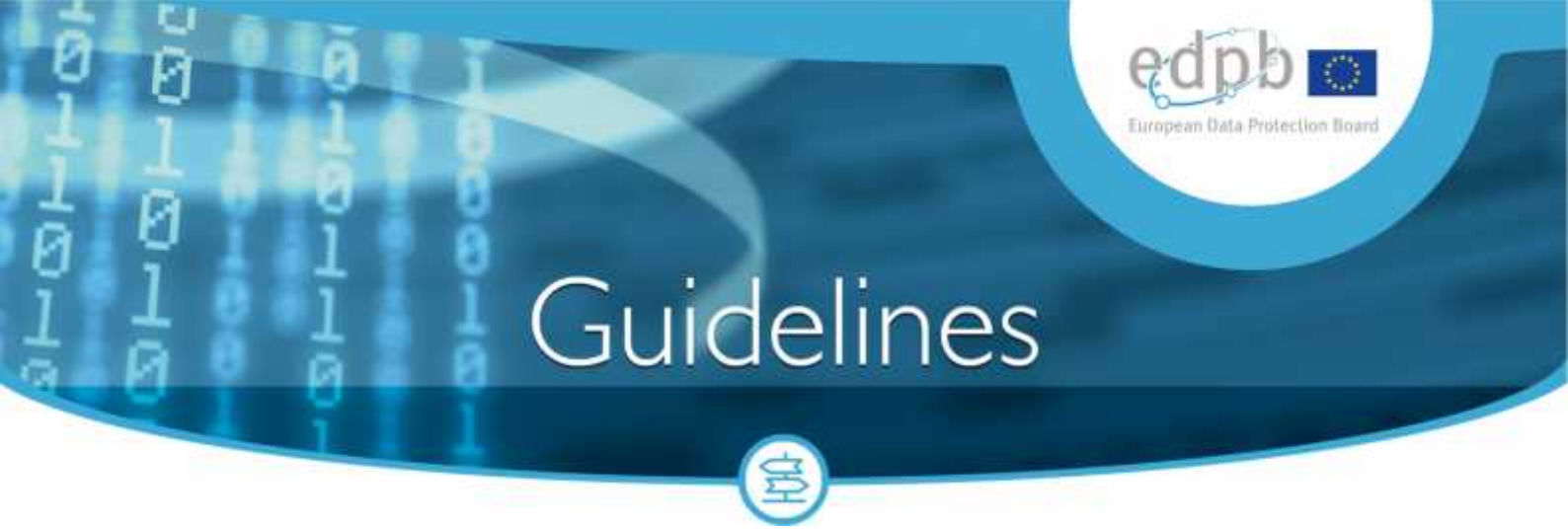

Smjernice 4/2020 o upotrebi podataka o lokaciji i alatima za praćenje kontakata u kontekstu pandemije bolesti COVID-19

donesene 21. travnja 2020.

Translations proofread by EDPB Members.
This language version has not yet been proofread.

Doneseno

Povijest verzija

Verzija 1.1.	5. svibnja 2020.	Manji ispravci
Verzija 1.0.	21. travnja 2020.	Donošenje smjernica

Sadržaj

Sadržaj 3
1. Uvod i kontekst 4
2. Upotreba podataka o lokaciji 6
2.1. Izvori podataka o lokaciji 6
2.2. Naglasak na upotrebi anonimiziranih podataka o lokaciji 6
3. Aplikacije za praćenje kontakata 8
3.1. Općenita pravna analiza 8
3.2. Preporuke i funkcionalni zahtjevi 10
4. Zaključak 11
Prilog – Aplikacije za praćenje kontakata – Vodič za analizu 12

Europski odbor za zaštitu podataka,

uzimajući u obzir članak 70. stavak 1. točku (e) Uredbe (EU) 2016/679 Europskog parlamenta i Vijeća od 27. travnja 2016. o zaštiti pojedinaca u vezi s obradom osobnih podataka i o slobodnom kretanju takvih podataka te o stavljanju izvan snage Direktive 95/46/EZ (dalje u tekstu „Opća uredba o zaštiti podataka”),

uzimajući u obzir Sporazum o EGP-u, a posebno njegov Prilog XI. i Protokol 37., kako su izmijenjeni Odlukom Zajedničkog odbora EGP-a br. 154/2018 od 6. srpnja 2018.[1],

uzimajući u obzir članke 12. i 22. svojeg poslovnika,

DONIO JE SLJEDEĆE SMJERNICE:

1. UVOD I KONTEKST

1. U borbi protiv pandemije bolesti COVID-19 vlade i privatni dionici sve se češće okreću rješenjima koja se temelje na podacima, zbog čega se postavlja niz pitanja u pogledu privatnosti.
2. EDPB naglašava da je pravni okvir za zaštitu podataka osmišljen kako bi bio fleksibilan i kao takav omogućio učinkovit odgovor za ograničavanje pandemije, uz zaštitu temeljnih ljudskih prava i sloboda.
3. EDPB je uvjeren da je, u slučajevima kad je obrada osobnih podataka nužna za borbu protiv pandemije bolesti COVID-19, zaštita podataka neophodna kako bi se izgradilo povjerenje, stvorili uvjeti za društvenu prihvatljivost svakog rješenja, te zajamčila djelotvornost predviđenih mjera. Koronavirus ne poznaje granice, pa se čini najboljim razviti zajednički europski pristup kao odgovor na trenutačnu krizu, ili barem uspostaviti interoperabilan okvir.
4. EDPB općenito smatra da bi se podaci i tehnologije koji se upotrebljavaju u borbi protiv pandemije bolesti COVID-19 trebali upotrebljavati za jačanje položaja pojedinaca, a ne za uspostavu kontrole nad njima, njihovu stigmatizaciju ili ograničavanje. Nadalje, iako podaci i tehnologija mogu biti važni alati, imaju suštinska ograničenja i mogu samo potaknuti djelotvornost drugih javnozdravstvenih mjera. Sve mjere koje donesu države članice ili institucije EU-a, a uključuju obradu osobnih podataka u borbi protiv bolesti COVID-19 moraju se voditi načelima djelotvornosti, nužnosti i proporcionalnosti.
5. U ovim se smjernicama pojašnjavaju uvjeti i načela za proporcionalnu upotrebu podataka o lokaciji i alata za praćenje kontakata, i to za dvije posebne namjene:
   - upotrebu podataka o lokaciji za potporu odgovoru na pandemiju kako bi se izradio model širenja virusa te procijenila općenita djelotvornost karantenskih mjera,
   - praćenje kontakata, čija je svrha obavještavati pojedince o tome da su bili izloženi nekome tko kasnije bude potvrđen kao nositelj virusa, a sve s ciljem da se što prije prekinu putevi širenja zaraze.
6. Koliko će aplikacije za praćenje kontakata doprinijeti borbi protiv pandemije ovisi o nizu čimbenika (npr. postotku osoba koje bi trebale preuzeti te aplikacije na svoje uređaje, definiciji „kontakta” u smislu fizičke udaljenosti i trajanja). Osim toga, takve aplikacije trebaju biti dio

1 Upućivanja na „države članice” u ovom dokumentu trebaju se tumačiti kao upućivanja na „države članice EGP-a”.

sveobuhvatne javnozdravstvene strategije za borbu protiv pandemije, uključujući, među ostalim, testiranje i naknadno ručno praćenje kontakata radi uklanjanja sumnje. Uvođenje tih aplikacija trebalo bi biti popraćeno mjerama potpore kako bi se osiguralo da se korisnicima daju kontekstualizirane informacije i da upozorenja mogu koristiti sustavu javnog zdravstva. U suprotnom se ne bi mogao ostvariti njihov puni učinak.

