Obvestilo o varstvu podatkov

Aplikacija #OstaniZdrav

Obvestilo o varstvu podatkov vsebuje informacije o tem, kateri podatki se zbirajo pri uporabi aplikacije #OstaniZdrav, kako se podatki obdelujejo in katere pravice ima posameznik glede obdelave osebnih podatkov.

1. Kdo je upravljavec aplikacije #OstaniZdrav?

Aplikacijo #OstaniZdrav (»aplikacijo«) sta pripravila Nacionalni inštitut za javno zdravje (NIJZ) in Ministrstvo za javno upravo (MJU), pri čemer NIJZ skrbi za vsebinski del aplikacije, MJU pa za tehničnega. Oba sta tako skupna upravljavca podatkov, ki se obdelujejo v okviru aplikacije #OstaniZdrav.

Elektronski naslov pooblaščene osebe za varstvo podatkov:

- pri NIJZ je vop@nijz.si
- pri MJU je dpo.mju@gov.si.

V primeru potrjene okužbe s koronavirusim SARS-CoV-2, ter pod pogojem, da omogočite beleženje izpostavljenosti, opozorite tudi uporabnike drugih mobilnih aplikacij držav članic Evropske unije (ki so po nadzorovanem postopku vključene v sistem za izmenjavo dnevnih ključev preko centralnega strežnika, ki ga upravlja Evropska komisija). V tem primeru se MJU in NIJZ ter upravljavci aplikacije v sodelujočih državah članicah Evropske unije, ki so vključene v čezmejen sistem obveščanja, štejejo kot skupni upravljavci.

2. Ali je uporaba aplikacije prostovoljna?

Uporaba aplikacije je popolnoma prostovoljna.

3. Ali se za delovanje aplikacije obdelujejo osebni podatki?

Za delovanje aplikacije se obdelujejo naključni dnevni ključi in oddajne kode, ki imajo pravno gledano status psevdonimiziranih osebnih podatkov. Več o konkretnih podatkih je zapisano v nadaljevanju.

Če se odločite za uporabo aplikacije, se morate strinjati z dotikom na gumb »Omogoči beleženje izpostavljenosti«, ob prvi prijavi v aplikacijo. Brez vašega soglasja aplikacija ne more dostopati do funkcionalnosti beleženja izpostavljenosti v vašem pametnem telefonu.

Posebno soglasje pa je potrebno za obdelavo podatkov, ki se izvaja za namene obveščanja drugih uporabnikov aplikacije o tem, da ste okuženi s SARS-CoV-2.

Kadar koli lahko v aplikaciji onemogočite funkcionalnost beleženja izpostavljenosti, kar pomeni, da takrat aplikacija ne more delovati.

4. Na kakšni pravni podlagi se obdelujejo vaši podatki?

NIJZ in MJU obdelujeta vaše podatke samo na podlagi soglasja, in sicer preko vašega strinjanja s funkcionalnostjo »Omogoči beleženje izpostavljenosti«.

Vzpostavitev aplikacije in njena prostovoljna uporaba je predvidena z Zakonom o začasnih ukrepih za omilitev in odpravo posledic COVID-19, ki je bil objavljen v Uradnem listu RS, št. 152/20 z dne 21. 10. 2020. Slednji je bil z Zakonom o interventnih ukrepih za omilitev posledic drugega vala epidemije COVID-19, Uradni list RS, št. 175/20 z dne 27. 11. 2020, dopolnjen v delu, ki se nanaša na aplikacijo, na način, da se omogoči njena interoperabilnost s centralnim sistemom, ki ga zagotavlja Evropska komisija z namenom povezave zalednih sistemov držav članic Evropske unije, ki jih za enake namene zagotavljajo države članice Evropske unije.

Soglasje lahko kadarkoli prekličete, več informacij v zvezi s preklicem pa si lahko preberete v 5. poglavju.

Aplikacija ne beleži vaše izpostavljenosti, če:

- onemogočite beleženje izpostavljenosti,
- izklopite sistem Bluetooth,
- pri sistemih Android izklopite lokacijo, ki sama po sebi nima funkcionalnosti v zvezi z aplikacijo (torej nima dostopa do podatka o lokaciji) je pa telefon narejen tehnično na način, da zahteva njen vklop za delovanje sistema Bluetooth,
- imate izklopljen telefon,
- aplikacijo odstranite s svojega telefona.

