatoti netiktu norādīts trešo personu kontakttālrunis). Brīdinājuma aktivizācijas koda apstrāde un ar to saistītā informācija (atbildīgais SPKC darbinieks, koda derīgums un tml.) – ir nepieciešama, lai nodrošinātu Lietotnes drošību un lietotāju tiesību aizsardzību, t.i., lai lietotājiem netiktu nosūtīts nepamatots paziņojums. Lietotnes tehniskie dati (valodas izvēle un tml.) – ir nepieciešami, lai lietotājam Lietotnes funkcionalitāte būtu pieejama saprotamā un ērtā veidā. SPKC sistēmas tehniskie dati, tostarp auditācijas pieraksti ir nepieciešami, lai sistēmas drošību varētu īstenot ilgtermiņā.
Kā tiek noteikti personas datu glabāšanas termiņi (piemēram, atbilstoši normatīvajam aktam, līgumam, datu subjekta piekrišanai)? Pamatojiet termiņa izvēli	Personas datu apstrādes termiņi tiek noteikti atbilstoši konkrēto datu specifikai: Ja datu apstrādes pamats ir piekrišana – attiecīgi tiek ņemts vērā piekrišanas spēkā esamības termiņš. Ja lietotājs dzēš Lietotni – Lietotnes dati tiek dzēsti atbilstoši Datu regulas 5.panta principam "glabāšanas ierobežojums". Ja datu apstrādes tiesiskais pamats ir normatīvie akti – tiek ņemts vērā SPKC pienākumu veikšanai nepieciešamais laiks. Piemēram, attiecībā uz fiksēto kontaktu apstrādes termiņu papildus tiek ņemtas vērā šobrīd pieejamās

IEROBEŽOTAS PIEEJAMĪBAS INFORMĀCIJA

	klīniskās vadlīnijas, ka Covid-19 simptomi var parādīties 14 dienu laikā pēc saskares ar vīrusu. Plašāk par konkrēto datu apstrādes termiņu skat. augstāk.
Ja personas datu glabāšanas termiņš ir noteikts normatīvajā aktā, norādiet to	Piemēram: Datu regulas 5.panta paredz "glabāšanas ierobežojuma" principu, atbilstoši kuram personas dati <i>"tiek glabāti veidā, kas pieļauj datu subjektu identifikāciju, ne ilgāk kā nepieciešams nolūkiem, kādos attiecīgos personas datus apstrādā [..]"</i>. Attiecīgi Lietotnē dati tiek glabāti ne ilgāk kā tiek dzēsta Lietotne. SPKC sistēmā dati tiek glabāti ne ilgāk, kā tas nepieciešams SPKC pienākumu veikšanai saskaņā ar normatīvajiem aktiem epidemioloģiskās drošības jomā. Attiecībā uz auditācijas pierakstiem termiņu nosaka Fizisko personu datu apstrādes likuma 37.pants, paredzot, ka tie <i>"ir uzglabājami ne ilgāk kā vienu gadu pēc ieraksta izdarīšanas, ja normatīvie akti vai apstrādes raksturs nenosaka citādi."</i>
Ja personas datu glabāšanas termiņš netiek regulēts ar ārēju normatīvo aktu, norādiet, cik bieži tiek izvērtēti personas datu glabāšanas termiņi	Attiecībā uz fiksēto kontaktu glabāšanas ilgumu dati tiks pārskatīti, ņemot vērā klīnisko vadlīniju attīstību. Šis termiņš, attīstoties Covid-19 vīrusa izpētei, ar laiku varētu tikt pagarināts vai saīsināts, lai sasniegtu epidemioloģiskās drošības mērķi. Dati, kas tiek apstrādāti uz piekrišanas pamata – tiks ņemts vērā piekrišanas spēkā esamības termiņš (to nosaka katrs lietotājs pats – attiecīgi atstājot spēkā piekrišanu vai to atsaucot). Dati, kas ir nepieciešami Lietotnes funkcionalitātei (piemēram, valodas izvēle) – tiks dzēsti ar Lietotnes dzēšanu. Glabāšanas ilguma nepieciešamība tiks pārskatīta, ja tiks veidota jauna Lietotnes funkcionalitāte un ja tās mērķa sasniegšanai būs nepieciešami citi apstrādes termiņi. Attiecībā uz SPKC sistēmā pienākumu veikšanai nepieciešamo datu apstrādes termiņiem - tie tiks pārskatīti atbilstoši SPKC iekšējo procesu uzraudzībai un aktualizācijai.
Kāda kārtība ir paredzēta, lai periodiski izvērtētu apstrādājamo personas datu apjomu un to atbilstību personas datu apstrādes mērķa sasniegšanai? Cik bieži šī kārtība tiek pārskatīta? Ja kārtība nav paredzēta, norādiet iemeslus un paskaidrojiet, kā tiek nodrošināts, lai personas datu apjoms visā to apstrādes laikā nepārsniegtu personas datu apstrādes mērķa sasniegšanai nepieciešamo	SPKC regulāri sekos līdzi, vai Lietotnes darbība dod iespēju sasniegt iecerēto mērķi, jo Lietotne būs tiešais SPKC darba instruments savu pienākumu izpildei – sadarbībai ar Lietotājiem, lai aizsargātu sabiedrību pret Covid-19 izplatību. Lietotnes saturs tiks pārskatīts un mainīts, to pilnveidojot pēc nepieciešamības.
Ja personas datu apstrāde vairs nav nepieciešama personas datu apstrādes mērķa sasniegšanai: 1. Kā tiek izvērtēta personas datu apstrāde, lai noteiktu, kuri dati ir dzēšami?	1. Priekšroka tiek dota lietotāja tiesību aizsardzībai – dati, kas vairs nav nepieciešami, tiek dzēsti. Piemēram, ja Lietotnē fiksētajiem kontaktiem ir pagājis 14 dienu termiņš – tie tiek Lietotnē automātiski dzēsti.

