Službeni list Europske unije

C 124 I

Hrvatsko izdanje

Informacije i objave

Godište 63.

17. travnja 2020.

Sadržaj

II. *Informacije*

INFORMACIJE INSTITUCIJA, TIJELA, UREDA I AGENCIJA EUROPSKE UNIJE

Europska komisija

2020/C 124 I/01 Komunikacija Komisije — Smjernice za zaštitu podataka u aplikacijama kojima se podupire suzbijanje pandemije bolesti COVID-19 1

HR

II

(Informacije)

INFORMACIJE INSTITUCIJA, TIJELA, UREDA I AGENCIJA EUROPSKE UNIJE

EUROPSKA KOMISIJA

KOMUNIKACIJA KOMISIJE

Smjernice za zaštitu podataka u aplikacijama kojima se podupire suzbijanje pandemije bolesti COVID-19

(2020/C 124 I/01)

1 KONTEKST

Pandemija bolesti COVID-19 nezabilježen je izazov za zdravstvene sustave, način života, gospodarsku stabilnost i vrijednosti Unije i njezinih država članica. Digitalne tehnologije i podaci imaju važnu ulogu u suzbijanju krize uzrokovane bolešću COVID-19. U praćenju i zaustavljanju pandemije bolesti COVID-19 javnozdravstvenim tijelima na nacionalnoj razini i razini EU-a mogu pomoći mobilne aplikacije koje se obično instaliraju na pametne telefone i izrazito su važne u fazi ukidanja mjera ograničavanja. One mogu građanima osigurati izravne savjete i pomoći u praćenju kontakata. Nacionalna i regionalna tijela i programeri iz brojnih zemalja unutar i izvan EU-a najavili su uvođenje aplikacija s različitim funkcijama čiji je cilj pomoći u borbi protiv virusa.

Komisija je 8. travnja 2020. donijela Preporuku o zajedničkom Unijinom paketu mjera za primjenu tehnologije i podataka radi suzbijanja i prevladavanja krize prouzročene bolešću COVID-19, posebno u vezi s mobilnim aplikacijama i upotrebom anonimiziranih podataka o mobilnosti (dalje u tekstu „Preporuka”) ([1]). Svrha je Preporuke, među ostalim, razviti paneuropski pristup primjeni mobilnih aplikacija („paket mjera”), koordiniranoj na razini EU-a, kao sredstva koje će pomoći građanima da učinkovito ograniče socijalne kontakte i kao sredstva za upozoravanje, prevenciju i praćenje socijalnih kontakata kako bi se obuzdalo širenje bolesti COVID-19. Preporukom su utvrđena opća načela za razvoj tog paketa mjera i navedeno je da će Komisija objaviti dodatne smjernice, među ostalim o implikacijama zaštite osobnih podataka i privatnosti za upotrebu aplikacija u tom području.

U Zajedničkom europskom planu za ukidanje mjera ograničavanja povezanih s bolešću COVID-19 Komisija je u suradnji s predsjednikom Europskog vijeća utvrdila niz načela za postupno ukidanje mjera ograničavanja uvedenih zbog pandemije bolesti COVID-19. Mobilne aplikacije, uključujući funkcije praćenja kontakata, mogu imati važnu ulogu u tom kontekstu. Aplikacije bi mogle, ovisno o svojim funkcijama i razmjerima u kojima ih stanovništvo upotrebljava, znatno utjecati na dijagnosticiranje, liječenje i kontroliranje bolesti COVID-19 unutar i izvan bolničkog okruženja. One su izrazito važne pri ukidanju mjera ograničavanja, kad se povećava rizik od zaraze jer sve više ljudi dolazi u međusobni kontakt. Aplikacije mogu pomoći u prekidu lanaca zaraze brže i učinkovitije od općih mjera ograničavanja te mogu smanjiti rizik od znatnog širenja virusa. Stoga bi one trebale biti važan element izlazne strategije i dopuna ostalim mjerama kao što je povećanje kapaciteta za testiranje ([2]). Za razvoj takvih aplikacija, njihovo prihvaćanje i proširenost među stanovništvom preduvjet je povjerenje. Građani moraju biti sigurni da je zajamčeno poštovanje temeljnih prava i da će se aplikacije koristiti samo u posebne definirane svrhe, da se neće upotrebljavati za masovni nadzor i da će pojedinci i dalje imati kontrolu nad svojim

([1]) Preporuka C(2020) 2296 final od 8. travnja 2020.https://ec.europa.eu/info/sites/info/files/recommendation_on_apps_for_contact_tracing_4.pdf.

([2]) https://ec.europa.eu/info/sites/info/files/communication_-_a_european_roadmap_to_lifting_coronavirus_containment_measures_0.pdf

podacima. To je osnova za točnost i učinkovitost takvih aplikacija u ograničavanju širenja virusa. Stoga je ključno utvrditi rješenja koja su najmanje nametljiva i u potpunosti usklađena sa zahtjevima u pogledu zaštite osobnih podataka i privatnosti kako su utvrđeni pravom EU-a. Nadalje, aplikacije bi trebalo deaktivirati najkasnije kad se proglasi da je pandemija pod kontrolom. Aplikacije bi trebale imati i najmodernije zaštite u području informacijske sigurnosti.