Posredovanje podatka o potrjeni okužbi s SARS-CoV-2 na strežnik okuženih ključev preko posredovanja dnevnih ključev, se zagotovi šele po vnosu posebne kode za posredovanje ter po dodatnem posebnem soglasju v okviru aplikacije. Tako posredovani podatki se s strežnika okuženih ključev izbrišejo v 14 dneh od posredovanja.

5. Preklic soglasja

Soglasje, ki ste ga dali NIJZ in MJU v aplikaciji, ni časovno omejeno, lahko pa ga kadar koli prekličete. Preklic ne vpliva na zakonitost obdelave, ki je bila izvedena na podlagi vaše privolitve, preden ste jo preklicali.

Soglasje za uporabo funkcionalnosti beleženja izpostavljenosti s posredovanjem naključnih oddajnih kod lahko prekličete tako, da funkcionalnost onemogočite s preklopnim stikalom v aplikaciji ali aplikacijo izbrišete. Če se odločite za ponovno uporabo funkcionalnosti beleženja izpostavljenosti, lahko funkcionalnost ponovno vklopite s preklopnim gumbom ali si ponovno namestite aplikacijo. NIJZ in MJU nimata

dostopa do naključnih oddajnih kod, ki so bile posredovane preko bluetootha drugemu uporabniku, je pa aplikacija pripravljena na način, da se izbrišejo po 14 dneh.

Posredovanje podatka o potrjeni okužbi s koronavirusom SARS-CoV-2 na strežnik okuženih ključev preko posredovanja dnevnih ključev, se zagotovi šele po vnosu posebne kode za posredovanje ter po dodatnem posebnem soglasju v okviru aplikacije. Soglasje velja za enkratni prenos okuženih ključev uporabnika na strežnik okuženih ključev. Tako posredovani podatki se s strežnika okuženih ključev izbrišejo v 14 dneh od posredovanja.

6. Komu je aplikacija namenjena?

Aplikacija je namenjena osebam, ki prebivajo v Republiki Sloveniji in so stare najmanj 16 let.

7. Kateri osebni podatki se obdelujejo?

Aplikacija je postavljena decentralizirano, kar ji omogoča, da obdeluje podatke v najmanjši možni meri, hkrati se ti podatki obdelujejo razpršeno na različnih napravah. Iz podatkov, ki jih obdeluje aplikacija, NIJZ in MJU ne moreta na noben način pridobiti podatkov o vaših stikih ali podatkov o tem, da ste okuženi, prav tako ne moreta odkriti vaše identitete ali lokacije. Stiki, ki se obravnavajo v okviru aplikacije, so zaznave telefona posameznega uporabnika, da se v zaznavni bližini nahaja telefon drugega uporabnika.

Poleg tega aplikacija tudi ne uporablja nobenih orodij za analiziranje vaše uporabe aplikacije. V okviru aplikacije:

- se obdelujejo naključno dodeljeni dnevni ključ (»dnevni ključ«), ki ga ustvari aplikacija, ko jo posameznik namesti na telefon. Dnevni ključ se menja na dnevni ravni in se hrani izključno na telefonu tega posameznika 14 dni, nato se samodejno izbriše. Zgolj v primeru, da posameznik v aplikacijo vnese posebno potrditveno kodo, in izrazi izrecno strinjanje, se dnevni ključ začasno prenese na poseben strežnik (»strežnik okuženih ključev«), ki se nahaja na infrastrukturi MJU. Iz telefonov se na strežnik okuženih ključev v primeru izrecnega strinjanja posameznika prenese izključno dnevni ključ, brez kakršnihkoli drugih podatkov o telefonu,

- aplikacija vsakih 15 minut na podlagi dnevnega ključa s pomočjo zgoščevanja in šifriranja ustvari oddajno kodo, ki se hrani na telefonu posameznika, ta ista oddajna koda pa se ob zaznanem stiku prenese na telefon drugega uporabnika. Ob prenosu telefon drugega uporabnika ustvari set metapodatkov, iz katerega je razviden čas stika in decibeli, iz katerih aplikacija izračuna oddaljenost stika in stopnjo tveganja za okužbo.
- NIJZ posamezniku s potrjeno okužbo s SARS-CoV-2 po telefonu ustno sporoči potrditveno kodo (»teleTAN«), s katero lahko posameznik v roku ene ure preko aplikacije potrdi, da je okužen. Po potrditvi se potrditvena koda preko uporabe registracijskega žetona spremeni v dokazilo, s katerim se nato v strežnik