IEROBEŽOTAS PIEEJAMĪBAS INFORMĀCIJA

2. Kurš ir atbildīgs par personas datu novērtēšanu, lai noteiktu, kuri dati un kad ir dzēšami? 3. Vai informācijas sistēmā ir ieviesta automatizēta paziņojuma saņemšana, kas norāda uz nepieciešamību dzēst personas datus?	2. Dati, kas tiek apstrādāti Lietotnē – tiek dzēsti automātiski līdz ar Lietotnes dzēšanu. Lietotnes dzēšanas termiņu nosaka pats lietotājs. Lietotājam pašam ir iespēja atsevišķi ātrāk dzēst, piemēram, norādīto kontakttālruni. Datiem, kas tiek apstrādāti SPKC sistēmā, dzēšanas procesu nodrošina saskaņā ar SPKC iekšējām procedūrām. 3. Lietotnes dati tiek dzēsti automātiski – papildu paziņojums nav nepieciešams. Datiem, kas tiek apstrādāti SPKC sistēmā, dzēšanas procesu nodrošina saskaņā ar SPKC iekšējām procedūrām. SPKC sistēmā esošo datu aizsardzības nolūkos sākotnēji dzēšanas process tiks veikts manuāli – papildu automātisks paziņojums nav nepieciešams. Šāds paziņojums tiks ieviests, ja, SPKC sistēmā apstrādāto datu dzēšanu tā apjoma pieauguma dēļ vairs nebūs iespēja veikt manuāli. SPKC sistēmā kontakttālruni tiks dzēsti ar dzēšanas skriptu, no SPKC sistēmas to palaižot manuāli.
Vai ir izstrādātas vadlīnijas/kārtība attiecībā uz personas datu dzēšanu?	Jā ☒ Nē ☐ Lietotnes datu dzēšana tiek veikta Lietotnē un tas ir iestrādāts Lietotnes funkcionalitātē. Datiem, kas tiek apstrādāti SPKC sistēmā, dzēšanas procesu nodrošina saskaņā ar SPKC iekšējām procedūrām.
Kā tiek nodrošināta pareizu (precīzu, aktuālu) personas datu apstrāde?	Fiksētie kontakti, kas ir senāki par 14 dienām, tiek dzēsti un attiecīgi to apstrāde netiek turpināta. Lietotājs norādīto kontakttālruni apstiprina ar kodu, tādējādi pārliedzinoties, ka norādītā informācija ir korekta. Lietotājam ir iespēja pašam mainīt un dzēst Lietotnē norādīto kontakttālruni, piemēram, ja tas ir mainījies vai nav vairs aktuāls. Brīdinājuma paziņojuma izsūtīšanai SPKC Covid-19 saslimušajam lietotājam piešķir aktivizācijas kodu – tas nodrošina citu lietotāju aizsardzību pret nepamatotu ziņojumu saņemšanas. Ziņojums tiek sūtīts, ja kontakts ir bijis ne senāk kā 14 dienas un tā ilgums un signāla stiprums liecina par iespējamo inficēšanās risku – tas palīdz nodrošināt, ka lietotājs netiek traucēts par kontaktiem, kam ir zems inficēšanās risks. Lietotājam ir tiesības īstenot Datu regulā paredzētās datu subjekta tiesības – lietotājs var sazināties ar SPKC un pieteikt lūgumu par SPKC rīcībā esošajiem datiem. SPKC to izskata atbilstoši normatīvajiem aktiem un veic korekcijas, kur tas ir tiesiski pamatoti (piemēram, attiecībā uz kontakttālruna precizēšanu, ja ir mainījušies kontakttālruna lietotāji).
Norādiet dokumentu, kurā ir noteikta kārtība, kā un cik bieži tiek aktualizēti (precizēti) personas dati	Lietotnē esošo datu aktualizēšana tiek veikta atbilstoši Lietotnē iestrādātai funkcionalitātei, piemēram, fiksēto kontaktu dzēšana nodrošina, ka netiek Lietotnē apstrādāti kontakti, kas nav vairs aktuāli. Lietotnes darbības apraksts ietverts Lietotnes noteikumos un Privātuma politikā. Datiem, kas tiek apstrādāti SPKC sistēmā, aktualizācijas procesu nodrošina saskaņā ar SPKC iekšējām procedūrām.
Cik bieži veic pārbaudes, vai apstrādāti tiek pareizi (precīzi, aktuāli) dati? Norādiet pamatojumu, kādēļ ir izvēlēts šāds periodiskums un vai tas nodrošina tikai pareizu	Lietotnes ietvaros apstrādāto datu ilgums ir salīdzinoši īss un attiecināms tikai uz konkrēto situāciju. Lietotnes ietvaros saņemtie dati netiek izmantoti atkārtoti pret dažādām situācijām. Piemēram, SPKC sistēmā saņemtais kontakttālrunis tiek apstrādāts pret konkrēto kontakta gadījumu. Ja lietotājam rodas jauns kontakts, pret jauno kontaktu no jauna no Lietotnes tiek saņemts attiecīgajā brīdī norādītais lietotāja

IEROBEŽOTAS PIEEJAMĪBAS INFORMĀCIJA

(precīzu, aktuālu) personas datu apstrādi	kontakttālrunis. Šāds risinājums ir paredzēts jau Lietotnes funkcionalitātē, lai uzreiz nodrošinātu datu precizitāti pret konkrēto situāciju. Kontakttālruna precizitāte papildus tiek pārbaudīta, sazinoties ar konkrēto lietotāju, kad potenciālā Covid-19 kontakta gadījumā ir saņemts lietotāja kontakttālrunis. Persona, kurai saskaņā ar lietotnes algoritmu ir notikusi saskare ar inficēto personu, var apgalvot, ka visu dienu attiecīgā datumā pavadīja ar mutes aizsegu un vienmēr ievērojot 2m. Tādā gadījumā mēs klasificējam šo saskari kā "Nav tuvs kontakts" un personai nav jāievēro pašizolācija. Šeit vajag parunāt par saslimšanas datuma ievadīšanu un vairāk par backend pusi. SPKC sistēmas un Lietotnes darbības vispārējā drošība tiks uzraudzīta regulāri, ikdienas procesos sekojot līdzī audītārijas pierakstiem saskaņā ar SPKC iekšējām procedūrām.
Vai ir vērtēti zaudējumi*, kas var rasties no neaktuālu datu apstrādes? <i>*Pārzinim varētu būt nepieciešams izvērtēt gan zaudējumus datu subjektam no iespējamā risku viedokļa, gan pārzinim no potenciālā apdraudējuma pārziņu mērķu sasniegšanai viedokļa.</i>	Jā ☒ Nē ☐ Tiešie zaudējumu riski SPKC kā pārzinim un Lietotnes lietotājam kā datu subjektam ir zemi. <u>Šobrīd nav konstatējams, ka Lietotne varētu lietotājam radīt fizisku kaitējumu</u> (piemēram, ievainojumu), jo Lietotnes ietvaros fiksētais kontakts netiek automātiski uzskatīts par kontaktpersonu un personai šāds statuss tiek piešķirts normatīvo aktu ietvaros. <u>Nav konstatējams, ka lietotājam varētu rasties materiāls kaitējums</u> (piemēram, lietu zudums vai finanšu zaudējums), jo Lietotne nesatur datus, kas dotu piekļuvi lietotāja finanšu līdzekļiem vai tml. <u>Morālā kaitējuma iestāšanās risks ir vērtējuma kā zems</u> (piemēram, bailes, apmulsums un tml.). Ja sazvānītā persona nav Lietotnes lietotājs – teorētiski personai varētu rasties bailes vai apmulsums - tomēr risks ir vērtējams kā zems, jo riska mazināšanai Lietotnes funkcionalitātē uzreiz ir paredzēts, ka kontakttālruni apstiprina ar kodu – tas palīdz novērst situācijas, ka varētu tikt norādīts bez šīs personas ziņas kontakttālrunis. Lietotnes ietvaros no lietotāja tiek saņemts kontakttālrunis – tas nedod iespēju tiešā veidā identificēt konkrēto personu – ja sazvānītā persona nav Lietotnes lietotājs (piemēram, ja ir mainījušies kontakttālruna lietotāji), tas tiek ņemts vērā un tālāka saziņa ar šo personu netiek veikta. Pret katru konkrēto situāciju tiek no jauna saņemts kontakttālrunis. Personai ir iespēja dzēst Lietotni vai mainīt kontakttālruni, ja persona vairs nevēlas lietot Lietotni vai ir mainījis kontakttālruni. Tas attiecīgi minimizē riskus attiecībā uz neaktuālu datu izmantošanu. Lietotne dod būtisku atbalstu SPKC – tomēr Lietotne nemaina SPKC manuālos procesus Covid-19 kontaktpersonu apzināšanā un informēšanā. Ja persona nelieta Lietotni vai nav norādījusi kontakttālruni – SPKC manuālā veidā (esošo procesu ietvaros) – turpinās apzināt personas, lai brīdinātu par iespējamo kontaktu ar Covid-19 saslimušu personu. Attiecīgi Lietotnes neizmantošanu vai datu iespējamā neaktualitāte, ja tāda rastos - nemazinātu šo personu tiesības saņemt informāciju esošā SPKC procesa ietvaros, ja vien SPKC būs bijusi iespēja šo personu kā potenciālo kontaktu apzināt, piemēram,