7. EDPB naglašava da Opća uredba o zaštiti podataka i Direktiva 2002/58/EZ (dalje u tekstu „Direktiva") sadržavaju posebna pravila o odobravanju upotrebe anonimnih i osobnih podataka kako bi se javnim tijelima i drugim dionicima na nacionalnoj razini i razini EU-a pomoglo u praćenju i ograničavanju širenja virusa SARS-CoV-2[2].

8. U tom je pogledu EDPB već zauzeo stajalište da bi upotreba aplikacija za praćenje kontakata trebala biti na dobrovoljnoj osnovi i ne bi se trebala oslanjati na praćenje kretanja pojedinaca, nego na informacije o međusobnoj blizini korisnika[3].

[2]Vidjeti prethodnu izjavu EDPB-a o obradi osobnih podataka u okviru pandemije COVID-a 19.
[3] [3] https://edpb.europa.eu/sites/edpb/files/files/file1/edpbletterecadvisecodiv-appguidance_final.pdf

2. UPOTREBA PODATAKA O LOKACIJI

2.1. Izvori podataka o lokaciji

9. Za izradu modela širenja virusa i općenitu djelotvornost karantenskih mjera dostupna su dva glavna izvora podataka o lokaciji:
   - podaci o lokaciji koje pružatelji usluga elektroničkih komunikacija (npr. mobilni operateri) prikupljaju tijekom pružanja usluga i
   - podaci o lokaciji koje prikupljaju aplikacije pružatelja usluga informacijskog društva za čiji su rad potrebni ti podaci (npr. navigacija, usluge prijevoza itd.).

10. EDPB podsjeća na to da se podaci o lokaciji[4] dobiveni od pružatelja usluga elektroničkih komunikacija mogu obrađivati samo u skladu s člancima 6. i 9. Direktive. To znači da se ti podaci mogu prenijeti javnim tijelima ili ostalim trećim stranama samo ako ih je pružatelj anonimizirao ili, ako je riječ o podacima koji ukazuju na zemljopisni položaj terminalne opreme korisnika, a nisu podaci o prometu, ako je korisnik za to prethodno dao pristanak[5].

11. Na informacije koje se prikupljaju izravno od terminalne opreme, uključujući podatke o lokaciji, primjenjuje se članak 5. stavak 3. Direktive. Stoga je pohranjivanje podataka na korisnikovu uređaju ili pristupanje već pohranjenim podacima dopušteno samo uz uvjet i. da je korisnik na to pristao[6] ili ii. da su pohranjivanje i/ili pristup strogo potrebni za pružanje usluge informacijskog društva koju je korisnik izričito zatražio.

12. Međutim, odstupanja od prava i obveza propisanih u Direktivi moguća su u skladu s člankom 15. ako predstavljaju nužnu, prikladnu i proporcionalnu mjeru u demokratskom društvu za određene ciljeve[7].

13. Za ponovnu upotrebu podataka o lokaciji koje je prikupio pružatelj usluga informacijskog društva (npr. preko operativnog sustava ili neke prethodno instalirane aplikacije) za potrebe izrade modela moraju se ispuniti dodatni uvjeti. Ako su podaci prikupljeni u skladu s člankom 5. stavkom 3. Direktive, mogu se dalje obrađivati samo uz dodatni pristanak ispitanika ili na temelju prava Unije ili države članice kojim je propisano da je riječ o nužnoj i proporcionalnoj mjeri u demokratskom društvu kojom se štite ciljevi navedeni u članku 23. stavku 1. Opće uredbe o zaštiti podataka[8].

2.2. Naglasak na upotrebi anonimiziranih podataka o lokaciji

14. EDPB naglašava da bi se pri upotrebi podataka o lokaciji prednost uvijek trebala dati obradi anonimiziranih, a ne osobnih podataka.

15. Anonimizacija se odnosi na upotrebu niza tehnika kojima se onemogućuje da se uz razuman napor podaci povežu s fizičkom osobom čiji je identitet utvrđen ili se može utvrditi. U tom se testu „razumnosti" moraju uzeti u obzir objektivni aspekti (vrijeme, tehnička sredstva) i kontekstualni elementi koji mogu varirati ovisno o slučaju (rijetkost pojave uzimajući u obzir gustoću stanovništva, prirodu i količinu podataka). Ako podaci ne prođu taj test, to znači da nisu anonimizirani i stoga su i dalje obuhvaćeni područjem primjene Opće uredbe o zaštiti podataka.

16. Procjena pouzdanosti anonimizacije temelji se na tri kriterija: 1. izdvajanju (izoliranju pojedinca unutar veće skupine na temelju podataka); 2. povezivosti (povezivanju dvaju zapisa

---

[4] Vidjeti članak 2. točku (c) Direktive.
[5] Vidjeti članke 6. i 9. Direktive.
[6] Pojam pristanka u Direktivi i dalje je isti kao pojam privole u Općoj uredbi o zaštiti podataka te mora ispunjavati sve zahtjeve privole propisane člankom 4. stavkom 11. i člankom 7. Opće uredbe o zaštiti podataka.
[7] Za tumačenje članka 15. Direktive vidjeti presudu Suda Europske unije od 29. siječnja 2008. u predmetu C-275/06 Productores de Música de España (Promusicae) protiv Telefónica de España SAU.
[8] Vidjeti odjeljak 1.5.3. smjernica 1/2020 o obradi osobnih podataka u kontekstu povezanih vozila.

koji se odnose na istog pojedinca); i 3. izvođenju zaključaka (dedukciji, uz značajnu vjerojatnost, nepoznatih informacija o pojedincu).

17. Pojam anonimizacije često se pogrešno tumači i često se miješa sa pseudonimizacijom. Anonimizacija omogućuje upotrebu podataka bez ograničenja, a pseudonimizirani podaci i dalje su obuhvaćeni Općom uredbom o zaštiti podataka.

18. Postoje mnoge mogućnosti za učinkovitu anonimizaciju[9], ali uz napomenu. Podatke nije moguće anonimizirati pojedinačno, odnosno samo se skupovi podataka u cjelini mogu anonimizirati ili ne. U tom se smislu svaka intervencija na pojedinačnim podacima (šifriranje ili bilo koja druga matematička transformacija) može u najbolju ruku smatrati pseudonimizacijom.