U ovim smjernicama uzeti su u obzir doprinos Europskog odbora za zaštitu podataka (EDPB) ([3]) i rasprave u okviru mreže e-zdravstva. EDPB planira u narednim danima objaviti smjernice o alatima za geolokaciju i drugim alatima za praćenje u kontekstu pandemije bolesti COVID-19.

Područje primjene smjernica

Kako bi se osigurao dosljedan pristup u cijelom EU-u i pružile smjernice državama članicama i razvojnim inženjerima aplikacija, u ovom se dokumentu utvrđuju funkcije i zahtjevi koje bi aplikacije trebale ispuniti kako bi se osigurala usklađenost sa zakonodavstvom EU-a o zaštiti privatnosti i osobnih podataka, posebice s Općom uredbom o zaštiti podataka (GDPR) ([4]) i Direktivom o e-privatnosti ([5]). Ovim smjernicama nisu obuhvaćeni nikakvi dodatni zahtjevi ni ograničenja koji su možda propisani nacionalnim zakonima država članica u pogledu obrade podataka koji se odnose na zdravlje.

Smjernice nisu pravno obvezujuće. Njima se ne dovodi u pitanje uloga Suda Europske unije kao jedine institucije koja može vjerodostojno tumačiti pravo EU-a.

Ove se smjernice odnose samo na dobrovoljne aplikacije kojima se podupire suzbijanje pandemije bolesti COVID-19 (aplikacije koje pojedinci dobrovoljno preuzimaju, instaliraju i upotrebljavaju), a imaju najmanje jednu od sljedećih funkcija:

— davanje preciznih informacija korisnicima o pandemiji bolesti COVID-19,

— upitnici za samodijagnozu i upute za korisnike (funkcija provjere simptoma) ([6]),

— funkcija uzbunjivanja osoba koje su određeno vrijeme bile u blizini zaraženih kako bi ih se obavijestilo trebaju li se samoizolirati i gdje se mogu testirati (funkcija praćenja kontakata i upozoravanja),

— forum za komunikaciju pacijenata i liječnika u slučaju samoizolacije ili kad se pružaju dodatni dijagnostički i terapijski savjeti (povećana uporaba telemedicine).

U skladu s Direktivom o e-privatnosti, uporaba aplikacije koja uključuje pravo na povjerljivost komunikacija utvrđeno u članku 5. može se nametnuti samo zakonodavnim propisom koji je potreban, primjeren i razmjeran svrsi zaštite određenih posebnih ciljeva. S obzirom na visoku razinu nametljivosti takvog pristupa i povezane izazove, među ostalim u pogledu uspostave odgovarajućih zaštitnih mjera, Komisija smatra da je prije upotrebe te mogućnosti potrebna pomna analiza. Stoga Komisija preporučuje uporabu dobrovoljnih aplikacija.

Smjernice ne obuhvaćaju aplikacije čiji je cilj provedba obvezne karantene (uključujući one čija je uporaba obvezna).

2 ULOGA APLIKACIJA U SUZBIJANJU BOLESTI COVID-19

Funkcija provjere simptoma alat je koji može pomoći javnozdravstvenim tijelima pri upućivanju građana na testiranje na COVID-19 i pružanju informacija o samoizolaciji, izbjegavanju prijenosa zaraze i o tome kada zatražiti liječničku pomoć. Njome se može dopuniti nadzor u okviru primarne zdravstvene zaštite i bolje pratiti stopa prijenosa zaraze bolešću COVID-19 među stanovništvom.

([3]) https://edpb.europa.eu/sites/edpb/files/files/file1/edpbletterecadvisecodiv-appguidance_final.pdf

([4]) Uredba (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 (Opća uredba o zaštiti podataka), SL L 119, 4.5.2016., str. 1.

([5]) Direktiva 2002/58/EZ Europskog parlamenta i Vijeća od 12. srpnja 2002. o obradi osobnih podataka i zaštiti privatnosti u području elektroničkih komunikacija (Direktiva o privatnosti i elektroničkim komunikacijama), SL L 201, 31.7.2002., str. 37.

([6]) Ako aplikacije pružaju informacije povezane s dijagnostikom, prevencijom, praćenjem, predviđanjima ili prognozama, trebalo bi procijeniti njihovu potencijalnu klasifikaciju kao medicinski proizvodi u skladu s regulatornim okvirom za medicinske proizvode. Za navedeni regulatorni okvir vidjeti Direktivu Vijeća 93/42/EEZ od 14. lipnja 1993. o medicinskim proizvodima (SL L 169, 12.7.1993., str. 1.) i Uredbu (EU) 2017/745 Europskog parlamenta i Vijeća od 5. travnja 2017. o medicinskim proizvodima (SL L 117, 5.5.2017., str. 1.).

Funkcija praćenja kontakata i upozoravanja alat je za identifikaciju osoba koje su bile u kontaktu s osobom zaraženom bolešću COVID-19 i njihovo informiranje o sljedećim koracima, kao što su samoizolacija i testiranje te savjetovanje o tome što učiniti ako razviju simptome. Ta funkcija stoga pomaže i pojedincima i javnozdravstvenim tijelima. One mogu imati i važnu ulogu u upravljanju mjerama ograničavanja tijekom njihova postupnog ukidanja, a njihov učinak moguće je poboljšati strategijom koja podržava šire testiranje osoba koje su razvile blaže simptome.

