ANALIZA APLIKACIJE STOP COVID-19

Politiscope, veljača 2021.

UVOD

Premda je uobičajeni proces epidemiološkog praćenja kontakata zaraženih i izloženih osoba u svrhu sprečavanja širenja virusa COVID-19 donosio opipljive rezultate, istovremeno su uočene i brojne manjkavosti. Osim što zahtijeva značajne ljudske resurse, radi se o sporom procesu jer uključuje vrijeme čekanja dostave pozitivnih rezultata testiranja. Naposljetku, ovisi o sjećanju osobe o svim kontaktima ostvarenima kroz nekoliko dana. Manjkavost ovog modela je i što se oslanja na dobru volju zaražene osobe da prijavi sve svoje kontakte. Naime, praksa je pokazala da, u slučaju prisustvovanju događanju s većim brojem ljudi, **građani ponekad odbijaju surađivati** s epidemiolozima zbog straha da će biti osuđivani ili kritizirani. Stoga se već u ranim fazama pandemije razmatrala tehnologija koja bi mogla omogućiti digitalno praćenje kontakata putem pametnih mobilnih uređaja, koje danas koristi poprilično visok postotak građana. Ubrzo je krenuo razvoj potrebnih tehnologija i protokola te je od samog početka bilo jasno kako ovakve aplikacije mogu biti učinkovite samo ako javnost u njih ima potpuno povjerenje. Jedan od ključnih uvjeta koje takve aplikacije moraju ispuniti je potpuna zaštita privatnosti korisnika aplikacije, s obzirom da podrazumijevaju obradu osjetljivih podataka građana, zbog kojih oni potencijalno mogu biti i diskriminirani.

Prve aplikacije koristile su **GPS za praćenje blizine** dvaju uređaja, no ubrzo se Bluetooth pokazao znatno efikasnijom tehnologijom za ovu svrhu: precizniji je u zatvorenim prostorima, može jasnije otkriti duljinu međusobnog kontakta, a omogućuje decentraliziran pristup u kojem osobni podaci ne napuštaju uređaj korisnika. Tehnološki giganti Apple i Google u travnju su objavili partnerski rad na tehnologiji za praćenje kontakata, sada poznatom kao ***Exposure Notifications***, koja koristi Bluetooth i radi na Googleovim Android mobilnim uređajima, kao i na Appleovim iPhoneovima. Tehnologija je dizajnirana s ciljem da zabilježi kontakt jedne osobe s drugom i pošalje taj zapis u decentraliziranu bazu, a funkcionira tako da se tehnologija implementira u aplikacije koje moraju razviti zdravstvene javne ustanove svake države.

Prednost suradnje dvaju giganata je globalni doseg, budući da je riječ o vlasnicima najvećih mobilnih platformi (iOS i Android), dok zajednički razvoj omogućuje funkcioniranije aplikacija na obje platforme. Tijekom razvoja su isticani fokus na privatnost, transparentnost te kontrolu od strane korisnika. U svibnju 2020., **Google/Apple Exposure Notification (GAEN)** je službeno izdan i implementirale su ga brojne države u svrhu praćenja kontakata. Ministarstvo zdravstva RH **predstavilo je 27. srpnja 2020. aplikaciju Stop COVID-19**, koju je razvila tvrtka APIS IT. Istaknuli su, kako je sukladno preporukama EU aplikacija Stop COVID-19: dobrovoljna, transparentna, privremena, kibernetički sigurna te koristi samo privremene i pseudoanonimne podatke.

Razine korištenja aplikacije u Hrvatskoj su **izrazito niske**. Statistika korištenja aplikacije na **službenoj stranici** posljednji put je osvježena u veljači, do kada je aplikaciju preuzelo preko 85 tisuća građana. Poražavajuća je informacija da je od desetak tisuća verifikacijskih kodova, koje su doktori izdali zaraženim osobama kako bi unosom u aplikaciju obavijestili bliske kontakte o izloženosti virusu, iskorišteno tek njih pedesetak.

Izuzev niskog interesa Vlade za promociju korištenja alata, dio objašnjenja zasigurno leži i u nedostatku povjerenja građana u potpunu zaštitu privatnosti korisnika, koje je u nekim zemljama EU istaknuto kao bitan faktor koji utječe na razine korištenja. Ministar Beroš je u srpnju 2020. najavio da bi najesen mobilna aplikacija **mogla postati obvezna za sve građane**, što bi bilo protuzakonito, protuustavno i u suprotnosti s pravom EU. Iako ovakav prijedlog više nikada nije iznesen u javnosti, pretpostavka je da je ova najava također doprinijela niskim razinama dobrovoljnog korištenja aplikacije.

