



DRAFT VERSION

Ocena učinkov v zvezi z varstvom osebnih podatkov pri delovanju aplikacije #OstaniZdrav (revidirana verzija)

Ljubljana,

1.1 POSTOPEK SPREJEMA OCENE UČINKOV V ZVEZI Z VARSTVOM OSEBNIH PODATKOV

Potrjevalci in podpisnik ocene učinkov v zvezi z varstvom osebnih podatkov pri delovanju aplikacije #OstaniZdrav

Potrjevanje/p odpisovanje	Vloga	Oseba	Datum
potrjevalec	Vodja projektne skupine		
Potrjevalec DPO	Pooblaščen oseb za varstvo podatkov MJU		
Potrjevalec DPO	Pooblaščen oseb za varstvo podatkov NIJZ		
Podpisnik	Odgovorna oseb za delovanje aplikacije na MJU		
Podpisnik	Odgovorna oseb za delovanje aplikacije na NIJZ		

VSEBINA

1.1	POSTOPEK SPREJEMA OCENE UČINKOV V ZVEZI Z VARSTVOM OSEBNIH PODATKOV	2
1	SPLOŠNO O PREDMETU OCENE UČINKOV	5
1.1	Pojasnilo.....	5
1.2	Razlogi za sprejem ocene učinkov	6
1.3	Predstavitev projekta vzpostavitve aplikacije #OstaniZdrav	6
1.4	Namen in cilji vzpostavitve delovanja aplikacije za obveščanje o stikih z okuženimi z virusom SARS-CoV-2	7
1.5	Vključitev zainteresiranih strani.....	8
1.6	Skrbnik aplikacije #OstaniZdrav	8
1.7	Postavitev odgovornih oseb za varstvo osebnih podatkov.....	9
2	PREDMET OCENE UČINKOV	10
2.1	Nabor podatkov, ki se obdelujejo	10
2.2	Načini in sredstva obdelave	11
2.2.1	Postopek	11
	Statistični nameni	12
2.2.2		12
2.3	Psevdonimizacija podatkov	12
3	OCENA TVEGANJ IN UKREPI ZA OBVLADOVANJE TVEGANJ ZA VARSTVO PODATKOV	13
3.1	OCENA NUJNOSTI IN SORAZMERNOSTI OBDELAVE.....	13
3.1.1	Pravna podlaga in namen obdelave.....	13
3.1.2	Sorazmernost obdelave osebnih podatkov.....	14
3.1.3	Posredovanje in dostop do podatkov v aplikaciji #OstaniZdrav	14
3.1.4	Udeleženi subjekti.....	15
3.1.5	Uporaba istega povezovalnega znaka	16
3.1.6	Rok hrambe podatkov v aplikaciji #OstaniZdrav	16
3.1.7	Varnost podatkov v aplikaciji #OstaniZdrav in pogodbeni obdelava	16
3.1.8	Sistemi za upravljanje varovanja informacij (SUVI).....	17
3.1.9	Uničenje podatkov	17
3.1.10	Notranja sledljivost obdelave.....	17
3.1.11	Sledljivost posredovanja (zunanja sledljivost)*.....	18
3.1.12	Interni nadzor.....	18
3.1.13	Izobraževanje	18
3.1.14	Iznos osebnih podatkov v tretje države	18
3.1.15	Evidenca dejavnosti obdelave osebnih podatkov	18
3.1.16	Povezovanje zbirk osebnih podatkov.....	18
3.2	UKREPI VARSTVA PRAVIC POSAMENIKOV	18
3.2.1	Točnost in ažurnost podatkov.....	18
3.2.2	Preglednost in informiranje posameznika	18
3.2.3	Ostale pravice posameznika.....	19

4	ZAKLJUČKI OCENE UČINKOV.....	21
2	SEZNAM UPORABLJENIH KRATIC.....	22
3	VIRI	23
4	PRILOGE OCENE UČINKOV.....	24
5	Priloga 1: Tveganja in ukrepi za obvladovanje tveganj v povezavi z varnostjo podatkov	25
6		
7	Priloga 2: Postopki prenosa podatkov med lokalno namestitvijo aplikacije na mobilni telefon in centralno zbirko.....	43
8	Priloga 3: Postopek generiranja in uporabe kode za potrditev statusa okuženosti na strežniku CWA.....	47

1 SPLOŠNO O PREDMETU OCENE UČINKOV

1.1 Pojasnilo

NIJZ in MJU se pri svojem delovanju zelo dobro zavedata nujnosti proučitve vpliva določenih odločitev na varstvo osebnih podatkov in se zavedata, da je priprava ocene učinkov v zvezi z varstvom osebnih podatkov (v nadaljnjem besedilu: ocena učinkov) dokument, ki bi ga bilo treba pripraviti čimprej v procesu vodenja projekta. Vendar pa po svojih izkušnjah tudi ocenjujeta, da je oceno učinkov ne le obvezno pripraviti v določenih primerih, temveč je njena priprava tudi smiselna. Tako se je v preteklosti že mnogokrat izkazalo, da so se šele v času priprave ocene učinkov nekateri vidiki obdelave osebnih podatkov pokazali kot takšni, da je v zvezi z njimi treba sprejeti določene ukrepe. To se je zgodilo tudi pri pripravi te ocene učinkov, ki je nastala po tem, ko sta se NIJZ in MJU odločila, da je aplikacija »CORONA WARN APP«, ki jo je razvila Zvezna republika Nemčija, med takšnimi, ki v najmanjši možni meri obdeluje osebne podatke in da jo bosta uporabili za potrebe Republike Slovenije. Vendar morata NIJZ in MJU ob tem poudariti, da sta že od začetka prve razglasitve epidemije, torej več mesecev, spremljala mednarodne razprave o zagotavljanju tovrstnih aplikacij, proučevala različne rešitve z vidika vplivov na zasebnosti in s tehničnega vidika, opazovala prizadevanja Zvezne republike Nemčije, da bi zagotovila ustrezno stopnjo varstva osebnih podatkov, ki je na koncu rezultirala v popolnoma decentralizirani aplikaciji, in ugotavljala, kaj bi bilo primerno za slovenski prostor, ki postavlja varstvo osebnih podatkov zelo visoko.

Neodvisno od aplikacije, ki jo obravnava ta ocena učinkov in pred njeno uporabo, je zakonodajalec¹ pripravil pravno podlago za to, da bi lahko država ponudila državljanom aplikacijo, ki bi bila za okužene osebe obvezna, prav tako pa bi jo bilo mogoče uporabljati za posameznike, ki jim je bila odrejena karantena. Tako predvidena zakonska podlaga vsebuje tudi kazenske določbe, ki same po sebi pomenijo to, da bi morala država razpolagati s podatkom o tem, kateri posameznik si je aplikacijo naložil, torej že samo izvajanje zakona zahteva identifikacijo posameznika v določenih delih. Zaradi takšnih določil gre za popolnoma drugo pravno in posledično informacijsko rešitev, kot jo obravnava pričujoča ocena učinkov, zato teh dveh rešitev ne gre enačiti. Res pa je, da je v javnosti prihajalo do nesporazumov zaradi sočasnosti izvajanja obeh ukrepov, kar je predstavljalo izziv, ki sta ga NIJZ in MJU praktično dnevno naslavljala. Z zagotavljanjem aplikacije, ki jo obravnava ta ocena učinkov, se torej MJU ni postavil v vlogo zakonodajalca, saj ni odločalo tem, kaj od sprejetega zakona bi se upoštevalo, temveč je zagotovil vse potrebno za delovanje aplikacije, ki bi jo lahko država ponudila državljanom kot pripomoček za boj proti COVID-19. MJU pa se je istočasno tudi zavedal svoje vloge, ki jo je dobil s sprejemom Zakona o interventnih ukrepih za pripravo na drugi val COVID-19 (Uradni list RS, št. 98/20, v nadaljnjem besedilu: ZIUPDV), in je za namene zagotavljanja aplikacije iz 25. člena ZIUPDV ustanovil delovno skupino, ki proučuje tehnične možnosti za zagotovitev predpisanega. Na trgu namreč ni mogoče dobiti aplikacije, ki bi ustrezala v ZIUPDV opisanim zahtevam.

Kakršnokoli povezovanje aplikacije, ki jo obravnava pričujoča ocena učinkov, in sprejetega ZIUPDV je bilo torej neosnovano in utemeljeno zavrnjeno s strani NIJZ in MJU.² Da ima aplikacija svojstveno pravno naravo je bilo nato tudi razvidno s sprejemom Zakona o začasnih ukrepih za omilitev in odpravo posledic COVID-19 (v nadaljevanju: ZZUOOP), ki je bil objavljen v Uradnem listu RS, št. 152/20 z dne 21. 10. 2020, s katerim se je na še na zakonski ravni izrecno uredila aplikacija, ki je predmet te ocene učinkov. Iz razloga same jasnosti je ZZUOOP v 54. členu izrecno določil oz. še vedno določa, da se za

¹ Zakon o interventnih ukrepih za pripravo na drugi val COVID-19 (ZIUPDV – t. i. PKP#4), Uradni list RS, št. 98/2020 z dne 10. 7. 2020.

² V času priprave izvorne ocene učinkov je Informacijski pooblaščenec izrazil bojazen, da navedbe ministrstva za javno upravo, da se zakon v okviru te aplikacije ne uporablja, ne zadostujejo v smislu pravne varnosti, ker navedbe ministra ne razveljavljajo veljavnih zakonskih predpisov, niti nadzornim organom ne omogočajo, da v primeru prijav ne bi izrekli glob, poleg tega sprejeta zakonodaja nalaga obvezno uporabo aplikacije. Na takšne pomisleke je težko odgovarjati, saj je predpostavka napačna – ker gre za aplikacijo, ki ni povezana s sprejetim zakonom, nihče ne more zahtevati njene uporabe, tudi ne nadzorni organi. V tem primeru gre za zatiranje negativnega dejstva, kar je pa z vidika zaključka argumenta težavno.

mobilno aplikacijo, katero vzpostavitev in delovanje ureja ta zakon, ne uporabljajo določbe ZIUPDV, tj. določbe poglavja 4.

ZZUOOP 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, med drugim tudi na način, da se omogoči njena interoperabilnost s centralnim sistemom (European Federation Gateway Service – EFGS), ki ga zagotavlja Evropska komisija z namenom povezave zalednih sistemov držav članic Evropske unije, ki jih za enake namene zagotavljajo države članice Evropske unije.

1.2 Razlogi za sprejem ocene učinkov

Namen priprave ocene učinkov v zvezi z varstvom podatkov je ocena učinkov v zvezi z varstvom osebnih podatkov, kot so opredeljeni v 35. členu Uredbe (EU) 2016/679 Evropskega parlamenta in Sveta z dne 27. aprila 2016 o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem pretoku takih podatkov ter o razveljavitvi Direktive 95/46/ES (v nadaljnjem besedilu: Splošna uredba o varstvu podatkov).

V Republiki Sloveniji se je pojavila nova nalezljiva bolezen COVID-19), zaradi katere je bila na območju države večkrat razglašena epidemija. In sicer prvič z dnem 12. marca 2020 ob 18.00 uri z Odredbo o razglasitvi epidemije nalezljive bolezni SARS-CoV-2 COVID-19) na območju Republike Slovenije (Uradni list RS, št. 19/20 in 68/20). Slednja odredba je bil preklicana z 31. majem 2020, epidemija pa je bila nato tudi večkrat ponovno razglašena (in sicer s t. i. Odloki o razglasitvi epidemije nalezljive bolezni COVID-19 na območju Republike Slovenije, ki so bili vsakokrat objavljeni v Uradnem listu RS). Pojav nove nalezljive bolezni brez dvoma zahteva spremljanje njenega razvoja v Republiki Sloveniji. Kar zaradi same narave tovrstne bolezni nedvomno velja tudi za časovna obdobja, ko sama epidemija morda ni razglašena, bolezen COVID-19 pa še vedno predstavlja grožnjo zdravju ljudem. Nacionalni inštitut za javno zdravje (v nadaljnjem besedilu: NIJZ) in Ministrstvo za javno upravo (v nadaljnjem besedilu: MJU) sta ugotovila, da bi lahko kot pomoč pri boju proti nalezljivi bolezni COVID-19, služila tudi aplikacija za obveščanje o stikih z okuženimi z virusom SARS-CoV-2. Ker pri vzpostavitvi delovanja te aplikacije kljub dosledni in celoviti uporabi psevdonimizacijskih ukrepov pride do »obdelave posebnih vrst osebnih podatkov« (sicer v najmanjšem obsegu, ki je še potreben za doseg namena) in ker bo za izdelavo potrebna »inovativna uporaba obstoječih in novih tehnologij«, kar oboje sodi v seznam dejanj, ki terjajo izvedbo ocene učinka in ga je na podlagi četrtega odstavka člena 35. Splošne uredbe o varstvu podatkov sprejel IP ter potrdil Evropski odbor za varstvo podatkov, istočasno pa bo aplikacijo uporabljalo veliko število posameznikov, sta NIJZ in MJU ugotovila, da je treba pripraviti oceno učinkov, saj pristopata k vprašanju varstva osebnih podatkov sistematično in na način, ki bo kar največ zmanjšal morebitna tveganja za varstvo zasebnosti posameznikov.