okuženih ključev posreduje podatek o dnevnih ključih. Dnevni ključi uporabnikov s potrjeno okužbo se na strežniku okuženih ključev hranijo 14 dni, nato se samodejno pobrišejo, enkrat dnevno aplikacija iz strežnika okuženih ključev pridobi podatke o okuženih ključih, te podatke preračuna na način, da posamezen dnevni ključ zgosti in ga šifrira ter ga primerja z oddajno kodo stikov (torej uporabnikov aplikacije, ki so bili v zaznavnem območju Bluetooth uporabnikovega telefona), šele ob ugotovitvi ujemanja, lahko aplikacija odpre set metapodatkov in oceni tveganje za okužbo.

Dodatni poudarki:

Beleženje stikov na telefonu posameznega uporabnika iz druge alineje se torej izvaja izključno od trenutka potrditve beleženja stikov v aplikaciji. Prejšnje evidentiranje stikov ni mogoče, saj ne obstaja tehnična rešitev, ki bi to omogočala. V primeru prejema informacije o okuženosti posameznega dnevnega ključa je posledično možnost preverjanja te informacije s stiki omejena le na čas, ko je bila aplikacija delujoča na posameznem telefonu.

Evidenca okuženih oseb, ki se vodi na NIJZ v okviru Priloge 1 Zakona o zbirkah podatkov s področja zdravstvenega varstva, ni na noben način tehnično povezana z aplikacijo #OstaniZdrav in jo NIJZ vodi neodvisno od aplikacije #OstaniZdrav, prav tako pa evidenca tudi ne vsebuje nobenih podatkov, ki jih vsebuje aplikacija #OstaniZdrav.

Seznam uporabnikov aplikacije #OstaniZdrav ne obstaja.

Podatke, ki se obdelujejo v okviru aplikacije #OstaniZdrav, je torej mogoče deliti na:

a. Tehnične podatke za dostop

Tehnični podatki za dostop se ustvarijo, ko uporabljate ali omogočite spodaj navedene funkcionalnosti:

- beleženje izpostavljenosti;
- obveščanje drugih uporabnikov aplikacije o tem, da ste okuženi

Vsakokrat, ko mobilna aplikacija izmenjuje podatke z zalednim sistemom, se spremljajo podatki o dostopu. To je potrebno, da aplikacija lahko pridobi pravilne podatke ali prenese podatke iz telefona na strežnik. Podatki o dostopu se obdelujejo za vzdrževanje in zaščito tehničnih podatkov delovanje aplikacije in zalednega sistema. Iz teh podatkov ne boste identificirani kot uporabnik aplikacije, prav tako se ne ustvarja uporabniški profil.

IP številka, ki jo dodeli vaš operater, s katerega vaša mobilna naprava dostopa do zalednega sistema, se hrani po pravilih o hranjenju dnevniških zapisov dostopa. Ti podatki se hranijo na strežniku zalednega sistema do 6 mesecev ter v varnostni kopiji do 12 mesecev, potem se izbrišejo. Nadaljnja obdelava IP številke brez sodne odrede ni možna. Identificiranje posameznika s strani upravljavca podatkov na podlagi teh zapisov ni mogoče.

Obdelujejo se tudi spodaj navedeni podatki:

- datum in čas dostopa (časovni žig);
- količina posredovanih podatkov (ali dolžina paketa);
- obvestilo o uspešnem dostopu.

Ti tehnični podatki za dostop se obdelujejo samo zaradi zagotavljanja in vzdrževanja tehnične infrastrukture. Iz teh podatkov posameznika ni mogoče identificirati kot uporabnika aplikacije, prav tako ni mogoče ustvariti uporabniškega profila.

b. Kontaktne podatke

Če dovolite operacijskemu sistemu svojega pametnega telefona beleženje izpostavljenosti, ki zapisuje stike z drugimi uporabniki, vaš pametni telefon nenehno oddaja naključno ustvarjene oddajne kode, zgoščene in šifrirane vrednosti dnevnega ključa, ki se spreminjajo na največ 15 minut (RPI) prek nizkoenergijskega bluetootha, ki jih lahko prejmejo drugi pametni telefoni v vaši okolici, ki prav tako beležijo izpostavljenost. Vaš pametni telefon ob tem prejme naključne oddajne kode drugih pametnih telefonov. Poleg naključnih oddajnih kod, ki jih prejmete od drugih pametnih telefonov, funkcionalnost beleženja izpostavljenosti na vašem pametnem telefonu omogoča zapis in hrambo naslednjih kontaktnih podatkov:

- datum in čas stika;
- trajanje stika;
- jakost bluetooth signala stika;
- šifrirane druge metapodatke (različica protokola in jakost prenosa).