Politiscope smatra kako ovakva i slična rješenja mogu biti od iznimne koristi u budućnosti, no istodobno smo uvjereni da mogu biti učinkovita isključivo ako uživaju puno povjerenje građana i javnosti. Smatramo da se javno povjerenje građana, kao preduvjet za široku dobrovoljnu upotrebu ovakve tehnologije, može izgraditi jedino kroz najvišu razinu zaštite privatnosti te punu transparentnost prema korisnicima. Ova analiza je stoga usmjerena na detekciju eventualnih nedostataka u zaštiti privatnosti i osobnih podataka korisnika te uključuje pravno-tehničku analizu s ciljem ocjene usklađenosti aplikacije s javno dostupnim informacijama o njenom radu te temeljnim načelima Opće uredbe o zaštiti podataka. Analiza je namijenjena donositeljima odluka u izvršnoj vlasti, u čiji raspon odgovornosti spada i razvoj digitalnih rješenja za upravljanje pandemijom. Analiza sadrži preporuke koje treba primijeniti prilikom izrada budućih digitalnih rješenja, posebice onih koji su kreirani zbog upravljanja eventualnim novim pandemijama. Pravnu analizu aplikacije proveo je Duje Kozomara, zamjenik izvršnog direktora udruge Poltiscope, stručnjak za zaštitu osobnih podataka certificiran od organizacije International Association of Privacy Professionals (IAPP). Tehničku analizu koda aplikacije proveli su developeri – Tomislav Homan (Flabbergast d.o.o) za Android, Ivan Blagajić (Source Code d.o.o) za iOS.

O KORIŠTENOJ TEHNOLOGIJI

Exposure Notification tehnologija funkcionira na način da se nasumični (randomizirani) ključevi dodijeljuju svim mobitelima, a uređaji koji se nalaze u blizini kontinuirano razmjenjuju svoje ključeve putem Bluetooth veze. Korisnici koji dobiju pozitivan laboratorijski nalaz mogu dobrovoljno poslati svoje nasumične ključeve emitirane u prethodnom razdoblju, čime oni postaju dostupni ostalim korisnicima aplikacije. Aplikacija povremeno provjerava ključeve koji su

podijeljeni s poslužiteljem i uspoređuje ih s ključevima koji su pohranjeni na uređaju, a korisnik dobiva obavijest ako je aplikacija pronašla podijeljeni ključ na njegovom mobitelu. Ako je korisnik bio u kontaktu s osobom koja je nakon pozitivnog nalaza podijelila svoje ključeve, dobit će obavijest i uputu kako postupiti. Za funkcioniranje aplikacija ne treba podatak gdje je niti s kime korisnik bio u kontaktu, čime se štiti privatnost korisnika.

Google i Apple razvili su pozadinski *Exposure Notification* servis, dok je državama ostavljen razvoj i pokretanje tzv. klijent aplikacije, koja pruža korisničko sučelje te je zadužena za: komunikaciju s back-end serverima države s cljem učitavanja ključeva zaražene osoba; preuzimanje objavljenih ključeva kako bi korisnici mogli provjeriti jesu li bili u kontaktu sa zaraženom osobom; preuzimanja osvježenja za postavke aplikacije.

Uloga Google/Apple *Exposure Notification* servisa (dalje u tekstu: GAEN) je upravljanje prijenosom i prijemom Bluetooth LE beacona te bilježenje trajanja i jačine signala primljenih beacona – zbog čega igra centralnu ulogu u funkcionalnosti aplikacija.

Istraživanje na Sveučilištu Trinity u Dublinu ukazalo je na ozbiljan problem vezan uz zaštitu privatnosti korisnika ove tehnologije kod Android verzije. Naime, na Googleovoj platformi događa se učestalo slanje osobnih podataka o korisnicima Google Play servisu - koji inače služi za ažuriranje aplikacija na Android mobilnim telefonima. Upravo je funkcioniranje Google Play Servicea iznimno zabrinjavajuće jer servis šalje zahtjeve Googleovim serverima u prosjeku svakih 20 minuta, svaki put dijeleći niz podataka: IMEI uređaja, serijski broj hadrvera, serijski broj SIM kartice, telefonski broj uređaja, WiFiMAC adresu, kao i e-mail adresu korisnika. Svi navedeni podaci šalju se Googleu, zajedno s metapodacima o korištenju svih aplikacija na telefonu.

Niz navedenih podataka ujedno čini identifikatore koji omogućavaju da zahtjevi s istog uređaja budu naknadno povezani, zbog čega Google može detaljno prikupljati podatke o korisnicima aplikacija u svrhu profiliranja. Navedena praksa ne samo da je u potpunoj suprotnosti sa svim obećanjima vezanim uz najveći mogući stupanj privatnosti korisnika prilikom upotrebe servisa, nego je i direktno kršenje najosnovnijih načela Opće uredbe o zaštiti podataka (dalje u tekstu: Uredba).

Iako klijent aplikacije, razvijane uz suradnju sa zdravstvenim javnim tijelima, uglavnom imaju objavljene i Procjene učinka na zaštitu podataka (ili barem sažetak, kao u slučaju Hrvatske), iznimno je problematično da ovakav dokument (s detaljnim opisom rizika tehnologije i poduzetim mjerama za njihovo otklanjanje) nikada nije objavljen za GAEN komponentu aplikacije.