IEROBEŽOTAS PIEEJAMĪBAS INFORMĀCIJA

	saņemot informāciju no saslīmušās personas. Manuālais process prasa ilgāku laiku un SPKC resursus. Lietotne tos palīdzēs ietaupīt.
Integritāte	Lietotnes drošības risku vērtējums veikts saskaņā ar Ministru kabineta 2015.gada 28.jūlija noteikumiem Nr. 442 "Kārtība, kādā tiek nodrošināta informācijas un komunikācijas tehnoloģiju sistēmu atbilstība minimālajām drošības prasībām": C integritātes klase – Lietotnes ietvaros apstrādāto datu integritātes apdraudējums nerada risku valsts un pašvaldību institūcijas pamatfunkciju nodrošināšanai. Lietotne dod būtisku atbalstu SPKC – tomēr Lietotne nemaina SPKC manuālos procesus Covid-19 kontaktpersonu apzināšanā un tas attiecīgi tiks turpināts arī paralēli Lietotnes pieejamībai.
Pārskatatbildība	Atbilstoši Datu regulas 5.panta 2.punktam SPKC nodrošinās pārskatatbildību. Lietotnes funkcionalitāte (piemēram, fiksēto kontaktu dzēšana pēc 14 dienu termiņa), kā arī kontakttālruna apstrāde pret katru konkrēto situāciju no jauna, kā arī kontakttālruna saņemšana tikai pēc tam, kad lietotājs ir konstatēts kā iespējamais Covid-19 kontakts, kam paziņojumu aktivizē ar SPKC piešķirto kodu - būtiski atvieglo pārskatatbildības procesa uzturēšanu un mazina neaktuālu (nekorektu) datu nonākšanu pie SPKC.
2. Datu subjekta tiesību nodrošināšana	
Vai personas dati tiek iegūti no datu subjekta?	Jā ☒ Nē ☐ Lietotnes lietošana ir brīvprātīga – dati no Lietotnes uz SPKC sistēmu tiek saņemti tikai tad, ja Lietotājs ir lejupielādējis lietotni, aktivizējis bluetooth un norādījis kontakttālruni. Lietotnes dati uz SPKC sistēmu tiek padoti automatizētā veidā – tikai tad, ja ir iestājies Covid-19 potenciālā kontakta gadījums. Dati par personu, kam ir apstiprināts Covid-19, tiek saņemti ārpus Lietotnes tvēruma no ārstniecības iestādēm saskaņā ar normatīvajiem aktiem un Lietotne uz šo procesu neattiecas.
Vai informācija par datu subjektu tiek saņemta no trešajām personām? Ja atbilde ir "jā", norādiet informācijas saņemšanas kārtību un tiesisko pamatu šādas informācijas saņemšanai	Jā ☐ Nē ☒ Lietotnes ietvaros dati tiek saņemti no Lietotnes kontekstā ar paša lietotāja izdarīto izvēli (lejupielādēta lietotne, aktivizēta kontaktu fiksēšana, norādīts kontakttālrunis) Dati par personu, kam ir apstiprināts Covid-19, tiek saņemti ārpus Lietotnes tvēruma no ārstniecības iestādēm saskaņā ar normatīvajiem aktiem un Lietotne uz šo procesu neattiecas.
Kādi norādītie apstrādē izmantotie personas dati tiek iegūti no datu subjekta.	Ja lietotājs Lietotnē ir aktivizējis kontaktu fiksēšanu un validējis savu tālruna numuru – Covid-19 iespējamā kontakta gadījumā SPKC saņem no Lietotnes lietotāja norādīto kontakttālruni un lietotāja norādīto pazīmi, ja tas ir pārstāvja kontakttālrunis un Lietotnes fiksētos kontakta datus – kontakta datums, ilgums, signāla stiprums.
Vai ir nodrošināta datu subjekta informēšana par viņa personas datu apstrādi neatkarīgi no tā, vai personas dati ir vai nav iegūti no datu subjekta?	Jā ☒ Nē ☐ Pirms Lietotnes uzsākšanas lietotājs apstiprina, ka piekrīt Lietotnes noteikumiem un ir iepazinies ar Privātuma politiku. Minētajos dokumentos ir detalizēti aprakstīti par datu apstrādi un Lietotnes funkcionalitāti.

IEROBEŽOTAS PIEEJAMĪBAS INFORMĀCIJA

Ja atbilde ir "jā", norādiet, kādā veidā un kādā gadījumā datu subjekts tiek informēts par viņa personas datu apstrādi, un kāda satura informācija tiek sniegta. Ja atbilde ir "nē", norādiet, kādēļ datu subjekts netiek informēts	
Vai ir izstrādāta kārtība/procedūra datu subjekta identifikācijai?	Jā ☒ - tiktāl, cik tas nepieciešams Lietotnes mērķim. Nē ☐ Lietotnes ietvaros tiek ievērots datu minimizācijas princips un dati tiek apstrādāti tikai apjomā, kas nepieciešams Lietotnes mērķa sasniegšanai. Lietotnes ietvaros nav paredzēts ievākt vairāk datus, kā tas nepieciešams priekš Lietotnes (netiek prasīts vārds, uzvārds un tml.). Tiek attiecināts Datu regulas 11.pants, kas paredz, ka – <i>“Ja nolūki, kādos pārzinis apstrādā personas datus, neprasa vai vairs neprasa pārzinim identificēt datu subjektu, pārzinim nav pienākuma saglabāt, iegūt vai apstrādāt papildu informāciju, lai identificētu datu subjektu, ja vienīgais nolūks ir ievērot šo regulu. [..]”</i>
Vai datu subjektam tiek nodrošināta iespēja iegūt informāciju par personām, kuras ir saņēmušas informāciju par šo datu subjektu? Ja atbilde ir "jā", norādiet, par kādu laikposmu šāda informācija tiek sniegta. Ja atbilde ir "nē", norādiet, kādēļ informācija netiek sniegta	Jā ☒ Nē ☐ Lietotnes ietvaros saņemtos datus nav paredzēts sniegt citām institūcijām vai trešajām personām. Datu saņēmējs ir SPKC. Uz datiem, kas tiek apstrādāti ārpus Lietotnes, piemēram, ja personai tiek apstiprināts kontaktpersonas statuss – datu saņēmēji tiek noteikti saskaņā ar normatīvajiem aktiem un Lietotnes tvērumu uz to neattiecas. Saskaņā ar Fizisko personu datu apstrādes likuma 27.panta trešo daļu – <i>“Datu subjekts var saņemt informāciju par tā datu saņēmējiem vai saņēmēju kategorijām, kam dati ir izpausti <u>pēdējo divu gadu laikā</u>.”</i>
Vai datu subjektam ir nodrošinātas tiesības piekļūt saviem personas datiem? Ja atbilde ir "jā", raksturojiet kārtību, kādā tiek nodrošinātas datu subjekta piekļuves tiesības saviem personas datiem.	Jā ☒ Nē ☐ Kontakttālruni, kas ir norādīts Lietotnē, lietotājam ir iespēja apskatīt un mainīt pašā Lietotnē. Lietotnes galiekārtā fiksētajiem kontaktiem netiek nodrošināta piekļuve, lai aizsargātu pašu lietotāju pret trešajām personām un netiktu ietekmēta šo datu integritāte. Saskaņā ar Datu regulas 15.pantu ikvienai personai ir tiesības vērsties SPKC ar lūgumu saņemt informāciju, vai SPKC sistēmā tiek apstrādāti konkrētās personas dati.