19. Postupci anonimizacije i napadi s ciljem ponovne identifikacije aktivna su područja istraživanja. Ključno je da svaki voditelj obrade koji provodi rješenja za anonimizaciju prati najnovija događanja i spoznaje u tom području, posebno kad je riječ o podacima o lokaciji (koje prikupljaju telekomunikacijski operateri i/ili pružatelji usluga informacijskog društva), koje je posebno teško anonimizirati.

20. Velik broj istraživanja pokazao je da[10] *podaci o lokaciji za koje se misli da su anonimizirani* to možda uopće nisu. Putanje mobilnosti pojedinaca međusobno su izrazito povezane i jedinstvene. Stoga mogu biti osjetljive na pokušaje ponovne identifikacije u određenim okolnostima.

21. Jedinstven obrazac podataka o praćenju lokacija pojedinca tijekom duljeg razdoblja ne može se u potpunosti anonimizirati. Anonimizacija bi mogla ostati nemoguća ako se preciznost zabilježenih zemljopisnih koordinata dovoljno ne smanji, pa čak i ako se uklone podaci o putanjama ili ako se zadrže samo podaci o lokacijama na kojima se ispitanik dugo zadržava. To vrijedi i za loše agregirane podatke o lokaciji.

22. Želimo li ih anonimizirati, podaci o lokaciji moraju se pažljivo obraditi kako bi prošli test razumnosti. Ta pažljiva obrada uključuje razmatranje skupova podataka o lokaciji kao cjeline i obradu podataka iz razumno velikog skupa pojedinaca na temelju dostupnih pouzdanih tehnika anonimizacije, pod uvjetom da se primjereno i djelotvorno primjenjuju.

23. Naposljetku, s obzirom na složenost procesa anonimizacije, posebno se potiče transparentnost u pogledu metoda za anonimizaciju.

---

[9] (de Montjoye et al., 2018) „On the privacy-conscientious use of mobile phone data".
[10] (de Montjoye et al., 2013) „Unique in the Crowd: The privacy bounds of human mobility" i (Pyrgelis et al., 2017) „Knock Knock, Who's There? Membership Inference on Aggregate Location Data"

3. APLIKACIJE ZA PRAĆENJE KONTAKATA

3.1. Općenita pravna analiza

24. Sustavno i opsežno praćenje lokacije i/ili kontakata fizičkih osoba ozbiljno je zadiranje u njihovu privatnost. Ono se može opravdati samo oslanjajući se na to da će ih korisnici dobrovoljno prihvatiti za svaku pojedinačnu svrhu. To bi konkretno značilo da pojedinci koji odluče da neće ili ne mogu upotrebljavati takve aplikacije ne bi trebali zbog toga biti u nepovoljnom položaju.

25. Kako bi se osigurala odgovornost, za svaku aplikaciju za praćenje kontakata trebao bi se jasno definirati voditelj obrade podataka. EDPB smatra da bi nacionalna zdravstvena tijela trebala biti voditelji obrade[11] za takve aplikacije; mogu se predvidjeti i drugi voditelji obrade. U svakom slučaju, ako uvođenje aplikacija za praćenje kontakata uključuje različite dionike, njihove uloge i odgovornosti moraju se od početka jasno utvrditi i objasniti korisnicima.

26. Osim toga, kad je riječ o načelu ograničenja svrhe, svrhe moraju biti dovoljno specifične da se isključi daljnja obrada u svrhe koje nisu povezane s upravljanjem zdravstvenom krizom koju je izazvao COVID-19 (npr. u komercijalne svrhe ili u svrhe kaznenog progona). Nakon što se jasno definira cilj, trebat će osigurati da je upotreba osobnih podataka primjerena, nužna i proporcionalna.

27. U kontekstu aplikacija za praćenje kontakata posebno bi trebalo uzeti u obzir načelo smanjenja količine podataka te tehničke i integrirane zaštite podataka:
    - za rad aplikacija za praćenje kontakata nije nužno praćenje lokacije pojedinačnih korisnika. Umjesto toga trebali bi se upotrebljavati podaci o blizini
    - budući da aplikacije za praćenje kontakata mogu funkcionirati bez izravne identifikacije pojedinaca, trebale bi se uvesti odgovarajuće mjere za sprečavanje ponovne identifikacije
    - trebale bi se prikupljati isključivo relevantne informacije, samo kad je to apsolutno nužno, a prikupljene informacije trebale bi biti pohranjene na terminalnoj opremi korisnika.

28. Kad je riječ o zakonitosti obrade, EDPB napominje da aplikacije za praćenje kontakata uključuju pohranu informacija i/ili pristup informacijama koje su već pohranjene na terminalu, koje podliježu članku 5. stavku 3. Direktive. Ako su te radnje nužne kako bi pružatelj aplikacije mogao pružati uslugu koju je korisnik izričito zatražio, za obradu podataka ne bi bio potreban pristanak korisnika. Za radnje koje nisu nužne pružatelj usluge trebao bi zatražiti pristanak korisnika.

29. Osim toga, EDPB napominje da to što je upotreba aplikacija za praćenje kontakata dobrovoljna ne znači da će se obrada osobnih podataka nužno temeljiti na pristanku. Ako javna tijela pružaju uslugu koja se temelji na ovlasti koja im je dodijeljena i koja je u skladu s mjerodavnim pravom, čini se da je najrelevantnija pravna osnova za obradu podataka nužnost za izvršavanje zadaće od javnog interesa, odnosno članak 6. stavak 1. točka (e) Opće uredbe o zaštiti podataka.

30. U članku 6. stavku 3. Opće uredbe o zaštiti podataka pojašnjava se da se osnova za obradu iz članka 6. stavka 1. točke (e) utvrđuje u pravu Unije ili pravu države članice kojem podliježe voditelj obrade. Svrha obrade određuje se tom pravnom osnovom ili, u pogledu obrade iz stavka 1. točke (e), mora biti nužna za izvršavanje zadaće od javnog interesa ili izvršavanje službene ovlasti voditelja obrade[12].

[11] Vidjeti i Smjernice Europske komisije za zaštitu podataka u aplikacijama kojima se podupire suzbijanje pandemije bolesti COVID-19, Bruxelles, 16.4.2020. C(2020) 2523 final.
[12] Vidjeti uvodnu izjavu 41.

31. Međutim, pravna osnova ili zakonodavna mjera koja predstavlja zakonsku osnovu za upotrebu aplikacija za praćenje kontakata trebala bi uključivati smislene zaštitne mjere, među ostalim i upućivanje na dobrovoljnu prirodu aplikacije. Trebala bi uključivati i jasnu definiciju svrhe i izričitih ograničenja u vezi s daljnjom upotrebom osobnih podataka, kao i uključenih voditelja obrade. Trebali bi se utvrditi i kategorije podataka te subjekti kojima se mogu otkriti osobni podaci (i svrhe tog otkrivanja). Ovisno o razini interferencije, trebale bi se uključiti dodatne zaštitne mjere, pri čemu treba uzeti u obzir prirodu, opseg i svrhe obrade. Naposljetku, EDPB preporučuje da se, čim to bude moguće, u pravnu osnovu uključe i kriteriji za utvrđivanje kada će se aplikacija ukinuti te subjekt koji će biti odgovoran za donošenje te odluke.