PRAVNA ANALIZA STOP COVID-19 APLIKACIJE

Zaštita privatnosti dobila je relevantno mjesto u javnom predstavljanju hrvatske aplikacije Stop COVID-19: istaknute su metode kojima se štiti privatnost korisnika, objavljena pravila privatnosti koja pokrivaju osnovne zahtjeve Uredbe, čitavi kod aplikacije javno je objavljen na GitHubu te je naknadno objavljen i sažetak Procjene učnika na zaštitu podataka. Ovakav pristup svakako je napredak u smislu odnosa prema zaštiti osobnih podataka korisnika u usporedbi s bilo kojim digitalnim servisom prethodno izdanim od vlade ili hrvatskog javnog tijela.

Čitljivost i sadržaj Pravila privatnosti

Pravila privatnosti hrvatske aplikacije sadrže najosnovnije informacije sukladne zahtjevima Uredbe, no zapravo se radi o iznimno teško čitljivom i nepreglednom tekstu. Za početak, preglednost bi se mogla povećati umetanjem sadržaja na samom početku dokumenta, s hyperlinkanim naslovima poglavlja. U Journal of Medical Internet Researchu objavljeno je istraživanje fokusirano upravo na čitljivost politika privatnosti aplikacija za Covid-19 praćenje kontakata. Istraživanje je pokazalo da je za većinu aplikacija potrebna znatno viša sposobnost čitanja od one koju ima prosječni građanin te apelira na povećavanje razine čitljivosti, odnosno smanjenje razine sposobnosti čitanja potrebne za razumijevanje takvih dokumenata. Kako bi se to postiglo, potrebno je smanjiti duljine rečenica, uzimajući u obzir građane nižih razina obrazovanja, u čemu iznimno korisne mogu biti infografike i ilustracije. Ovakav pristup trebalo je primijeniti i prilikom kreiranja Pravila privatnosti hrvatske aplikacije te vrijedi i za izradu politika privatnosti za sva buduća digitalna rješenja.

Kontakt podaci službenika za zaštitu podataka nisu dovoljno istaknuti, iako se radi o jednom od ključnih elemenata ovakve obavijesti. Pozitivna praksa je da kontaktna mail-adresa bude objavljena u obliku linka s ciljem olakšanja slanja maila, što ovdje nije slučaj.

Jedna od obveznih stavki ovakve ovakve obavijesti prema Uredbi je i period zadržavanja podataka. Informacija o tome da se nasumični ključevi brišu u roku od 14 dana je navedena u tekstu, no nalazi se u sklopu opširnog dijela poglavlja „Korištenje Aplikacije“. Smatramo da bi takva informacija trebala biti jasnije istaknuta.

Kako je spomenuto ranije u analizi, nezavisna istraživanja pokazuju kako *Exposure Notification* servis funkcionira na način da Google Play Services Googleu šalje veću količinu podataka o korisniku u prosjeku svakih 20 minuta. Istovremeno, naša tehnička analiza koda hrvatske aplikacije pokazuje kako upravo Android verzija potpuno nepotrebno koristi i Google

Analytics, servis za analitiku koji tehnološkom gigantu šalje dodatan niz podataka o korištenju aplikacije. Navedene informacije znače da u Pravilima privatnosti Google mora biti naveden kao treća strana koja ima pristup podacima, a s tvrtkom mora biti potpisan ugovor koji uređuje takve obrade podataka. Navedeno nije slučaj i predstavlja ozbiljan propust. Dapače, objavljeni sažetak Procjene učinka na zaštitu podataka netočno navodi i pritom obmanjuje građane: „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.)".

U lipnju 2020., Apple je najavio uvođenje **obvezne sekcije s informacijama o privatnosti** za svaku aplikaciju objavljenu na App Storeu. Za aplikaciju Stop COVID-19 ti podaci u trenutku pisanja ove analize još uvijek nisu navedeni. Ako se Ministarstvo zdravstva odluči za prijavu nove verzije aplikacije, ovu sekciju će morati ispuniti. Nakon što se unesu, ove informacije se provjeravaju od strane Applea te imaju veću vjerodostojnost od informacija koje sam izdavač napiše u opisu aplikacije, što povećava transparentnost obrade podataka.

Neobjavljivanje ostale dokumentacije

Osim toga, postoje i određene nelogičnosti/neusklađenosti između Pravila o privatnosti i **Sažetka Procjene učinka na zaštitu podataka**. Naime, Sažetak Procjene kao izvršitelja obrade podataka navodi tvrtku APIS IT d.o.o., koja je razvila samu aplikaciju za Ministarstvo zdravstva Istovremeno, u Pravilima privatnosti APIS nije naveden kao poslovni subjekt koji ima bilo kakve veze s obradom podataka korisnika aplikacije. Sigurno nije korisno potencijalne korisnike zbunjivati neusklađenim i netočnim informacijama o ulozi APIS-a u obradi podataka.

Dok u Hrvatskoj imamo javno objavljen isključivo sažetak Procjene učinka na zaštitu podataka, ukupne duljine od svega 4 stranice, brojne druge EU članice pokazale su znatno višu razinu transparentnosti te su objavljene **sveobuhvatne Procjene učinka**, u kojima su detaljno identificirani rizici korištenja takvih aplikacija te mjera koje su poduzete da bi ih se rizici umanjili.