Obje bi funkcije mogle javnozdravstvenim tijelima biti i relevantan izvor podataka te olakšati prijenos tih podataka nacionalnim epidemiološkim tijelima i Europskom centru za sprečavanje i kontrolu bolesti (ECDC). Ti bi podaci mogli pomoći da se otkriju obrasci prijenosa zaraze te, ako se kombiniraju s rezultatima testiranja, da se procijeni pozitivna prediktivna vrijednost respiratornih simptoma u određenoj skupini i pruže informacije o razmjeru širenja virusa.

Razina pouzdanosti procjena izravno je povezana s količinom i pouzdanošću prenesenih podataka.

Stoga funkcije provjere simptoma i praćenja kontakata, u kombinaciji s primjerenim strategijama testiranja, mogu pomoći u prikupljanju informacija o razmjeru širenja virusa te u ocjenjivanju učinka mjera držanja fizičke udaljenosti i izolacije. Kako je utvrđeno u Preporuci, da bi se omogućila prekogranična suradnja i osiguralo otkrivanje kontakata među korisnicima različitih aplikacija (što je posebno važno kod prekograničnog kretanja građana), trebalo bi osigurati interoperabilnost informatičkih rješenja različitih država članica. Ako zaražena osoba dođe u kontakt s korisnikom aplikacije druge države članice, mora biti moguć prekogranični prijenos osobnih podataka tog korisnika zdravstvenim tijelima njegove države članice u mjeri u kojoj je to apsolutno nužno. Na tom će se pitanju raditi u okviru paketa mjera najavljenog u Preporuci. Interoperabilnost bi trebalo osigurati tehničkim zahtjevima i poboljšanjem komunikacije i suradnje među nacionalnim zdravstvenim tijelima. Model posebne suradnje ([7]) mogao bi poslužiti kao model upravljanja za aplikacije za praćenje kontakata tijekom pandemije bolesti COVID-19.

3 ELEMENTI ZA POUZDANU I ODGOVORNU UPORABU APLIKACIJA

Funkcije aplikacija mogu različito utjecati na niz prava utvrđenih u Povelji EU-a o temeljnim pravima, na primjer pravo na ljudsko dostojanstvo, poštovanje privatnog i obiteljskog života, zaštitu osobnih podataka, slobodu kretanja, nediskriminaciju, slobodu poduzetništva i slobodu okupljanja i udruživanja. Posebno je istaknuto zadiranje u privatnost i zaštitu osobnih podataka, s obzirom na to da se neke funkcije temelje na modelu koji upotrebljava velike količine podataka.

Svrha je elemenata navedenih u nastavku pružiti smjernice o tome kako ograničiti nametljivost funkcija aplikacija kako bi se osigurala usklađenost sa zakonodavstvom EU-a o zaštiti osobnih podataka i privatnosti.

3.1 Nacionalna zdravstvena tijela (ili subjekti koji obavljaju zadaće od javnog interesa u području zdravstva) kao voditelji obrade podataka

Ključno je odrediti tko odlučuje o načinima i svrhama obrade podataka (voditelj obrade podataka) kako bi se utvrdilo tko je odgovoran za usklađenost s propisima EU-a o zaštiti osobnih podataka, a posebice tko bi pojedince koji preuzmu aplikaciju trebao informirati o tome što će se dogoditi s njihovim osobnim podacima (već postojećima ili podacima koje će generirati uređaj, primjerice pametni telefon, na kojem je aplikacija instalirana), koja će prava imati, tko je odgovoran u slučaju povrede podataka itd.

S obzirom na osjetljivost predmetnih osobnih podataka i svrhu obrade podataka kako je opisano u nastavku, Komisija smatra da bi aplikacije trebale biti osmišljene tako da nacionalna zdravstvena tijela (ili subjekti koji obavljaju zadaće od javnog interesa u području zdravlja) budu voditelji obrade ([8]). Voditelji obrade odgovorni su za usklađenost s Općom uredbom o zaštiti podataka (načelo pouzdanosti). Pristup bi trebalo ograničiti na temelju načela opisanih u odjeljku 3.5. u nastavku.

([7]) Takva suradnja već postoji u okviru projekta MyHealth@EU za razmjenu sažetaka medicinskih podataka o pacijentima i e-recepata. Vidjeti i članak 5. stavak 5. i uvodnu izjavu 17. Provedbene odluke Komisije 2019/1765.

([8]) Vidjeti uvodnu izjavu 45. Opće uredbe o zaštiti podataka.

Time će se pridonijeti i većem povjerenju među stanovništvom, a time i prihvaćanju aplikacija (i sustava za informiranje o lancima prijenosa zaraze na kojima se aplikacije temelje) te osigurati da one ispunjavaju predviđenu svrhu zaštite javnog zdravlja. Temeljne politike, zahtjeve i kontrole trebala bi uskladiti i koordinirano provoditi nadležna nacionalna zdravstvena tijela.