IEROBEŽOTAS PĪEEJAMĪBAS INFORMĀCIJA

Ja atbilde ir "nē", norādiet, kāpēc datu subjekta piekļuves tiesības nav nodrošinātas	Atbilde uz personas lūgumu tiek gatavota, standarta kārtībā izskatot saņemto iesniegumu. Informācija par personas tiesībām iesniegt šādu lūgumu ir gan Lietotnes Privātuma politikas 9.punktā, gan arī SPKC kopējās darbības Privātuma politikā, kas ir pieejama SPKC mājas lapā. Lietotāja tiesību praktisko izpildi SPKC ir iespēja īstenot attiecībā uz lietotāja datiem, ko var identificēt kā konkrētā lietotāja datus. Atbilstoši normatīvajiem aktiem datu subjekta tiesības netiek attiecinātas uz anonīmas informācijas apstrādi, t.i., informāciju, kas neattiecas uz identificējamu personu, un datiem, kas ir apstrādāti anonīmā veidā, kas nedod iespēju identificēt personu.
Kā tiek nodrošināta personas datu atrašana pēc datu subjekta pieprasījuma?	SPKC nav pieejas Lietotnes galiekārtā fiksētajiem kontaktiem – attiecīgi SPKC nav iespēja lietotājam sniegt informāciju par šiem datiem. Personas atrašanas SPKC sistēmā tiek veikta pēc saņemtā kontakttālruņa. Lai personai sniegtu precīzu atbildi par datiem, kas uz to varētu tikt attiecināti, personai var tikt pieprasīta papildu informācija tieši pieprasījuma izskatīšanas kontekstā (piemēram, vai izmanto Lietotni un vai ir saņemts brīdinājuma paziņojums un tml.). Tas nepieciešams, lai nepamatoti netiktu skartas citu personu intereses. Pieprasījums tiek īstenots tiktāl, cik tas nerada šaubas par pieprasījuma izmantošanas godprātīgumu (piemēram, ka persona ir patiesais Lietotnes lietotājs) un atbilstoši Datu regulas 15.panta 4.punktam neskar citu personu tiesības un brīvības (piemēram, ka netiek prasīta informācija par citu lietotāju).
Vai datu subjektam pēc tā pieprasījuma tiek sniegta informācija par personas datu apstrādi? Ja atbilde ir "jā", norādiet informācijas sniegšanas kārtību	Jā ☒ Nē ☐ Informācija par personas datu apstrādi ikvienam lietotājam ir pieejama jau pirms Lietotnes uzsākšanas atbilstoši Lietotnes noteikumiem un Privātuma politikai. Pieprasījuma gadījumā lietotājam tiek sniegta papildu informācija – nodrošinot izvērstāku informāciju tieši par tiem aspektiem, kas interesē konkrēto lietotāju. Piemēram, ja lietotāju interesē, vai SPKC saņem informāciju par kontaktu, kam nav norādīts kontakttālrunis – SPKC ir iespēja konkrētam lietotājam sniegt informāciju, ka šādā gadījumā SPKC informāciju par kontaktu nesaņem. Šāda pieprasījuma gadījumā nav nepieciešama lietotāja identifikācija – jo lietotāja pieprasījums ir par Lietotnes funkcionalitāti kā tādu.
Vai pārzinim ir tiesības atteikt datu subjektam piekļuvi viņa personas datiem? Ja atbilde ir "jā", norādiet, kādā gadījumā	Jā ☒ Nē ☐ Saskaņā ar Datu regulas 11.pantu un 15.panta 4.punktu SPKC var atteikt piekļuvi datiem, ja personu nav iespējams identificēt vai arī piekļuve datiem var skart citu personu tiesības un brīvības (piemēram, ja personas pieprasījums ir ar mērķi saņemt informāciju par citu lietotāju). Vispārējs automātisks aizliegums saņemt informāciju par SPKC rīcībā esošiem datiem šobrīd nav paredzēts.

IEROBEŽOTAS PIEEJAMĪBAS INFORMĀCIJA

Vai notiek automatizēta lēmumu pieņemšana, pamatojoties uz apstrādātajiem personas datiem? Kādā gadījumā pārzinis pārskata šādus lēmumus?	Jā ☒ tiktāl, cik tas attiecas uz automatizētu brīdinājuma paziņojumu izsūtīšanu. Brīdinājuma paziņojuma saņemšana nerada lietotājam saistošu lēmumu vai sekas. Nē ☐ Brīdinājuma paziņojuma saņemšana Lietotnē automātiski nenozīmē, ka lietotājam ir piešķirts kontaktpersonas statuss. Kontaktpersonas statusu nosaka manuālā veidā ārpus Lietotnes tvēruma normatīvo aktu ietvaros, SPKC sazinoties ar lietotāju. Lietotnes funkcionalitāte – iespēja norādīt kontakttālruni – ir veidota, lai lietotājam būtu iespēja papildus saņemt manuālu SPKC darbinieku atbalstu. Lietotāja izvēle nenorādīt Lietotnē kontakttālruni ir vienlaikus lietotāja vēlme, lai SPKC Lietotnes ietvaros ar lietotāju kontakta gadījumā nesazinās. Un SPKC par šādiem kontaktiem attiecīgi arī nesaņem informāciju. Lietotne nemazina ikviena lietotāja tiesības pašam sazināties ar SPKC citos pieejamos veidos, lai saņemtu SPKC sniegto atbalstu.
Vai datu subjektam ir nodrošinātas tiesības labot savus personas datus atbilstoši Regulas 16.pantam? Ja atbilde ir "jā", norādiet, kādā veidā šīs datu subjekta tiesības tiek nodrošinātas. Ja atbilde ir "nē", norādiet iemeslus	Jā ☒ Nē ☐ Lietotājam ir iespēja Lietotnē mainīt savu norādīto kontakttālruni – dzēšot vai aizstājot to ar citu. Attiecībā uz datiem, kas ir saņemti SPKC – ja lietotājs informē, ka konkrēto kontakttālruni vairs neizmanto – tas tiek atzīmēts SPKC sistēmā un turpmākā saziņa uz šo kontakttālruni netiek veikta. Tehniskā veidā fiksētos kontakta datus (kontakta datumu, ilgumu un signāla stiprumu) – lietotājam nav iespēja mainīt – jo šie ir tehniskie dati, kuru izmaiņas radītu nepareizu pārējās Lietotnes darbību.
Vai datu subjektam ir nodrošinātas tiesības dzēst savus datus atbilstoši Regulas 17.pantam? Ja atbilde ir "jā", norādiet, kādā veidā šīs datu subjekta tiesības tiek nodrošinātas. Ja atbilde ir "nē", norādiet iemeslus.	Jā ☒ Nē ☐ Lietotājam ir tiesības dzēst Lietotni jebkurā laikā un tādejādi dzēst visus Lietotnes datus. Lietotājam ir iespēja atsevišķi dzēst un mainīt Lietotnē norādīto kontakttālruni. SPKC sistēmā datu dzēšanas tiek veikta atbilstoši SPKC pienākumu izpildes laikam saskaņā ar normatīvajiem aktiem. Ja SPKC ir saņēmis lietotāja kontakttālruni, bet sarunā ar lietotāju tiek noskaidrots, ka nav bijis faktiskais kontakts – tas tiek atzīmēts sistēmā un tālāka saziņa ar šo lietotāju netiek veikta.
Vai datu subjektam ir nodrošinātas tiesības ierobežot savu datu apstrādi atbilstoši Regulas 18.pantam? Ja atbilde ir "jā", norādiet, kādā veidā šīs datu subjekta tiesības tiek nodrošinātas.	Jā ☒ Nē ☐ Šādas tiesības lietotājam tiks nodrošinātas attiecībā uz SPKC sistēmā esošajiem datiem, ja tiks saņemts pamatots lietotāja iesniegums. Šobrīd praksē nav konstatēti reāli gadījumi, kad lietotājs Lietotnes kontekstā šādas tiesības varētu izmantot. Jebkurš šāds pieteikums tiks izvērtēts un risināts individuāli. Attiecībā uz Lietotnē esošo kontaktu fiksēšanu – datu ierobežošana nav paredzēta – jo dati glabājas Lietotnes galiekārtā un lai aizsargātu lietotāju – ne lietotājam, ne SPKC tiem nav piekļuves. Izmaiņas šajos datos ietekmētu