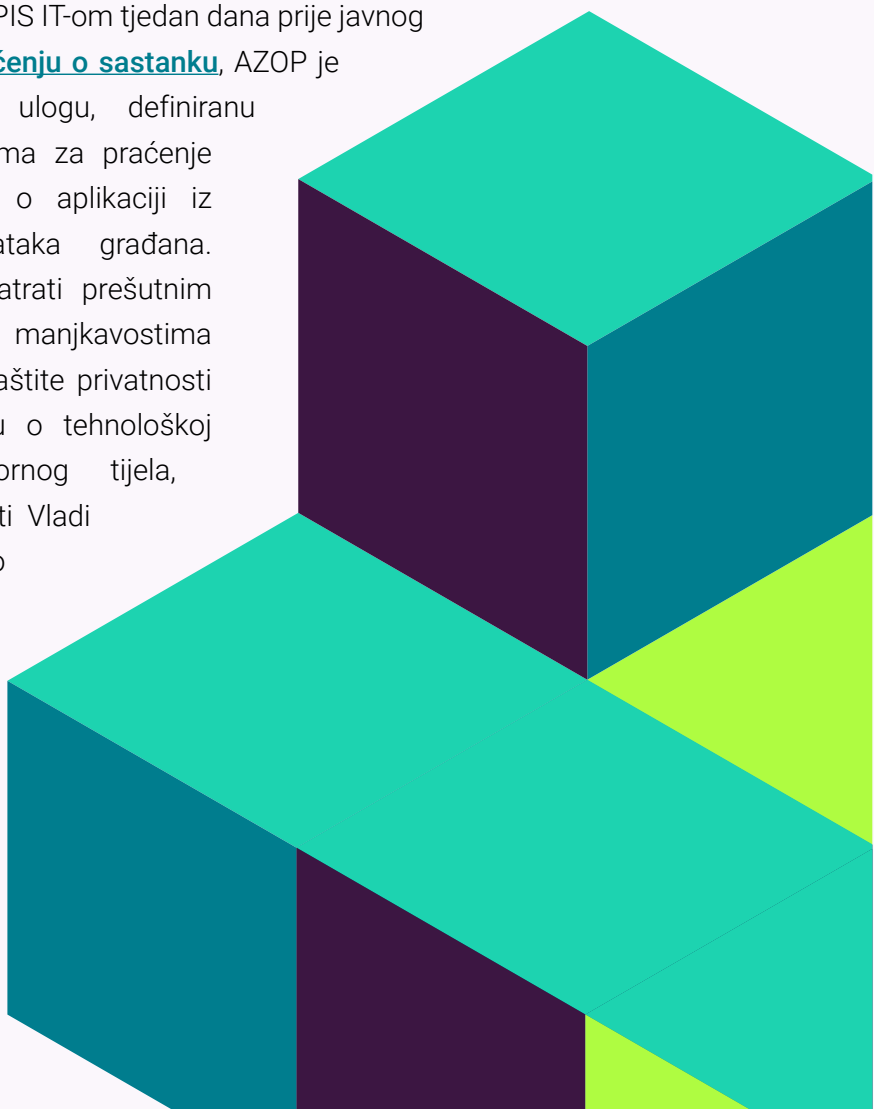
Osim toga, **neke države** javno su objavile i **niz dodatnih dokumenata** koji ujedno dokazuju usklađenost rada aplikacije sa **zahtjevima Europskog odbora za zaštitu podataka** te **Common EU toolboxa for member states**. Ovakvi dokumenti nisu kreirani u Hrvatskoj, te se usklađenost s navedenim zahtjevima spominje samo usputno. Hrvatska tijela javne vlasti propuštaju osiguranjem visokih razina transparentnosti izgraditi povjerenje građana u razvijenu tehnologiju.

Uloga nadzornog tijela za zaštitu podataka

Nadzorno tijelo za zaštitu podataka svake države odgovorno je za nadzor prikupljanja i obrade podataka koje provode klijent aplikacije GAEN-a. Brojne države imale su problema s izdavanjem aplikacija upravo jer su ih **nadzorna tijela zabranila** zbog brige da zaštita privatnosti korisnika nije na adekvatnoj razini. Primjerice, **litvansko nadzorno tijelo** je zabranilo aplikaciju jer je smatralo kako nije jasno objašnjeno tko je pravno odgovoran za rukovanje podacima, dok je **norveško tijelo objasnilo** kako je premalen broj korisnika preuzeo aplikaciju, zbog čega smatraju da alat nije dovoljno koristan ni važan da bi bio u upotrebi.

U kolovozu 2020., **nizozemsko nadzorno tijelo** također je zaključilo kako aplikacija u tom trenutku ne garantira privatnost korisnika te zbog toga ne može dobiti preporuku za korištenje. Istaknuli su važnost potpisivanja ugovora s Appleom i Googleom, kako bi se jasno uredilo što se točno događa s podacima korisnika kojima ove tvrtke mogu imati pristup. Također, nizozemsko tijelo smatra kako bi najlogičniji način reguliranja aplikacije bio donošenje novog zakonodavstva za njeno korištenje, koje bi postavilo jasnu pravnu osnovu za obradu njihovog ministarstva zdravstva, zajedno s garancijama privatnosti. Ističu kako nije dovoljno jasno što se događa na back-end serverima aplikacije niti tko je zadužen za sigurnost tog dijela.

