Aplikacija „Stop COVID-19“

Procjena učinka na zaštitu podataka (*sažetak*)

Obrazloženje

Otkako se virus SARS-CoV-2 počeo širiti diljem Europe i svijeta početkom 2020. godine, javne i političke rasprave su se sve više usredotočile na tehnološko rješenje goruće problema. Može li se epidemija bolesti COVID-19 obuzdati korištenjem aplikacije na pametnom telefonu?

Takav sustav bi automatski evidentirao međuljudske kontakte korisnika i na taj način bi pravovremeno mogao anonimno informirati one koji su bili u epidemiološki relevantnom kontaktu s laboratorijskim nalazom potvrđenom COVID-19 oboljelom osobom. Tada bi se izloženi pojedinci mogli učinkovito obavijestiti oko postupanja u potencijalnoj ranoj fazi infekcije.

Kako bi usporili širenje bolesti COVID-19 među populacijom u Republici Hrvatskoj, Vlada Republike Hrvatske i Ministarstvo zdravstva razvili su aplikaciju **„Stop COVID-19“** koja obavještava korisnike da su bili u kontaktu s osobom kojoj je naknadno potvrđena zaraza bolešću COVID-19.

Aplikacija se temelji na servisu kojeg su zajednički razvili Google i Apple te koristi Bluetooth tehnologiju za razmjenu nasumičnih ključeva između pametnih uređaja korisnika koji su u epidemiološki relevantnom bliskom kontaktu. Ti kriptirani ključevi mijenjaju se nekoliko puta tijekom svakog sata, čime je dodatno zajamčena zaštita privatnosti korisnika.

Ako jedan od korisnika naknadno dobije pozitivan laboratorijski nalaz na COVID-19, može donijeti odluku da tu informaciju podijeli putem aplikacije korištenjem jednokratnog verifikacijskog kôda. Na taj način aplikacija utvrđuje je li korisnik bio u kontaktu sa COVID-19 pozitivnom osobom te, ako jest, navodi datum ostvarenog kontakta i preporučuje sljedeće korake. Preuzimanje aplikacije je dobrovoljno, i korisnik je može isključiti kad god želi. Podaci o ključevima razmjenjivat će se i putem EU federacijskog pristupnika (EFGS) i to samo u slučaju da korisnik nakon instalacije aplikacije omogući uključivanje postavke za prekograničnu razmjenu podataka. Instalacija i korištenje aplikacije ne zahtijeva registraciju korisnika niti se pritom traže ili bilježe osobni podaci, niti se u bilo kojem trenutku prikupljaju geolokacijski podaci korisnika.

Promatrajući planirane sustave za sprječavanje širenja COVID-19 diljem Europe, radi se o opsežnim socijalnim eksperimentima koji uključuju digitalno snimanje ponašanja pojedinaca pod državnim nadzorom. Učinkovitost i implikacije takvih aplikacija još se ne mogu predvidjeti i može se pretpostaviti da će se uvesti i ocjenjivati razne inačice.

Posljedice u pogledu zaštite podataka, a time i na temeljna prava, potencijalno neće utjecati samo na pojedince, već i na društvo u cjelini. Iz tog razloga, smatramo relevantnim provesti procjenu učinka na zaštitu podataka.

U čitav postupak uključeno je i hrvatsko nadzorno tijelo za zaštitu podataka, Agencija za zaštitu osobnih podataka (AZOP), s kojom se redovito provode savjetovanja u slučaju promjene funkcionalnosti aplikacije.

Sažetak procjene učinka na zaštitu podataka objavljen je dana 16. studenog 2020. godine. Ministarstvo zadržava pravo izmjene i ažuriranja ovog dokumenta.