IEROBEŽOTAS PIEEJAMĪBAS INFORMĀCIJA

Ja atbilde ir “nē”, norādiet iemeslus.	Lietotnes darbību un radītu negatīvas sekas (nepamatotu paziņojumu saņemšana un tml.), ja tiktu individuāli mainīts šo datu apstrāde ilgums un veids. Lietotnes darbību Lietotājam ir iespēja pārtraukt – izdzēšot pašu Lietotni vai arī izslēdzot bluetooth funkcijas darbību, ja lietotājs konkrētā laikā nevēlas kontaktu fiksēšanu.
Vai pārzinim ir izstrādāta kārtība attiecībā uz Regulas 19.pantā noteiktā pienākuma realizāciju? Ja nav izstrādāta – Kāpēc?	Jā ☐ Nē ☒ Lietotnes ietvaros saņemto datu pārzinis ir SPKC. Datus nav paredzēts dot citām institūcijām vai trešajām personām. Uz datiem, kas tiek apstrādāti ārpus Lietotnes, tiek piemērotas normatīvo aktu prasības un Lietotnes tvērums uz to neattiecas.
Vai datu subjektam ir nodrošinātas tiesības uz savu datu pārnesamību atbilstoši Regulas 20.pantam? Ja atbilde ir “jā”, norādiet, kādā veidā šīs datu subjekta tiesības tiek nodrošinātas. Ja atbilde ir “nē”, norādiet iemeslus.	Jā ☐ Nē ☒ Saskaņā ar Datu regulas 20.panta 3.punktu tiesības uz datu pārnesamību neattiecas uz apstrādi, kas ir vajadzīga, lai izpildītu uzdevumu, ko veic sabiedrības interesēs vai īstenojot pārzinim likumīgi piešķirtas oficiālas pilnvaras.
Vai datu subjektam ir nodrošinātas tiesības iebilst savu datu apstrādei atbilstoši Regulas 21.pantam? Ja atbilde ir “jā”, norādiet, kādā veidā šīs datu subjekta tiesības tiek nodrošinātas. Ja atbilde ir “nē”, norādiet iemeslus.	Jā ☒ - ciktāl tas attiecas uz lietotāja kopējo izvēles brīvību izmantot Lietotni vai neizmantot. Tiešā veidā Datu regulas 21.pants nav piemērojams, jo Lietotnes izmantošanu kā obligātu pienākumu neparedz normatīvie akti un uz SPKC neattiecas Datu regulas 6.panta f) apakšpunkts par legītimajām interesēm – jo to nepiemēro, pildot publiskas iestādes uzdevumus. Nē ☐ Ja lietotājam ir iebildumi pret Lietotni – lietotājam ir tiesības to neizmantot. Lietotnes izmantošana ir brīvprātīga – lietotājs pats var izvēlēties lietot lietotni vai neliidot. Lietotājam ir tiesības izvēlēties, vai aktivizēt Lietotnē kontaktu fiksēšanu un vai norādīt Lietotnē kontakttālruni. SPKC lietotāja kontakttālruni un informāciju par kontaktu saņem tikai tad, ja lietotājs ir izdarījis minētās izvēles. Ja lietotājs nav aktivizējis bluetooth un nav norādījis kontakttālruni – šādā gadījumā SPKC šo informāciju par lietotāju nesaņem.

III. Risku datu subjekta tiesībām un brīvībām analīze

1. Risku analīze veicama to datu apstrādes darbību kopumam/iem, kas nepieciešams/i norādītā personas datu apstrādes mērķa sasniegšanai, atbilstoši Regulas 35.panta 1.punktam.	
Identificējiet cik pirmajā punktā minēto datu apstrādes kopumu ir Jūsu organizācijā	
DK1	Lietotnes galiekārtā kontaktu fiksēšana (t.sk. kontakta datums, ilgums, signāla stiprums)
DK2	SPKC sistēmā kontakttālruna un kontakta informācijas apstrāde saziņai ar lietotāju iespējamā Covid-19 riska gadījumā

DK3	SPKC sistēmā brīdinājuma paziņojuma aktivizācijas koda, kas piešķirts ar Covid-19 saslimušajam lietotājam, un ar kodu saistītās informācijas (t.sk. koda derīgums, atbildīgais SPKC darbinieks u.c.) apstrāde		
Novērtējiet, cik lielā mērā 1.punktā minētais datu apstrādes kopums/i rada riskus datu subjekta tiesībām un brīvībām. Novērtējiet ietekmi skalā Augsta (A), Vidēja (V), Zema (Z). Sekojiet, lai vairākumā rindu būtu vismaz viens Augsts un viens Zems vērtējums.			
	DK1	DK2	DK3
Informācijas pilnīga vai daļēja atklāšana neautorizētām personām (konfidencialitāte)	Z	V	V
Informācijas neautorizēta labošana (integritāte)	Z	V	Z
Informācijas sistēmas nepieejamība vienu stundu (pieejamība)	Z	Z	Z
Informācijas sistēmas nepieejamība vienu dienu (pieejamība)	V	Z	Z
Identificējiet 10 riska scenārijus, kas var radīt iepriekšējā solī ietvertajā tabulā norādīto ietekmi, kas novērtēta kā Augsta. No visiem scenārijiem iekļaujiet tos, kuri var radīt lielāko ietekmi. Katram scenārijam norādiet, kāda informācija vai informācijas sistēma tiks ietekmēta (vai visas), kādā veidā tas notiks, kāda tieši būs ietekme, kas tieši to uzsāks (darbinieks, neautorizēta persona, dabas spēki, tehnoloģiska kļūda vai tml.). Esiet īsi, bet konkrēti.			
Nevienā no minētajām pozīcijām risks nav vērtējams kā augsts.			
R1 Ja lietotājs atstāj atvērtu Lietotni un galiekārta nonāk trešo personu rīcībā	Trešajām personām var kļūt zināms kontakttālrunis, kas ir norādīts lietotnē un trešajām personām varētu rasties iespēja redzēt vai lietotājam ir/nav aktivizēta kontaktu fiksēšana un, vai lietotājs ir/nav saņēmis brīdinājuma paziņojumu par iespējamo kontaktu ar Covid-19 saslimušu lietotāju. Trešajām personām nebūs iespēja redzēt fiksētos kontaktus – tie tiek glabāti galiekārtā šifrētā veidā un arī pašam lietotājam nav pieejami.		
R2 Ja trešās personas nesakcionēti piekļūst SPKC sistēmai, kur ir norādīts kontakttālrunis	Trešajām personām varētu kļūt zināmi kontakttālruni, kas ir saņemti saziņai ar personām kā potenciālajiem Covid-19 kontaktiem. Trešo personu nesankcionētas piekļuves risks ir risks, ar ko var nākties saskarties jebkurai valsts sektora sistēmai. Lietotnes funkcionalitāte šo risku nepaaugstina un nerada papildus, bet ievērojami samazina, jo Lietotnē apstrādāto datu apjoms ir veidots atbilstoši datu minimizācijas principam un Lietotnes kontekstā netiek apstrādāts lietotāja vārds, uzvārds un tml. Tiešā veidā persona pēc kontakttālruna nav identificējama. No pieejamās informācijas var būt redzams kontakttālrunis, pazīme, ja tas ir pārstāvja kontakttālrunis, informācijas saņemšanas datums, kontakta datums, un provizoriski aprēķinātais pašizolācijas laiks un SPKC norādītais statuss – vai ar personu SPKC ir veikta sazināšanās. No pieejamās informācijas nav iespēja identificēt, ar kuru personu ir radies kontakts, kurā vietā un tieši cikos.		
R3 Ja trešās personas nesankcionēti piekļūst SPKC sistēmai, kur ir informācija par brīdinājuma paziņojuma aktivizācijas kodu	Trešajām personām varētu būt iespēja redzēt piešķirto kodu, koda datumu, saslimšanas datumu, personas šifrētu ID, ko piešķir SPKC (gadījuma numurs) un atbildīgo SPKC darbinieku, koda statusu – vai tas ir aktivizēts un uz kādu tālruni kods ir nosūtīts.		