Vaši naključni dnevni ključi in oddajne kode, ki jih prejmete od drugih pametnih telefonov in drugi podatki (datum in čas stika, trajanje stika, jakost signala stika), se beležijo v dnevniku izpostavljenosti v vašem pametnem telefonu in se hranijo 14 dni.

Funkcionalnost, ki beleži srečanja z drugimi uporabniki, se imenuje »Obveščanje o izpostavljenosti bolezni COVID-19« na pametnih telefonih Android in »Beleženje izpostavljenosti bolezni COVID-19« na pametnih telefonih iPhone. Upoštevajte, da funkcionalnost beleženja izpostavljenosti ni del aplikacije, temveč sestavni del operacijskega sistema vašega pametnega telefona, kar pomeni, da funkcionalnost beleženja izpostavljenosti omogočata Apple (iPhone) oziroma Google (pametni telefoni Android) in zanjo veljajo ustrezna pravila o varstvu podatkov teh družb. NIJZ in MJU nista odgovorna oz. ne vplivata na obdelavo podatkov, ki jo izvaja operacijski sistem v povezavi z beleženjem izpostavljenosti.

Več informacij o funkcionalnosti beleženja izpostavljenosti na pametnih telefonih Android najdete v nastavitvah pod “Google”>“Obveščanje o izpostavljenosti bolezni COVID-19”je na: https://support.google.com/android/answer/9888358?hl=sl. Funkcionalnost beleženja izpostavljenosti je na voljo samo, če je na vašem pametnem telefonu nameščena različica Android 6 ali več.

Več informacij o funkcionalnosti beleženja izpostavljenosti, ki jo omogoča Apple, lahko najdete v nastavitvah iPhone pod “Zasebnost”>“Zdravje”>"Beleženje izpostavljenosti

bolezni COVID-19". Funkcionalnost beleženja izpostavljenosti je na voljo samo, če je na vašem pametnem telefonu iPhone nameščena različica iOS 13.5 ali več.

Aplikacija obdeluje zgoraj omenjene podatke, ustvarjene in shranjene v vašem pametnem telefonu, samo če je omogočena funkcionalnost beleženja izpostavljenosti.

c. Podatki o naključnih dnevnih ključih posameznika, ki želi deliti informacijo o tem, da je okužen

Če želite drugim uporabnikom aplikacije ali uporabnikom drugih mobilnih aplikacij držav članic Evropske unije, omogočiti seznanitev s podatkom o tem, da je bil rezultat testa na okužbo s SARS-CoV-2 pozitiven, se to izvede na način, da:

- za strinjanje s posredovanjem podatka uporabite potrditveno kodo (teleTAN), ki jo prejmete s strani epidemiološke službe in je veljavna tri ure;
- preko uporabe registracijskega žetona, ki spremeni potrditveno kodo v dokazilo, posredujete na strežnik okuženih ključev podatek o vaših naključnih dnevnih ključih za zadnjih 14 dni.

8. Funkcionalnosti aplikacije

a. Beleženje izpostavljenosti

Glavna funkcionalnost aplikacije je beleženje stika z drugimi napravami ter ocena tveganja za okužbo s SARS-CoV-2. Aplikacija poleg na podlagi ocenjenega tveganja prikaže tudi nasvete, ki jih za posamezno stanje predpripravil NIJZ. Gre za besedila generično pripravljena v aplikaciji in vezana na prikazano stanje.

Če omogočite funkcionalnost beleženja izpostavljenosti, aplikacija enkrat dnevno, medtem ko deluje v ozadju, prikliče iz strežniška okuženih ključev seznam okuženih ključev uporabnikov, pri katerih je bila potrjena okužba in so želeli obvestiti druge uporabnike aplikacije o tem, da obstaja tveganje za okužbo. Priklic se izvede na način, da se pokliče strežnik, ki kot avtomatiziran odgovor posreduje ključe. Aplikacija te preračuna v naključne oddajne kode ter jih nato primerja z naključnimi oddajnimi kodami, ki so shranjeni v dnevniku izpostavljenosti na vašem pametnem telefonu. Če funkcionalnost beleženja izpostavljenosti na vašem pametnem telefonu zazna ujemanje, posreduje podatke (datum, trajanje, jakost signala) aplikaciji, ne pa tudi naključnih dnevnih ključev zadevnega stika.