1.3 Predstavitev projekta vzpostavitve aplikacije #OstaniZdrav

Epidemija oz. pandemija SARS-CoV-2 je glede na trenutno epidemiološko znanje hitro nalezljiv virus, ki lahko ogrozi življenje in zdravje posameznika. Da bi se širitev SARS-CoV-2 v čim večji meri zaježila, je Republika Slovenija (ter več drugih držav članic) uvedla aplikacijo, ki omogoča opozarjanje na stike z okuženo osebo in olajšanje prekinitev morebitne verige okužb. V okviru teh okoliščin sta se NIJZ in MJU odločila, da bi se kot eno od orodij za spodbujanje samozaščitnega vedenja posameznikov lahko uporabila tudi aplikacija za obveščanje uporabnika o njegovih stikih. V okviru tega je bilo pregledanih več tehničnih možnosti, po tehtnem pregledu informacij pa je bila kot najbolj primerna aplikacija za obveščanje posameznika o stikih z okuženimi z virusom SARS-CoV-2 za uporabo v Republiki Sloveniji prepoznana aplikacija »CORONA WARN APP«, ki jo je razvila Zvezna republika Nemčija in jo objavila kot odprtokodno rešitev na platformi GitHub.

Načelna primernost se je ugotovila tako na podlagi dejstva, da imata obe državi podobno urejeno pravno varstvo osebnih podatkov, kot na podlagi dejstva, da aplikacija uporablja Java kot osnovni jezik, kar s tehničnega vidika omogoča enostavno nameščanje v informacijsko komunikacijsko infrastrukturo MJU.

Na podlagi ugotovljene načelne primernosti, je bila izvedena podrobnejša tehnična analiza razpoložljive dokumentacije, na podlagi katere pa je nastala pričujoča ocena učinkov.

EFGS

Da bi olajšali čezmejno interoperabilnost posameznih nacionalnih aplikacij za sledenje in opozarjanje na stike, se je s podporo Evropske komisije in sodelovanjem držav članic, ki so sestavni del t. i. mreže eZdravje, razvila digitalna infrastruktura, imenovana EFGS (European Federation Gateway Service). Sodelovanje držav članic pri čezmejni interoperabilnosti in s ciljem zaježitve epidemije je prostovoljno. Države se v tovrstni sistem izmenjave podatkov vključijo po nadzorovanem postopku, ki ga spremlja Evropska komisija, slednja priključitev na EFGS tudi odobri. Po vzpostavitvi aplikacije je tudi Republika Slovenija pristopila k projektu omogočanja interoperabilnosti nacionalnih sistemov informacijske in komunikacijske tehnologije ter čezmejne prenosljivosti oz. izmenjave dnevnih ključev preko centralnega strežnika, ki ga upravlja Evropska komisija (via EFGS). Za te potrebe je bila sprejeta ustrezna (zakonska) podlaga, saj bil ZZUOOP z Zakonom o interventnih ukrepih za omilitev posledic drugega vala epidemije COVID-19 noveliran oz. dopolnjen med drugim na način, ki izrecno omogoča interoperabilnost aplikacije s centralnim sistemom Evropske komisije (EFGS).

Za potrebe čezmejne povezljivosti aplikacij je Evropska komisija sprejela sklep, tj. [Izvedbeni sklep komisije \(EU\) 2020/1023 z dne 15. julija o spremembi Izvedbenega sklepa \(EU\) 2019/1765 glede čezmejne izmenjave podatkov med nacionalnimi aplikacijami za sledenje stikom in opozarjanje v zvezi z bojem proti pandemiji COVID-19 \(v nadaljevanju: Sklep Evropske komisije\)](#).

DNEVNIK SREČANJ

V okviru aplikacije je vzpostavljen t. i. dnevnik srečanj, v katerega lahko uporabnik na svojem telefonu vpisuje osebe s katerimi se je srečal in tudi kraje, kjer se je gibal oz. nahajal v preteklih 14 dneh. Njegova uporaba je prostovoljna in je kot digitalni pripomoček namenjen tvornemu sodelovanju med posameznikom in epidemiološko stroko v primeru, kadar se pri posamezniku potrdi okužba s SARS-CoV-2 in je s strani NIJZ naprošen za pomoč pri ugotavljanju epidemiološke verige stikov oz. srečanj.

Podatki, ki jih posameznik vpisuje v dnevnik srečanj, so shranjeni lokalno na mobilnem telefonu uporabnika in so dostopni le njemu. NIJZ in MJU niti katerikoli drug organ javnega sektorja do teh podatkov ne morejo dostopati. Dnevnik srečanj ni na nikakršen način povezan s stiki, ki jih ima posameznik v telefonu, niti z drugimi funkcionalnostmi aplikacije. Dnevnik srečanj je nastavljen tako, da je podatke v njem možno dodajati in brisati ter izvoziti v tekstovni datoteki. V kolikor posameznik podatke iz dnevnika srečanj ne izbriše, so ti samodejno izbrisani po 16 dneh.

Ker v tem primeru podatke obdeluje uporabnik aplikacije oz. mobilnega telefona, nosi tudi odgovornost za skladno obdelavo podatkov, ki jih obdeluje. Iz tega razloga je vsakokratni uporabnik dnevnika srečanj izrecno opozorjen, da mora spoštovati zasebnost drugih ljudi, in da je dnevnik srečanj namenjen NIJZ - v primeru, da prosi za pomoč, ter da je potrebno preprečevati posredovanje podatkov nepooblaščenim osebam in upoštevati želje tistih, ki ne želijo biti zabeleženi v dnevnik srečanj (istovrstno opozorilo je navedeno tudi v obvestilu o zasebnosti).

1.4 Namen in cilji vzpostavitve delovanja aplikacije za obveščanje o stikih z okuženimi z virusom SARS-CoV-2

Aplikacija je namenjena osebam, ki prebivajo v Republiki Sloveniji in so stare najmanj 16 let. Namen³ vzpostavitve delovanja aplikacije za obveščanje o stikih okuženimi z virusom SARS-CoV-2 (v nadaljnjem besedilu: okuženi) je ponudba pripomočka za boj proti nalezljivi bolezni COVID-19, ki bi prebivalcem Republike Slovenije ponudil dodaten vir podatkov za samozaščitno vedenje posameznika,

³ Namen mobilne aplikacije #OstaniZdrav je jasno definiran tudi v 46. členu ZZUOOP.

tako na območju Republike Slovenije kot tudi na območju drugih držav članic Evropske unije in Evropskega gospodarskega prostora, ki so vključene v čezmejni sistem obveščanja preko Evropskega centralnega strežnika. Pripomoček, ki je predmet pričujoče ocene učinkov, bi posameznikom omogočil ugotavljanje stopnje lastne ogroženosti glede na stike z drugimi uporabniki aplikacije, ki jih je imel v zadnjih dveh tednih, pri čemer je treba upoštevati tako množičnost uporabe aplikacije kot tudi število izvedenih testov. Cilj vzpostavitve delovanja aplikacije #OstaniZdrav je namestitve aplikacije s strani čim večjega števila prebivalcev Republike Slovenije, ki bi to aplikacijo lahko uporabili za pomoč pri vedenju v javnosti ali pri druženju z drugimi posamezniki.

Aplikacija je pripomoček v primerih, ko se posameznik, misleč da je zdrav, giblje med drugimi in šele kasneje ugotovi, da je bil v tem času že okužen – s pomočjo te aplikacije lahko opozori tudi popolne neznance, ki pa so bili mogoče zaradi različnih razlogov v njegovi bližini dlje časa (javni mestni promet), o tem, da so bili v rizičnem stiku. Ti posamezniki lahko potem spremljajo svoje počutje z več informacijami in drugače razumejo zdravstvene znake, kot je na primer sicer neproblematičen glavobol.

Takšen pripomoček seveda ne more nadomestiti dela epidemiologov, ki bodo svoje delo opravljali še vedno na enak način, lahko pa pomaga prebivalcem Slovenije in strokovnim delavcem pri zmanjševanju števila okuženih ter nam tako pomaga ohraniti visoko raven kvalitete življenja tudi v času, ko je po svetu zaradi COVID-19 še vedno mnogo družb prisiljenih v omejevanje človekovih pravic.

1.5 Vključitev zainteresiranih strani

NIJZ in MJU sta k aplikaciji pristopila s poznavanjem epidemiološke slike Republike Slovenije, razprav v času razglašene prve epidemije in po njej, ter poznavanjem raziskav javnega mnenja, iz katerih je mogoče razbrati zainteresiranost prebivalcev Republike Slovenije za pripomoček, ki je kot aplikacija predmet te ocene učinkov. Iz medijev znane ugotovitve so (povzeto nekaj spletnih strani iz svetovnega spleta – po vrstnem redu zadetkov):

- Vir: Raziskava #Novanormalnost, 10.-13. julij 2020, n=566; Valicon: »verjetnost prostovoljne namestitve brez okužbe ali odrejene karantene je ocenjena na kvečjemu 27 % prebivalcev v starosti od 18 do 75 let«; (<https://www.valicon.net/sl/2020/07/aplikacijo-za-sledenje-okuzb-s-covid-19-si-bo-po-oceni-na-osnovi-raziskave-namestilo-kvecjemu-27-prebivalcev-v-starosti-od-18-do-75-let/>),
- Vir: Raziskava Mediana 17. julij 2020, n=506: »38 % vprašanih uvedbo aplikacije podpira in meni, da bomo z njeno pomočjo zagotovili lažjo sledljivost širjenja virusa. Na drugi strani 36 % vprašanih aplikacije ne podpira, saj jo vidijo kot vdor v zasebnost posameznika, še nadaljnjih 18 % pa aplikacije ne podpira, saj jo vidijo kot neučinkovito. Skupno torej aplikacije iz različnih razlogov ne podpira 54 % vprašanih. Neodločenih glede te tematike je 9 %« (<https://www.mediana.si/vecina-prebivalcev-slovenije-uvedbe-aplikacije-za-sledenje-okuzb-s-covid-19-se-vedno-ne-podpira/>).

Javno mnenje je v tem primeru pomembno za proučevanje zainteresiranosti, saj so potencialni uporabniki aplikacije vsi prebivalci Republike Slovenije, ki pa so istočasno tudi iste osebe, ki bi jih COVID-19 lahko prizadel. Bistveno pa je nenazadnje dejstvo, da je aplikacija dana kot pripomoček oz. izbirna možnost v zagotavljanju spremljanja poteka epidemije in omejevanje njenega širjenja, ki jo lahko zainteresirani posameznik uporablja po svoji svobodni oz. lastni presoji.

Na podlagi poznavanja zgornjih ugotovitev in dejstva, da NIJZ dnevno ugotavlja, da vsak posameznik, ki ni okužen, pripomore k boljši epidemiološki sliki Republike Slovenije, sta se NIJZ in MJU odločila, da je s stališča dela prebivalcev Republike Slovenije potreba po tovrstni aplikaciji takšna, da ne zahteva dodatnih raziskav o stališčih zainteresiranih straneh.

1.6 Skrbnik aplikacije #OstaniZdrav

Aplikacija #OstaniZdrav je dostopna kot odprta koda na portalu GitHub.

Njen:

- vsebinski skrbnik bo NIJZ, ki je pristojen za izvajanje nalog v skladu z Zakonom o nalezljivih boleznih (Uradni list RS, št. 33/06 – uradno prečiščeno besedilo in 49/20 – ZIUZEOP) ki v okviru osnovnega področja delovanja vzdržuje zbirke osebnih podatkov skladno z Zakonom o zbirkah podatkov s področja zdravstvenega varstva (Uradni list RS, št. 65/00 z dne 21. 7. 2000). Vloga NIJZ je podrobneje določena še z ZZUOOP, kjer je v prvi alineji 53. člena navedeno, da je odgovoren za določanje namena obdelave podatkov v okviru aplikacije in sistema potrditvenih kod
- tehnični skrbnik bo MJU, saj bo aplikacija nameščena v infrastrukturo državnega računalniškega oblaka (v nadaljnjem besedilu: DRO), ki je kot del informacijsko komunikacijske infrastrukture v skladu s 74.a členom Zakona o državni upravi (Uradni list RS, št. 113/05 – uradno prečiščeno besedilo, 89/07 – odl. US, 126/07 – ZUP-E, 48/09, 8/10 – ZUP-G, 8/12 – ZVRS-F, 21/12, 47/13, 12/14, 90/14 in 51/16) v upravljanju MJU. Skladno z navedenim je v drugi alineji 53. člena ZZUOOP še izrecno navedeno, da je MJU z namenom delovanja aplikacije odgovoren za določanje načina in sredstev obdelave podatkov ter zagotavljanja infrastrukture njenega delovanja.

1.7 Postavitev odgovornih oseb za varstvo osebnih podatkov

Damjana Moškrič, odgovorna oseba za varstvo osebnih podatkov na NIJZ.

Mateja Peterca , odgovorna oseba za varstvo osebnih podatkov na MJU.

2 PREDMET OCENE UČINKOV

Po informacijah stroke je bila kot ena najbolj primernih aplikacij za obveščanje posameznika o stikih z okuženimi z virusom SARS-CoV-2 za uporabo v Republiki Sloveniji prepoznana aplikacija »CORONA WARN APP«, ki jo je razvila Zvezna republika Nemčija in jo objavila kot odprtokodno rešitev na platformi GitHub. NIJZ in MJU sta se odločila, da jo bosta prilagodila za uporabo v Republiki Sloveniji, kar pomeni tako prilagoditev programske kode kot tudi uporabo lastne infrastrukture, ki je v upravljanju MJU.

Predmet ocene učinkov je torej ocena učinkov v zvezi z varstvom osebnih podatkov pri delovanju aplikacije #OstaniZdrav.

2.1 Nabor podatkov, ki se obdelujejo

Aplikacija #OstaniZdrav je postavljena na način, ki predvideva kolikor mogoče omejeno obdelavo osebnih podatkov. Obdelava podatkov v okviru aplikacije #OstaniZdrav je izrazito decentralizirana, saj se večina podatkov obdeluje na mobilnih telefonih, manjši del pa na strežnikih aplikacije.

Posledično se spodaj navedeni podatki ne nahajajo v eni podatkovni bazi, temveč gre za nabor vseh podatkov, ki bi sploh lahko prišli v poštev za delovanje celotnega sistema aplikacije #OstaniZdrav.

