ITIESĪBAS

Datu aizsardzība 07:00, 5. Jūn. 2020

Mobilās lietotnes nedrīkst iejaukties privātumā

Ieva Andersone, ZAB "SORAINEN", zvērināta advokāte, LL.M

https://www.itiesibas.lv/raksti/komercdarbiba/datu-aizsardziba/mobilas-lietotnes-nedrikst-iejaukties-privatuma/17057

Tehnoloģiju uzņēmumi gan pasaulē, gan Latvijā ziņo par plāniem attīstīt mobilās lietotnes, kas palīdzētu noskaidrot un izsekot Covid-19 kontaktpersonas. Viena no pirmajām valstīm pasaulē, kas izstrādājusi kontaktu izsekošanas mobilo lietotni, ir Singapūra. Arī citas valstis visā pasaulē pandēmijas apkarošanā izvērtē iespēju izmantot mūsdienu tehnoloģijas. Skaidrs, ka šādu mobilo lietotņu veiksmīga darbība sniegtu būtisku ieguldījumu sabiedrības veselības aizsardzībā, tomēr vienlaikus to lietošana bez atbilstošas uzraudzības un drošības pasākumiem var radīt būtiskus riskus iedzīvotāju privātumam un cilvēktiesībām.

Raksta līdzautore: Lūcija Strauta, ZAB "SORAINEN" jurista palīdze

Šajā rakstā īsi aplūkosim būtiskākos datu aizsardzības noteikumus, kas jāievēro, lai lietotņu izmantošana neradītu bažas par iejaukšanos privātumā. Analizēsim arī jaunās Eiropas Komisijas (EK) Vadlīnijas mobilo lietotņu izstrādātājiem.

Lietotņu darbības veids un ietekme uz privātumu

Lietotņu izveidē plānots izmantot tādus tehnoloģiskos risinājumus kā *bluetooth* un globālās pozicionēšanas sistēmu (GPS), ar ko iespējams iegūt datus par laiku un attālumu, kādā mobilo tālruņu lietotāji atradušies viens no otra. Tādējādi, ja kādai personai tests uzrādītu pozitīvu Covid-19 rezultātu, lietotne atpazītu visas slimnieka kontaktpersonas un automātiski tām ziņotu par nepieciešamību pašizolēties un veikt testu.

Šāda lietotne būtiski paātrinātu kontaktpersonu apzināšanu un informēšanu, kas šobrīd vairumā valstu notiek sarežģītā epidemioloģiskās izmeklēšanas procesā, epidemiologiem pašiem iegūstot informāciju par slimnieka gaitām un satiktajiem cilvēkiem. Tā kā izmeklēšanas pamatā ir slimnieka atmiņa un spējas atcerēties, kādas vietas viņš apmeklējis un ar ko ticies, šāds process ir smagnējs un lēns. Turklāt epidemiologiem pašiem jāsazinās un jāinformē kontaktpersonas. Kā izpētījuši speciālisti, lai kontaktu izsekošanas lietotnes darbotos efektīvi, nepieciešams, lai tās lietotu vismaz 50% sabiedrības.

Lejuplādējot tālrunī jebkuru mobilo lietotni, ikreiz jāapzinās, ka šī vienkāršā darbība var ietekmēt mūsu privātumu. Parasti lietotnēm pievienoti detalizēti privātuma noteikumi, taču retajam ir laiks un pacietība tos lasīt un iedziļināties. Tomēr tad, ja lietotne tiecas piekļūt mūsu ikdienas gaitu un kontaktu lokam tiešā nozīmē, ir vērts iepriekš apdomāt un saprast, kādos apstākļos un ciktāl tas būtu vai nebūtu pieļaujams.

Jautājumos, kas attiecas uz privātuma aizsardzību un personas datu apstrādi, visā Eiropā pašlaik ir spēkā vienots regulējums – Eiropas Parlamenta un Padomes regula 2016/679 jeb Vispārīgā datu aizsardzības regula (Regula). Tādēļ arī atbildes, kādos apstākļos un kādā veidā jaunās mobilās lietotnes drīkstētu piekļūt personas datiem, sākotnēji jāmeklē Regulā. Svarīgākais ir saprast, kas šādā situācijā būtu personas datu apstrādes pamats, jo ikvienai datu apstrādei jānotiek, pamatojoties uz kādu no Regulā noteiktajiem pamatiem.

Ja lietotnē izmantotie dati ir pilnībā anonimizēti

Ja mobilā lietotne vāc anonimizētus datus, ko izmanto apkopotā veidā, lai pētītu un prognozētu ar vīrusa izplatīšanos saistītus aspektus, Regulas ietvaros tā nav uzskatāma par personas datu apstrādi, līdz ar to datu aizsardzības principi anonīmas informācijas apstrādei nav jāpiemēro.