Če pride do stika, aplikacija analizira kontaktne podatke, ki jih posreduje funkcionalnost beleženja izpostavljenosti, da se oceni vaše tveganje za okužbo. Algoritem za ocenjevanje, ki določa razlago podatkov (kako na primer trajanje stika vpliva na tveganje za okužbo), temelji na trenutnih znanstvenih ugotovitvah. Ob upoštevanju novih dognanj lahko NIJZ in MJU posodobita algoritem za ocenjevanje s prilagajanjem svojih nastavitev. Nastavitve algoritma za ocenjevanje se pošljejo v aplikacijo skupaj s seznamom naključnih dnevnih ključev okuženih uporabnikov.

Ocena vašega tveganja za okužbo poteka samo lokalno na vašem pametnem telefonu. Podatek o oceni tveganja se hrani samo v aplikaciji in se ne posreduje drugim prejemnikom (vključno z NIJZ, MJU, Apple, Google in drugimi osebami).

Pravna podlaga za obdelavo vaših tehničnih podatkov za dostop, kontaktnih podatkov in podatkov o naključnih dnevnih ključih posameznika, ki želi deliti informacijo o tem, da je okužen, je na podlagi zakona dano soglasje uporabnika, podano ob vključitvi funkcionalnosti beleženja izpostavljenosti.

b. Obveščanje drugih uporabnikov aplikacije ali uporabnikov drugih mobilnih aplikacij držav članic Evropske unije, o tem, da ste okuženi

Če uporabljate funkcionalnost za obveščanje drugih uporabnikov aplikacije ali uporabnikov drugih mobilnih aplikacij držav članic Evropske unije, o tem, da je bila pri vas potrjena okužba s SARS-CoV-2 in želite posvariti druge uporabnike, to lahko storite šele, ko vas NIJZ obvesti o pozitivnem rezultatu testiranja in vam podeli potrditveno kodo(TeleTAN).

Epidemiološka služba preko vstopnega portala ustvari številko TeleTAN s posebnim dostopom do strežniškega sistema in sporoči številko TeleTAN. Ko številko TeleTAN vpišete v aplikacijo, jo ta pošlje nazaj v strežniški sistem aplikacije za primerjavo in preverjanje. Aplikacija prejme iz strežniškega sistema žeton, tj. digitalni ključ za dostop, shranjen v aplikaciji. Z žetonom aplikacija od strežniškega sistema zahteva dokazilo (številko TAN). Številko teleTAN je mogoče uporabiti le enkrat.

Obveščanje drugih uporabnikov aplikacije ali uporabnikov drugih mobilnih aplikacij držav članic Evropske unije, o tem, da je bila pri vas potrjena okužba s SARS-CoV-2 se izvaja med mobilnimi aplikacijami, ki delujejo v državah Evropske unije in so po nadzorovanem postopku vključene v sistem za izmenjavo dnevnih ključev, ki ga upravlja Evropska komisija.

Strežnik v Republiki Sloveniji in evropski centralni strežnik izmenjujeta podatke o dodeljenih dnevnih ključih uporabnikov mobilne aplikacije, ki so bili pozitivni na okužbo s SARS-CoV-2, z drugimi primerljivimi prostovoljnimi aplikacijami za obveščanje o stikih z okuženimi znotraj Evropske unije. Evropski centralni strežnik je sestavni del digitalne infrastrukture mreže e-zdravje, ustanovljeno med državami članicami Evropske unije. Izmenjava dnevnih ključev uporabnikov mobilnih aplikacij, ki so bili pozitivni na okužbo s SARS-CoV-2, se izvaja med mobilnimi aplikacijami, ki delujejo v državah Evropske unije in so po nadzorovanem postopku vključene v sistem za izmenjavo dnevnih ključev, ki ga upravlja Evropska komisija. Samo države članice Evropske unije, ki izpolnjujejo ustrezne kriterije varovanja podatkov lahko sodelujejo v čezmejnem izmenjavanju podatkov. Podrobnejše informacije o tovrstnem sodelovanju držav članic, ter druge tehnične podrobnosti so razvidne iz Sklepa Evropske komisije, tj. Izvedbeni sklep komisije (EU) 2020/1023 z dne 15. julija 2020 o spremembi Izvedbenega sklepa (EU) 2019/1765 glede čezmejne izmenjave podatkov med nacionalnimi aplikacijami za sledenje stikom in opozarjanje v z zvezi z bojem proti pandemiji COVID-19 - https://eur-lex.europa.eu/legal-content/SL/TXT/PDF/?uri=CELEX:32020D1023&qid=1611223443281&from=EN

Za namen delovanja mobilne aplikacije in drugih mobilnih aplikacij držav članic Evropske unije se na evropskem centralnem strežniku hranijo naključno dodeljeni dnevni ključi, ki jih posredujejo strežnik iz Republike Slovenije.