Nalazi i procjena

Aplikacija „Stop COVID-19“ je u nadležnosti Ministarstva zdravstva Republike Hrvatske, Ksaver 200a, 10000 Zagreb, Republika Hrvatska, tel: 01 46 07 555. U skladu s propisima o zaštiti podataka, ministarstvo je **voditelj obrade** i odgovorno je za obradu podataka u sklopu aplikacije. **Izvršitelj obrade** je APIS IT d.o.o., Paljetkova 18, 10001 Zagreb. U slučaju potrebe, službenika za zaštitu podataka u ministarstvu možete kontaktirati na gore navedenoj adresi ili slanjem e-pošte na zastita.podataka@miz.hr.
Opis obrade koja je predmet procjene, mjere koje doprinose pravima korisnika aplikacije i kako su kontrolirani eventualni rizici za prava korisnika sadržani su u odgovorima na pitanja iz ove procjene.

Je li obavezna uporaba aplikacije?

Instalacija i korištenje aplikacije u potpunosti je dobrovoljno. Korisnici samostalno odlučuju hoće li preuzeti instalaciju na svoj mobilni uređaj, kako će je koristiti i kada će ukloniti aplikaciju sa svojeg mobilnog uređaja. Korisnici sami odlučuju hoće li omogućiti razmjenu anonimnih ključeva i putem European Federated Gateway servisa. Pravna osnova za obradu podataka je izvršavanje zadaće od javnog interesa.

Koje se vrste podataka obrađuju i gdje?

Nasumični ključevi kontakata i zaraženih osoba, jednokratni verifikacijski kôd te datum kontakta dva korisnika. Aplikaciju mogu koristiti i maloljetne osobe, no sustav to ne provjerava niti utvrđuje. Obrada uparivanja nasumičnih ključeva se odvija isključivo na mobitelu korisnika, jednokratni verifikacijski kôd aplikacija komunicira prema nacionalnom pozadinskom sustavu kriptiranim i zaštićenim kanalima.

Podaci koji se obrađuju korištenjem Aplikacije nalaze se na mobilnom uređaju korisnika, na poslužiteljima Aplikacije u Republici Hrvatskoj ili drugoj zemlji članici Europske unije. Podaci se ne prenose u treće zemlje.

Koji je opseg obrade podataka?

Da bi aplikacija bila što učinkovitija potrebno je da ju instalira što veći dio populacije. Geografsko područje pokriva čitav teritorij Hrvatske, a nakon uspostave interoperabilnosti sa državama članica EU koje koriste iste Google/Apple servise ostvarit će se i razmjena ključeva s poslužiteljima u tim zemljama. Isključena je mogućnost daljnje obrade u svrhe koje nisu povezane s upravljanjem zdravstvenom krizom koju je izazvao virus COVID-19. Podaci će se koristiti za vrijeme epidemije s mogućnošću gašenja aplikacije u slučaju mogućeg opterećivanja zdravstvenog sustava ili radi završetka epidemije.

Koja je priroda odnosa između ispitanika te voditelja i izvršitelja obrade?

Voditelj i izvršitelj obrade ne mogu saznati tko su korisnici jer ne postoji nikakav popis niti registar korisnika aplikacije. Jedini podatak koji korisnik dobrovoljno unosi u aplikaciju je verifikacijski kôd, generiran od strane nadležnog zdravstvenog djelatnika nakon pozitivnog laboratorijskog nalaza na zarazu, radi omogućavanja slanja obavijesti drugim korisnicima o izloženosti zarazi. Korisnik ne unosi nikakve druge

podatke i može u bilo kojem trenutku ukloniti aplikaciju s uređaja. Ne postoji nikakva praktična mogućnost intervencije u obradu podataka.

Kakva je zrelost tehnologije?

Aplikacija uključuje primjenu potpuno nove tehnologije i načina obrade podataka. Tehnologija je u ranim fazama primjene, no nema posebne zabrinutosti jer se istim metodama koristi ili se planira koristiti većina članica EU i ostale zemlje koje odluče funkcionalnosti svojih aplikacija osloniti na Google/Apple servise za obavještavanje o izloženosti. Europska komisija u suradnji sa Svjetskom zdravstvenom organizacijom pripremaju zajednički okvir za procjenu učinkovitosti korištenja ovih aplikacija.

Je li obrada podataka razmjerna pravnoj osnovi?