3.2 **Osiguravanje da pojedinac zadrži kontrolu**

Jedan od glavnih preduvjeta povjerenja pojedinaca u aplikacije jest dokaz da oni i dalje imaju kontrolu nad svojim osobnim podacima. Kako bi se to osiguralo, Komisija smatra da bi posebno trebalo ispuniti sljedeće uvjete:

— instaliranje aplikacije na uređaj trebalo bi biti dobrovoljno i bez ikakvih negativnih posljedica za pojedinca koji odluči da neće preuzeti/upotrebljavati aplikaciju,

— različite funkcije aplikacija (npr. informiranje, provjera simptoma, praćenje kontakata i upozoravanje) ne bi trebalo spajati, tako da pojedinac može dati privolu zasebno za svaku funkciju. To ne bi trebalo sprječavati korisnika da kombinira različite funkcije aplikacije ako pružatelj nudi tu mogućnost,

— ako se koriste podaci o blizini (podaci dobiveni razmjenom signala u sustavu Bluetooth niske razine energije – *Bluetooth Low Energy*, BLE, među uređajima unutar epidemiološki relevatne udaljenosti i u epidemiološki relevatnom vremenu), oni bi se trebali pohranjivati na korisnikovu uređaju. Ako se ti podaci trebaju podijeliti sa zdravstvenim tijelima, to bi trebalo učiniti tek nakon što se potvrdi da je dotična osoba zaražena bolešću COVID-19 te uz uvjet da ta osoba pristane na to,

— zdravstvena tijela trebala bi pojedincu dati sve potrebne informacije povezane s obradom njegovih osobnih podataka (u skladu s člancima 12. i 13. Opće uredbe o zaštiti podataka i člankom 5. Direktive o e-privatnosti),

— pojedinac bi trebao moći ostvarivati svoja prava na temelju Opće uredbe o zaštiti podataka (posebno prava na pristup, ispravak i brisanje). Svako ograničavanje prava iz Opće uredbe o zaštiti podataka i Direktive o e-privatnosti trebalo bi biti u skladu s tim aktima te potrebno, razmjerno i predviđeno zakonodavstvom,

— aplikacije bi trebalo deaktivirati najkasnije kad se proglasi da je pandemija pod kontrolom; deaktivacija ne bi trebala ovisiti o tome da korisnik deinstalira aplikaciju.

3.3 **Pravna osnova za obradu**

Instaliranje aplikacija i pohranjivanje podataka na korisnikovu uređaju

Kako je navedeno, na temelju Direktive o e-privatnosti (članak 5.) pohranjivanje podataka na korisnikovu uređaju ili pristupanje već pohranjenim podacima dopušteno je samo uz uvjet i. da je korisnik pristao na to ili ii. da su pohranjivanje i/ili pristup strogo potrebni za pružanje usluge informacijskog društva (npr. aplikacije) koju je korisnik izričito zatražio (tj. instalirao i aktivirao).

Pohranjivanje podataka na uređaju pojedinca i pristup već pohranjenim podacima na tom uređaju obično su potrebni za funkcioniranje aplikacija. Za funkciju praćenja kontakata i upozoravanja potrebno je i pohranjivanje dodatnih podataka na korisnikovu uređaju (kao što su druga korisnička imena korisnika te funkcije u blizini, koja se koriste kratko i periodički se mijenjaju). Usto, za tu bi se funkciju od (zaraženog ili vjerojatno zaraženog) korisnika moglo tražiti da učita podatke o blizini. Učitavanje tih podataka nije potrebno za funkcioniranje same aplikacije. Stoga zahtjevi iz opcije ii. iz prethodnog stavka nisu ispunjeni pa je privola (opcija i.) najprikladnija osnova za predmetne aktivnosti. Ta bi privola trebala biti „dobrovoljna", „posebna" „nedvosmislena" i „informirana" u smislu Opće uredbe o zaštiti podataka. Trebala bi biti izražena jasnom potvrdnom radnjom pojedinca; to isključuje prešutno davanje privole (npr. šutnja, neaktivnost) ([9]).

([9]) Vidjeti smjernice Europskog odbora za zaštitu podataka o privoli: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=623051

Pravna osnova za obradu podataka u nacionalnim zdravstvenim tijelima – zakonodavstvo Unije ili država članica

Nacionalna zdravstvena tijela obično obrađuju osobne podatke ako je u zakonodavstvu EU-a ili zakonodavstvu države članice utvrđena pravna obveza kojom se predviđa takva obrada i ispunjavaju uvjeti iz članka 6. stavka 1. točke (c) i članka 9. stavka 2. točke (i) Opće uredbe o zaštiti podataka ili ako je takva obrada nužna za izvršavanje zadaće od javnog interesa koji je priznat pravom EU-a ili države članice ([10]).

Nacionalnim zakonodavstvom moraju biti predviđene posebne i odgovarajuće mjere za zaštitu prava i sloboda ispitanika. Opće je pravilo da bi za veći utjecaj na slobode pojedinaca trebalo predvidjeti strože odgovarajuće zaštitne mjere u mjerodavnom zakonodavstvu.

Zakonodavni akti EU-a i država članica koji su postojali prije pandemije bolesti COVID-19 te oni koje države članice provode posebno radi suzbijanja širenja te bolesti mogu se u načelu koristiti kao pravna osnova za obradu podataka pojedinaca ako se njima predviđaju mjere koje omogućavaju praćenje širenja bolesti te ako ti akti ispunjavaju dodatne zahtjeve iz članka 6. stavka 3. Opće uredbe o zaštiti podataka.