Evropska komisija se kot ponudnik tehničnih in organizacijskih rešitev pri čezmejni izmenjavi podatkov šteje za obdelovalca v smislu določb Splošne uredbe o varstvu podatkov ter je zavezana varstvu podatkov kot določa pogodba ali ustrezni pravni akti. V že navedem Sklepu Evropske komisije so določena pravila o obdelavi, ki jo izvaja Evropska komisija kot obdelovalec.

Pravna podlaga za obdelavo vaših tehničnih podatkov za dostop, kontaktnih podatkov in podatkov o naključnih dnevnih ključih posameznika, ki želi deliti informacijo o tem, da je okužen, je na podlagi zakona dano vaše soglasje, podano ob usposobitvi funkcionalnosti beleženja izpostavljenosti.

c. Uporaba aplikacije samo za informativne namene

Če uporabljate aplikacijo samo za informativne namene, tj. ne uporabljate nobenih zgornjih funkcionalnosti in ne vnašate nobenih podatkov, poteka obdelava samo lokalno na vašem pametnem telefonu in osebni podatki se ne ustvarijo. Spletne strani, povezane v aplikaciji, kot je https://gov.si/ostanizdrav se odprejo v običajnem brskalniku vašega pametnega telefona. Podatki, ki se obdelujejo, so odvisni od uporabljenega brskalnika, nastavitev brskalnika in praks obdelave podatkov na spletni strani, ki jo obiščete.

9. Kakšna dovoljenja in funkcionalnosti zahteva aplikacija?

Aplikacija zahteva dostop do nekaterih funkcionalnosti in vmesnikov na vašem pametnem telefonu, zato ji morate odobriti določena dovoljenja. Različni proizvajalci različno uvrščajo svoja dovoljenja. Posamezna dovoljenja je na primer mogoče združiti v kategorije dovoljenj, kjer se je mogoče strinjati s kategorijo dovoljenj samo kot celoto. Če je aplikaciji onemogočen dostop, ne morete uporabljati nekaterih ali vseh funkcionalnosti aplikacije.

a. Tehnične zahteve (vsi pametni telefoni)

- Internet
  Aplikacija potrebuje internetno povezavo za delovanje funkcionalnosti beleženja izpostavljenosti in komuniciranje s strežniškim sistemom.
- Bluetooth
  Vmesnik bluetooth na vašem pametnem telefonu mora biti omogočen, da lahko pametni telefon beleži naključne oddajne kode drugih pametnih telefonov in jih shrani v dnevniku izpostavljenosti naprave.
- Delovanje v ozadju
  Aplikacija deluje v ozadju (tj. ko aplikacije ne uporabljate dejavno), da lahko samodejno oceni vaše tveganje. Če aplikaciji ne dovolite delovanja v ozadju v operacijskem sistemu svojega pametnega telefona, aplikacija ne bo delovala pravilno.

b. Pametni telefoni Android

Če uporabljate napravo Android, morajo biti omogočene tudi spodnje funkcionalnosti sistema:

- Obvestila o izpostavljenosti bolezni COVID-19
  Ta funkcionalnost beleženja izpostavljenosti je nujna v aplikaciji, sicer dostop do dnevnika izpostavljenosti z naključnimi oddajnimi kodami ni mogoč. Funkcionalnost mora biti omogočena v okviru aplikacije, da lahko aplikacija dostopa do dnevnika izpostavljenosti.
- Lokacija
  Storitve ugotavljanja lokacije vašega pametnega telefona morajo biti omogočene na vaši napravi za iskanje signalov bluetooth z drugih pametnih telefonov. Za delovanje te aplikacije se podatki o lokaciji ne zbirajo.
- Obvestilo
  Uporabnik je lokalno obveščen o ocenjenem tveganju. Potrebna funkcionalnost obveščanja je že nameščena v operacijskem sistemu.