Aplikacija je ograničena samo na najnužnije podatke i koristi Google/Apple servis koji je sastavni dio operacijskog sustava (Android ili iOS) na mobilnom uređaju, prema javno dostupnoj dokumentaciji, opisu rada i arhitekturi aplikacije te izvornom programskom kôdu. Obrada podataka svedena je na strogi minimum, te se obrađuju isključivo nužni podaci u skladu sa svrhom (ne obrađuju se identifikatori uređaja, geolokacijski podaci, komunikacijski identifikatori i dr.)

Koje informacije o obradi podataka ima ispitanik?

Korisnik prije instalacije aplikacije ili kasnije u bilo kojem trenutku u samoj aplikaciji ima mogućnost pročitati Politiku privatnosti, Uvjete korištenja, Izjavu o pristupačnosti i korištene programske komponente. Sve informacije o aplikaciji su također dostupne putem Službene stranice Vlade za pravodobne i točne informacije o koronavirusu na mrežnoj adresi koronavirus.hr.

Kakva je sigurnost podataka?

Izvršitelj obrade osigurava povjerljivost, cjelovitost i raspoloživost podataka sukladno standardima i najboljim praksama (izrada sigurnosnih kopija, ograničene ovlasti na produkcijskoj bazi podataka, itd.), a neporecivost je osigurana izradom i nadzorom dnevničkih zapisa. Sustav je također podvrgnut provjeri ranjivosti te nisu uočeni nedostaci. Izvršitelj obrade posjeduje važeći certifikat ISO 27001. Za razmjenu podataka između nacionalnog sustava i European Federated Gateway servisa koristi se sigurnosna arhitektura definirana na razini eHealth Network-a.

Kako je očuvana privatnost korisnika?

Izvršitelj obrade je u fazi dizajna primijenio principe očuvanja privatnosti i sve značajke početno postavio na način da očuvaju privatnost korisnika te time neutralizirao navedene rizike i sveo ih na najmanju moguću mjeru. Poduzete su sve dostupne i odgovarajuće mjere za sprječavanje identifikacije korisnika aplikacije. U cilju prosudbe usklađenosti aplikacije s Općom uredbom o zaštiti podataka, kao i smjernicama i mišljenjima Europskog odbora za zaštitu podataka o korištenju podataka o lokaciji te interoperabilnosti alata za praćenje kontakata sa zaraženima u kontekstu epidemije bolesti COVID-19 sa Agencijom za zaštitu osobnih podataka (AZOP) je provedeno prethodno savjetovanje.

Kako je osigurana usklađenost s obvezama i postupanje izvršitelja obrade? Odlukama Vlade Republike Hrvatske i ministra zdravstva, ugovornom obavezom

izvršitelja obrade, implementacijom svih potrebnih procedura i protokola za zaštitu podataka te poštivanjem zakonskih propisa.

Obrađuju li se podaci o zdravstvenom stanju?

Ne obrađuju se. Postupak se sastoji od obrade podataka o kontaktima na mobilnim uređajima koji imaju aktiviranu aplikaciju, prijenosa tih podataka na poslužitelj nakon pozitivne dijagnoze i distribucije tih podataka na sve ostale mobilne uređaje radi utvrđivanja postojanja mogućih kontakata s oboljelim osobama. Aplikacija ne daje zdravstvene savjete niti joj je zadatak zamijeniti liječnike ili drugo zdravstveno osoblje u liječenju pacijenata bilo vezano uz bolest COVID-19 ili bilo koje druge bolesti i zaraze.

Je li moguća de-anonimizacija korisnika?

Upućivanje na fizičku osobu je učinkovito i nepovratno odvojeno od obrađenih podataka višedimenzionalnim pristupom, tako da je spriječena mogućnost ponovne identifikacije korisnika . Primjenom pravnih, tehničkih i organizacijskih mjera osigurava se učinkovito i nepovratno razdvajanje podataka u praksi što rezultira neidentificirajućim podacima koji ukazuju na izloženost bolesti, a koji se pohranjuju na poslužitelj i distribuiraju na ostale aplikacije.