S obzirom na prirodu predmetnih osobnih podataka (posebno zdravstvenih podataka kao posebnih kategorija osobnih podataka) i okolnosti trenutačne pandemije bolesti COVID-19, oslanjanje na zakonodavstvo kao pravnu osnovu doprinijelo bi pravnoj sigurnosti jer bi se njime i. detaljno propisala obrada posebnih zdravstvenih podataka i jasno odredile svrhe te obrade; ii. jasno odredilo tko je voditelj obrade, tj. tijelo koje obrađuje podatke, i tko osim voditelja obrade može imati pristup takvim podacima; iii. isključila mogućnost obrade takvih podataka u svrhe osim onih navedenih u zakonodavstvu i iv. predvidjele posebne zaštitne mjere. Kako se ne bi ugrozila javna korisnost i prihvaćanje aplikacija, nacionalni zakonodavci posebno bi trebali nastojati da odabrano rješenje bude što uključivije za građane.

Obrada u zdravstvenim tijelima na temelju zakonodavstva ne mijenja činjenicu da pojedinci i dalje mogu odlučiti hoće li instalirati aplikaciju i hoće li podijeliti svoje podatke sa zdravstvenim tijelima. Stoga deinstaliranje aplikacije ne bi trebalo imati negativne posljedice za korisnike.

Aplikacije za praćenje kontakata i upozoravanje šalju pojedincima upozorenja. Kad aplikacija izravno šalje upozorenja, Komisija skreće pozornost na zabranu da se pojedinac podliježe odluci koja se temelji isključivo na automatiziranoj obradi, a koja proizvodi pravni učinak ili na sličan način znatno utječe na pojedinca (članak 22. Opće uredbe o zaštiti podataka).

3.4 **Smanjenje količine podataka**

Podaci koje generiraju uređaji i podaci koji su već bili pohranjeni na tim uređajima zaštićeni su kako slijedi:

— kao „osobni podaci”, tj. svi podaci koje se odnose na fizičku osobu čiji je identitet utvrđen ili se može utvrditi (članak 4. stavak 1. Opće uredbe o zaštiti podataka) zaštićeni su na temelju Opće uredbe o zaštiti podataka. Zdravstveni podaci dodatno su zaštićeni (članak 9. Opće uredbe o zaštiti podataka),

— kao „podaci o lokaciji”, tj. podaci koji se obrađuju u elektroničkoj komunikacijskoj mreži ili u sklopu elektroničke komunikacijske usluge, a ukazuju na geografski položaj terminalne opreme korisnika, zaštićeni su u skladu s Direktivom o e-privatnosti (članak 5. stavak 1. te članci 6. i 9.) ([11]),

— svi podaci koji su pohranjeni i kojima se pristupa na terminalnoj opremi korisnika zaštićeni su u skladu s člankom 5. stavkom 3. Direktive o e-privatnosti.

Podaci koji nisu osobni (npr. nepovratno anonimizirani podaci) nisu zaštićeni Općom uredbom —zaštiti podataka.

Komisija podsjeća da se u skladu s načelom smanjenja količine podataka smiju obrađivati samo osobni podaci koji su primjereni, relevantni i ograničeni na ono što je nužno u odnosu na svrhu obrade ([12]). Procjenu nužnosti obrade osobnih podataka i relevantnosti takvih osobnih podataka trebalo bi provoditi s obzirom na svrhu ili svrhe.

Komisija napominje da, na primjer, ako je svrha funkcije provjera simptoma ili telemedicina, za to nije potreban pristup popisu kontakata vlasnika uređaja.

([10]) Članak 6. stavak 1. točka (e) Opće uredbe o zaštiti podataka.
([11]) Zakonik elektroničkih komunikacija propisuje da su obuhvaćene i usluge koje su funkcionalno ekvivalentne elektroničkim komunikacijskim uslugama.
([12]) Načelo smanjenja količine podataka.

Generiranjem i obradom manje podataka ograničavaju se sigurnosni rizici. Stoga se poštovanjem načela smanjenja količine podataka osiguravaju i sigurnosne mjere.

— Funkcija informiranja:

U aplikaciji koja ima samo tu funkciju neće biti potrebna obrada nikakvih zdravstvenih podataka pojedinaca. Samo će im se pružati informacije. Za tu se svrhu ne smiju obrađivati nikakvi podaci koji su pohranjeni i kojima se pristupa na terminalnoj opremi osim onih koji su nužni za pružanje informacija.

— Funkcije provjere simptoma i telemedicine:

Ako aplikacija uključuje bilo koju od tih funkcija, u njoj će se obrađivati osobni zdravstveni podaci. Stoga bi u temeljnom zakonodavstvu koje se primjenjuje na zdravstvena tijela trebalo navesti popis podataka koji se smiju obrađivati.

Usto, zdravstvenim tijelima mogu zatrebati brojevi telefona osoba koje su se koristile provjerom simptoma i učitale rezultate. Podaci koji su pohranjeni i kojima se pristupa na terminalnoj opremi smiju se obrađivati samo u onoj mjeri u kojoj je to nužno za funkcioniranje aplikacije i ispunjavanje njezine svrhe.