32. Međutim, ako se obrada podataka temelji na nekoj drugoj pravnoj osnovi, kao što je privola (članak 6. stavak 1. točka (a))[13], voditelj obrade morat će osigurati da su ispunjeni strogi zahtjevi za valjanost te pravne osnove.

33. Osim toga, upotreba aplikacije u borbi protiv pandemije bolesti COVID-19 mogla bi dovesti do prikupljanja zdravstvenih podataka (npr. statusa zaražene osobe). Obrada takvih podataka dopuštena je ako je nužna u svrhu javnog interesa u području javnog zdravlja, u skladu s uvjetima iz članka 9. stavka 2. točke (i) Opće uredbe o zaštiti podataka[14], ili u svrhe zdravstvene skrbi kako je opisano u članku 9. stavku 2. točki (h) Opće uredbe o zaštiti podataka[15]. Ovisno o pravnoj osnovi, obrada se može temeljiti na izričitoj privoli (članak 9. stavak 2. točka (a) Opće uredbe o zaštiti podataka).

34. U skladu s prvotnom svrhom, člankom 9. stavkom 2. točkom (j) Opće uredbe o zaštiti podataka omogućuje se obrada zdravstvenih podataka ako je nužna u svrhe znanstvenog istraživanja ili u statističke svrhe.

35. Trenutačnu zdravstvenu krizu ne bi trebalo iskorištavati za uvođenje neproporcionalnih ovlasti za zadržavanje podataka. Ograničenje pohrane trebalo bi biti u skladu sa stvarnim potrebama i medicinskom važnosti (to može uključivati epidemiološke aspekte, npr. razdoblje inkubacije itd.), a osobni podaci trebali bi se čuvati samo tijekom trajanja krize koju je uzrokovao COVID-19. Kao opće pravilo, nakon toga bi se svi osobni podaci trebali izbrisati ili anonimizirati.

36. EDPB smatra da takve aplikacije ne mogu zamijeniti, nego samo podupirati, ručno praćenje kontakata koje provodi kvalificirano javno zdravstveno osoblje, koje može zaključiti koliko je vjerojatno da bliski kontakti dovedu do zaraze virusom (npr. interakcija s osobom koja jest ili nije zaštićena odgovarajućom opremom – blagajnicima itd.). EDPB naglašava da bi postupci i procesi, uključujući odgovarajuće algoritme u aplikacijama za praćenje kontakata, trebali biti pod strogim nadzorom kvalificiranog osoblja kako bi se ograničilo pojavljivanje lažno pozitivnih i negativnih rezultata. Konkretnije, zadaća pružanja savjeta o sljedećim koracima ne bi se trebala temeljiti isključivo na automatiziranoj obradi.

37. Kako bi se osigurala njihova pravednost, pouzdanost i općenito njihova usklađenost s pravom, algoritmi se moraju moći revidirati te bi ih trebali redovito preispitivati nezavisni stručnjaci. Izvorni kôd aplikacije trebao bi biti dostupan javnosti radi što šireg javnog nadzora.

38. Lažno pozitivni rezultati uvijek će se pojavljivati u određenoj mjeri. Budući da utvrđivanje rizika od zaraze vjerojatno može imati velik utjecaj na pojedince, npr. morali bi biti u samoizolaciji sve dok ne dobiju nalaz negativan na virus, nužno je uvesti mogućnost za ispravljanje podataka i/ili naknadnih rezultata analize. To bi, naravno, trebalo primijeniti samo na slučajeve i primjene u kojima se podaci obrađuju i/ili pohranjuju na način koji s tehničke strane omogućuje unos takvih ispravaka te u kojima je vjerojatno da će nastati prethodno spomenuti negativni utjecaji.

---

[13] Voditelji obrade (posebno javna tijela) moraju obratiti posebnu pozornost na to da se privola ne može smatrati dobrovoljnom ako pojedinac nema stvarnu mogućnost izbora da odbije ili povuče svoju privolu, a da mu to ne uzrokuje štetu.

[14] Obrada se mora temeljiti na pravu Unije ili države članice u kojem su predviđene odgovarajuće i posebne mjere za zaštitu prava i sloboda ispitanika, posebno čuvanje poslovne tajne.

[15] Vidjeti članak 9. stavak 2. točku (h) Opće uredbe o zaštiti podataka.

39. Naposljetku, EDPB smatra da se prije uvođenja takvih alata mora provesti procjena učinka na zaštitu podataka jer se smatra da će obrada vjerojatno prouzročiti visok rizik (zdravstveni podaci, predviđeno široko uvođenje, sustavno praćenje, upotreba novog tehnološkog rješenja)[16]. EDPB snažno preporučuje da se procjene učinka na zaštitu podataka objave.

3.2. Preporuke i funkcionalni zahtjevi

40. U skladu s načelom smanjenja količine podataka, među ostalim mjerama tehničke i integrirane zaštite podataka[17], podaci koji se obrađuju trebali bi se svesti na strogi minimum. Aplikacija ne bi trebala prikupljati nepovezane ili nepotrebne informacije, kao što su osobno stanje, komunikacijski identifikatori, popisi uređaja, poruke, liste poziva, podaci o lokaciji, identifikatori uređaja itd.

41. Podaci koje aplikacija odašilje moraju uključivati samo jedinstvene i pseudonimizirane identifikatore koje aplikacija generira i koji su za nju specifični. Ti se identifikatori moraju redovito obnavljati, učestalošću koja je u skladu sa svrhom ograničavanja širenja virusa, te dovoljno često da se ograniči rizik od identifikacije i fizičkog praćenja pojedinaca.

42. Provedbe praćenja kontakata mogu biti u skladu s centraliziranim ili decentraliziranim pristupom[18]. Oba bi pristupa trebala biti prihvatljiva, ali pod uvjetom da se uvedu odgovarajuće sigurnosne mjere, a svaki pristup ima vlastite prednosti i nedostatke. Zbog toga bi konceptualna faza razvoja aplikacije uvijek trebala uključivati temeljito razmatranje oba pristupa, pri čemu treba odmjeriti njihove učinke na zaštitu podataka / privatnost i mogući utjecaj na prava pojedinaca.

43. Svaki poslužitelj uključen u sustav praćenja kontakata mora prikupljati povijest kontakata ili pseudonimizirane identifikatore isključivo korisnika kojem je na temelju procjene zdravstvenih tijela i dobrovoljnog djelovanja korisnika potvrđena zaraza. U suprotnom, poslužitelj mora voditi popis pseudonimiziranih identifikatora zaraženih korisnika ili povijest njihovih kontakata onoliko dugo koliko je to potrebno za obavještavanje potencijalno zaraženih korisnika da su bili izloženi virusu te ne bi trebao pokušati identificirati potencijalno zaražene korisnike.

44. Za uvođenje globalne metodologije za praćenje kontakata, uključujući aplikacije i ručno praćenje, u nekim bi slučajevima mogla biti potrebna obrada dodatnih informacija. U tom bi kontekstu te dodatne informacije trebale ostati na terminalu korisnika i obraditi se samo ako je to strogo nužno te uz prethodnu izričitu privolu korisnika.