Za namene uporabe aplikacije #OstaniZdrav se beseda »stik« razume kot zaznano povezavo preko vmesnika Bluetooth med dvema posameznikoma, ki imata nameščeno aplikacijo #OstaniZdrav. API vmesnik za Bluetooth zagotavljata Apple in Google.

V okviru aplikacije:

- se obdelujejo naključno dodeljeni dnevni ključ (v nadaljnjem besedilu: 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 (v nadaljnjem besedilu: strežnik CWA), ki se nahaja na infrastrukturi MJU. Iz telefonov se na strežnik CWA 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 identifikator (v nadaljnjem besedilu: oddajna koda), 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 meta podatkov, iz katerega je razviden čas stika in decibeli, iz katerih aplikacija sklepa na oddaljenost stika,
- NIJZ posamezniku s potrjeno okužbo s SARS-CoV-2 preko SMS ob potrditvi okužbe sporoči tudi verifikacijsko kodo (v nadaljnjem besedilu: TAN), s katero lahko posameznik v roku treh ur preko aplikacije potrdi, da je okužen. Po potrditvi se TAN preko uporabe registracijskega žetona spremeni v dokazilo, s katerim se nato na strežnik CWA posreduje podatek o dnevni ključih. Podroben postopek pretvorbe je opisan v Prilogi 3. Dnevni ključi uporabnikov s potrjeno okužbo se na strežniku CWA hranijo 14 dni, nato se samodejno izbrišejo,
- aplikacija do šestkrat dnevno iz strežnika CWA pridobi podatke o okuženih dnevni ključih, te podatke preračuna na način, da posamezen dnevni ključ zgosti in ga šifrira ter tako spremeni v oddajno kodo, ki ga primerja z oddajnimi kodami stikov (torej uporabnikov aplikacije, ki so bili v zaznavnem območju Bluetooth uporabnikovega telefona), šele ob ugotovitvi ujemanja, aplikacija odpre set meta-podatkov in izračuna stopnjo tveganja.

DODATNI POUDARKI

Beleženje stikov na telefonu posameznega uporabnika iz druge alineje se torej izvaja izključno od trenutka namestitve aplikacije na telefon. 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, kot je bila aplikacija delujoča na posameznem telefonu.

Celoten postopek dodeljevanja dnevnih ključev in posredovanja informacij je prikazan v Prilogi 2.

Evidenca okuženih oseb se vodi na NIJZ v okviru Priloge 1 Zakona o zbirkah podatkov s področja zdravstvenega varstva (Uradni list RS, št. 65/00, 47/15 in 31/18) in ni na noben način povezana z aplikacijo #OstaniZdrav. Vodi neodvisno od aplikacije #OstaniZdrav in tudi ne vsebuje nobenih podatkov, ki jih vsebuje aplikacija #OstaniZdrav.

Seznam uporabnikov aplikacije #OstaniZdrav ne obstaja.

Uporabniki pametnih telefonov Android, ki uporabljajo starejšo različico operacijskega sistema (do verzije 10), ki uporabljajo vmesnik bluetooth, bodo morali imeti za delovanje vmesnika vklopljeno storitev ugotavljanja lokacije, saj to s tehnične vidika zahteva sam vmesnik, isto pa tudi določajo splošni pogoji za uporabo vmesnika, vendar pa se ti podatki ne hranijo v okviru aplikacije #OstaniZdrav niti se ne na kakršenkoli drug način ne obdelujejo.

Uporabniki Android verzije 11 lokacijskih storitev ne potrebujejo, saj je bilo delovanje vmesnika posodobljeno tako, da bluetooth ne potrebuje lokacijskih storitev.

Vsakokrat, ko 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 delovanja aplikacije in zalednega sistema. Iz teh podatkov se ne identificira uporabnika aplikacije, prav tako se ne ustvarja uporabniški profil.

IP naslov, ki jo dodeli uporabniku aplikacije operater, s katerega 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 brez sodne odredbe ni možna. Identificiranje posameznika s strani upravljavca na podlagi teh zapisov ni možna.

2.2 Načini in sredstva obdelave

2.2.1 Postopek

Ko posameznik namesti aplikacijo, se mu dodeli dnevni ključ, ki ga ustvari aplikacija. 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 strežnik CWA, ki se nahaja na infrastrukturi MJU. Iz telefonov se na strežnik CWA 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 isti identifikator pa se ob zaznanem stiku prenese na telefon drugega uporabnika. Ob prenosu telefon drugega uporabnika ustvari set meta podatkov, iz katerega je razviden čas stika in decibeli, iz katerih aplikacija sklepa na oddaljenost stika (v nadaljnjem besedilu: AEM ključ).

Posameznik s potrjeno okužbo SARS-CoV-2 pridobi TAN kodo s katero lahko v roku treh ur preko aplikacije potrdi, da je okužen. Po potrditvi se TAN preko uporabe registracijskega žetona spremeni v dokazilo, s katerim se nato v strežnik CWA posreduje podatek o dnevnem ključu. Dnevni ključi uporabnikov s potrjeno okužbo se na strežniku CWA hranijo 14 dni, nato se samodejno izbrišejo.

Aplikacija do šestkrat dnevno iz strežnika CWA pridobi podatke o okuženih dnevnih ključih, te podatke preračuna na način, da posamezen dnevni ključ zgosti in ga šifrira ter tako spremeni v oddajno kodo, ki

ga primerja z oddajnimi kodami stikov (torej uporabnikov aplikacije, ki so bili v zaznavnem območju Bluetooth uporabnikovega telefona), šele ob ugotovitvi ujemanja, odpre aplikacija set meta podatkov in izračuna ogroženost.

Popoln postopek obdelave podatkov je grafično prikazan kot Priloga 2 tega dokumenta.

2.2.2 Statistični nameni

Za namen statistike se periodično iz verifikacijskega strežnika objavijo podatki o številu izdanih TAN kod in številu uporabljenih TAN kod. Podatki se pridobijo iz shranjenih zgoščenih vrednosti na verifikacijskem strežniku. Podatki se objavijo 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.

Gre za obdelavo podatkov v statistične in znanstveno-raziskovalne namene v skladu s 17. členom ZVOP-1. Navsezadnje pa gre za obdelavo takšnih podatkov, ki niti niso povezani z določenim ali določljivim posameznikom.

2.3 Psevdonimizacija podatkov

Psevdonimizacija podatkov se izvaja na več ravneh.

Na ravni aplikacije se ne obdeluje osebnih podatkov iz naprave, temveč se vsa obdelava izvaja preko dnevnik ključev in oddajnih kod, ki se menjajo v kratkih časovnih intervalih (15 minut) in sami po sebi ne omogočajo identifikacije posameznika ali posamezne naprave in določevanja lokacije naprave, pač pa zgolj potrditev ali se je posamezni uporabnik aplikacije v zadnjih 14 dneh nahajal v bližini okuženih posameznikov – tistih uporabnikov aplikacije, ki so izrecno potrdili preko aplikacije, da so okuženi.

Na ravni izvedbe posredovanja TAN-a na način, da je strežnik za generiranje TAN-a ločen od zbirke okuženih posameznikov. In da TAN po SMS dobi vsaka oseba, ki je bila na testu pozitivna na SARS-CoV-2.

Na ravni strežnikov tako, da se na strežniku CWA hranijo zgolj dnevni ključi okuženih uporabnikov in ID dogodkov, ki so izrecno potrdili svojo okužbo brez drugih podatkov, ki bi omogočali identifikacijo posameznika. Dnevni ključi okuženih uporabnikov se samodejno pobrišejo po 14 dneh.

3 OCENA TVEGANJ IN UKREPI ZA OBVLADOVANJE TVEGANJ ZA VARSTVO PODATKOV

Opis tveganj in ukrepi za odpravo tveganj so konkretizirani v Prilogi 1 tega dokumenta.

3.1 OCENA NUJNOSTI IN SORAZMERNOSTI OBDELAVE

3.1.1 Pravna podlaga in namen obdelave

NIJZ je kot organ, pristojen za javno zdravje, aplikacijo, ki je predmet te ocene učinkov, prepoznal kot ustrezen pripomoček posameznikom za samozaščitno vedenje, in je tudi pristojen za določanje njene vsebine.

NIJZ in MJU sta bila pred uveljavitvijo ZZUOOP kot skupna upravljavca pristojna v skladu s točko e 1. odstavka 6. člena Splošne uredbe o varstvu podatkov, ki določa, da je obdelava osebnih podatkov dopustna, če je potrebna za opravljanje naloge v javnem interesu ali pri izvajanju javne oblasti, dodeljene upravljavcu, prav tako pa tudi točke g 2. odstavka 9. člena, ki določa, da prepoved obdelave posebnih vrst osebnih podatkov ne velja v primeru, ko je obdelava »potrebna iz razlogov bistvenega javnega interesa na podlagi prava Unije ali prava države članice, ki je sorazmerno z zastavljenim ciljem, spoštuje bistvo pravice do varstva podatkov ter zagotavlja ustrezne in posebne ukrepe za zaščito temeljnih pravic in interesov posameznika, na katerega se nanašajo osebni podatki«.

V zvezi s tem 46. uvodni stavek Splošne uredbe o varstvu podatkov pojasnjuje, da »nekatero vrste obdelave lahko služijo tako pomembnim razlogom v javnem interesu kot življenjskim interesom posameznika, na katerega se nanašajo osebni podatki, na primer kadar je obdelava potrebna v humanitarne namene, tudi za spremljanje epidemij in njihovega širjenja ali v izrednih humanitarnih razmerah, zlasti pri naravnih nesrečah in nesrečah, ki jih povzroči človek«, iz česar nedvoumno izhaja, da v okvir javnega interesa sodi spremljanje epidemij in omejevanje njihovega širjenja, kar je edini namen obdelave osebnih podatkov v okviru aplikacije #OstaniZdrav.

Glede na to, da se je življenje v Republiki Sloveniji v letu 2020, prav tako v letošnjem letu zaradi vsem znanih okoliščin večkrat ustavilo, glede na to, da države članice EU določajo omejitve v zvezi z najosnovnejšim evropskim integracijskim momentom – prost pretok ljudi, glede na to, da se je posameznih obdobjih v Republiki Sloveniji določalo po več tisoč karanten za posameznike na vikend, NIJZ in MJU ocenjujeta, da gre pri boju zoper COVID-19 za bistven javni interes.

V skladu z vsebino in *rationem* zgoraj navedene podlage je bil sprejet tudi ZZUOOP, ki je podrobneje uredil nekatere sestavine aplikacije, ki je predmet pričujoče ocene ter kot upravljavca osebnih podatkov izrecno tudi določil, da sta to NIJZ in MJU (53. člen ZZUOOP).

Veljavni ZZUOOP tako podrobneje določa, da je namestitev in uporaba aplikacije prostovoljna, v njem so določeni nabori podatkov, ki se obdelujejo, namen obdelave, hramba podatkov in njena interoperabilnost ter nekatere druge določbe glede zasnove mobilne aplikacije.

Dodatni pojasnili

Pojasnilo o v javnosti izpostavljeni povezavi med sprejetim Zakonom o interventnih ukrepih za pripravo na drugi val COVID-19 (ZIUPDV) in aplikacijo:

Državni zbor RS je na seji DZ RS 9. 7. 2020 sprejel Zakon o interventnih ukrepih za pripravo na drugi val COVID-19 (ZIUPDV), v okviru katerega je v četrtem poglavju Mobilna aplikacija za obveščanje o stikih z okuženimi z virusom SARS-CoV-2 in osebami, ki jim je bila odrejena karantena, predvidel pravno podlago za vzpostavitev tovrstne aplikacije, vendar določila ZIUPDV vključujejo tudi zahteve po obvezni namestitvi aplikacije ter po namestitvi aplikacije s strani oseb, ki jim je bila odrejena karantena. Te pravne podlage ni mogoče uporabiti za zagotavljanje aplikacije, kot je pričujoča, saj, poleg tega, da imata popolnoma drugačne predpostavke⁴ in ju posledično tudi ni mogoče zamenjevati, je bila aplikacija

⁴Več o predpostavkah je zapisano v uvodu ocene učinkov pod točko 1.1 Pojasnilo.

#OstaniZdrav naknadno z izrecno zakonsko določbo v 54. členu ZZUOOP jasno izvzeta iz določb ZIUPDV v delu, ki se nanaša na mobilno aplikacijo. Aplikacija #OstaniZdrav torej ni povezana z ZIUPDV in pravno gledano ni mogoče zahtevati njene obvezne uporabe, kot tudi ni mogoče zahtevati njene uporabe za osebe, ki jim je bila odrejena karantena (kar je sicer tudi tehnično nemogoče), kot je to veljajo tudi za obdobje pred sprejetjem ZZUOOP Aplikacije #OstaniZdrav pa še zaradi drugih pravnih omejitev na strani aplikacije tudi ni mogoče zagotoviti za primere, ki jih je predvidel ZIUPDV.

Druge pravne omejitve na strani aplikacije so namreč dejstvo, da aplikacija #OstaniZdrav deluje s pomočjo uporabe Google Apple Exposure Notification (v nadaljnjem besedilu: GAEN) pri čemer Splošni pogoji uporabe⁵ Googla in Appla vključujejo med drugim tudi, da se uporablja izključno za napore na odzive na COVID-19 in ne za kakršnekoli druge namene, kot je na primer pregon kaznivih dejanj in sankcioniranje prekrškov (e.g. uveljavljanje posameznikove karantene)⁶.

Pri aplikaciji #OstaniZdrav torej ne gre za aplikacijo, ki bi bila kakorkoli povezana z izvrševanjem določb ZIUPDV.