— Funkcija praćenja kontakata i upozoravanja:

Bolest COVID-19 uglavnom se prenosi kapljicama koje se šire samo na ograničenoj udaljenosti. Kako bi se prekinuo lanac zaraze, ključno je što brže utvrditi osobe koje su bile u blizini zaražene osobe. Blizina se utvrđuje s obzirom na udaljenost i trajanje kontakta te bi je trebalo utvrđivati s epidemiološkog gledišta. Prekid lanca zaraze posebno je važan kako bi se izbjegla ponovna pojava zaraze u fazi izlaska iz krize.

Za to bi mogli biti potrebni podaci o blizini. Čini se da je za mjerenje blizine i bliskih kontakata komunikacija među uređajima u sustavu Bluetooth niske razine energije preciznija i stoga primjerenija od uporabe geolokacijskih podataka (GNSS/GPS ili podaci o lokaciji mobilnih telefona). Korištenjem sustava Bluetooth niske razine energije izbjegava se mogućnost praćenja (za razliku od geolokacijskih podataka). Stoga Komisija preporučuje korištenje komunikacijskih podataka iz sustava Bluetooth niske razine energije (ili podataka dobivenih istovrijednom tehnologijom) za utvrđivanje blizine.

Lokacijski podaci nisu potrebni za funkciju praćenja kontakata jer njezin cilj nije praćenje kretanja pojedinaca ni provedba mjera. Usto, bilo bi teško opravdati obradu lokacijskih podataka u kontekstu praćenja kontakata s obzirom na načelo smanjenja količine podataka te bi takva obrada mogla prouzrokovati probleme u smislu sigurnosti i privatnosti. Zbog toga Komisija ne savjetuje korištenje lokacijskih podataka u tom kontekstu.

Neovisno o tehničkim sredstvima koja se koriste za utvrđivanje blizine, čini se da nije nužno pohranjivati točno vrijeme ili mjesto kontakta (ako je dostupno). Međutim, moglo bi biti korisno pohraniti dan kontakta kako bi se znalo je li do kontakta došlo kada je osoba razvila simptome (ili 48 sata prije ([13])) te kako bi se prilagodila poruka sa savjetom, na primjer o trajanju samoizolacije.

Podaci o blizini trebali bi se generirati i obrađivati samo ako postoji stvarna opasnost od zaraze (ovisno o blizini i trajanju kontakta).

Treba napomenuti da će neophodnost i proporcionalnost prikupljanja podataka ovisiti o čimbenicima kao što je dostupnost testiranja, posebno ako su već naložene mjere kao što je izolacija. Upozoravanje osoba koje su bile u bliskom kontaktu sa zaraženom osobom može se izvesti na dva načina:

Prvi je način da se upozorenje bliskim kontaktima automatski šalje aplikacijom kada korisnik obavijesti aplikaciju – uz uvjet odobrenja ili potvrde zdravstvenog tijela, na primjer s pomoću QR ili TAN koda – da se testirao i da je pozitivan (decentralizirana obrada). Preporučljivo je da zdravstveno tijelo određuje sadržaj poruke upozorenja. Drugi je način da se nasumični privremeni identifikatori pohranjuju na backend poslužitelju zdravstvenog tijela (rješenje s backend serverom). Korisnike se pomoću tih podataka ne smije moći izravno identificirati. Identifikatori omogućuju da korisnici koji su bili u bliskom kontaktu s korisnikom koji se testirao i pozitivan je dobiju upozorenje na svoj uređaj. Ako se zdravstvena tijela žele obratiti korisnicima koji su bili u bliskom kontaktu sa zaraženom osobom i telefonom ili SMS-om, za dobivanje njihovih brojeva telefona trebaju pristanak tih korisnika.

([13]) Zaražena osoba zarazna je 48 sati prije pojave simptoma.

3.5 **Ograničavanje otkrivanja podataka/pristupa podacima**

— Funkcija informiranja:

Podaci koji se pohranjuju u terminalnoj opremi i kojima se pristupa s pomoću terminalne opreme ne smiju se dijeliti sa zdravstvenim tijelima u većoj mjeri nego što je to nužno za funkciju informiranja. Budući da ta funkcija osigurava samo sredstvo komunikacije, zdravstveno tijelo neće imati pristup drugim podacima.

— Funkcije provjere simptoma i telemedicine:

Funkcija provjere simptoma može biti korisna državama članicama kako bi mogle savjetovati građanima trebaju li se testirati, pružiti informacije o izolaciji i o tome kada i kako zatražiti liječničku pomoć, posebno kad je riječ o ugroženim skupinama. Ta funkcija može nadopunjavati nadzor u okviru primarne zdravstvene skrbi i može pomoći u procjeni stope zaraze stanovništva bolešću COVID-19. Stoga se može donijeti odluka da bi nadležna zdravstvena tijela i nacionalna epidemiološka tijela trebala imati uvid u informacije koje pruža pacijent. Europski centar za sprečavanje i kontrolu bolesti mogao bi dobivati agregirane podatke od nacionalnih tijela za svrhe epidemiološkog nadzora.