45. Moraju se primijeniti najsuvremenije kriptografske tehnike kako bi se osigurali podaci pohranjeni na poslužiteljima i u aplikacijama, kao i razmjene između aplikacija i udaljenog poslužitelja. Mora se provesti i uzajamna autentifikacija između aplikacije i poslužitelja.

46. Evidentiranje korisnika kao zaraženih virusom SARS-CoV-2 u aplikaciji mora podlijegati odgovarajućem odobrenju, npr. putem kôda za jednokratnu uporabu povezanog sa pseudonimiziranim identifikatorom zaražene osobe i sa stanicom za testiranje ili zdravstvenim djelatnikom. Ako se potvrda ne može dobiti na siguran način, ne smije se provesti obrada podataka u kojoj se pretpostavlja valjanost statusa korisnika.

47. Voditelj obrade mora u suradnji s javnim tijelima jasno i izričito javnosti staviti na raspolaganje poveznicu za preuzimanje službene nacionalne aplikacije za praćenje kontakata kako bi ublažio rizik od toga da pojedinci preuzimaju aplikacije treće strane.

---

[16] Vidjeti Smjernice Radne skupine iz članka 29. (koje je donio EDPB) o procjeni učinka na zaštitu podataka i utvrđivanje mogu li postupci obrade „vjerojatno prouzročiti visok rizik" u smislu Uredbe 2016/679.

[17] Vidjeti Smjernice EDPB-a 4/2019 o članku 25. – Tehnička i integrirana zaštita podataka.

[18] Decentralizirano je rješenje općenito više u skladu s načelom smanjenja količine podataka.

4. ZAKLJUČAK

48. Svijet se suočava s velikom javnozdravstvenom krizom na koju mora dati snažan odgovor, čiji će utjecaj prijeći granice ove krize. Automatizirana obrada podataka i digitalne tehnologije mogu biti ključni elementi u borbi protiv pandemije bolesti COVID-19. Međutim, treba izbjeći ireverzibilnost mjera. Naša je odgovornost osigurati da svaka mjera koja se poduzme u ovim izvanrednim okolnostima bude nužna, vremenski ograničena, minimalnog opsega i da podliježe periodičnoj i stvarnoj reviziji te znanstvenoj evaluaciji.

49. EDPB naglašava da ne bi trebalo birati između učinkovitog odgovora na trenutačnu krizu i zaštite naših temeljnih prava: možemo postići oboje, a načela zaštite podataka mogu imati važnu ulogu u borbi protiv virusa. Europskim pravom o zaštiti podataka dopuštena je odgovorna upotreba osobnih podataka u svrhe upravljanja zdravljem, ako se pritom osigura zaštita pojedinačnih prava i sloboda.

Za Europski odbor za zaštitu podataka

Predsjednica

(Andrea Jelinek)

PRILOG – APLIKACIJE ZA PRAĆENJE KONTAKATA
VODIČ ZA ANALIZU

0. Izjava o ograničenju odgovornosti

Sljedeće smjernice nisu obvezujuće niti je njihov sadržaj iscrpan. Jedina je svrha ovog vodiča dati općenite smjernice razvojnim programerima i uvoditeljima aplikacija za praćenje kontakata. Mogu se zakonito upotrebljavati i rješenja koja nisu opisana u nastavku, pod uvjetom da su u skladu s relevantnim pravnim okvirom (tj. s Općom uredbom o zaštiti podataka i Direktivom).

Valja napomenuti i da je ovaj vodič općenite prirode. Zbog toga se popis preporuka i obveza u ovom dokumentu ne smije smatrati iscrpnim. Svaka procjena treba se provesti ovisno o konkretnom slučaju, a za posebne aplikacije mogle bi biti potrebne dodatne mjere koje nisu navedene u ovom vodiču.

1. Sažetak

U mnogim državama članicama dionici razmatraju upotrebu *aplikacija za praćenje kontakata* kako bi njihovi stanovnici lakše doznali jesu li bili u kontaktu s osobom koja je zaražena virusom SARS-CoV-2.

Uvjeti pod kojima bi takve aplikacije stvarno pridonijele upravljanju pandemijom još nisu utvrđeni. Ti bi se uvjeti trebali utvrditi prije bilo kakvog uvođenja takve aplikacije. Ipak, važno je dati smjernice o informiranju razvojnih timova na početku lanca kako bi se zaštita osobnih podataka zajamčila od ranih faza dizajna.

Valja napomenuti da je ovaj vodič općenite prirode. Zbog toga se popis preporuka i obveza u ovom dokumentu ne smije smatrati iscrpnim. Svaka procjena treba se provesti ovisno o konkretnom slučaju, a za posebne aplikacije mogle bi biti potrebne dodatne mjere koje nisu navedene u ovom vodiču. Svrha je ovog vodiča dati općenite smjernice razvojnim programerima i uvoditeljima aplikacija za praćenje kontakata.

Neki kriteriji mogu nadilaziti stroge zahtjeve koji proizlaze iz okvira za zaštitu podataka. Tim se kriterijima nastoji osigurati najviša razina transparentnosti kako bi se potaknulo društveno prihvaćanje tih aplikacija.

Zato bi izdavači aplikacija za praćenje kontakata trebali uzeti u obzir sljedeće kriterije:

- Upotreba takvih aplikacija mora biti isključivo dobrovoljna. O upotrebi takvih aplikacija ne može ovisiti pristup nikakvim pravima koja su zajamčena zakonodavstvom. Pojedinci moraju u svakom trenutku imati potpunu kontrolu nad svojim podacima te bi trebali moći odabrati hoće li upotrebljavati aplikaciju.
- Aplikacije za praćenje kontakata vjerojatno će prouzročiti visok rizik za prava i slobode pojedinaca te će prije njihova uvođenja biti nužno provesti procjenu učinka na zaštitu podataka.
- Informacije o međusobnoj blizini korisnika aplikacije mogu se prikupiti bez geografskog lociranja tih korisnika. Rad te vrste aplikacije ne bi trebao uključivati upotrebu podataka o lokaciji jer oni nisu nužni za njezin rad.