3.1.2 Sorazmernost obdelave osebnih podatkov

Posameznik, ki bi se odločil za uporabo aplikacije #OstaniZdrav, se bo zanjo odločil prostovoljno, prav tako se bo prostovoljno odločil za posredovanje informacije o tem, da je bil okužen z virusom SARS-CoV-2, ob čemer se drugim osebam, ki so bile z njim v stiku, ne bo posredoval podatek o tem, za katero osebo gre.

Podatki, ki se bodo obdelovali v okviru te aplikacije, bodo pomagali skupini posameznikov, ki se bo odločila za takšen pripomoček, za večjo obveščenost o rizičnosti stikov, ki jih je posameznik imel v zadnjih 14 dneh.

Glede na epidemiološko stanje v Republiki Sloveniji, ko je od števila okuženih odvisna kvaliteta življenja, ki se kaže tudi v možnosti neomejenosti človekovih pravic (kot je na primer pravica svobodnega gibanja), NIJZ in MJU ocenjujeta, da gre pri aplikaciji #OstaniZdrav za pripomoček, ki je, sploh pod predpostavko, da gre za njegovo prostovoljno uporabo, ne le primeren, temveč tudi izpolnjuje zahtevo po sorazmernosti pri obdelavi osebnih podatkov.

Za namene zagotavljanja ustrezne in sorazmerne obdelave osebnih podatkov bo NIJZ ob bistveni spremembi epidemiološke slike ugotavljal primernost nadaljnjega zagotavljanja delovanja aplikacije. Tudi z ZZUOOP je določeno, da gre v primeru aplikacije za začasen ukrep, torej ni bil sprejet za nedoločen čas. Njegova začasna narava je razvidna iz samega naslova zakona, kot tudi sistematike navedenega zakona z ozirom na aplikacijo.⁷ Tudi iz 7. točka 7a. člena Sklepa Evropske komisije je razvidna začasna narava EFGS oz. evropskega centralnega strežnika, saj predvideva, da EFGS preneha delovati najpozneje 14 dni po tem, ko vse povezane nacionalne mobilne aplikacije prenehajo prenašati ključne preko združevalnega prehoda oz. evropskega centralnega strežnika.

Posredovanje in dostop do podatkov v aplikaciji #OstaniZdrav.

Podatki, ustvarjeni med uporabo aplikacije #OstaniZdrav se obdelujejo na strežnikih v Republiki Sloveniji in evropskem centralnem strežniku, ki ga zagotavlja Evropska komisija z namenom povezave

⁵ZA

Google

ENS:https://blog.google/documents/72/Exposure_Notifications_Service_Additional_Terms.pdf

⁶Is used exclusively for COVID-19 response efforts and not for any other purpose, such as law-enforcement or any punitive action (e.g., individual quarantine enforcement)

⁷ V ZZUOOP je 9. poglavje, ki ureja mobilno aplikacijo, umeščeno pod točko I četrtega dela z naslovom »ZAČASNI UKREPI NA PODROČJU ZDRAVSTVA«. V tretjem odstavku 1. člena je tudi določeno, da »s tem zakonom se določajo tudi začasni ukrepi za omilitev in odpravo posledic COVID-19 na področju zdravstva, dela, socialnega varstva, gospodarstva, vzgoje in izobraževanja, izvrševanja kazenskih sankcij in pravosodja, kmetijstva, gospodarstva in prehrane, infrastrukture in obrambe.«

zalednih sistemov držav članic, ki jih za enake namene zagotavljajo te države. Tovrstni podatki ne bodo posredovali nikamor izven okvirja aplikacije.

Do podatkov v lokalno nameščeni aplikaciji bo dostopal posameznik, ki je aplikacijo namestil, do podatkov v evidenci okuženih kod ne bo dostopal nihče, razen če bo to nujno potrebno za vzdrževanje delovanja informacijskega sistema. Ti dostopi bodo podvrženi omejitvam, ki izhajajo iz pravic oseb, ki bodo vzdrževanje izvajale, prav tako pa bodo tehnično nadzorovani na ustaljene načine, ki jih tudi sicer uporablja MJU za upravljanje DRO.

3.1.3 Udeleženi subjekti

3.1.3.1 Upravljavce:

V zvezi z varovanjem osebnih podatkov in s tem povezano odgovornostjo bo:

- a) skupni upravljavce za vsebinski del: NIJZ

V tem okviru bo NIJZ:

- posredoval TAN okuženemu posamezniku;
- spremljal postopek delovanja aplikacije in zahteval njene spremembe;
- pripravljaj besedila za navodila posameznikom za ravnanje v primeru okuženosti;
- pripravljaj besedila na spletnih straneh z navodili in usmeritvami;

- b) skupni upravljavce za tehnični del: MJU

V tem okviru bo MJU:

- zagotovil zunanega izvajalca za namestitve in prilagajanje aplikacije #OstaniZdrav;
- izvajal delovanje aplikacije in zagotavljal njene spremembe po navodilu NIJZ;
- zagotavljal delovanje DRO, na katerega se namesti strežniški del aplikacije #OstaniZdrav;
- skrbel za izvajanje organizacijskih in tehničnih ukrepov za varovanje podatkov, ki se bodo obdelovali v okviru aplikacije #OstaniZdrav.

Skupna upravljavca sta svoje dolžnosti in odgovornosti dogovorila v dogovoru o skupnem upravljanju v skladu s členom 26 Splošne uredbe o varstvu podatkov.

Sodelujoče države članice pri čezmejni izmenjavi podatkov (via EFGS), ki jih zastopajo imenovani nacionalni organi ali uradni organi, skupaj določajo namen in načine obdelave podatkov prek evropskega strežnika oz. združevalnega prehoda ter so posledično skupaj z upravljalcema iz Republike Slovenije skupni upravljavci. Samo države, ki izpolnjujejo ustrezne kriterije varovanja podatkov lahko sodelujejo v čezmejni uporabi aplikacije, skladno s Sklepom Evropske komisije.

Dolžnosti posameznih skupnih upravljavcev so določene v prilogi II navedenega sklepa Evropske komisije, kjer je določena:

- delitev odgovornosti skupnih upravljavcev ((1) (1)),
- odgovornosti in vloge pri obravnavanju zahtevkov in obveščanju posameznikov, na katere se nanašajo osebni podatki ((1) (2))obvladovanje varnostnih incidentov, vključno s kršitvami varstva osebnih podatkov (2)

- ocena učinkov – zagotavljanje informacij drugemu upravljavcu (3).

Nacionalni skupni upravljavci držav, ki so vključene v čezmejno izmenjavo podatkov, ter njihova obvestila o varstvu podatkov so vsakemu posamezniku na voljo na spletni strani Evropske komisije: https://ec.europa.eu/health/sites/health/files/ehealth/docs/gateway_jointcontrollers_en.pdf. Do nje lahko vsak zainteresiran posameznik dostopa tudi preko povezave navedene v obvestilu o varstvu podatkov.

3.1.3.2 Obdelovalec

Obdelovalci z vidika Splošne uredbe o varstvu podatkov bodo vsi zunanji izvajalci, ki jih bo MJU najel za izvajanje določenih segmentov storitev. Pred pooblastitvijo zunanjih izvajalcev za (pogodbene) obdelovalce, bo MJU ugotovil ali zagotovil izpolnjevanje vseh pogojev, ki jih morajo obdelovalci izpolnjevati, da bodo svoje naloge izvajali v skladu s Splošno uredbo o varstvu podatkov in drugimi predpisi, ki urejajo varstvo osebnih podatkov.

MJU ima v pogodbah, ki jih sklepa z zunanjimi izvajalci, predvidene določbe v zvezi z obdelavo osebnih podatkov, prav tako pa ima tudi dogovorjeno, da če gre za obdelavo osebnih podatkov, mora pogodbo pred njeno sklenitvijo pregledati odgovorna oseba za varstvo osebnih podatkov na MJU.

Evropska komisija se kot ponudnik tehničnih in organizacijskih rešitev pri čezmejni izmenjavi podatkov (via EFGS) šteje za obdelovalca v smislu določb Splošne uredbe o varstvu podatkov ter je zavezana varstvu podatkov kot določa veljana pravna ureditev. V že navedenem sklepu Evropske komisije so določena pravila o obdelavi, ki jo izvaja Evropska komisija kot obdelovalec (11. točka uvodnih ugotovitev). Konkretni varnostni ukrepi in navodila v skladu z namenom varne in zakonite obdelave podatkov so določeni v Prilogi III Sklepa Evropske komisije – »Odgovornost komisije kot obdelovalca podatkov na združevalnem prehodu za čezmejno obdelavo med nacionalnimi mobilnimi aplikacijami za sledenje stikom in opozarjanje«. Evropska komisija je skladno z zahtevami Splošne uredbe o varstvu podatkov izvedla tudi svojo oceno učinkov.

3.1.4 Uporaba istega povezovalnega znaka

V okviru delovanja aplikacije #OstaniZdrav se ne bo uporabljal isti povezovalni znak.

3.1.5 Rok hrambe podatkov v aplikaciji #OstaniZdrav

Podatki o stikih posameznikov se bodo v obliki na 15 minut izvedene oddajne kode hranili lokalno na mobilnem telefonu posameznika, ki je namestil aplikacijo. Ti podatki se hranijo 14 dni od stika.

Podatki o tem, da določena koda pripada osebi, ki je okužena, se bodo hranili na strežniku CWA. Ti podatki se hranijo 14 dni od vnosa v evidenco.

3.1.6 Varnost podatkov v aplikaciji #OstaniZdrav in pogodbeni obdelava

Zavarovanje celotnega sistema bo izvedeno v skladu s pravili poslovanja MJU ter dokumentacijo, ki je že bila pripravljena za izvedbo projekta in vključuje vse aktivnosti, ki so našteje tako v tem, kot spremljajočih dokumentih. Zavarovanje celotnega sistema, ki zagotavlja čezmejno izmenjavo podatkov preko evropskega centralnega strežnika (EFGS) je izvedeno skladno s pravili in standardi poslovanja Evropske komisije.

Splošno o informacijski varnosti na MJU

Celovitost in zaupnost obdelave osebnih podatkov bosta zagotovljeni z varovanjem podatkov v celotnem podatkovnem toku, ki je razviden iz Priloge 2 te ocene učinkov.

Varnost podatkov

Delovanje aplikacije #OstaniZdrav se bo zagotavljalo na DRO infrastrukturi, ki ima vzpostavljen sistem upravljanja varovanja informacij skladno z internimi akti. Obenem je MJU tudi že pridobil certifikat ISO27001 za DRO.

Na MJU je za informacijsko varnost pristojen Sektor za informacijsko varnost (v nadaljnjem besedilu: SIV) v sklopu MJU, DI. Tudi aplikacija #OstaniZdrav bo, pred njeno namestitvijo na DRO infrastrukturo

pri MJU, šla skozi vrsto postopkov in presojo skladnosti, ki so urejene v različnih dokumentih, potrjene pa preko izpolnjevanja Generičnih tehničnih zahtev. Da se rešitev lahko začne razvijati in je na voljo uporabnikom, mora prestati vse teste in s tem zadovoljiti zahtevam informacijsko-varnostnih politik MJU. To bo zagotovljeno tudi v primeru nameščanja aplikacije #OstaniZdrav.

Delovanje evropskega centralnega strežnika bo zagotavljala Evropska komisija, ki ima prav tako vzpostavljen sistem upravljanja varovanja. Evropska komisija ima že definirane zavezujoče standarde glede varnosti informacijske tehnologije v Sklepu komisije (EU, Euratom) 2017/46 z dne 10. januarja o varstvu komunikacijskih in informacijskih sistemov v Evropski komisiji, ki so skladno s 14. členom pravno zavezujoči in je njihova uporaba obvezna.

Pogodbena obdelava

MJU bo pri tehničnem zagotavljanju delovanja aplikacije #OstaniZdrav sodelovalo z več pogodbenimi izvajalci, ki se bodo v času zagotavljanja storitve lahko spreminjali.

Vsi pogodbeni izvajalci bodo skladno s pogodbenimi določili podatke obdelovali le v imenu in za račun MJU kot skupnega upravljavca aplikacije #OstaniZdrav v zagotavljanju tehničnega delovanja aplikacije.

MJU bo pred podelitvijo pravic za dostop do sistema, ki ga upravlja zunanji izvajalec in vsebuje osebne podatke, zagotovil, da bo zunanji izvajalec razpolagal s pravno podlago za izvajanje konkretne storitve, ki vključuje pravno podlago za morebitno obdelavo osebnih podatkov (pogodba, dogovor,...).

Zavarovanje celotnega sistema bo izvedeno v skladu s pravili poslovanja MJU ter dokumentacijo, ki bo pripravljena za izvedbo projekta in vključuje vse aktivnosti, ki so našteje tako v tem, kot spremljajočih dokumentih.

V povezavi z EFGS je potrebno še dodati, da tudi Evropska komisija svoje izvajalce zavezuje s posebno pogodbeno klavzulo za kakršnokoli obdelavo osebnih podatkov v imenu komisije, skladno s Splošno uredbo o varstvu podatkov.

3.1.7 Sistemi za upravljanje varovanja informacij (SUVI)

Delovanje aplikacije #OstaniZdrav se bo zagotavljalo na DRO infrastrukturi, ki ima vzpostavljen sistem upravljanja varovanja informacij skladno z internimi akti. Obenem je MJU pridobil certifikat ISO27001 za DRO.

Za zagotavljanje delovanja aplikacije #OstaniZdrav se pravila postavljajo z navedenimi v tem dokumentu, torej s pravili, po katerih posluje MJU, DI.

Za delovanje evropskega centralnega strežnika (EFGS) skrbi Evropska komisija skladno z zgoraj navedenim Sklepom komisije o varstvu komunikacijskih in informacijskih sistemov v Evropski komisiji, ki veljajo za vse informacijske sisteme Evropske komisije.