Ako se odluči omogućiti kontakt sa zdravstvenim djelatnicima, a ne isključivo putem same aplikacije, potrebno je dati i telefonski broj korisnika aplikacije nacionalnim zdravstvenim tijelima.

— Funkcija praćenja kontakata i upozoravanja:

— Podaci zaražene osobe

Aplikacije generiraju pseudonasumične kratkotrajne, periodično promjenjive identifikatore telefona koji su u kontaktu s korisnikom. Jedna je mogućnost da se identifikatori pohranjuju na uređaj korisnika (takozvana decentralizirana obrada). Druga je mogućnost da se ti nasumični identifikatori pohranjuju na serveru kojem imaju pristup zdravstvena tijela (takozvano rješenje s backend serverom). Decentralizirano je rješenje u većoj mjeri u skladu s načelom smanjenja količine podataka. Zdravstvena tijela trebala bi imati pristup samo podacima o blizini s uređaja zaražene osobe kako bi mogla kontaktirati osobe kojima prijeti opasnost od zaraze.

Ti bi podaci bili dostupni zdravstvenim tijelima tek nakon što ih zaražena osoba (nakon što se testira) proaktivno podijeli s njima.

Zaraženoj osobi ne bi trebalo otkriti identitet osoba s kojima je bila u potencijalno epidemiološki relevantnom kontaktu i koje će biti upozorene.

— Podaci osoba koje su bile u (epidemiološkom) kontaktu sa zaraženom osobom

Identitet zaražene osobe ne bi trebalo otkriti osobama s kojima je ona bila u epidemiološkom kontaktu. Dovoljno im je javiti da su tijekom proteklih 16 dana bili u epidemiološkom kontaktu sa zaraženom osobom. Kako je već navedeno, podaci o vremenu i mjestu takvih kontakata ne bi se smjeli čuvati. Stoga nije ni nužno ni moguće dojavljivati takve podatke.

Kako bi se pratilo epidemiološke kontakte korisnika aplikacije za kojeg je utvrđeno da je zaražen, nacionalna zdravstvena tijela trebala bi biti obaviještena samo o identifikatoru osobe s kojom je zaražena osoba bila u epidemiološkom kontaktu u razdoblju koje je započelo 48 sati prije pojave simptoma i završilo 14 dana nakon pojave simptoma, i to prema načelu blizine i trajanja kontakta.

Europski centar za sprečavanje i kontrolu bolesti od nadležnih bi tijela mogao primati agregirane podatke o praćenju kontakata za svrhe epidemiološkog nadzora indikatora definiranih u suradnji s državama članicama.

3.6 **Propisivanje točnih svrha obrade**

Za svrhe obrade mora postojati pravni temelj (u pravu Unije ili države članice). Svrha bi trebala biti konkretna i eksplicitna, tako da nema sumnje koju je vrstu osobnih podataka potrebno obraditi kako bi se postigao očekivani cilj.

Točna svrha odnosno svrhe ovisit će o funkcijama aplikacije. Svaka funkcija aplikacije može imati više od jedne svrhe. Kako bi se građanima dala potpuna kontrola nad njihovim podacima, Komisija predlaže da se različite funkcije ne spajaju. U svakom slučaju građanin bi trebao imati mogućnost izbora različitih funkcija, od kojih svaka ima zasebnu svrhu.

Komisija ne preporučuje korištenje podataka prikupljenih u gore navedenim uvjetima za bilo koje druge svrhe osim suzbijanja bolesti COVID-19. Ako podaci budu potrebni za druge svrhe, kao što su znanstvena istraživanja i statistika, te bi svrhe trebalo uključiti u prvobitni popis svrha i o tome jasno obavijestiti korisnike.

— Funkcija informiranja:

Svrha te funkcije je pružanje informacija koje su relevantne s točke gledišta zdravstvenih tijela u kontekstu krize.

— Funkcije provjere simptoma i telemedicine:

Funkcija provjere simptoma može pružiti naznake koliki je udio osoba koje prijavljuju simptome koji odgovaraju bolesti COVID-19 stvarno zaražen (npr. uzimanjem briseva i testiranjem svih ili nasumičnog broja osoba s takvim simptomima, ako postoje kapaciteti za to). U identifikaciji svrhe trebalo bi jasno navesti da će se osobni zdravstveni podaci obraditi u cilju: i. pružanja mogućnosti pojedincu da samostalno procijeni, na temelju skupa pitanja, ima li simptome bolesti COVID-19, ili ii. dobivanja liječničkog savjeta ako ima simptome bolesti COVID-19.

— Funkcije praćenja kontakata i upozoravanja:

Jednostavno navođenje svrhe „prevencije daljnje zaraze bolešću COVID-19” nije dovoljno konkretno. U tom slučaju Komisija predlaže dodatno specificiranje svrhe/svrha u smislu: „čuvanje kontakata osoba koje se koriste aplikacijom i koje su možda bile izložene zarazi bolešću COVID-19 kako bi se upozorilo osobe koje su možda zaražene”.

3.7 **Strogo ograničavanje čuvanja podataka:**

Načelom ograničenja pohrane uvjetuje se da se osobni podaci ne smiju čuvati dulje nego što je to neophodno. Trajanje čuvanja podataka trebalo bi ovisiti o medicinskoj važnosti (ovisno o namjeni aplikacije: razdoblje inkubacije itd.) te realnom trajanju administrativnih koraka koje će možda trebati poduzeti.