- Ako se korisniku dijagnosticira zaraza virusom SARS-CoV-2, o tome bi trebale biti obaviještene samo osobe s kojima je korisnik bio u bliskom kontaktu u epidemiološki relevantnom razdoblju na koje se odnose čuvani podaci o praćenju kontakata.
- Ovisno o odabranoj arhitekturi, za rad te vrste aplikacije mogla bi biti nužna upotreba centraliziranog poslužitelja. U tom slučaju i u skladu s načelima smanjenja količine podataka te tehničke zaštite podataka podaci koje obrađuje centralizirani poslužitelj trebali bi se svesti na najmanju moguću mjeru:
    - ako se korisniku dijagnosticira zaraza, informacije o njegovim prethodnim bliskim kontaktima ili identifikatori koje odašilje aplikacija tog korisnika mogu se prikupiti samo uz njegovu suglasnost. Potrebno je utvrditi metodu provjere kojom se omogućuje da se sa sigurnošću potvrdi da je korisnik zaražen, ali da se taj korisnik ne identificira. To bi se tehnički moglo izvesti tako da se upozorenje pošalje osobama s kojima je bio u kontaktu tek nakon intervencije zdravstvenog djelatnika, npr. slanjem posebnog jednokratnog kôda.
    - Informacije pohranjene na središnjem poslužitelju ne bi trebale omogućiti voditelju obrade identifikaciju korisnika kojima je dijagnosticirana zaraza ni identifikaciju korisnika koji su bili u kontaktu sa zaraženim korisnicima. Jednako tako, na temelju tih informacija ne bi se smjeli moći izvoditi zaključci o obrascima kontakata koji nisu potrebni za utvrđivanje relevantnih kontakata.
- Za rad takvih aplikacija one moraju odašiljati podatke, koje zatim očitavaju uređaji drugih korisnika, te moraju primati tako odaslane podatke:
    - dovoljno je da mobilni korisnički uređaji (računala, tableti, pametni satovi itd.) razmjenjuju pseudonimizirane identifikatore, primjerice tako da ih emitiraju (npr. sustavom Bluetooth niske razine potrošnje energije).
    - Identifikatori se moraju generirati upotrebom najsuvremenijih kriptografskih postupaka.
    - Osim toga, identifikatori se moraju redovito obnavljati kako bi se smanjio rizik od fizičkog praćenja korisnika i napada s ciljem ponovne identifikacije.
- Ta vrsta aplikacije mora se osigurati kako bi se zajamčila sigurnost tehničkih postupaka. Konkretno:
    - Aplikacija ne bi trebala korisnicima prenositi informacije koje bi im omogućile da identificiraju druge korisnike ili doznaju jesu li zaraženi. Središnji poslužitelj ne smije niti identificirati korisnike niti izvoditi zaključke o njima.

Napomena: prethodno navedena načela povezana su isključivo s navedenom svrhom aplikacija za *praćenje kontakata*, čiji je cilj samo automatski obavijestiti osobe koje su potencijalno bile izložene virusu (a da se te osobe pritom ne identificiraju). Operatere nadležne za aplikaciju i njezinu infrastrukturu moglo bi nadzirati nadležno nadzorno tijelo. Postupanje u skladu sa svim tim smjernicama ili s dijelom tih smjernica nije nužno dostatno za osiguravanje potpune usklađenosti s okvirom za zaštitu podataka.

2. Definicije

Kontakt	Za potrebe aplikacije za praćenje kontakata, kontakt znači korisnik koji je sudjelovao u interakciji s korisnikom za kojeg je potvrđeno da je nositelj virusa, a zbog trajanja kontakta i udaljenosti postoji rizik od znatne izloženosti virusu. Parametre trajanja izlaganja i udaljenosti između osoba moraju procijeniti zdravstvene službe te se ti parametri mogu postaviti u aplikaciji.
Podaci o lokaciji	Podaci o lokaciji znači svi podaci obrađeni u elektroničkoj komunikacijskoj mreži ili podaci koje je obradila služba za elektroničke komunikacije, a koji se odnose na zemljopisni položaj terminalne opreme korisnika javno dostupne elektroničke komunikacijske usluge (kako su definirani u Direktivi), te podaci iz potencijalnih drugih izvora koji se odnose na: - geografsku širinu, dužinu ili visinu terminalne opreme - smjer putovanja korisnika ili - vrijeme bilježenja podataka o lokaciji.
Interakcija	U kontekstu aplikacije za praćenje kontakata interakcija se definira kao razmjena informacija između dvaju uređaja koji se nalaze u međusobnoj blizini (vremenskoj i prostornoj), unutar dometa upotrijebljene komunikacijske tehnologije (npr. Bluetooth). Ta definicija ne uključuje lokaciju dvaju korisnika u interakciji.
Nositelj virusa	U ovom dokumentu nositeljem virusa smatraju se korisnici kojima je testiranjem potvrđena zaraza virusom i koji su od liječnika ili zdravstvenog centra dobili službenu dijagnozu.
Praćenje kontakata	Za osobe koje su bile u bliskom kontaktu (u skladu s kriterijima koje odrede epidemiolozi) s pojedincem koji je zaražen virusom postoji znatna vjerojatnost da su također zaražene i da mogu zaraziti druge. Praćenje kontakata metoda je kontrole bolesti u kojoj se bilježe sve osobe koje su bile u bliskom kontaktu s nositeljem virusa kako bi se provjerilo postoji li za njih rizik od zaraze te kako bi se u pogledu tih osoba poduzele odgovarajuće sanitarne mjere.

3. Općenito

GEN-1	Aplikacija mora biti dopunski alat za tradicionalne tehnike praćenja kontakata (posebno razgovore sa zaraženim osobama), tj. mora biti dio šireg javnozdravstvenog programa. Aplikacija se mora upotrebljavati samo do trenutka kad se samo tehnikama ručnog praćenja uspije upravljati brojem novih slučajeva zaraze.

GEN-2	Najkasnije kad nadležna javna tijela donesu odluku o „povratku u normalno stanje” mora se uspostaviti postupak za zaustavljanje prikupljanja identifikatora (globalna deaktivacija aplikacije, upute za deinstalaciju aplikacije, automatska deinstalacija itd.) te pokrenuti brisanje svih prikupljenih podataka iz svih baza podataka (mobilnih aplikacija i poslužitelja).
GEN-3	Izvorni kôd aplikacije i njezine temeljne arhitekture moraju biti otvoreni, a tehničke specifikacije dostupne javnosti kako bi svaka zainteresirana strana mogla pregledati kôd i, ako je primjereno, pridonijeti njegovu poboljšanju, ispraviti eventualne pogreške i pomoći osigurati transparentnost obrade osobnih podataka.
GEN-4	Faze uvođenja aplikacije moraju omogućiti postupnu validaciju njezine djelotvornosti sa stajališta javnog zdravstva. Za te se potrebe na početku lanca mora utvrditi evaluacijski protokol s posebnim pokazateljima koji omogućuju mjerenje djelotvornosti aplikacije.

4. Svrhe

PUR-1	Jedina svrha aplikacije mora biti praćenje kontakata kako bi se upozorile osobe potencijalno izložene virusu SARS-CoV-2 i na tim osobama provele daljnje mjere. Aplikacija se ne smije upotrebljavati ni u jednu drugu svrhu.
PUR-2	Aplikacija se ne smije prenamijeniti u odnosu na primarnu upotrebu u svrhe praćenja poštovanja karantenskih mjera, samoizolacije ili ograničavanja socijalnih kontakata.
PUR-3	Aplikacija se ne smije upotrebljavati za izvlačenje zaključaka o lokaciji korisnika na temelju njihove interakcije ni u bilo kakvu drugu svrhu.