	Tiešā veidā pēc pieejamiem datiem persona nav identificējama, ja vien trešās personas rīcībā nav papildu informācija par pieejamo kontakttālruni vai SPKC piešķirto šifrēto ID (gadījuma numuru).
R4 Ja SPKC darbinieks sistēmā ievada nepareizu saslimušās personas kontakttālruni (piemēram, kļūdās, to pārrakstot no informācijas, kas saņemta no ārstniecības iestādes)	Aktivizācijas kods šādā gadījumā varētu tikt nosūtīts uz nepareizu kontakttālruni. Ja persona neizmanto Lietotni, šo kodu nebūs iespēja izmantot. Ja persona izmanto Lietotni un apzināti aktivizē kodu (piemēram, jo arī ir apstiprināta kā Covid-19 saslimusī persona) – šī lietotāja kontakti varētu saņemt brīdinājuma informāciju, ja ir bijis kontakts pēdējās 14 dienās. Ja persona lieto Lietotni, bet nav apstiprināta kā Covid-19 saslimusī persona, persona attiecīgi šo kodu neizmantos. Lai tiktu nosūtīts nepamatos paziņojums, būtu jānotiek divu faktoru sakritībai – SPKC būtu jākļūdās tālruņa numurā un personai, kas saņem šo kodu, būtu jāveic apzināti aktīva rīcība par citu informēšanu (lai gan persona zinātu, ka tai nav apstiprināts Covid-19, piemēram, jo nemaz nebūtu veikusi analīzes).
R5 Ja SPKC, veicot saziņu ar iespējamo kontaktu, nepareizi ievada saziņas kontakttālruni	Šādā gadījumā zvanu varētu saņemt persona, kas nelieto lietotni un/vai nav konstatēta kā iespējama kontakts. Sarunas laikā līdzīgi arī standarta procedūras ietvaros tiktu noskaidrots, vai personai kontakts varēja būt reāls – ja personai šāda kontakta iespējamības nav – saruna netiktu turpināta. Personai nerastos sekas un uzreiz sarunas ietvaros būtu iespēja uzzināt, ja tālrunis ir bijis kļūdainš (atbilstoši personas sacītajam SPKC darbinieks uzreiz varētu pats pārbaudīt, vai nav kļūdījies numurā un tālāka saruna netiktu turpināta).
R6 Ja SPKC sistēma pati sāk nesankcionēti ģenerēt aktivizācijas kodus	Šos kodus nevarētu saņemt citas personas, jo, lai saņemtu kodu būtu nepieciešams arī kontakttālrunis, uz kuru kodu nosūtīt. Tālruni saņem no ārstniecības iestādes, ja konkrētai personai ir apstiprināta saslimšanas ar Covid-19.
R7 Ja Lietotne pati sāk nesankcionēti ģenerēt kontaktus un sūta uz SPKC kontakttālruni	SPKC šos kontakttālrunus varētu izmantot saziņai ar lietotājiem – taču to būtu iespēja ātri identificēt, ja vairāki lietotāji pēc kārtas informētu, ka brīdinājuma paziņojumu nav saņēmuši vai nav bijuši ar citiem kontaktā, bet SPKC sistēmā ir ienācis šo personu kontakttālrunis.
R8 Ja dabas stihiju vai citu ārkārtas apstākļu rezultātā tiek bojāta SPKC sistēma, kur ir kontakttālrunis	SPKC varētu rasties ierobežota iespēja saņemt informāciju par pieejamiem Covid-19 kontaktiem. SPKC šo procesu varētu veikt manuālā veidā, izmantojot esošos manuālo kontaktu apzināšanas risinājumus
R9 Ja dabas stihiju vai citu ārkārtas apstākļu rezultātā tiek bojāta SPKC sistēma, kur ir aktivizācijas kods (piemēram, nevar tehniski nosūtīt aktivizācijas kodu)	Lietotāja, kam ir apstiprināta Covid-19 saslimšana, šo kodu varētu nebūt iespēja saņemt īsziņas veidā. Taču SPKC būtu iespēja to darīt zināmu citā veidā, piemēram, nosaucot, manuālā saziņas procesā caur kontakttālruni. Ja arī tas nebūtu iespējams, SPKC ir iespēja manuāli sazināties ar lietotāju un manuālā veidā esošā procesa ietvaros apzināt iespējamus Covid-19 kontaktus. Tas varētu prasīt SPKC resursus – taču neizslēdz kopējās personu tiesības uz informācijas saņemšanu, ja ir iespējams inficēšanās risks.

R10 Ja dabas stihiju vai citu ārkārtas apstākļu rezultātā tiktu bojāta Lietotnes darbība		Lietotājiem, kas izmanto kontaktu fiksēšanu, varētu rasties traucējumi kontaktu fiksēšanā un attiecīgi par to varētu netikt nosūtīts paziņojums, ja kontakts ar Covid-19 saslimušu personu netiktu fiksēts. Paralēli Lietotnei SPKC saglabātos iespēja veikt kontaktu apzināšanu manuālā veidā – attiecīgi faktiskā kontaktu apzināšana varētu prasīt resursus – tomēr šī iespēja nebūtu pilnībā izslēgta.		
Novērtējiet riskus:		Kopējais risks ir vērtējams kā zems		
Novērtējiet relatīvo risku ietekmi uz organizāciju skalā no 6 līdz 10. Piešķiriet 10 riskam, kurš iestāšanās gadījumā datu apstrādi ietekmēs visvairāk. Piešķiriet 6 riskam, kurš iestāšanās gadījumā datu apstrādi ietekmēs vismazāk. Novērtējiet relatīvo risku varbūtību skalā no 1 līdz 5. Piešķiriet 1 riskam, kura iestāšanās varbūtība ir mazākā. Piešķiriet 5 riskam, kura iestāšanās varbūtība ir lielākā. Sareiziniet ietekmi un varbūtību un ierakstiet riska vērtējumu kolonnā. Kolonnā prioritāte ierakstiet 1 riskam ar lielāko vērtību un secīgi līdz 10 – riskam ar mazāko vērtību.				
	Ietekme	Varbūtība	Riska vērtējums	Prioritāte
R1 Ja lietotājs atstāj atvērtu Lietotni un galiekārta nonāk trešo personu rīcībā	6	3	18	2a
R2 Ja trešās personas nesakcionēti piekļūst SPKC sistēmai, kur ir kontakttālrunis	8	2	16	3
R3 Ja trešās personas nesankcionēti piekļūst SPKC sistēmai, kur ir informācija par brīdinājuma paziņojuma aktivizācijas kodu	7	2	14	4c
R4 Ja SPKC darbinieks sistēmā ievada nepareizu saslimušās personas kontakttālruni (piemēram, kļūdās, to pārrakstot no informācijas, kas saņemta no ārstniecības iestādes)	8	3	24	1
R5 Ja SPKC, veicot saziņu ar iespējamo kontaktu, nepareizi ievada saziņas kontakttālruni	6	3	18	2b
R6 Ja SPKC sistēma pati sāk	7	1	7	6a

IEROBEŽOTAS PĪEEJAMĪBAS INFORMĀCIJA

nesankcionēti ģenerēt aktivizācijas kodus				
R7 Ja Lietotne pati sāk nesankcionēti ģenerēt kontaktus un sūta uz SPKC kontakttālruni	7	1	7	6b
R8 Ja dabas stihiju vai citu ārkārtas apstākļu rezultātā tiek bojāta SPKC sistēma, kur ir kontakttālrunis	7	2	14	4a
R9 Ja dabas stihiju vai citu ārkārtas apstākļu rezultātā tiek bojāta SPKC sistēma, kur ir aktivizācijas kods (piemēram, nevar tehniski nosūtīt aktivizācijas kodu)	6	2	12	5
R10 Ja dabas stihiju vai citu ārkārtas apstākļu rezultātā tiktu bojāta Lietotnes darbība	7	2	14	4b
Identificējiet esošos riska mazināšanas pasākumus	Lietotnes uzturēšanā ir piesaistīts apstrādātājs - LVRTC, kas sniegs profesionālu atbalstu Lietotnes un SPKC sistēmas darbības drošībai. SPKC darbiniekiem jau līdzšinējo procesu ietvaros ir pieredze ar personas datu aizsardzības jautājumiem un attiecīgi ir iemaņas darbā, lai dati tiktu apstrādāti iespējami precīzā veidā (samazinātos risks datu ievades kļūdām)			
Vai ir izstrādāti personas datu apstrādes aizsardzības noteikumi?	Jā ☒ Nē ☐			
Kādā kārtībā darbiniekus informē par pienākumu neizpaust personas datus (tostarp pēc darba, dienesta vai citu tiesisko attiecību izbeigšanās)? Kā tiek kontrolēta šā pienākuma ievērošana?	Pienākums neizpaust ir paredzēts darba attiecības reglamentējošos dokumentos. Ar darbiniekiem tiek veiktas regulāras sarunas, lai uzklautu darbiniekus un pilnveidotu procesus un risinātu jautājumus datu drošības īstenošanai atbilstoši praksē sastopamajām situācijām.			
Par informācijas resursiem, tehniskajiem resursiem un personas datu aizsardzību atbildīgā persona	Atbildīgās personas ir noteiktas.			
Kādi personas datu aizsardzības pasākumi tiek piemēroti informācijas tehnoloģijām?	Tiek veikti tehniski un organizatoriski drošības pasākumi, kas nodrošina personas datu drošību, tostarp aizsardzību pret neatļautu vai nelikumīgu piekļuvi.			