3.1.8 Uničenje podatkov

Podatki o stikih posameznikov se bodo v obliki na 15 minut izvedene oddajne kode hranili lokalno na posameznem mobilnem telefonu. Ti podatki se hranijo 14 dni od stika. Aplikacija #OstaniZdrav je sprogramirana na način, da se po tem času podatki avtomatično izbrišejo.

Podatki o tem, da določena koda pripada osebi, ki je okužena, se bodo hranili na strežniku CWA. Ti podatki se hranijo 14 dni od vnosa v evidenco. Aplikacija #OstaniZdrav je sprogramirana na način, da se po tem času podatki avtomatično izbrišejo s strežnika CWA.

MJU zagotavlja, da se bodo nosilci podatkov po prenehanju njihove uporabe uničili v skladu s predpisi MJU o uničevanju nosilcev zapisov.

3.1.9 Notranja sledljivost obdelave

Notranjo sledljivost obdelave se bo zagotavljala z upoštevanjem varnostne sheme in dnevniškimi zapisi.

3.1.10 Sledljivost posredovanja (zunanja sledljivost)

Podatki iz aplikacije #OstaniZdrav se ne bodo posredovali tretjim osebam.

3.1.11 Interni nadzor

Interni nadzor se bo zagotavljal tako, da bo odgovorna oseba MJU enkrat mesečno pregledala statistike, analize ali poročila aplikacije #OstaniZdrav o:

- ažurnosti seznama tehničnih skrbnikov aplikacije #OstaniZdrav,
- seznam morebitnih evidentiranih napak in težav.

3.1.12 Izobraževanje

NIJZ in MJU bosta na svojih spletnih straneh zagotovila objavo navodil za uporabo aplikacije ter ustrezna obvestila posameznikom o obdelavi osebnih podatkov.

NIJZ in MJU bosta zagotovila delovanje enotnega kontaktnega centra za pomoč uporabnikom.

V okviru izobraževanja se bo posebej naslovilo tudi dejstvo, da je morebitno zlorabljanje aplikacije (posojanje telefona s podatkom, da gre za okuženega uporabnika, osebam, ki niso okužene), neželeno ravnanje, ki lahko škoduje dobrobiti prebivalcev Slovenije.

3.1.13 Iznos osebnih podatkov v tretje države

Podatki se ne bodo iznašali v tretje države. Podatki se obdelujejo izključno na strežniku v Republiki Sloveniji in evropskem centralnem strežniku, ki ga zagotavlja Evropska komisija.

3.1.14 Evidenca dejavnosti obdelave osebnih podatkov

Vsak od skupnih upravljavcev vzpostavi lastno evidenco dejavnosti obdelave osebnih podatkov ter skrbi za njeno ustreznost.

3.1.15 Povezovanje zbirk osebnih podatkov

Povezovanje zbirk iz aplikacije #OstaniZdrav z drugimi zbirkami se ne bo izvajalo.

3.2 UKREPI VARSTVA PRAVIC POSAMENIKOV

3.2.1 Točnost in ažurnost podatkov

Pred vzpostavitvijo delovanja aplikacije #OstaniZdrav se je izvedlo testiranje, na podlagi katerega se je potrdilo ustreznost delovanja aplikacije, točnost in ažurnost podatkov v aplikaciji #OstaniZdrav pa zaradi odsotnosti identifikatorjev, ki bi omogočali določanje posameznika, težko preverjati.

Ob morebitnih sporočilih o netočnosti ali neažurnosti podatkov bosta NIJZ in MJU pristopila k dodatnim testiranjem in izvedbam popravkov, ki bodo odpravili morebitne naknadno ugotovljene pomanjkljivosti.

Glede na to pa, da gre za pripomoček, ter v luči dejstva, da bo točnost podatkov odvisna od mnogih dejavnikov iz okolice, se od aplikacije #OstaniZdrav pričakuje nekoliko manjša točnost podatkov.

Ažurnost podatkov se zahteva pri njihovem brisanju.

3.2.2 Preglednost in informiranje posameznika

Celotna koda slovenske različice aplikacije #OstaniZdrav je objavljena na spletnih straneh Github.

NIJZ in MJU sta na svojih spletnih straneh zagotovila tudi objave, s katerimi se bodo zagotavljale pravice posameznikov o informiranosti pri obdelavi osebnih podatkov.

3.2.3 Ostale pravice posameznika

Ker gre v primeru uporabe aplikacije #OstaniZdrav za obdelavo, ki ne zahteva identifikacije posameznika, se ostale pravice posameznika ne zagotavljajo v skladu s členom 11 Splošne uredbe o varstvu podatkov. 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 drugih odstavkom 11. člena Splošne uredbe o varstvu podatkov). Poleg tega bi bilo v nasprotju s ciljem, ki teži k temu, da je količina podatkov, obdelanih za aplikacijo, čim manjša. Konkretnije velja:

1. Informacije v zvezi z obdelavo osebnih podatkov – na spletnih straneh NIJZ in MJU je mogoče pridobiti splošne informacije o obdelavi podatkov, informacij, ki bi bile vezane na posameznika, pa zaradi odsotnosti ustreznega osebnega identifikatorja ni mogoče zagotavljati;
2. Pravica do popravka – pravice do popravka ni mogoče izvajati, saj tako posameznik kot upravljavec ne vesta, kateri podatek se nanj sploh nanaša in posledično napake ni mogoče ugotoviti.
3. Pravica do izbrisa – izbris osebnega podatka je mogoč le iz lastne namestitve aplikacije, v okviru katere je posameznik lahko izbrisal vse podatke, ki so nastali v okviru delovanja aplikacije.
4. Pravica do omejitve obdelave in pravica do ugovora – pravico do omejitve obdelave posameznik lahko izvršuje, če dokaže, da je imetnik 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, kar ta obdelava ne zahteva identifikacije, v tem delu ni mogoče izvrševati. Pravice do ugovora ni mogoče izvrševati drugače, kot v delu, v katerem se podatki obdelujejo lokalno, in sicer z njihovim izbrisanjem.

Glede na to, da se člen 11 ne uporablja, če posameznik, na katerega se nanašajo osebni podatki, za uresničevanje svojih pravic na podlagi teh členov zagotovi dodatne informacije, s katerimi ga je mogoče identificirati, skupna upravljavca ugotavljata, da:

- bi bilo mogoče te pravice uveljavljati le s posredovanjem dnevnega ključa, kar je identifikator, s katerim posameznik ne razpolaga in bi bilo treba narediti posebno informacijsko rešitev, ki bi omogočala pridobitev tega podatka izven rednih podatkovnih poti aplikacije #OstaniZdrav,
- bi se vsaj eden od upravljavcev seznanil z dejstvom ali posameznik uporablja aplikacijo, pri čemer je anonimnost uporabe pred javnim sektorjem ena najpomembnejši organizacijskih ukrepov, poleg tega pa bi se lahko v okviru obdelave postopkov tudi z drugimi osebnimi podatki posebnih vrst, kar pomeni, da bi začel eden od skupnih upravljavcev obdelovati podatke, za katere sploh nima pravne podlage, saj teh podatkov noben od skupnih upravljavcev ne obdeluje z vidika vsebine.

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. 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 posameznik posreduje neposredno na upravljavca v Republiki Sloveniji; lahko pa se obrne tudi na upravljavca države članice ali Evropsko komisijo. Sklep Evropske komisije podrobneje določa, da vsak upravljavec deluje kot vstopna točka za uporabnike svoje nacionalne aplikacije ter obravnava zahtevke v zvezi z uveljavljanjem pravic posameznikov. Vsak nacionalni upravljavec imenuje posebno kontaktno točko, namenjeno zahtevkom, ki jih prejmejo od posameznikov. Sklep Evropske komisije določa tudi protokol v primeru, da skupni upravljavec prejme zahtevek posameznika, za katerega ni pristojen, mora ta zahtevek nemudoma posredovati pristojnemu skupnemu upravljavcu. Kljub enotni vstopni točki nacionalnega upravljavca, to ni ovira, da se posameznik, v primeru, če tako želi, obrni tudi sam neposredno na Evropsko komisijo ali skupnega upravljavca v drugi državi članici, ki sodeluje v čezmejni izmenjavi podatkov.

4 ZAKLJUČKI OCENE UČINKOV

Na podlagi opravljene ocene učinkov, s pomembnim vplivom Priloge 1, NIJZ in MJU ocenjujeta, da so nameni in cilji vzpostavitve aplikacije #OstaniZdrav ustrezni in skladni z veljavno pravno podlago in nameni zbiranja podatkov.

Ocenjuje se, da bo z navedenimi ukrepi, ki so tako preventivne kot kurativne narave, zagotovilo primerno varstvo osebnih podatkov posameznikov.

Datum:
Številka:

Nacionalni inštitut za javno zdravje
Milan Krek, dr. med., spec.

direktor

Datum:
Številka:

Ministrstvo za javno upravo
Boštjan Koritnik

po pooblastilu Peter Geršak
državni sekretar

2 SEZNAM UPORABLJENIH KRATIC

Kratica	Slovenski izraz/pojasnilo
API	Vmesnik za namensko programiranje (angleško: Application programming interface)
CWA	Corona Warn App, uporabljano v okviru besedne zveze strežnik CWA, torej strežnik, na katerem se nahaja seznam dnevniških ključev ki pripadajo uporabnikom aplikacije, ki so se strinjale z njihovim prenosom na strežnik CWA
DRO	Državni računalniški oblak
GAEN	Google Apple Exposure Notifications
MJU	Ministrstvo za javno upravo
NIJZ	Nacionalni inštitut za javno zdravje
OP	Osebni podatki
RPI	Identifikator, pridobljen iz zgoščenega in šifriranega dnevnega ključa na 15 minut (angleško: Rolling Proximity Identifier) imenovano kot oddajno kodo
TAN	Transaction Authentication number
TEK	Naključno določeni ključ (angleško: Temporary Exposure Key) imenovan kot dnevni ključ

3 VIRI

1. Ocene učinkov na varstvo podatkov, Smernice Informacijskega pooblaščenca, Verzija: 1.1, datum izdaje: 24. 5. 2018;
2. Smernice glede ocene učinka v zvezi z varstvom podatkov in opredelitve, ali je »verjetno, da bi (obdelava) povzročila veliko tveganje«, za namene Uredbe (EU) 2016/679 sprejete 4. aprila 2014 in revidirane 4. oktobra 2017 – Delovna skupina za varstvo osebnih podatkov iz člena 29;
3. Presoje vplivov na zasebnost pri projektih eUprave, Smernice Informacijskega pooblaščenca, Verzija: 1.0, datum izdaje: 22. 7. 2010;
4. Zakon o varstvu osebnih podatkov (Uradni list RS, št. 94/07 – uradno prečiščeno besedilo)
5. UREDBA (EU) 2016/679 EVROPSKEGA PARLAMENTA IN SVETA z dne 27. aprila 2016 o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem pretoku takih podatkov ter o razveljavitvi Direktive 95/46/ES (Splošna uredba o varstvu podatkov)
6. Izvedbeni sklep komisije (EU) 2020/1023 z dne 15. julija o spremembi Izvedbenega sklepa (EU) 2019/1765 glede čezmejne izmenjave podatkov med nacionalnimi aplikacijami za sledenje stikom in opozarjanje v zvezi v zvezi z bojem proti pandemiji COVID-19
7. Spletna stran Evropske komisije (tiskovni kotiček)

4 PRILOGE OCENE UČINKOV

Priloga 1: Tveganja in ukrepi za obvladovanje tveganj v povezavi z varnostjo podatkov

Priloga 2: Postopki prenosa podatkov med lokalno namestitvijo aplikacije na mobilni telefon in centralno zbirko

Priloga 3: Postopek generiranja in uporabe kode za potrditev statusa okuženosti na strežniku CWA

5 Priloga 1: Tveganja in ukrepi za obvladovanje tveganj v povezavi z varnostjo podatkov

NIJZ in MJU v okviru te ocene tveganja ne ocenjujeta splošnih tveganj, ki se nanašajo na uspešnost zagotavljanja vseh storitev MJU (na primer: poplava, ki lahko uniči sistemsko sobo,...), temveč se omejujeta na tveganja v zvezi z varstvom osebnih podatkov in zasebnosti. Splošna tveganja obravnava MJU v okviru aktivnosti MJU ter zagotavljanja infrastrukture DRO.

Ravni tveganja se ocenjujejo na lestvici: nizka, srednja, visoka. Raven tveganja je ocenjena kot nizka, če sta majhni verjetnost in resnost, kot srednja, če sta ali verjetnost ali resnost srednji, ter kot visoka, če sta verjetnost in resnost veliki, ali če je resnost velika zaradi pomanjkanja pravne podlage za obdelavo OP. Če sta verjetnost in resnost le stopnjo razlike, je raven tveganja enaka višji stopnji.