S druge strane, hrvatska Agencija za zaštitu osobnih podataka održala je radni sastanak s Ministarstvom zdravstva i APIS IT-om tjedan dana prije javnog pokretanja aplikacije. U izdanom **priopćenju o sastanku**, AZOP je propustio ispuniti vlastitu ključnu ulogu, definiranu europskim dokumentima o aplikacijama za praćenje kontakta - nije zauzeo jasan stav o aplikaciji iz perspektive zaštite osobnih podataka građana. Izostanak kritike se stoga treba smatrati prešutnim zelenim svijetlom, unatoč očiglednim manjkavostima koje ne udovoljavaju uvjetu potpune zaštite privatnosti korisnika. Navedeno odgovara dojmu o tehnološkoj potkapacitiranosti hrvatskog nadzornog tijela, nesamostalnosti u radu i podređenosti Vladi RH, o čemu je Politiscope detaljno izvijestio u **Analizi rada Agencije za zaštitu osobnih podataka**. Također, radi se o još jednom primjeru izostanka proaktivnosti nadzornog tijela, detektiranom u **Politiscope analizi** praksi prikupljanja i obrade podataka uspostavljenih tokom pandemije.



TEHNIČKA ANALIZA KODA STOP COVID-19 APLIKACIJE

Tehnička analiza aplikacije rađena je prema izvornom kodu javno dostupnom na GitHubu, s fokusom na sljedeća pitanja: Koje osobne podatke aplikacija direktno prikuplja; Koje dozvole su prikupljene od strane korisnika te koji značajke operativnog sustava se koriste, a potencijalno bi mogle ugroziti sigurnost podataka; Ostavlja li se mogućnost da se odobrene dozvole povuku; Ostavlja li se mogućnost da se povuku dozvole specifične za ovu aplikaciju: dozvola za dijeljenje ključeva drugim uređajima i dozvola da se ključevi dijele s drugim europskim državama uključenim u projekt; Kako se postupa s lokalnim podacima i jesu li zaštićeni (kriptirani); Kako se postupa s podacima koji se šalju na poslužitelj i koristi li se protokol HTTPS; Kako se postupa s ključevima koji se dijele preko protokola BLE (Bluetooth Low Energy), jesu li zaštićeni; Koji 3rd party libraryji (odnosno softverske komponente trećih strana) se koriste te utječu li na sigurnost korisničkih podataka?

U sklopu ove analize ne možemo provjeriti na koji se način tretiraju podaci na poslužitelju Ministarstva zdravstva kao niti gdje su fizički pohranjeni ili kako se razmjenjuju s drugim europskim državama. Također, u segmentu koji se odnosi na funkcioniranje GAEN servisa i mrežnog prometa koji servis šalje prema *backend serverima*, oslanjamo se na nalaze dublinskog sveučilišta Trinity jer Politiscope u ovom trenutku nema tehnološke resurse za provedbu ovog tipa testiranja.

Direktno prikupljanje podataka

iOS verzija aplikacije ne koristi direktno identifikatore korisnika niti uređaja. Iste indikatore indirektno mogu koristiti servisi treće strane, što je obrađeno u poglavlju “Rješenja trećih strana”. Isto tako, iOS verzija ne traži pristup lokacijskim uslugama, iz čega možemo zaključiti da aplikacije ne koriste lokacijske podatke.

Analizom koda Android aplikacije, ustanovljeno je da se osobni podaci ni u kojem obliku ne sakupljaju direktno od korisnika te aplikacija ne prati direktno lokaciju korisnika.

Spremanje podataka na uređaj - iOS

Podaci se na uređaj spremaju korištenjem **UserDefaults** sučelja.
Ključevi i podaci koji se spremaju su:

- dateLastPerformedExposureDetection (datum zadnje provjere izloženosti)
- exposureDetectionErrorLocalizedDescription (informacije o mogućoj grešci pri provjeri izloženosti)

- urlCheckedList (lista URL-ova za provjeru izloženosti)
- transmissionRisk informacije (model koji opisuje rizik od prenošenja zaraze):
  - riskType (mali, srednji ili veliki tip rizika)
  - daysSinceLastExposure (broj dana od posljednje izloženosti)
  - dateOfExposure (datum izloženosti)
- transmissionRisk interni modeli, poput:
  - maximumRiskScoreFullRange (rezultat izloženosti; opisano u **Exposure Notification** dokumentaciji: "The value that represents the highest, full-range risk score of all the exposures for the user")
  - matchedKeyCount (broj izloženih ključeva; opisano u **Exposure Notification** dokumentaciji: "The number of keys that matched for an exposure
- detection")passedEnableExposure (informacije o tome je li korisnik već vidio obavijest o dijeljenju informacija o izloženosti)
- onboardingPassed (informacije o tome je li korisnik već prošao *onboarding*)
- consentToFederation (informacije o tome je li korisnik pristao da se ključevi izmjenjuju s drugim državama)

Spremanje podataka koristeći UserDefaults generalno se ne preporuča jer ti podaci **nisu enkriptirani ili na bilo koji način zaštićeni**. Apple od 8.3 verzije iOS-a nudi dodatan mehanizam zaštite, zbog čega je pristup podacima na disku otežan, čak i ako nisu enkriptirani.