5. Funkcionalni aspekti

FUNC-1	Aplikacija mora imati funkciju koja korisnicima omogućuje primanje upozorenja u slučaju da su potencijalno bili izloženi virusu, pri čemu se ta informacija temelji na blizini zaraženom korisniku u roku od X dana prije nego što je zaraženom korisniku potvrđena prisutnost virusa (vrijednost X definiraju zdravstvena tijela).
FUNC-2	Aplikacija bi trebala dati preporuke korisnicima za koje je utvrđeno da su potencijalno bili izloženi virusu. Trebala bi im prenositi upute o mjerama kojih bi se trebali pridržavati te bi trebala omogućiti korisniku da zatraži savjete. U takvim slučajevima ljudska intervencija bila bi obvezna.
FUNC-3	Algoritam kojim se mjeri rizik od zaraze tako da se u obzir uzimaju čimbenici udaljenosti i vremena te se na temelju njih odlučuje kada treba zabilježiti kontakt na popisu za praćenje kontakta mora biti sigurno podesiv kako bi se uzele u obzir najnovije spoznaje o širenju virusa.

FUNC-4	**Korisnici moraju biti obaviješteni ako su bili izloženi virusu** ili moraju redovito dobivati informacije o tome jesu li ili nisu bili izloženi virusu u razdoblju inkubacije virusa.
FUNC-5	Aplikacija bi trebala biti interoperabilna s drugim aplikacijama koje razviju države članice kako bi korisnici koji se kreću kroz različite države članice mogli nastaviti primati obavijesti.

6. Podaci

DATA-1	U svrhu praćenja kontakata aplikacija mora moći odašiljati i primati podatke putem komunikacijskih tehnologija koje se temelje na blizini kao što je sustav Bluetooth niske razine potrošnje energije.
DATA-2	Ti podaci koje aplikacija odašilje moraju uključivati kriptografski snažne pseudonasumične identifikatore koje aplikacija generira i koji su za nju specifični.
DATA-3	Rizik od preklapanja pseudonasumičnih identifikatora treba biti dovoljno nizak.
DATA-4	Pseudonasumični identifikatori moraju se redovito obnavljati, učestalošću kojom se ograničava rizik da bilo tko, uključujući operatore središnjeg poslužitelja, druge korisnike aplikacije ili zlonamjerne treće strane, može ponovno identificirati, fizički pratiti ili povezati pojedince. Te identifikatore mora generirati aplikacija koju korisnik upotrebljava, po mogućnosti na temelju inicijalizacije pseudonasumičnog niza koju osigurava središnji poslužitelj.
DATA-5	U skladu s načelom smanjenja količine podataka aplikacija ne smije prikupljati podatke koji nisu nužni za svrhu praćenja kontakata.
DATA-6	Aplikacija ne smije prikupljati podatke o lokaciji za svrhu praćenja kontakata. Podaci o lokaciji mogu se obrađivati isključivo kako bi se aplikaciji omogućila interakcija sa sličnim aplikacijama u drugim zemljama i ta bi obrada trebala biti precizno ograničena na ono što je nužno za tu svrhu.
DATA-7	Aplikacija ne bi trebala prikupljati zdravstvene podatke povrh onih koji su nužni za svrhe aplikacije, osim na dobrovoljnoj osnovi i isključivo kao pomoć u donošenju odluke u postupku informiranja korisnika.
DATA-8	Korisnike se mora obavijestiti o svim osobnim podacima koji će se prikupljati. Ti bi se podaci trebali prikupljati samo uz odobrenje korisnika.

7. Tehnička svojstva

TECH-1	Aplikacija bi trebala upotrebljavati dostupne tehnologije kao što su komunikacijske tehnologije koje se temelje na blizini (npr. sustav Bluetooth niske

	razine potrošnje energije) za otkrivanje korisnika u blizini uređaja na kojem aplikacija radi.
TECH-2	Aplikacija bi trebala na uređaje bilježiti povijest kontakata među korisnicima tijekom unaprijed određenog ograničenog razdoblja.
TECH-3	Aplikacija se može oslanjati na središnji poslužitelj za provedbu nekih funkcija.
TECH-4	Aplikacija se mora temeljiti na arhitekturi koja se što više oslanja na uređaje korisnika.
TECH-5	Na zahtjev korisnika koji su prijavljeni kao zaraženi te nakon što njihov status potvrdi odgovarajuće certificirani zdravstveni stručnjak, njihova povijest kontakata ili njihovi vlastiti identifikatori trebali bi se prenijeti na središnji poslužitelj.

8. Sigurnost

SEC-1	Mora postojati mehanizam koji će provjeravati status korisnika koji su u aplikaciji evidentirani kao pozitivni na virus SARS-CoV-2, npr. tako da se stanici za testiranje ili zdravstvenom djelatniku pošalje kôd za jednokratnu uporabu. Ako se potvrda ne može dobiti na siguran način, ti se podaci ne smiju obraditi.
SEC-2	Podaci poslani na središnji poslužitelj moraju se prenositi preko sigurnog kanala. Upotreba usluga obavješćivanja koje pružaju pružatelji platforme otvorenog kôda trebala bi se pažljivo procijeniti i ne bi trebala dovesti do otkrivanja nikakvih podataka trećim stranama.
SEC-3	Zahtjevi ne smiju biti osjetljivi na neovlaštene izmjene zlonamjernih korisnika.
SEC-4	Moraju se primijeniti najsuvremenije kriptografske tehnike kako bi se osigurale razmjene između aplikacije i poslužitelja te između aplikacija i kako bi se općenito zaštitile informacije pohranjene u aplikacijama i na poslužitelju. Primjeri tehnika koje se mogu primijeniti uključuju: simetričnu i asimetričnu enkripciju, funkcije za izračun sažetka (*hash functions*), enkripcijske protokole PTM (*private membership test*), PSI (*private set intersection*) i PIR (*private information retrieval*), Bloom filtre, homomorfnu enkripciju itd.
SEC-5	Središnji poslužitelj ne smije čuvati mrežne identifikatore (npr. IP adrese) nijednog korisnika, uključujući korisnike koji su pozitivni na virus i koji su na poslužitelj prenijeli svoju povijest kontakata ili svoje identifikatore.
SEC-6	Kako bi se izbjeglo lažno predstavljanje ili stvaranje lažnih korisnika, poslužitelj mora provjeriti autentičnost aplikacije.
SEC-7	Aplikacija mora provjeriti autentičnost središnjeg poslužitelja.
SEC-8	Funkcije poslužitelja trebaju se zaštititi od napada reprodukcijom.
SEC-9	Informacije koje prenosi središnji poslužitelj moraju biti potpisane kako bi se mogli potvrditi njihov izvor i cjelovitost.
SEC-10	Pristup svim podacima koji su pohranjeni na središnjem poslužitelju, a nisu dostupni javnosti mora biti ograničen samo na ovlaštene osobe.

SEC-11	Upravitelj dopuštenja na razini operativnog sustava uređaja smije zatražiti samo dopuštenja za pristup komunikacijskim modulima i njihovu upotrebu kad je to potrebno, za pohranu podataka na terminalu te za razmjenu informacija sa središnjim poslužiteljem.