Par anonīmu uzskatāma informācija, kas nav attiecināma uz identificētu fizisku personu, kā arī personas dati tiek sniegti tādējādi, ka personu, par kuru vāc datus, nav iespējams identificēt nekādiem līdzekļiem, proti, apstrādājot mobilās lietotnes datus, ne ar kādiem līdzekļiem vairs nav iespējams noteikt, tieši no kuras personas ierīces informācija nākusi. Ja, apstrādājot datus, tomēr iespējams identificēt konkrētu fizisku personu un dati ir izsekojami, tad tie nav anonimizēti dati, bet gan pseidonimizēti dati, tas ir, informācija, kas attiecināma uz netieši identificējamām personām, pastāvot iespējai iegūt konkrētu personu.

Identificējamu personu datu apstrāde

Ja dati nav anonimizēti un pēc tiem iespējams identificēt konkrētu personu, piemērojami datu apstrādes principi. Atbilstoši Regulai datus iespējams apstrādāt tikai tad, ja pastāv kāds no Regulas 6. pantā minētajiem datu apstrādes pamatiem. Viens no tiem ir mobilās lietotnes lietotāja skaidra un nepārprotama piekrišana, taču datu apstrāde pieļaujama arī bez tās. Proti, kā piemēroti datu apstrādes pamati šajā situācijā varētu būt arī Regulas 6.panta 1. punkta d) vai e) apakšpunkti – vajadzība aizsargāt datu subjekta vai citas fiziskas personas vitālas intereses vai uzdevums, kas jāveic sabiedrības interesēs.

Pandēmijas seku mazināšana un rūpes par sabiedrības veselību un drošību, visticamāk, uzskatāmas par atbilstošām sabiedrības interesēm, turklāt, vērtējot plašākā mērogā, epidēmijas izplatīšanās mazināšana aizsargātu gan mobilās lietotnes lietotāja, gan citu fizisku personu vitālās intereses. Regulas preambulas 41. apsvērumā paredzēts, ka juridisks pamats var pastāvēt bez atsevišķa tiesiska regulējuma, ja vien tas ir skaidrs un precīzs un personas, uz kurām tas attiecināms, spēj saprast tā piemērošanu. Turklāt preambulas 46. apsvērums pat konkrēti norāda, ka svarīgas sabiedrības intereses un datu subjekta vitālajās intereses var ietvert epidēmiju un to izplatīšanās monitoringu.

Datu drošība un pārskatāmība

Neatkarīgi no datu apstrādes mērķa un tiesiskā pamata mobilo lietotņu izstrādātājiem jānodrošina datu apstrādes pārskatāmība un drošība. Pārskatāmība nozīmē, ka datu subjektiem ir saprotams, kādi personas dati tiek iegūti un kādas apstrādes darbības tiek veiktas. Vienlaikus šie dati jāapstrādā ar tehnoloģiskām un organizatoriskām metodēm, kas atbilst datu drošības riskiem un samazina to iestāšanās iespējamību. Datu drošības riski ir, piemēram, neatļauta vai nelikumīga apstrāde, nejauša nozaudēšana, iznīcināšana vai sabojāšana, neatļauta izpaušana vai piekļuve.

Atbilstoši apstrādes pasākumi ir būtiski, lai novērstu riskus un nepieļautu kaitējuma radīšanu datu subjektiem, tostarp svarīgi nodrošināt, lai mobilo lietotņu apkopotajiem datiem, īpaši, ja tie nav anonīmi, var piekļūt tikai šaurs, precīzi noteiktu personu loks un tie netiek uzglabāti ilgāk, nekā obligāti nepieciešams mērķa sasniegšanai.

Eiropas Komisijas vadlīnijas

Šomēnes EK, reaģējot uz Eiropas valstu izrādīto iniciatīvu veidot nacionālas mobilās lietotnes Covid-19 izplatības ierobežošanai, publicējusi Vadlīnijas mobilo lietotņu izstrādātājiem. Vadlīnijās ieteiktas prasības lietotņu tehniskajiem risinājumiem, pārrobežu sadarbībai, kiberdrošībai un iegūstamo datu kritērijiem. Tajās noteiktas četras pamatnostādnes, kas jāievēro nacionālo mobilo lietotņu veidotājiem:

- mobilo lietotņu lejupielādei jābūt personas brīvai izvēlei;
- mobilās lietotnes kvalitāte un atbilstība jāapstiprina atbildīgajai valsts institūcijai veselības aizsardzības jomā;
- mobilai lietotnei datu apstrādē jānodrošina datu šifrēšana;
- līdz ar datu apstrādes pamata izbeigšanos jānodrošina nekavējoša datu dzēšana.