IEROBEŽOTAS PIEEJAMĪBAS INFORMĀCIJA

	Pieļauve SPKC sistēmā ir tikai tam pilnvarotām personām. Pieļauve SPKC sistēmas servera telpām ir tikai tam pilnvarotām personām
Raksturojiet aizsardzības pasākumus, kas ir ieviesti pēc neautorizētas un prettiesiskas piekļuves personas datiem, kas ir apstrādāti automatizēti vai manuāli	Līdz šim attiecībā uz Lietotni nav konstatēti neautorizēti un prettiesiski piekļuves mēģinājumi.
Vai ģpašo kategoriju personas datu apstrādei ir noteikts lielāks (augstāks) datu aizsardzības līmenis? Ja atbilde ir "jā", raksturojiet noteikto aizsardzības līmeni	Jā ☒ Nē ☐ SPKC sistēmā, kurā tiek apstrādāti Lietotnes dati, netiek apstrādāti identificējami ģpašas kategorijas personas dati. Identificējami dati par personām, kas ir saslimušas ar Covid-19, - vārds, uzvārds un tml. – tiek glabāti ārpus SPKC sistēmas un nav saistīti ar Lietotni.
Vai pārzinim ir izstrādāti informācijas sistēmu drošības noteikumi?	Jā ☒ Nē ☐
Vai ir noteiktas par informācijas sistēmu drošības pārvaldību un īstenošanu atbildīgās personas?	Jā ☒ Nē ☐
Vai iestādē tiek veikta informācijas sistēmu risku analīze?	Jā ☒ Nē ☐
Vai pārzinis ir izstrādājis informācijas sistēmu piekļuves kontroles procedūras? Ja atbilde ir "jā", kā iestāde pārvalda informācijas sistēmu lietotāju kontus?	Jā ☒ Nē ☐ Pieļauve SPKC sistēmā ir tikai tam pilnvarotām personām.
Kādas ir prasības lietotāju kontu parolēm vai citiem kontu aizsardzības rīkiem?	Prasības tiek noteiktas saskaņā ar normatīvajiem aktiem informācijas drošības jomā
Vai ir noteikti pienākumi informācijas sistēmu lietotājiem? Kādi?	Jā ☒ Nē ☐ Pieļauve SPKC sistēmā ir tikai tam pilnvarotām personām. Personām ir aizliegts veikt darbības, kas var radīt nesankcionētu piekļuves nonākšanu trešo personu rīcībā.
Vai pārzinis ir veicis drošības apmācība personālam, kas veic datu apstrādi informācijas sistēmās? Cik bieži minētā drošības apmācība tiek veikta, kāds ir tās saturs?	Jā ☒ Nē ☐

IEROBEŽOTAS PĪEEJAMĪBAS INFORMĀCIJA

	SPKC ir personas datu aizsardzības speciālists. SPKC darbiniekiem ir iespēja sazināties pēc nepieciešamības ar SPKC personas datu aizsardzības speciālistu un saņemt atbalstu personas datu apstrādes un drošības jautājumos. Papildu apmācības SPKC darbiniekiem tiek veiktas periodiski pēc nepieciešamības. Apmācībās tiek ietverti praktiskie datu apstrādes un drošības jautājumi, kas ir piemēroti SPKC darba specifikai.
Vai pārzinis pirms informācijas sistēmas nodošanas ekspluatācijā veic drošības atbilstības pārbaudi? Ja atbilde ir "jā", norādiet pārbaudes norises kārtību	Jā ☒ Nē ☐ Tiek veiktas drošības pārbaudes. Tiek sagatavots apraksts (angļu val. tā saucamais - Whitepaper), kurā būs ietverts kopsavilkums par drošības testēšanu.
Vai pārzinis ir izstrādājis informācijas sistēmas uzturēšanas kārtību un procedūras?	Jā ☒ Nē ☐
Vai pārzinis ir nodrošinājis informācijas sistēmas notikumu reģistrēšanu un monitorēšanu? Raksturojiet kārtību	Jā ☒ Nē ☐
Vai pārzinis nodrošina datu rezerves kopiju veidošanu un pārbaudi? Raksturojiet kārtību	Jā ☒ Nē ☐
Vai pārzinis izmanto ārējas informācijas sistēmas, kas savienotas ar pārziņa informācijas sistēmām? Ja atbilde ir "jā", kāda ir kārtība un nosacījumi, saskaņā ar kuriem izveido sadarbību ar citām iestādēm?	Jā ☒ EFGS Nē ☐
Kādas tehnoloģijas un rīki tiek izmantoti, lai savienotu sistēmas?	Detalizēta informācija par resursiem ir ietverta Lietotnes infrastruktūras diagrammā (detalizēta fiziskās arhitektūras shēmā).
Vai pārziņa informācijas sistēmām var piekļūt attālināti? Ja atbilde ir "jā", kāda ir attālinātas piekļuves procedūra un nosacījumi?	Jā ☐ Nē ☐ Jautājums neattiecas
Vai pārzinim ir noteikta kārtība ārējo atmiņas ierīču pārvaldībai un lietošanai?	Jā ☐ Nē ☐ Jautājums neattiecas.
Vai informācijas sistēmās tiek izmantota datu šifrēšana? Ja atbilde ir "jā", raksturojiet to	Jā ☒ Nē ☐

IEROBEŽOTAS PĪEEJAMĪBAS INFORMĀCIJA

	Lietotnes ietvaros fiksētie kontakti tiek glabāti šifrētā veidā – ne lietotājam, ne SPKC tie nav pieejami. SPKC sistēmā tiek apstrādāti tikai minimāli nepieciešami dati – netiek apstrādāts personas vārds, uzvārds un tml. Lai personu varētu identificēt pēc kontakttālruņa vai SPKC piešķirtā saslīmušās personas ID (gadījuma numura) – trešās personas rīcībā ir nepieciešama papildu informācija. Bez šādas informācijas personas vārds, uzvārds un tml. nav zināms no SPKC sistēmas, kurā tiek apstrādāti Lietotnes dati.	
Vai pirms informācijas publiskošanas tiek izvērtēts tās konfidencialitātes līmenis un iespējamie riski?	Jā ☒ Lietotnes informāciju nav paredzēts publiskot Nē ☐	
Vai pārzinis ir izstrādājis incidentu pārvaldības kārtību un procedūras?	Jā ☒ Nē ☐	
Vai pārzinis ir izstrādājis kārtību atklāto trūkumu novēršanai?	Jā ☒ Nē ☐	
Vai ir izstrādāti iekšējie noteikumi personas datu nodošanai valstīm, kas nav Eiropas Savienības vai Eiropas Ekonomikas zonas dalībvalstis? Ja atbilde ir "jā", raksturojiet tajos ietvertos principus. Ja atbilde ir "nē", norādiet, kādēļ šādi noteikumi nav izstrādāti	Jā ☐ Nē ☒ Lietotnes datus nav paredzēts nodot uz valstīm ārpus Eiropas Savienības.	
<i>Attiecībā uz riskiem ar prioritāti 1, 2 un 3 aprakstiet būtiskākos šobrīd organizācijā veiktos organizatoriskos un tehniskos kontroles pasākumus, kas samazina šo risku potenciālo ietekmi uz organizāciju vai risku iestāšanās varbūtību. Aprakstiet gan tādus pasākumus, kas novērš riska iestāšanos, gan tādus, kas atklāj riska iestāšanās faktu, gan arī tādus, kas novērš riska ietekmes radītās sekas.</i>		
Konstatēto risku prioritāte: [1]Ja SPKC darbinieks sistēmā ievada nepareizu saslīmušās personas kontakttālruni (piemēram, kļūdās, to pārrakstot no informācijas, kas saņemta no ārstniecības iestādes) [2a]Lietotājs atstāj atvērtu Lietotni un galiekārta nonāk trešo personu rīcībā [2b]Ja SPKC, veicot saziņu ar iespējamo kontaktu, nepareizi ievada saziņas kontakttālruni [3]Ja trešās personas nesakcionēti piekļūst SPKC sistēmai, kur ir kontakttālrunis	Apraksts	Riski
K1Manuāli ievadītās informācijas papildu pārbaude	SPKC darbiniekam ir pienākums pārliecināties, ka ievadītā informācija	[1] [2b]