9. Zaštita osobnih podataka i privatnosti fizičkih osoba

Podsjetnik: sljedeće smjernice odnose se na aplikaciju čija je jedina svrha praćenje kontakata.

PRIV-1	Pri razmjenama podataka mora se poštovati privatnost korisnika (a posebno načelo smanjenja količine podataka).
PRIV-2	Aplikacija ne smije omogućivati izravnu identifikaciju korisnika dok se služe aplikacijom.
PRIV-3	Aplikacija ne smije omogućivati praćenje kretanja korisnika.
PRIV-4	Upotreba aplikacije ne bi trebala omogućiti korisnicima da išta doznaju o drugim korisnicima (a posebno je li drugi korisnik nositelj virusa ili ne).
PRIV-5	Povjerenje u središnji poslužitelj mora biti ograničeno. Središnjim poslužiteljem mora se upravljati u skladu s jasno definiranim pravilima upravljanja te se moraju uvesti sve potrebne mjere kako bi se zajamčila njegova sigurnost. Smještaj središnjeg poslužitelja trebao bi omogućiti da poslužitelj bude pod stvarnim nadzorom nadležnog nadzornog tijela.
PRIV-6	Procjena učinka na zaštitu podataka mora se provesti, a trebala bi se i objaviti.
PRIV-7	Aplikacija bi korisniku trebala dati samo informaciju je li bio izložen virusu te, po mogućnost bez otkrivanja informacija o drugim korisnicima, koliko je puta bio izložen i datume izlaganja.
PRIV-8	Informacije koje aplikacija prenosi ne smiju omogućiti korisnicima da identificiraju korisnike koji su nositelji virusa niti praćenje njihovih kretanja.
PRIV-9	Informacije koje aplikacija prenosi ne smiju omogućiti zdravstvenim tijelima identifikaciju potencijalno izloženih korisnika bez njihove suglasnosti.
PRIV-10	Zahtjevi koje aplikacija upućuje središnjem poslužitelju ne smiju otkrivati nikakve informacije o nositelju virusa.
PRIV-11	Zahtjevi iz aplikacije upućeni središnjim poslužitelju ne smiju otkrivati nikakve nepotrebne informacije o korisnicima, osim eventualno i samo po potrebi njihove pseudonimizirane identifikatore i popise kontakata.
PRIV-12	Napadi s ciljem ponovne identifikacije moraju se onemogućiti.
PRIV-13	Korisnici moraju putem aplikacije moći ostvariti svoja prava.
PRIV-14	Brisanje aplikacije mora dovesti do brisanja svih lokalno prikupljenih podataka.
PRIV-15	Aplikacija bi trebala prikupljati samo podatke koje odašilje ista aplikacija s drugog uređaja ili interoperabilna istovjetna aplikacija. Ne smiju se prikupljati nikakvi podaci povezani s drugim aplikacijama i/ili uređajima za komunikaciju na temelju blizine.
PRIV-16	Kako bi se izbjeglo da središnji poslužitelj pokuša ponovnu identifikaciju, trebali bi se uvesti *proxy* poslužitelji. Svrha je tih *transparentnih i pouzdanih poslužitelja* pomiješati identifikatore nekoliko korisnika (i nositelja virusa i podnositelja zahtjeva) prije nego što ih prenesu na središnji poslužitelj kako središnji poslužitelj ne bi imao informaciju o identifikatorima (npr. IP adresi) korisnika.

PRIV-17	Aplikacija i poslužitelj moraju se pažljivo razviti i konfigurirati kako ne bi prikupljali nepotrebne podatke (npr. u zapisnike poslužitelja ne smiju se unositi identifikatori itd.) te kako bi se izbjegla upotreba kompleta za razvoj softvera (SDK) treće strane koji prikuplja podatke za druge svrhe.

Većina aplikacija za praćenje kontakata o kojima se trenutačno raspravlja primjenjuje jedan od dva pristupa ako se potvrdi da je neki korisnik zaražen: ili šalju na poslužitelj povijest kontakata tog korisnika koju su prikupili skeniranjem, ili šalju popis vlastitih odaslanih identifikatora. Sljedeća su načela predstavljena u skladu s ta dva pristupa. Iako se ovdje raspravlja o tim pristupima, to ne znači da drugi pristupi nisu mogući ili čak poželjni, npr. pristupi u kojima se primjenjuje neki oblik potpune *(end-to-end*, E2E) enkripcije ili neke druge tehnologije za veću sigurnost ili zaštitu privatnosti.

9.1. Načela koja se primjenjuju samo **kad aplikacija prenosi na poslužitelj popis kontakata:**

CON-1	Središnji poslužitelj mora prikupljati povijest kontakata korisnika koji su zabilježeni kao zaraženi virusom SARS-CoV-2 samo ako su korisnici na to dobrovoljno pristali.
CON-2	Središnji poslužitelj ne smije zadržavati niti dalje prenositi popis pseudonimiziranih identifikatora nositelja virusa.
CON-3	Povijest kontakata pohranjena na središnjem poslužitelju mora se izbrisati nakon što korisnici prime obavijest o tome da su bili u blizini osobe kojoj je potvrđena zaraza.
CON-4	Osim ako korisnik kojem je potvrđena zaraza podijeli svoju povijest kontakata sa središnjim poslužiteljem ili ako neki korisnik pošalje zahtjev poslužitelju kako bi doznao je li bio izložen virusu, s uređaja korisnika ne smiju se odašiljati nikakvi podaci.
CON-5	Svi identifikatori u lokalnoj povijesti moraju se izbrisati X dana nakon što su prikupljeni (vrijednost X određuju zdravstvena tijela).
CON-6	Povijesti kontakata koje podnesu različiti korisnici ne smiju se dalje obrađivati u druge svrhe, npr. uspoređivati kako bi se izradile globalne karte blizine.
CON-7	Podaci u zapisnicima poslužitelja moraju se svesti na najmanju moguću mjeru i biti u skladu sa zahtjevima zaštite podataka.

9.2. Načela koja se primjenjuju samo kad aplikacija prenosi na poslužitelj popis vlastitih identifikatora:

ID-1	Središnji poslužitelj mora prikupljati identifikatore koje odašilje aplikacija, a odnose se na korisnike koji su zabilježeni kao pozitivni na SARS-CoV-2 samo ako su ti korisnici na to dobrovoljno pristali.
ID-2	Središnji poslužitelj ne smije zadržavati niti dalje prenositi povijest kontakata nositelja virusa.

ID-3	Identifikatori pohranjeni na središnjem poslužitelju moraju se izbrisati nakon što se prenesu drugim aplikacijama.
ID-4	Osim ako korisnik kojem je potvrđena zaraza podijeli svoje identifikatore sa središnjim poslužiteljem ili ako neki korisnik pošalje zahtjev poslužitelju kako bi doznao je li bio izložen virusu, s uređaja korisnika ne smiju se odašiljati nikakvi podaci.
ID-5	Podaci u zapisnicima poslužitelja moraju se svesti na najmanju moguću mjeru i biti u skladu sa zahtjevima zaštite podataka.