Valja napomenuti da je u službenoj Appleovoj dokumentaciji i uputama kako koristiti *Exposure Notification* rješenje, u sekciji **Store User Data Locally**, također naveden primjer spremanja podataka koristeći UserDefaults, gdje Apple ističe da je user defaults privatna korisnička mapa koja ostaje na uređaju. Iako umanjeni rizik postoji, podaci koji se spremaju se ne smatraju osjetljivima.

Spremanje podataka na uređaj - Android

Od strane korisnika se prikupljaju dozvole za korištenje bluetooth tehnologije, pristup aplikacije Internetu, korištenje BLE tehnologije te Googleovog *exposure* sustava na kojem se ova aplikacija temelji. Sve dozvole i značajke su u skladu s namjenom

aplikacije te se ne zahtijeva više dozvola nego što je nužno. Sve odobrene dozvole se uvijek mogu povući u postavkama operacijskog sustava.

Dozvola za dijeljenje ključeva s drugim uređajima je isključena u tvorničkim postavkama aplikacije, što je pohvalno te se, ako se korisnik predomisli, mogu povući obje dozvole (dozvola za dijeljenje ključeva s drugim uređajima, dozvola za spremanje ključeva na poslužitelje unutar drugih EU zemalja koje su uključene u sustav).

Podaci koji se lokalno spremaju se ne kriptiraju. Lokalno se spremaju postavke jezika, pristanak na dijeljenje ključeva, kolekcija lokalnih ključeva, kolekcija ključeva s kojima smo bili u kontaktu, prijava da smo dobili pozitivan test. Postoji mala mogućnost da maliciozni korisnik dođe do tih podataka ako dođe u posjed uređaja. Savjetuje se zaštititi podatke prilikom lokalnog spremanja (u SharedPreferences). Podaci koji se šalju na poslužitelj zaštićeni su korištenjem HTTPS protokola.

Na **web stranicama s dokumentacijom za BLE** se napominje da su podaci koji se šalju preko Bluetooth konekcije dostupni svim aplikacijama, tako da bi se zaštita trebala koristiti na razini aplikacije. Ključevi koji se dijele u ovoj aplikaciji se ne kriptiraju, ali radi se o nasumičnim ključevima generiranim od strane Google libraryja, tako da u ovom slučaju kriptiranjem ne bi dobili na sigurnosti.

Rješenja trećih strana - iOS

Aplikacija koristi **CocoaPods** alat za utilizaciju nekih javno dostupnih rješenja razvijenih od trećih strana. Korištena rješenja su: **Alamofire 4.9.0**, **ObjectMapper 3.5.1**, **NVActivityIndicatorView 4.8.0**, **SwiftProtobuf 1.0**, **Zip 1.1.0**, **Lottie 3.1.8**.

Iako su sva rješenja popularna, često korištena i dobro održavana, bila bi potrebna detaljna analiza svakog od njih da bi se u potpunosti uklonio rizik od prikupljanja podatka i/ili sigurnosnih propusta. Na primjer, Lottie se koristi samo za animacije u aplikaciji te je upitno da li korist opravdava rizik s obzirom na činjenicu da je to alat koji je razvijen od strane Airbnba.

Rješenja trećih strana - Android

Uvidom u kod prikupljene su informacije koji se libraryji koriste u aplikaciji, koja verzija se koristi, je li korištenje libraryja ispravno navedeno u korisničkim postavkama, je li library koji se koristi nužan za funkcioniranje aplikacije te postoji li mogućnost da korišteni library sakuplja korisničke podatke. Sveobuhvatni pregled libraryja koji na neki način odskaču od željene primjene se nalazi u tablici koja je Prilog 1 ovom dokumentu, a niže u tekstu objašnjavamo njihovu kategorizaciju.

Esencijalni libraryji su dio standardnog paketa i njihovim korištenjem ne postoji mogućnost skupljanja osobnih podataka. Ovdje su navedeni samo zato što verzije koje se koriste ne odgovaraju verzijama koje su navedene u postavkama, čime korisnik ne dobiva točnu informaciju, ali isto ne predstavlja sigurnosni rizik. Posebno je izdvojen **library crashlytics** jer nije 100% esencijalan, ali je radi kvalitete aplikacije poželjno da se koristi jer nepravilnim logiranjem podataka postoji mogućnost curenja osobnih podataka. Detaljnijom analizom koda je utvrđeno da se u slučaju ove aplikacije koristi ispravno te je isto potrebno osigurati u daljnim verzijama aplikacije.