IEROBEŽOTAS PIEEJAMĪBAS INFORMĀCIJA

	ir korekta – attiecīgi salīdzinot vēlreiz saņemto informāciju pret SPKC sistēmā ievadīto informāciju	
K2 Ieklausīšanās saņemto informāciju teiktajā	Ja sarunas gaitā personas sniegtā informācija norāda uz iespējamu informācijas (kontakttālrunā) kļūdu, SPKC darbiniekam ir pienākums uzklaut personu un neturpināt sarunu, kamēr nav gūta pārliecība, ka informācija ir korekta. Tiek piemērots personas uzklautāšanas, nevis pārliecināšanas princips (ka informācija ir pareiza)	[1] [2b]
K3 Lietotāju informēšana par pienākumu parūpēties par galiekārtu drošību	Lietotnes noteikumos ir ietverta norāde, ka lietotājam ir pienākums aizsargāt savu galiekārtu, izmantojot pieejamos galiekārtas ekrāna aizsardzības risinājumus, un laiku pa laikam tos mainīt, īpaši, ja tie var būt kļuvuši zināmi citai personai, piemēram, ekrāna piekļuves kods un tml. SPKC nesaņem un neapstrādā Lietotāja izmantotās galiekārtas aizsardzības informāciju.	[2a]
K4 SPKC sistēmas auditācija pierakstu analīze	Tiek veikta SPKC sistēmas auditācijas pierakstu analīze, lai laikus varētu konstatēt, ja SPKC	[1] [2b] [3]

IEROBEŽOTAS PIEEJAMĪBAS INFORMĀCIJA

	sistēmai ir mēģinājums piekļūt nesankcionētā veidā	
K5 SPKC darbinieku periodiskas apmācības	Periodiski atgādinājumi ar praktiskiem risku piemēriem SPKC darbiniekiem, lai pievērstu uzmanību, cik būtiski ir droši aizsargāt SPKC sistēmai piešķirtās piekļuves	[3]
K6 SPKC darbinieku pārrunas	Praktiskas periodiskas pārrunas ar SPKC darbiniekiem, lai laikus uzklautu par praktiskām problēmsituācijām, ar ko saskaras SPKC darbinieki, izmantojot SPKC sistēmu un attiecīgi, lai laikus to varētu risināt un novērst.	[3]
K7 Tīrā galda un slēgtā ekrāna princips	Pabeidzot darbu, SPKC darbiniekam ir pienākums sakārtot galdu, uz kura atrodas par personām saņemtā informācija, un slēgt ekrānu (Ctrl+alt+delete), lai pie informācijas nevarētu piekļūt citas personas	[3]
K8 Veicot informācijas ievadi – darboties tikai vienā reizē ar viena lietotāja jautājumu	Lai novērstu datu savstarpējo sajukumu – veicot datu ievadi un/vai saziņu ar lietotāju, SPKC darbiniekam ir pienākums vienā reizē strādāt tikai ar viena lietotāja informāciju	[1] [2b]
K9Uzticamības veicināšana – nekavējoties ziņot par drošību atbildīgajam SPKC darbiniekam, ja ir konstatēts iespējamais datu apstrādes pārkāpums	Kopējās uzticamības kultūras veicināšana, lai par iespējamo kļūdu SPKC darbinieks varētu ziņot, nebaidoties no neadekvāta soda - jo tas var	[1] [2b] [3]

	samazināt ziņojumu skaitu un ilgtermiņā radīt iestādei daudz būtiskākas sekas	
K10 Nekavējoties informēt datu subjektus, ja datu drošība var to interesēm radīt augstu risku	Izskatot atsevišķa lietotāja pieteikto datu drošības jautājumu - pārbaudīt to pret kopējo SPKC sistēmas darbību, lai pārliecinātos, ka tas negatīvi neskar citu lietotāju tiesības. Ja tiek konstatēts augsts risks – nekavējoties par to informēt citus lietotājus.	[1] [2a] [2b] [3]
Riska mazināšanas pasākumu plāns		
<i>Nosakiet nākošās risku analīzes veikšanas datumu un izveidojiet plānu ar pasākumiem, kurus paredzat veikt līdz nākošajai riska analīzei. Šiem pasākumiem ir jāspēj mazināt vismaz viens no riskiem ar prioritāti 1, 2 vai 3. Vēlams izvēlēties potenciālās ietekmes ziņā lietderīgāko (cenas/ietekmes attiecības ziņā) piedāvājumu. Dodiet priekšroku īsā laikā īstenojamiem pasākumiem, kas var būtiski samazināt risku pēc iespējas lielākam būtisko informācijas sistēmu skaitam. Apsveriet arī esošo, iepriekšējā solī identificēto pasākumu uzlabošanas vai pilnveidošanas iespējas. Sakārtojiet izpildes prioritāšu secībā.</i>		
P1 2020.gada maijs - augusts	SPKC darbinieku informēšana, praktiskās apmācības un atbalsta sniegšana darbā ar Lietotni un SPKC sistēmu. Konstatēto praktisko problēmsituāciju uzskaitē un risināšanas plāna izstrādē atbilstoši veicamo pasākumu būtībai un prioritātei	
P2 2020.gada maijs - augusts	SPKC sistēmas auditācijas pierakstu papildu uzraudzība, lai pārliecinātos, ka SPKC sistēmā darbojas pareizi pieslēgšanās vai atslēgšanās no sistēmas, datu atlasī, kā arī konta izveidi, grozīšanu vai dzēšanu, fiksējot notikuma laiku, kas sakrīt ar faktiskā notikuma koordinēto pasaules laiku (UTC), interneta protokola adresi, no kuras veikta darbība, aprakstu, kā arī informāciju par darbības iniciatoru – identifikatoru, pieslēguma metadatus	

IV. Ieteikumi trūkumu novēršanai

Datu aizsardzības speciālista komentāri, ja tādi ir	Nepieciešams veikt papildu Novērtējumu un pārskatīt šo Novērtējumu, ja tiek īstenota Lietotnes 2.kārta un tajā tiek paredzēta jauna personas datu apstrāde un/vai risinājumi, kas maina esošo Lietotnes saturu personas datu apstrādes jomā
Secinājumi un konstatētie trūkumi	Kopumā Lietotnes izstrādē ir ievēroti Datu regulas 5.pantā minētie datu apstrādes principi, tostarp datu minimizācija un pārredzamība.

IEROBEŽOTAS PIEEJAMĪBAS INFORMĀCIJA

			Lietotnes izstrādē ir ņemts vērā arī lietotāja privātam draudzīgs risinājums – by design un by default – paredzot, ka izvēli par Lietotnes izmantošanu izdara pats lietotājs un lietotājam ir iespēja Lietotnes funkcionalitāti pēc savas izvēles īstenot pilnā apjomā vai daļēji (piemēram, aktivizēto kontaktu fiksēšanu, bet nenorādīt kontakttālruni saziņai ar SPKC). Šobrīd nav konstatējami trūkumi, kam būtu nepieciešami papildu pasākumi.
Ieteikumi	trūkumu	novēršanai	Rekomendācija - turpināt Lietotnes 2.kārtu – lai attiecīgi Lietotnes mērķi būtu iespēja sasniegt vēl pilnīgāk un attiecīgi lietotājiem būtu plašākas Lietotnes izmantošanas iespējas.
Termiņš	trūkumu	novēršanai	Rekomendācija - Lietotnes 2.kārtu īstenot 2020.gada ietvaros.
Nepieciešamība veikt iepriekšēju apspriešanos ar uzraudzības iestādi atbilstoši Regulas 36.pantam.			Jā ☐ Nē ☒ Lietotnes izstrādes ietvaros Lietotnes ideja tika apsvērta arī ar Datu valsts inspekciju un tika ņemts vērā Datu valsts inspekcijas sniegtais viedoklis. Novērtējuma ietvaros nav konstatēts, ka Lietotne varētu radītu personu tiesībām un brīvībām augstu risku. Sadarbības ietvaros Novērtējums tiek nosūtīts arī Datu valsts inspekcijai.

Novērtētājs Vārds, uzvārds, amats