— Funkcija informiranja:

Ako se prilikom instalacije ove funkcije prikupe bilo kakvi podaci, trebaju se odmah izbrisati. Nema opravdanja za čuvanje takvih podataka.

— Funkcije provjere simptoma i telemedicine:

Te bi podatke trebala izbrisati zdravstvena tijela nakon najviše mjesec dana (razdoblje inkubacije plus rezerva) ili nakon što se osoba testirala, a rezultat je negativan. Zdravstvena tijela mogu za svrhe izvješćivanja o nadzoru i za svrhe istraživanja zadržati podatke i duže, pod uvjetom da su ti podaci anonimizirani.

— Funkcije praćenja kontakata i upozoravanja:

Podaci o blizini trebali bi biti izbrisani čim ne budu više nužni za svrhe upozoravanja osoba. To bi trebalo biti nakon najviše mjesec dana (razdoblje inkubacije plus rezerva) ili nakon što se osoba testirala, a rezultat je negativan. Zdravstvena tijela mogu za svrhe izvješćivanja o nadzoru i za svrhe istraživanja zadržati podatke o blizini i duže, pod uvjetom da su ti podaci anonimizirani.

Podatke bi trebalo pohranjivati na korisnikovu uređaju, a na server koji je dostupan zdravstvenim tijelima, ako se odabere ta mogućnost, trebalo bi učitati samo podatke koje su poslali korisnici i koji su neophodni za predmetnu svrhu (tj. učitati na server samo podatke o „bliskim kontaktima” osobe za koju se testiranjem pokazalo da je zaražena bolešću COVID-19).

3.8 **Briga za sigurnost podataka**

Komisija preporučuje da se podaci pohranjuju na terminalnom uređaju pojedinca u šifriranom obliku upotrebom naprednih kriptografskih tehnika. Ako se podaci pohranjuju na centralnom serveru, pristup tom serveru – uključujući i administrativni pristup – trebao bi se evidentirati.

Podaci o blizini trebali bi se generirati i pohranjivati samo na terminalnom uređaju osobe, šifrirano i u obliku pseudonima. Kako bi se osiguralo da je isključena mogućnost praćenja koje vrše treće strane, aktivacija Bluetootha trebala bi biti moguća bez aktiviranja drugih usluga lokacije.

Tijekom prikupljanja podataka o blizini putem sustava Bluetooth niske razine energije preporučuje se da se kreiraju i pohranjuju privremeni korisnički identifikatori koji se redovito mijenjaju, a ne da se pohranjuje stvarni identifikator uređaja. Ta mjera pruža dodatnu zaštitu od hakera koji bi mogli prisluškivati i pratiti uređaj, i otežava identifikaciju osoba.

Komisija preporučuje da izvorni kod aplikacije bude javan i dostupan za provjeru.

Mogu se predvidjeti i dodatne mjere za osiguravanje obrađenih podataka, uključujući brisanje ili anonimizaciju podataka nakon isteka određenog razdoblja. Općenito bi stupanj sigurnosti trebao biti u skladu s količinom i osjetljivošću osobnih podataka koji se obrađuju.

Sve bi komunikacije između osobnog uređaja i nacionalnih zdravstvenih tijela trebale biti šifrirane.

Ako se nacionalnim pravom propisuje da se prikupljeni osobni podaci mogu obrađivati za svrhe znanstvenih istraživanja, u načelu bi trebalo pseudonimizirati podatke.

3.9 **Osiguravanje točnosti podataka**

Osiguravanje točnosti osobnih podataka koji se obrađuju nije samo preduvjet za učinkovitost aplikacije nego i zahtjev propisan Uredbom o zaštiti osobnih podataka.

U tom kontekstu ključno je osigurati točnost podataka o tome je li bilo kontakta sa zaraženom osobom (epidemiološka udaljenost i trajanje) kako bi se na najmanju mjeru smanjila mogućnost lažno pozitivnih rezultata. To se odnosi na scenarije kada su dva korisnika aplikacije u kontaktu na ulici, u sredstvu javnog prijevoza ili u zgradi. Nije vjerojatno da su podaci o lokaciji koji se temelje na mrežama mobilne telefonije dovoljno precizni za to.

Stoga se savjetuje oslanjanje na tehnologije koje omogućuju precizniju procjenu kontakta (na primjer Bluetooth).

3.10 **Uključivanje tijela za zaštitu podataka**

Tijela za zaštitu podataka trebala bi biti u potpunosti uključena i njihova mišljenja uzeta u obzir u kontekstu razvoja aplikacije te bi trebala kontrolirati uporabu aplikacije. S obzirom da će se obrada podataka u kontekstu aplikacije moći smatrati obradom posebnih kategorija podataka (zdravstvenih podataka) u velikim razmjerima, Komisija skreće pažnju na članak 35. Opće uredbe o zaštiti podataka o procjeni učinka na zaštitu podataka.

ISSN 1977-1088 (elektroničko izdanje)
ISSN 1977-060X (tiskano izdanje)

Ured za publikacije Europske unije
2985 Luxembourg
LUKSEMBURG

HR