NIJZ in MJU v zvezi s tveganji in ukrepi, ki se nanašajo na varstvo osebnih podatkov in zasebnosti, ugotavljata:

	A	B	C	Č	D	E	D
	Načelo/vsebin a	Tveganje	Verjetnost	Resnost	Raven tveganja	Ukrep	Raven tveganja po upoštevanju ukrepa
1.	Zakonitost	Zaradi potencialne politične spornosti aplikacij za obveščanje posameznikov o stikih z okuženimi je treba sproti ugotavljati ali dejansko obstaja javni interes za obdelavo osebnih podatkov.	Majhna, ker je v ZZUOOP izrecno urejena pravna podlaga delovanja mobilne aplikacije in namen njenega delovanja oziroma namen obdelave osebnih podatkov. Pred uveljavitvijo ZZUOOP je bila tovrstno tveganje kvalificirano kot srednje, ker je iz javnega mnenja mogoče razbrati, da se del javnosti strinja s pripomočkom,	Velika, pomanjkanje pravne podlage za obdelavo OP je največja kršitev varstva OP.	Visoka, zaradi velike resnosti	NIJZ bo za namene zagotavljanja ustrezne in sorazmerne obdelave osebnih podatkov ob bistveni spremembi epidemiološke slike ugotavljal primernost nadaljnjega zagotavljanja delovanja aplikacije, kot opisano v točki 3.1.2 Sorazmernost obdelave osebnih podatkov. Ta ukrep je veljal tudi za obdobje pred uveljavitvijo ZZUOOP, ob tem, da je NIJZ preverjal tudi obstoj	Srednja, zaradi velike resnosti

	A	B	C	Č	D	E	D
	Načelo/vsebin a	Tveganje	Verjetnost	Resnost	Raven tveganja	Ukrep	Raven tveganja po upoštevanju ukrepa
			kakršna je aplikacija #OstaniZdrav, ter da epidemiološka stroka ocenjuje potrebnost razvoja ter uporabe takšne aplikacije kot ene od koristnih metod obvladovanja epidemije.			pravne podlage za obdelavo (javni interes).	
2.	Zakonitost	Iz ključev, ki se nahajajo pri posamezniku na mobilnem telefonu, je mogoče sklepati na drugega posameznika, s katerim je bil prvi v stiku, zaradi poznavanja identitete posameznika, s katerim je bil v stiku v fizičnem svetu.	Majhna, ker je malo verjetno, da bi bil posameznik v stiku le z eno osebo na dan, če pa je bil, potem ve, katera je ta oseba.	Velika, pomanjkanje pravne podlage za obdelavo OP je največja kršitev varstva OP.	Visoka, zaradi velike resnosti	Da ne bi bilo mogoče preko pridobljenega ključa sklepati na istega posameznika na kakšen drug dan, se zgoščene kode posameznikov šifrirajo na 15 minut in menjajo enkrat dnevno – oddajna koda.	Nizka
3.	Zakonitost / pogodbeni obdelava	MJU z zunanjimi izvajalci ne bo sklenil potrebnih dogovorov.	Majhna, saj bo MJU v okviru izbire zunanjega izvajalca vključil določila v zvezi s pogodbeno obdelavo.	Srednja, pomanjkanje pravne podlage za obdelavo OP je največja kršitev varstva OP, vendar v primeru obdelovanja podatkov sekundarna – pravna podlaga za obdelavo bo že obstajala, manjkal bo vezni člen z morebitnim	Srednja	MJU pri izpolnjevanju obveznosti zunanjega izvajalca zagotovi vse ukrepe, opisane v podpoglavju »Pogodbeni obdelava«.	Nizka

	A	B	C	Č	D	E	D
	Načelo/vsebin a	Tveganje	Verjetnost	Resnost	Raven tveganja	Ukrep	Raven tveganja po upoštevanju ukrepa
				zunanjim izvajalcem.			
4.	Preglednost in informiranje (Pravice posameznika / informiranje posameznika) - NIJZ	Posamezniki, uporabniki aplikacije #OstaniZdrav bodo imeli vprašanja glede obdelave osebnih podatkov v okviru aplikacije #OstaniZdrav.	Srednja, saj bi morala biti aplikacija pripravljena na način, da bi bil način obdelave posameznikom poznan.	Srednja, saj je kljub temu, da ne gre za napačno obdelavo podatkov, razumevanje aplikacije s strani posameznikov izrednega pomena, saj bo le z ustreznim razumevanjem aplikacije mogoče zagotoviti njeno široko uporabo.	Srednja	NIJZ bo morebitnim zanimanim posameznikom zagotovil informacije v skladu s podpoglavjem 3.2.2 »Preglednost in informiranje posameznika«.	Nizka
5.	Preglednost in informiranje – MJU	Posamezniki, uporabniki aplikacije #OstaniZdrav bodo imeli vprašanja glede obdelave osebnih podatkov v okviru aplikacije #OstaniZdrav.	Srednja, saj bi morala biti aplikacija pripravljena na način, da bi bil način obdelave posameznikom poznan.	Majhna, saj ne gre za napačno obdelavo podatkov, temveč za potencialno dodatno delo lastnika področnega podatkovnega skladišča ISPAP.	Srednja, zaradi srednje verjetnosti	NIJZ bo morebitnim zanimanim posameznikom zagotovil informacije v skladu s podpoglavjem 3.2.2 »Preglednost in informiranje posameznika«.	Nizka
6.	Omejitev namena	Namen aplikacije #OstaniZdrav je sicer ponuditi dodaten pripomoček prebivalcem Republike Slovenije, vendar se aplikacijo začne uporabljati tudi za namene obvezne uporabe aplikacije	Majhna, saj ZZUOP izrecno predvideva, da za se za aplikacijo ne uporablja ZIUPDV. Tovrstno tveganje je majhne verjetnosti in je veljalo tudi za	Velika, obveznost uporabe aplikacije pomeni pomanjkanje pravne podlage za obdelavo podatkov. Pravna podlaga za obdelavo OP pa je	Visoka, zaradi velike resnosti	Skupna upravljavca bosta redno spremljala informacije v zvezi z morebitnimi kršitvami pravnih podlag in splošnih	Srednja, zaradi velike resnosti.

	A	B	C	Č	D	E	D
	Načelo/vsebin a	Tveganje	Verjetnost	Resnost	Raven tveganja	Ukrep	Raven tveganja po upoštevanju ukrepa
		ali za podatke o osebah, ki jih je bila određena karantena.	obdobje pred uveljavitvijo ZZUOOP. Poleg tega pa ni niti jasno, s strani koga bi se takšna obveznost vsiljevala. Gre za nejasnost, ki sta jo morala pred ZZUOOP skupna upravljavca redno pojasnjevati, istočasno pa so se vsi deležniki zavedali, da se je aplikacija uporablja na podlagi soglasja in ne na podlagi ZIUPDV, torej bi imeli posamezniki, ki bi bili izpostavljeni kakršnikoli prisili na voljo vsa pravna sredstva za to, da takšno prisilo preprečijo. Poleg tega pa je s tehničnega vidika relevantno tudi dejstvo, da splošni pogoji uporabe Google in Apple API- ja postavljajo omejitve za njihovo	največja kršitev varstva O.		določb aplikacije in ustrezno reagirala.	

	A	B	C	Č	D	E	D
	Načelo/vsebin a	Tveganje	Verjetnost	Resnost	Raven tveganja	Ukrep	Raven tveganja po upoštevanju ukrepa
			tovrstno uporabo, opisane v poglavju 3.1.1 Pravna podlaga in namen obdelave.				
7.	Točnost in ažurnost	Podatki, ki se bodo obdelovali v okviru aplikacije #OstaniZdrav, se bodo izkazali za netočne ali neažurne.	Majhna, saj bi morala predhodna testiranja odpraviti možnost netočnosti in neažurnosti, poleg tega je aplikacija že v uporabi tudi v drugih državah, kar pomeni, da so prve težave z morebitno netočnostjo in neažurnostjo verjetno že odpravljene.	Majhna, saj gre za pripomoček, v zvezi točnostjo pa se pričakuje, da bo odvisna od mnogih zunanjih dejavnikov iz okolice in se posledično od aplikacije #OstaniZdrav pričakuje nekoliko manjša točnost podatkov.	Nizka	Ob morebitnih sporočilih o netočnosti ali neažurnosti podatkov bosta NIJZ in MJU pristopila k dodatnim testiranjem.	Nizka
8.	Točnost	Napačni pozitivni zadetki povzročijo strah, tesnobo, (samo)izolacijo z možnimi posledicami na področju dela, šolanja ali drugega udejstvovanja, kar se lahko širi na njegove bližnje in na osebe, s katerimi je bil v stiku	Srednja, saj gre za potencialno resno okužbo	Srednja, saj lahko občutki tesnobe trajajo največ 14 dni od stika	Srednja	NIJZ pripravi ustrezna navodila o tem, kako ravnati v primeru, ko posameznik dobi informacijo o tem, da je bil v stiku z osebo, ki je sporočila, da je okužena. MJU redno spremlja ustreznost delovanja aplikacije testira in s tehničnega vidika ugotavlja njeno ustreznost ter sprejema morebitne ukrepe za izboljšave.	Nizka
9.	Točnost	Napačni pozitivni zadetki povzročijo povečan pritisk na zdravstveni sistem	Srednja, saj gre za potencialno resno okužbo	Srednja, saj so se v zadnjih mesecih postopki obravnave	Srednja	NIJZ pripravi ustrezna navodila o tem, kako ravnati v primeru, ko	Nizka

	A	B	C	Č	D	E	D
	Načelo/vsebin a	Tveganje	Verjetnost	Resnost	Raven tveganja	Ukrep	Raven tveganja po upoštevanju ukrepa
				potencialno okuženih izvajali v velikem obsegu in so se posledično pridobile številne izkušnje, ki postopke pohitrijo in racionalizirajo		posameznik dobi informacijo o tem, da je bil v stiku z osebo, ki je sporočila, da je okužena. MJU redno spremlja ustreznost delovanja aplikacije testira in s tehničnega vidika ugotavlja njeno ustreznost ter sprejema morebitne ukrepe za izboljšave.	
10.	Točnost	Napačni negativni zadetki povzročijo lažen občutek varnosti uporabnika aplikacije	Majhna, saj se bodo uporabniki zavedali, da uporaba aplikacije, ki ni obvezna za okužene, ne more zagotavljati varnosti	Majhna, saj je aplikacija le eden od načinov zagotavljanja varnosti posameznika	Nizka	NIJZ in MJU namenita posebno pozornost pri informiranju posameznikov o dejstvu, da aplikacija ni test okuženosti, temveč pripomoček za boj proti COVID-19. MJU redno spremlja ustreznost delovanja aplikacije testira in s tehničnega vidika ugotavlja njeno ustreznost ter sprejema morebitne ukrepe za izboljšave.	Nizka
11.	Omejitev shranjevanja	V okviru aplikacije #OstaniZdrav se ne bo zagotavljalo ustrezno brisanje podatkov.	Majhna, saj bi morale predhodne analize prenosa in obdelave podatkov odpraviti možnost neustrezne hrambe.	Velika, saj je časovno omejena obdelava podatkov eden osnovnih ukrepov za varstvo podatkov v primeru aplikacije #OstaniZdrav.	Visoka, zaradi velike resnosti	Vprašanje roka hrambe se obravna v okviru podpoglavja 3.1.6 Rok hrambe.	Srednja, zaradi velike resnosti

	A	B	C	Č	D	E	D
	Načelo/vsebin a	Tveganje	Verjetnost	Resnost	Raven tveganja	Ukrep	Raven tveganja po upoštevanju ukrepa
12.	Celovitost, zaupnost (informacijska varnost)	Pri zagotavljanju delovanja aplikacije #OstaniZdrav se ne zagotavlja ustrezna informacijska varnost.	Majhna, saj bo aplikacija #OstaniZdrav nameščena v okvir državnega računalniškega oblaka, ki deluje po uveljavljenih standardih za zagotavljanje informacijske varnosti.	Velika, morebitna neustrezna varnost bi na primer lahko pomenila posredovanje podatkov o stikih izven sistema. Kar bi pomenilo nezakonito obdelavo OP.	Visoka, zaradi velike resnosti	Na vprašanja o informacijski varnosti »3.1.7 Varnost podatkov v aplikaciji #OstaniZdrav in pogodbena obdelava«, »3.1.8 Sistemi za upravljanje varovanja informacij (SUVI)«, »3.1.10 Notranja sledljivost obdelave« in »3.1.11 Sledljivost posredovanja (zunanja sledljivost)«. Celotna koda slovenske različice aplikacije #OstaniZdrav bo objavljena.	Srednja, zaradi velike resnosti
13.	Celovitost, zaupnost (informacijska varnost via EFGS)	Pri zagotavljanju čezmejne izmenjave podatkov preko evropskega centralnega strežnika (EFGS) se ne zagotavlja ustrezna informacijska varnost	Majhna, saj EFGS zagotavlja Evropska komisija, ki deluje po zahtevah in uveljavljenih standardih za zagotavljanje informacijske varnosti	Velika, morebitna neustrezna varnost bi na primer lahko pomenila posredovanje podatkov o stikih izven sistema. Kar bi pomenilo nezakonito obdelavo OP.	Visoka, zaradi velike resnosti	Na vprašanja o informacijski varnosti »3.1.7 Varnost podatkov v aplikaciji #OstaniZdrav in pogodbena obdelava«, »3.1.8 Sistemi za upravljanje varovanja informacij (SUVI)«, »3.1.10 Notranja sledljivost obdelave« in »3.1.11 Sledljivost posredovanja (zunanja sledljivost)«.	Srednja, zaradi velike resnosti