Vadlīnijās paredzēts, ka mobilajām lietotnēm jāiegūst dati, kas derīgi epidemioloģiskajai izmeklēšanai, piemēram, lietotnei jāiegūst informācija, lai noteiktu kontaktpersonas, kas slimnieka klātbūtnē uzturējušās pietiekami ilgi, lai inficētos. Dažādu lietotņu izstrādātājiem jārūpējas, lai lietotnes būtu savstarpēji "draudzīgas" un spētu izsekot vīrusa izplatībai starp dažādu lietotņu izmantotājiem. Tāpat mobilajām lietotnēm jābūt ar tādām tehnoloģiskām prasībām, lai arī vienkāršu modeļu telefonu lietotāji tās varētu izmantot, aptverot iespējami lielāku sabiedrības daļu izmantotāju lokā. Vadlīnijās uzsvērta iekļaujamība (*inclusiveness*), kas ir nepieciešamība rūpēties, lai kontaktu izsekošanā ietvertu arī tādas sabiedrības grupas kā mazi bērni, seniori un medicīnas darbinieki, kuri nelieto vai ikdienas gaitās pastāvīgi nenēsā mobilos telefonus, paredzot tiem speciālus tehniskus risinājumus, piemēram, vienkāršas aproces.

Vadlīnijās paredzēts, ka datiem jābūt šifrētiem, lai nebūtu iespējams uzzināt, kura persona ir Covid-19 pozitīva un nenotiktu personu stigmatizācija. Vadlīnijas norāda uz diviem datu glabāšanas veidiem:

- decentralizētu datu glabāšanu, kad dati saglabājas mobilajā ierīcē;
- centralizētu datu glabāšanu serverī.

Tā kā datu glabāšana serverī saistīta ar paaugstinātu risku, ieteicams izvēlēties datus glabāt mobilajā ierīcē. Tomēr tad, ja dati tiek glabāti serverī, servera turētājs drīkst būt tikai valsts institūcija. Lietotnei un serverim jābūt aizsargātiem pret uzbrukumiem un ļaunprātīgu izmantošanu. Lai novērstu nepatiesu paziņojumu izsūtīšanu, jāparedz, ka saslimšanas gadījumu sistēmā drīkst apstiprināt tikai atbildīgās medicīnas iestādes darbinieks.

Ja personu kontaktu izsekošanas lietotne vāc un glabā datus par personu atrašanās vietu un pārvietošanās maršrutu, rodas datu apstrādes pārkāpums, jo netiek ievērots datu minimizācijas princips. Lai apzinātu personas, kas bijušas kontaktā ar Covid-19 slimnieku, nepieciešama informācija tikai par personu atrašanos tuvumā un kontakta ilgumu, nevis pastāvīga personas atrašanās vietas noteikšana. Tādējādi Vadlīnijās paredzēts, ka mobilo lietotņu izstrādātājiem rūpīgi jāizvērtē, kādu informāciju vākt un kāda informācija nav nepieciešama.

Kopsavilkums

Apkopojot minēto, svarīgi uzsvērt, ka par personu privātuma aizsardzību mobilo lietotņu izstrādātājiem jādomā jau datu apstrādes sākotnējā stadijā, piemērojot integrētas datu aizsardzības (*privacy by design)* principu un datu aizsardzību pēc noklusējuma (*privacy by*

default), kā arī izstrādes procesā jāapsver, vai veikt novērtējumu par ietekmi uz datu aizsardzību, apzinot visus riskus, ko plānotā datu apstrāde rada personu tiesībām uz privāto dzīvi.

Ja šādas lietotnes tiks piedāvātas sabiedrībai, pirms mobilās lietotne lejupielādes ikvienam ieteicams izlasīt privātuma noteikumus un saprast, kādus datus lietotne iegūs, kādā veidā tā piekļūs datiem un tos vāks, kā dati tiks izmantoti un kam tie būs pieejami. Svarīgi noskaidrot arī lietotnes izstrādātāja vai piedāvātāja reputāciju un, ja iespējams, tā iepriekšējo rīcību datu aizsardzības jomā, proti, vai tā darbībā bijuši kādi būtiski pārkāpumi. Tādējādi tiktu nodrošināts, ka sasniegts lietotņu mērķis – sabiedrības un mūsu katra veselības aizsardzība, vienlaikus iespējami respektējot personu tiesības uz privātumu.