Libraryji koji nisu esencijalni niti dio standardnog paketa, ali su s godinama korištenja postali *de-facto* standardni libraryji koji su sigurni što se tiče zaštite osobnih podataka. Navedeni su ovdje zato što verzija koja se koristi ne odgovara verziji navedenoj u korisničkom sučelju. Izdvojen je library logging-interceptor čija je svrha logiranje mrežnog prometa i čijim nepravilnim korištenjem bi osobni podaci mogli procuriti. To upozorenje stoji i na **web stranicama samog libraryja**. Analizom koda je utvrđeno da se ovaj library niti ne koristi u aplikaciji te bi trebalo ukloniti ovisnost o tom libraryju.

Google analytics library je dio standardnog Googleovog paketa, ali nije esencijalan i svrha mu je prikupljanje podataka o korištenju aplikacije za razne marketinške svrhe. Iako se nigdje u kodu ne referenciraju osobni podaci korisnika, Google analytics library može slati fingerprint samog uređaja na Google poslužitelje, tako da ovaj library predstavlja rizik. Savjetuje se provjeriti s vlasnikom aplikacije postoji li doista potreba za uključivanje ovog libraryja te library ukloniti ako potreba ne postoji.

Libraryji koji su neesencijalni nisu dio standardnog paketa niti su *de-facto* standard, ne predstavljaju sigurnosni rizik, ali se mogu smatrati nepotrebnima u ovakvom tipu aplikacije. Na primjer, možda nije potrebno uključivati ovisnost o libraryju treće strane samo radi tipografije, animacija ili UI kontrola (FAB - floating action button). Upozorenje pogotovo vrijedi za library com.wang.avi:library na čijim je stranicama navedeno **da više nije podržan**.

KLJUČNI NALAZI ANALIZE KODA

iOS

Spremanje podataka koristeći UserDefaults sučelje može se smatrati sigurnosnim rizikom, no podaci koji se spremaju ne utječu na privatnost korisnika. Također, korištenje rješenja trećih strana nije poželjno u aplikaciji čiji je razvoj financiran javnim sredstvima i namjena je tako osjetljive prirode.

Najveća uočena manjkavost odnosi se na komunikaciju, tj nedostatak iste u sekciji s informacijama o privatnosti na Apple App Storeu. Nakon što se unesu, ove informacije se provjeravaju od strane Applea te imaju veću vjerodostojnost od informacija koje sam izdavač napiše u opisu aplikacije. Ipak, analizom koda, tehnologija i korištenih rješenja trećih strana, možemo zaključiti da aplikacija ne izlaže korisnike ozbiljnijem sigurnosnom riziku niti ugrožava njihovu privatnost.

Android

Kod aplikacije je načelno siguran iz perspektive zaštite osobnih podataka korisnika, uz nekoliko zamjerki.

Bilo bi poželjno ažurirati postavke aplikacije da pokažu točne verzije trenutno korištenih libraryja. Nadalje, za ovaj tip aplikacije trebalo bi ukloniti ovisnost o libraryjima treće strane koji nisu nužni, pogotovo ako nisu podržani. Trebalo bi ukloniti ovisnost o libraryju logging-interceptor koji se ionako niti ne koristi, a krivim korištenjem postoji mogućnost curenja podataka.

Manji sigurnosni rizik predstavlja činjenica da se lokalno sačuvani podaci ne kriptiraju, pogotovo jer kriptiranje nije teško postići te se stoga preporuča u daljnjem razvoju aplikacije.

Korištenje Google Analytics libraryja može se smatrati manjim do srednjim rizikom za zaštitu podataka u uobičajenim aplikacijama. Uaplikaciji koja obrađuje osjetljive podatke korisnika, razina procijenjenog rizika je svakako još veća. Preporučuje se uklanjanje ovisnosti o tom libraryju osim ako ne postoji valjani razlog neophodnog korištenja.

PREPORUKE

Povećanje transparentnosti

Kako bi se ostvarila dobrovoljna široka upotreba ovakvog tipa aplikacije, Pravila o privatnosti moraju biti razumljivije napisana te lakše čitljiva osobama nižih razina obrazovanja. Cilj je da apsolutno svi razumiju što se događa s njihovim podacima prilikom korištenja aplikacije. Istovremeno, ključne informacije, poput kontakta službenika za zaštitu podataka i perioda zadržavanja podataka trebaju biti jasnije istaknute. Korisnici moraju biti obaviješteni da Google može imati pristup određenim podacima vezanima uz korištenje aplikacije. iOS verziji na Appleovom App Storeu nedostaju informacije o privatnosti koje dodaju na vjerodostojnosti i povećavaju transparentnost funkcioniranja aplikacije.

Kako bi razina javnog povjerenja bila veća, potrebno je podignuti transparentnost oko funkcioniranja aplikacija na najvišu moguću razinu. To znači i objavu čitavog teksta Procjene učinka na zaštitu podataka te pratećih dokumenata koji dokazuju usklađenost sa smjernicama tijela EU. Digitalna rješenja ovog tipa mogu biti učinkovita isključivo ako uživaju puno povjerenje građana i javnosti. Smatramo da se javno povjerenje građana, kao preduvjet za široku dobrovoljnu upotrebu ovakve tehnologije, može izgraditi jedino kroz najvišu razinu zaštite privatnosti te punu transparentnost prema korisnicima.