	A	B	C	Č	D	E	D
	Načelo/vsebin a	Tveganje	Verjetnost	Resnost	Raven tveganja	Ukrep	Raven tveganja po upoštevanju ukrepa
14.	Celovitost, zaupnost (informacijska varnost) / razkritje	Pri zagotavljanju delovanja aplikacije #OstaniZdrav pride do razkritja identitete posameznika, na katerega se podatki nanašajo.	Srednja, saj če se, ne glede na to, da sama aplikacija #OstaniZdrav ne bo vsebovala podatkov, na podlagi katerih bi bilo mogoče razkriti posameznika, izkaže, da zaradi možnosti uporabe drugih, od aplikacije #OstaniZdrav neodvisnih, virov pride do določitve posameznika.	Velika, čeprav bi lahko do razkritja prišlo le z dodatnimi viri podatkov, bi takšna obdelava pomenila pomanjkanje pravne podlage za njeno obdelavo, pomanjkanje pravne podlage za obdelavo OP pa je največja kršitev varstva OP	Velika, zaradi velike resnosti	Celotna aplikacija #OstaniZdrav je pripravljena na način, da ima že v svojem bistvu tehnično ločene zbirke, v katerih se nahajajo podatki (lokalno o stikih, centralno o tem, katera koda je okužena), kot dodaten ukrep se zagotavlja na 15 minut zamenjana oddajna koda, ki se ustvari iz dnevnega ključa,, ki se zamenja enkrat dnevno, kar prepreči obdelavo podatkov o posamezniku, ki bi lahko povezovala večdnevne rutine s posameznikom.	Srednja, zaradi velike resnosti.
15.	Tveganje nezakonite obdelave – uporabe aplikacije za namene, ki niso vnaprej določeni	Uporaba aplikacije se začne pogovarjati pri vstopu v javne prostore, sredstva javnega obveščanja in druge lokacije, pri prehodu državnih meja	Srednja, ker prebivalci v zadnjih tednih iščejo različne načine, kako bi se zaščitili, enako pa poizkušajo tudi različne osebe iz javnega sektorja	Velika. S siljenjem posameznika k uporabi aplikacije bi šlo za nezakonit poseg v zasebnost posameznika tako z vidika pregleda telefona posameznika, ali ima aplikacijo sploh nameščeno, kot z vidika siljenja posameznika v obdelavo osebnih	Visoka	NIJZ in MJU objavita na svojih spletnih straneh informacijo o tem, da so tovrstna ravnanja nezakonit poseg v zasebnost in sproti spremljata morebitne prijave kršitev.	Srednja

	A	B	C	Č	D	E	D
	Načelo/vsebin a	Tveganje	Verjetnost	Resnost	Raven tveganja	Ukrep	Raven tveganja po upoštevanju ukrepa
				podatkov posebnih vrst brez soglasja.			
16.	Tveganje nezakonite obdelave – uporabe aplikacije za namene, ki niso vnaprej določeni	Uporaba aplikacije se začne pogojevati pri delodajalcih ali za vstop v druge prostore v zasebnem sektorju	Srednja, ker prebivalci v zadnjih tednih iščejo različne načine, kako bi se zaščitili	Velika. S siljenjem posameznika k uporabi aplikacije bi šlo za nezakonit poseg v zasebnost posameznika tako z vidika pregleda telefona posameznika, ali ima aplikacijo sploh nameščeno, kot z vidika siljenja posameznika v obdelavo osebnih podatkov posebnih vrst brez soglasja.	Visoka	NIJZ in MJU objavita na svojih spletnih straneh informacijo o tem, da so tovrstna ravnanja nezakonit poseg v zasebnost in sproti spremljata morebitne prijave kršitev.	Srednja
17.	Tveganje nezakonite obdelave	Operacijska sistema Android in iOS imata drugotne namene pri zbiranju podatkov	Majhna, ker imata opredeljene splošne pogoje, če bi šlo za njihovo kršitev pa gre za kršitev varstva osebnih podatkov	Srednja, saj bi šlo pri zbiranju podatkov o stikih posameznikov za podatke, ki jih do sedaj še nismo zbirali	Srednja	MJU spremlja informacije o morebitnih kršitvah obdelave podatkov s strani sistemov in če na kršitve ne more vplivati, aplikacijo ugasne.	Srednja zaradi problematičn osti pridobivanja podatkov o kršitvah.
18.	Zloraba	Pri uporabi teleTAN-a pride do zlorabe (zlonamerna uporaba telefona s prevzeto verifikacijsko kodo, posojanje telefona, namestitve kode na drug telefon,...)	Srednja	Majhna, ker mora biti posameznik, ki razpolaga s telefonom, na katerem je nameščena aplikacija, ki »nosi« okuženo kodo, tudi v bližini drugega	Srednja	NIJZ teleTAN sporoči po SMS osebi, ki je bila na testiranju in se je izkazalo, da je okužena, prav tako pa je teleTAN veljaven tri ure in ga je mogoče uporabiti le enkrat – to pomeni, da tveganj v zvezi z uporabo kode večkrat ni,	Nizka

	A	B	C	Č	D	E	D
	Načelo/vsebin a	Tveganje	Verjetnost	Resnost	Raven tveganja	Ukrep	Raven tveganja po upoštevanju ukrepa
				uporabnika in to vsaj 15 minut, kar pomeni, da je zloraba omejena že s samim dejstvom, da je vezana na fizični prostor in čas			
19.	Zloraba	TAN pridobi nepooblaščen oseba ali pa se izgubijo	Majhna, ker NIJZ generira vsak TAN posebej, nato pa ga po SMS sporoči okuženemu posamezniku, ki ga lahko le v roku treh ur vnese v telefon – v tem času pa je verjetnost za izgubo kode majhna	Majhna, ker je TAN veljaven le tri ure in ga je mogoče uporabiti le enkrat, torej bi v primeru kraje TAN, le-to lahko uporabil le en uporabnik.	Majhna	NIJZ TAN sporoči osebi po SMS, ki je bila na testiranju in se je izkazalo, da je okužena, prav tako pa je TAN veljaven tri ure in ga je mogoče uporabiti le enkrat – to pomeni, da tveganj v zvezi z uporabo TAN večkrat ni.	Nizka
20.	Pravice posameznika / pravica do izbrisa	Posameznik bo na upravljalca naslovil zahtevo za izbris svojih osebnih podatkov iz aplikacije #OstaniZdrav, na katero NIJZ ali MJU morda ne bosta ustrezno odgovorila v zakonskem roku. (V primeru uporabe aplikacije #OstaniZdrav gre za obdelavo, ki ne zahteva identifikacije posameznika, zato se načeloma pravice posameznika lahko ne zagotavljajo v skladu s členom 11 Splošne uredbe	Majhna, ker: - je pravna podlaga za zbiranje in obdelavo podatkov podatkovnega vira soglasje posameznika, prav tako pa tudi dejanje volje z namestitvijo s strani posameznika, ki jo bo posameznik lahko kadarkoli preklical z izbrisanjem aplikacije z mobilnega telefona;	Srednja. Po eni strani gre lahko v primeru zamude ali napačnega ravnjanja upravljalca za kršitev pravic posameznika in s tem Splošne uredbe o varstvu podatkov, po drugi strani pa tudi, če organ ne bi odgovoril posamezniku, ima ta zagotovljeno pravno varnost	Srednja	Pred začetkom vzpostavitve delovanja aplikacije #OstaniZdrav bodo na spletni strani NIJZ in MJU objavljene informacije o tem, katere pravice lahko posameznik izvršuje. Prav tako bosta skupna upravljavca zagotovila vzpostavitev kontaktnega centra za posredovanje informacij posameznikom, ki bo razpolagal z osnovnimi informacijami z vidika varstva osebnih podatkov.	Nizka

	A	B	C	Č	D	E	D
	Načelo/vsebin a	Tveganje	Verjetnost	Resnost	Raven tveganja	Ukrep	Raven tveganja po upoštevanju ukrepa
		o varstvu podatkov, torej se v okviru tega tveganja obravnava le neustrezno ravnanje organa.)	- je rok za hrambo podatkov izredno kratek – 14 dni in se bo torej volja posameznika za izbris podatkov po tem času zgodila že avtomatizirano.	preko možnosti vložitve pritožbe na nadzorni organ za varstvo osebnih podatkov.			
21.	Pravice posameznika / pravica do ugovora	Posameznik bo na upravljavca naslovil ugovor za obdelavo osebnih podatkov, ki se obdelujejo v aplikaciji #OstaniZdrav, na katero NIJZ ali MJU morda ne bosta ustrezno odgovorila v zakonskem roku.	Srednja, ker: - je pravna podlaga za zbiranje in obdelavo podatkov javni interes, prav tako pa tudi dejanje volje z namestitvijo s strani posameznika, ki jo bo posameznik lahko kadarkoli preklical z izbrisom aplikacije z mobilnega telefona.	Srednja. Po eni strani gre lahko v primeru zamude ali napačnega ravnanja upravljavca za kršitev pravic posameznika in s tem Splošne uredbe o varstvu podatkov, po drugi strani pa tudi, če organ ne bi odgovoril posamezniku, ima ta zagotovljeno pravno varnost preko možnosti vložitve pritožbe na nadzorni organ za varstvo osebnih podatkov.	Srednja	Pred začetkom vzpostavitve delovanja aplikacije #OstaniZdrav bodo na spletni strani NIJZ in MJU objavljene informacije o tem, katere pravice lahko posameznik izvršuje. Prav tako bosta skupna upravljavca zagotovila vzpostavitev kontaktnega centra za posredovanje informacij posameznikom, ki bo razpolagal z osnovnimi informacijami z vidika varstva osebnih podatkov.	Nizka
22.	Pravice posameznika / pravica do popravka	Posameznik bo na upravljavca naslovil zahtevo za popravek osebnih podatkov, ki se obdelujejo v aplikaciji #OstaniZdrav, na	Majhna, ker se podatki zbirajo avtomatizirano in je pri obdelavi podatkov popolnoma izključen	Srednja. Po eni strani gre lahko v primeru zamude ali napačnega ravnanja	Srednja	Pred začetkom vzpostavitve delovanja aplikacije #OstaniZdrav bodo na spletni strani NIJZ	Nizka

	A	B	C	Č	D	E	D
	Načelo/vsebin a	Tveganje	Verjetnost	Resnost	Raven tveganja	Ukrep	Raven tveganja po upoštevanju ukrepa
		katero NIJZ ali MJU morda ne bosta ustrezno odgovorila v zakonskem roku.	človeški faktor, ki običajno pomeni največji dejavnik tveganja, torej bi morala biti organa sposobna ustrezno reagirati na zahtevek.	upravljavca za kršitev pravic posameznika in s tem Splošne uredbe o varstvu podatkov, po drugi strani pa tudi, če organ ne bi odgovoril posamezniku, ima ta zagotovljeno pravno varnost preko možnosti vložitve pritožbe na nadzorni organ za varstvo osebnih podatkov.		in MJU objavljene informacije o tem, katere pravice lahko posameznik izvršuje. Prav tako bosta skupna upravljavca zagotovila vzpostavitev kontaktnega centra za posredovanje informacij posameznikom, ki bo razpolagal z osnovnimi informacijami z vidika varstva osebnih podatkov. Ob morebitnih sporočilih o netočnosti ali neažurnosti podatkov pa bosta NIJZ in MJU pristopila k dodatnim testiranjem.	
23.	Pravice posameznika / uveljavljanje pravic	Posameznik na upravljavca naslovi zahtevo za uveljavljanje pravic posameznika, pri čemer NIJZ ali MJU morda ne bosta odreagira ustrezno.	Majhna, ker je glavnina pravic posameznika v konkretnem primeru skoncentrirana na pravicah do informiranosti in seznanjenosti, kar se v konkretnem primeru zagotavlja preko spletne strani MJU.	Srednja. Po eni strani gre lahko v primeru zamude ali napačnega ravnanja upravljavca za kršitev pravic posameznika in s tem Splošne uredbe o varstvu podatkov, po drugi strani pa tudi, če organ ne bi odgovoril posamezniku, ima ta zagotovljeno	Srednja	Pred začetkom vzpostavitve delovanja aplikacije #OstaniZdrav bodo na spletni strani NIJZ in MJU objavljene informacije o tem, katere pravice lahko posameznik izvršuje. Prav tako bosta skupna upravljavca zagotovila vzpostavitev kontaktnega centra za posredovanje informacij posameznikom, ki bo razpolagal z osnovnimi	Nizka

	A	B	C	Č	D	E	D
	Načelo/vsebin a	Tveganje	Verjetnost	Resnost	Raven tveganja	Ukrep	Raven tveganja po upoštevanju ukrepa
				pravno varnost preko možnosti vložitve pritožbe na nadzorni organ za varstvo osebnih podatkov.		informacijami z vidika varstva osebnih podatkov. NIJZ in MJU izdelata pričujočo oceno učinkov v zvezi z varstvom osebnih podatkov, ki jo predložita Informacijskemu pooblaščenцу, ki mu predlaga predhodno posvetovanje (člen 36 Splošne uredbe o varstvu podatkov).	
24.	Pravice posameznika / pravica do seznanitve	Posameznik bo na upravljavca naslovil zahtevo za seznanitev z osebnimi podatki, ki se obdelujejo v aplikaciji #OstaniZdrav, na katero NIJZ ali MJU morda ne bosta ustrezno odgovorila v zakonskem roku. (V primeru uporabe aplikacije #OstaniZdrav gre za obdelavo, ki ne zahteva identifikacije posameznika, zato se načeloma pravice posameznika lahko ne zagotavljajo v skladu s členom 11 Splošne uredbe o varstvu podatkov, torej se v okviru tega tveganja obravnavajo le neustrezno ravnanje organa.)	Majhna, ker: - se bodo podatki na lokalni namestitvi na posameznikovem mobilnem telefonu, obdelovali le, če bo imel posameznik aplikacijo nameščeno in - se bodo v centralnem strežniku zbirali le podatki, da je posameznik, ki si je aplikacijo namestil, okužen. Torej se bodo podatki obdelovali le z izrecno voljo (ne le soglasjem) posameznika.	Srednja. Po eni strani gre lahko v primeru zamude ali napačnega ravnjanja upravljavca za kršitev pravic posameznika in s tem Splošne uredbe o varstvu podatkov, po drugi strani pa tudi, če organ ne bi odgovoril posamezniku, ima ta zagotovljeno pravno varnost preko možnosti vložitve pritožbe na nadzorni organ za varstvo osebnih podatkov.	Srednja	Pred začetkom vzpostavitve delovanja aplikacije #OstaniZdrav bodo na spletni strani NIJZ in MJU objavljene informacije o tem, katere pravice lahko posameznik izvršuje. Prav tako bosta skupna upravljavca zagotovila vzpostavitev kontaktnega centra za posredovanje informacij posameznikom, ki bo razpolagal z osnovnimi informacijami z vidika varstva osebnih podatkov.	Nizka