c. Pametni telefoni iPhone (Apple iOS)

Če uporabljate iPhone, morajo biti omogočene tudi spodnje funkcionalnosti sistema:

- Beleženje izpostavljenosti bolezni COVID-19
- Funkcionalnost beleženja izpostavljenosti je nujna v aplikaciji, saj sicer dostop do dnevnika izpostavljenosti z naključnimi oddajnimi kodami vaših stikov ni mogoč. Funkcionalnost mora biti omogočena v okviru aplikacije, da lahko aplikacija dostopa do dnevnika izpostavljenosti.
- Obvestila
- Uporabnik je lokalno obveščen o ocenjenem tveganju. Obveščanje mora biti omogočeno.

10. Kdaj se podatki izbrišejo?

Vsi podatki, shranjeni v aplikaciji, se izbrišejo takoj, ko niso več potrebni za spodaj navedene funkcionalnosti aplikacije:

a. Beleženje izpostavljenosti

- Seznam naključnih dnevnih ključev in oddajnih kod drugih uporabnikov se samodejno izbriše iz dnevnika izpostavljenosti v vašem pametnem telefonu po 14 dneh.
- NIJZ in MJU ne moreta vplivati na izbris kontaktnih podatkov v dnevniku izpostavljenosti v vašem pametnem telefonu (vključno z vašimi naključnimi dnevnimi ključi) in kontaktnih podatkov v drugih pametnih telefonih, saj to funkcionalnost omogočata Apple ali Google. V tem primeru je izbris odvisen od odločitve, ki jo sprejmeta družbi Apple ali Google. Trenutno se podatki samodejno izbrišejo po 14 dneh. S funkcionalnostjo, ki jo omogočata Apple in Google, je mogoče podatke ročno izbrisati iz sistemskih nastavitev vaše naprave.

- Ocena tveganja, prikazana v aplikaciji, se izbriše takoj, ko aplikacija poda novo oceno tveganja. Nova ocena tveganja se običajno določi, ko aplikacija prejme nov seznam naključnih dnevnih ključev.

b. Obveščanje drugih uporabnikov aplikacije ali uporabnikov drugih mobilnih aplikacij držav članic Evropske unije o tem, da ste okuženi

- Naključni dnevni ključi v vašem pametnem telefonu, ki se uporabljajo v aplikaciji, se izbrišejo iz strežniškega sistema v Republiki Sloveniji po 14 dneh, iz evropskega centralnega strežnika pa v skladu s pravili upravljavca.
- Zgoščena vrednost številke TAN, ki je shranjena v strežniškem sistemu, se izbriše po 21 dneh.
- Številka TAN, shranjena v aplikaciji, se izbriše po objavi dnevnih ključev aplikacije na aplikacijski strežnik.
- Številka TeleTAN, shranjena v aplikaciji, se izbriše po objavi dnevnih ključev aplikacije na aplikacijski strežnik.
- Zgoščena vrednost številke TeleTAN, shranjena v strežniškem sistemu, se izbriše po 21 dneh.
- Številka TeleTAN, ki jo pridobi epidemiološka služba, se izbriše takoj, ko vam jo sporoči po telefonu.
- Zgoščena vrednost registracijskega žetona, shranjena v strežniškem sistemu, se izbriše po 21 dneh.
- Registracijski žeton, shranjen v aplikaciji, se izbriše po obveščanju drugih uporabnikov aplikacije o tem, da ste okuženi.

11. Kdo prejme vaše podatke?

Če želite obvestiti druge uporabnike aplikacije ali uporabnikov drugih mobilnih aplikacij držav članic Evropske unije, o tem, da ste okuženi, se vaši naključni dnevni ključi zadnjih 14 dni posredujejo na strežnik okuženih ključev, od tam pa jih aplikacije na pametnih telefonih drugih uporabnikov prevzamejo.

12. Ali so podatki posredovani v tretjo državo?

Če omogočite funkcionalnost za obveščanje drugih uporabnikov aplikacije lahko pride do komunikacije med aplikacijami ne glede na to kje se nahajate – na primer, dopust v tujini, poslovna pot. Sicer pa se podatki, ustvarjeni med uporabo aplikacije, obdelujejo na strežnikih v Republiki Sloveniji in evropskem centralnem strežniku, ki ga zagotavlja Evropska komisija z namenom povezave zalednih sistemov držav članic Evropske unije, in so podvrženi strogim pravilom Splošne uredbe o varstvu podatkov.