Smanjenje uključenja trećih strana

Autori tehničkih analiza koda za obje verzije aplikacije su preporučili uklanjanje ovisnosti o trećim stranama koje nisu nužne za funkcionalnost aplikacije. Navedeno pogotovo vrijedi za Google Analytics na Android verziji, library procijenjen najvećim rizikom za zaštitu podataka. Način funkcioniranja Google Play servisa u Android verziji aplikacije iznimno je zabrinjavajuć sam po sebi, budući da Googleu u prosjeku svakih 20 minuta šalje čitav opseg podataka korisnika. Istovremeno, korištenjem Google Analyticsa, tom tehnološkom gigantu, poznatom i kao najvećem kršitelju privatnosti današnjice, šalje se dodatan set osobnih podataka. Poznato je da tvrtka takve podatke koristi u svrhu profiliranja i serviranja targetiranih oglasa korisnicima. Vjerujemo da građani zasigurno ne žele da se njihovi podaci povezani s informacijom jesu li bili u epidemiološki rizičnom kontaktu obrađuju na taj način bez njihovog znanja i eksplicitne privole.

AZOP kao samostalno i kapacitirano tijelo

Agencija za zaštitu osobnih podataka mora imati tehnološke kapacitete za samostalnu analizu digitalnih rješenja i detektiranje manjkavosti prepoznatih u ovoj analizi. Osim toga, zbog podređenog položaja Vladi, koji proizlazi iz trajnog sukoba interesa politički umreženog ravnatelja agencije, AZOP propušta biti stvarno neovisno nadzorno tijelo koje upozorava Vladu na manjkavosti digitalnih rješenja koje razvija, ili čak zabranjuje korištenje iste do saniranja svih ključnih manjkavosti.

PRILOG 1 – SOFTVERSKE KOMPONENTE TREĆIH STRANA (ANDROID)

Radi dužine prikaza, navedeni su samo libraryji koji na neki način odskaču od željene primjene.

Library	Verzija	Navedeno u postavkama	Je li nužan?	Mogućnost skupljanja podataka?	Kategorija
androidx.appcompat: appcompat	1.3.0-alpha02	Da, ali verzija 1.3.0-alpha01	Da	Ne	1
androidx.concurrent: concurrent-futures	1.1.0	Da, ali verzija 1.0.0	Da	Ne	1
androidx.constraintlayout: constraintlayout	2.0.2	Da, ali verzija 1.1.3	Da	Ne	1
com.google.android.material:material	1.3.0-alpha03	Da, ali verzija 1.3.0-alpha01	Da	Ne	1
com.google.android.gms: play-services-base	17.5.0	Da, ali verzija 17.3.0	Da	Ne	1
com.google.android.gms: play-services-tasks	17.2.0	Da, ali verzija 17.1.0	Da	Ne	1
androidx.work: work-runtime	2.4.0	Da, ali verzija 2.3.4	Da	Ne	1
com.google.firebase: firebase-messaging	20.3.0	Da, ali verzija 20.1.3	Da	Ne	1
com.google.firebase: firebase-core	17.5.1	Da, ali verzija 17.2.3	Da	Ne	1
com.google.firebase: firebase-analytics	**17.6.0**	**Nije navedeno**	**Ne**	**Da**	**3**
com.google.firebase: firebase-crashlytics	**17.2.2**	**Nije navedeno**	**Ne, ali poželjno**	**Ako se krivo koristi**	**1***
com.squareup.retrofit2: retrofit	2.9.0	Da, ali verzija 2.6.1	Da	Ne	2
com.squareup.retrofit2: converter-gson	2.9.0	Da, ali verzija 2.4.0	Da	Ne	2
com.squareup.okhttp3: logging-interceptor	**4.8.1**	**Da, ali verzija 4.7.1**	**Ne**	**Da, lokalno**	**2***
com.squareup.okhttp3: okhttp	4.8.1	Da, ali verzija com.squareup.okhttp:okhttp:2.3.0	Da	Ne	2
com.squareup.okhttp3: okhttp-urlconnection	4.8.1	Da, ali verzija com.squareup.okhttp:okhttp-urlconnection:2.2.0	Da	Ne	2
io.github.inflationx: calligraphy3	3.1.1	3.1.1	Ne	Ne	4
io.github.inflationx: viewpump	2.0.3	2.0.3	Ne	Ne	4
com.wang.avi:library	2.1.3	Nije navedeno	Ne	Ne	4
com.airbnb.android:lottie	3.4.4	Nije navedeno	Ne	Ne	4

Iceland Liechtenstein Norway **Active citizens** fund

politiscope

Projekt "Privatnost u doba Corone" je podržan s 4.973 € financijske podrške Islanda, Lihtenštajna i Norveške u okviru EGP i Norveških grantova.

Kreiranje ove analize omogućeno je financijskom podrškom Islanda, Lihtenštajna i Norveške u okviru EGP i Norveških grantova. Sadržaj ove analize isključiva je odgovornost udruge Politiscope i ne odražava nužno stavove država donatorica i Upravitelja Fonda.