13. Druge pravice na podlagi Zakona o varstvu osebnih podatkov in Splošne uredbe o varstvu podatkov

Ker gre v primeru uporabe aplikacije #OstaniZdrav za obdelavo, ki ne zahteva identifikacije posameznika, se nekatere pravice posameznika v skladu s členom 11 Splošne uredbe o varstvu podatkov ne zagotavljajo. Ker pa za namene aplikacije to ni potrebno in to tudi ni njen namen, NIJZ in MJU nista dolžna zbirati dodatnih podatkov (v skladu z drugim odstavkom člena 11 Splošne uredbe o varstvu podatkov). Poleg tega bi bilo to v nasprotju z navedenim ciljem, ki teži k temu, da je količina podatkov, obdelanih za aplikacijo, čim manjša. Konkretneje velja:

- Informacije v zvezi z obdelavo osebnih podatkov – na spletnih straneh NIJZ in MJU bo mogoče pridobiti splošne informacije o obdelavi podatkov, informacij, ki bi bile vezane na posameznika, pa zaradi odsotnosti ustreznega osebnega identifikatorja ne bo mogoče zagotavljati;
- Pravica do popravka – pravice do popravka ne bo mogoče izvajati, saj tako posameznik kot upravljavec ne bosta vedela, kateri podatek se nanj sploh nanaša in posledično napake ne bo mogel ugotoviti;
- Pravica do izbrisa – izbris osebnega podatka bo mogoč le iz lastne namestitve aplikacije, v okviru katere bo posameznik lahko izbrisal vse podatke, ki so nastali v okviru delovanja aplikacije;
- Pravica do omejitve obdelave in pravica do ugovora – pravico do omejitve obdelave bo posameznik lahko izvrševal, če bo dokazal, da je imetnik določene naključno določenega dnevnega ključa, v zvezi s katerim naj bi se podatki o okuženosti zavarovali. Zaradi izvedbe aplikacije na način, da se podatki o posameznem stiku nahajajo le lokalno na posameznem mobilnem telefonu, pa pravice do omejitve obdelave, ker ta obdelava ne zahteva identifikacije, v tem delu ne bo mogoče izvrševati. Pravice do ugovora ne bo mogoče izvrševati drugače, kot v delu, v katerem se bodo podatki obdelovali lokalno, in sicer z njihovim izbrisom.
- Elektronski naslov pooblaščene osebe za varstvo podatkov:
    - pri NIJZ je: vop@nijz.si
    - pri MJU je: dpo.mju@gov.si.
- Informacije o obstoju avtomatiziranega sprejemanja odločitev, vključno z oblikovanjem profilov: NIJZ in MJU ne izvajata profiliranja in tudi ne avtomatiziranega odločanja na podlagi profiliranja z osebnimi podatki.
- Informacija o pravici do vložitve pritožbe pri nadzornem organu: Pritožbo lahko podate Informacijskemu pooblaščencu, Dunajska 22, 1000 Ljubljana, elektronski naslov: gp.ip@ip-rs.si, spletna stran: www.ip-rs.si.

Navedeno velja tudi v relaciji do Evropske komisije, ki zagotavlja evropski centralni strežnik in pristojnih nacionalnih organov ali uradnih organov držav članic, ki so pristopile k čezmejni izmenjavi podatkov, pod pogojem, da se omogoči beleženje izpostavljenosti. Morebitne zahtevke v zvezi z uveljavljanjem pravic posameznikov v skladu s Splošno uredbo o varstvu podatkov, ki se nanašajo na drugo državo članico ali Evropsko komisijo, lahko posredujete neposredno na upravljavca v Republiki Sloveniji; lahko pa se obrnete tudi na upravljavca države članice ali Evropsko komisijo (kontaktni podatki pooblaščene osebe za varstvo podatkov pri Komisiji – t. i. DPO: data-protection-officer@ec.europa.eu).

14. Statistika

Za namen statistike se periodično iz verifikacijskega strežnika objavijo podatki o številu izdanih teleTAN kod in število uporabljenih teleTAN kod. Podatki se pridobijo iz shranjenih zgoščenih vrednosti na verifikacijskem strežniku. Podatki se objavijo na spletnih straneh gov.si, celotna statistika pa na portalu OPSI. Prav tako se objavi podatek o številu prenosov aplikacije iz Google play in Apple store na spletnih straneh gov.si, celotna statistika pa na portalu OPSI.

Zadnja sprememba: 29. 1. 2021