	A	B	C	Č	D	E	D
	Načelo/vsebin a	Tveganje	Verjetnost	Resnost	Raven tveganja	Ukrep	Raven tveganja po upoštevanju ukrepa
25.	Pravice posameznika / pravica do omejitve obdelave	Posameznik bo na upravljavca naslovil ugovor za omejitev obdelave osebnih podatkov, ki se obdelujejo v aplikaciji #OstaniZdrav, na katero NIJZ ali MJU morda ne bosta v zakonskem roku ali izvedel ustreznih ukrepov. (V primeru uporabe aplikacije #OstaniZdrav gre za obdelavo, ki ne zahteva identifikacije posameznika, zato se načeloma pravice posameznika lahko ne zagotavljajo v skladu s členom 11 Splošne uredbe o varstvu podatkov, torej se v okviru tega tveganja obravnava le neustrezno ravnanje organa.)	Majhna, ker: - se bodo podatki na lokalni namestitvi na posameznikovem mobilnem telefonu, obdelovali le, če bo imel posameznik aplikacijo nameščeno in - se bodo v centralnem strežniku zbirali le podatki, da je posameznik, ki si je aplikacijo namestil, okužen. Torej se bodo podatki obdelovali le z izrecno voljo (ne le soglasjem) posameznika.	Srednja. Po eni strani gre lahko v primeru zamude ali napačnega ravnanja upravljavca za kršitev pravic posameznika in s tem Splošne uredbe o varstvu podatkov, po drugi strani pa tudi, če organ ne bi odgovoril posamezniku, ima ta zagotovljeno pravno varnost preko možnosti vložitve pritožbe na nadzorni organ za varstvo osebnih podatkov.	Srednja	Pred začetkom vzpostavitve delovanja aplikacije #OstaniZdrav bodo na spletni strani NIJZ in MJU objavljene informacije o tem, katere pravice lahko posameznik izvršuje. Prav tako bosta skupna upravljavca zagotovila vzpostavitev kontaktnega centra za posredovanje informacij posameznikom, ki bo razpolagal z osnovnimi informacijami z vidika varstva osebnih podatkov.	Nizka
26.	Zakonitost / pogodbeni obdelava	V obdelavo bo vključen zunanji izvajalec, ki ne bo identificiran kot (pogodbeni) obdelovalec	Majhna, ker ima MJU že v postopku priprave pogodb pripravljene splošne člene, ki se nanašajo na pogodbeno obdelavo osebnih podatkov, ki jih nato vsaka posamezna komisija za izvedbo javnega naročila uredi glede na konkretno vsebino.	Srednja, saj bi pomanjkanje identifikacije izvajalca kot pogodbenega obdelovalca lahko pomenilo tudi morebitno odsotnost pravne podlage za obdelavo OP	Srednja, zaradi velike resnosti	Glede na to, da ima MJU že v postopku priprave pogodb pripravljene splošne člene, ki se nanašajo na pogodbeno obdelavo osebnih podatkov, ki jih nato vsaka posamezna komisija za izvedbo javnega naročila uredi glede na konkretno vsebino, ocenjujemo, da dodaten ukrep ni potreben.	Srednja, zaradi velike resnosti

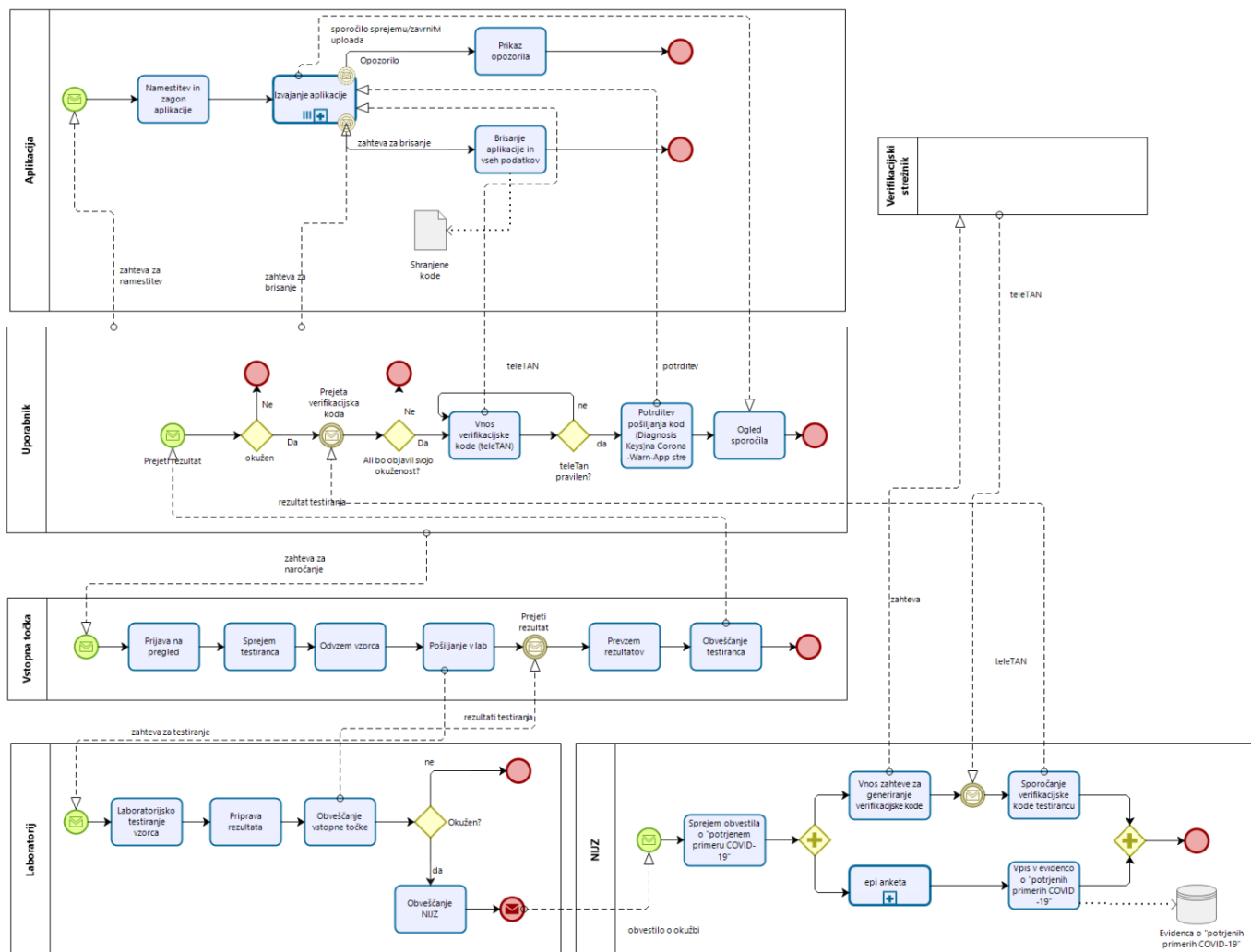
	A	B	C	Č	D	E	D
	Načelo/vsebin a	Tveganje	Verjetnost	Resnost	Raven tveganja	Ukrep	Raven tveganja po upoštevanju ukrepa
			Vsako pogodbo pred njenim podpisom pregleda tudi odgovorna oseba za varstvo osebnih podatkov na MJU.				
27.	Odgovornost / pogodbena obdelava	(Pogodbeni) obdelovalec bo imel podlago za obdelavo OP v pogodbi, ki ne bo vsebovala vseh elementov, kot jih zahteva člen 28 Splošne uredbe o varstvu podatkov	Majhna, ker ima MJU predvideno, da vsako pogodbo, v okviru katere se določa obdelava OP, pred njenim podpisom pregleda tudi odgovorna oseba za varstvo osebnih podatkov na MJU.	Majhna, saj morebitno pomanjkanje vsebine lahko pogodbeni stranki nadoknadi tudi med izvajanjem pogodbe	Nizka	Glede na to, da ima MJU predvideno, da vsako pogodbo, v okviru katere se določa obdelava OP, pred njenim podpisom pregleda tudi odgovorna oseba za varstvo osebnih podatkov na MJU, ocenjujemo, da dodaten ukrep ni potreben.	Nizka
28.	Odgovornost / vgrajeno in privzeto varstvo podatkov	Zahteva Splošne uredbe o varstvu podatkov ni ustrezno izpolnjena	Majhna, ker je varstvo podatkov osnova za zagotavljanje aplikacije #OstaniZdrav	Velika, ker gre za nov nabor podatkov, ki se do sedaj še ni obdeloval	Visoka, zaradi velike resnosti	NIJZ in MJU sta veliko pozornost namenila varstvu osebnih podatkov že pri izbiri aplikacije za beleženje stikov, prav tako pa ugotavljata s tega vidika ustreznost aplikacije – ukrep se je izvedel v času pred pripravo ocene učinkov	Nizka
29.	Odgovornost / skupni upravljavci	Zahteva Splošne uredbe o varstvu podatkov ni ustrezno izpolnjena	Majhna, ker je MJU že v okviru pričujoče ocene učinkov ugotovil potrebo po dogovoru o skupnem upravljanju, z vidika vsebine pa ima MJU predvideno, da vsako	Majhna, saj imata oba skupna upravljavca podlago za obdelavo podatkov, z vidika vsebine pa morebitno pomanjkanje	Nizka	Dodaten ukrep ni potreben	Nizka

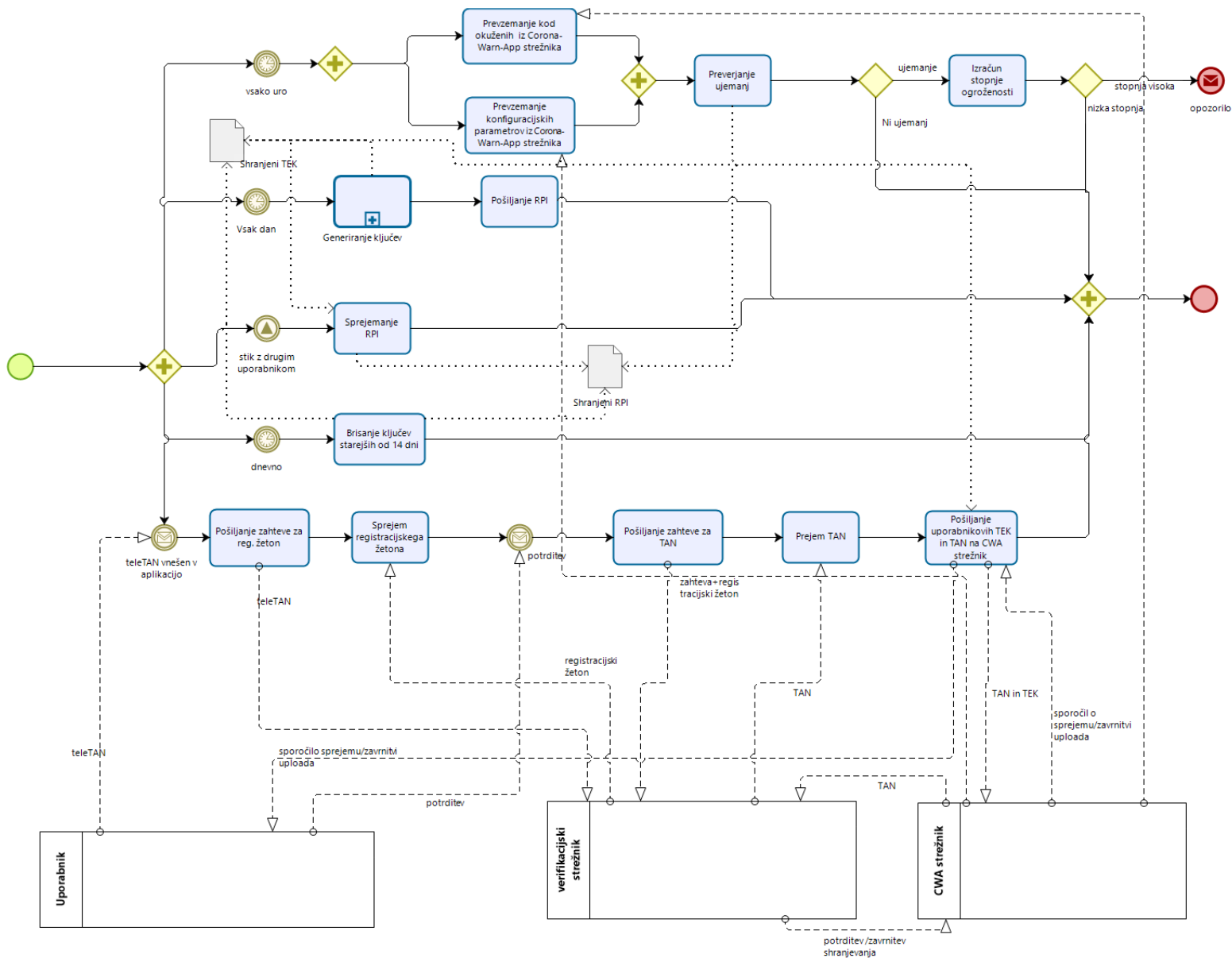
	A	B	C	Č	D	E	D
	Načelo/vsebin a	Tveganje	Verjetnost	Resnost	Raven tveganja	Ukrep	Raven tveganja po upoštevanju ukrepa
			pogodbo, v okviru katere se določa obdelava OP, pred njenim podpisom pregleda tudi odgovorna oseba za varstvo osebnih podatkov na MJU.	vsebine lahko skupna upravljavca nadoknadi tudi med izvajanjem pogodbe			
30.	Odgovornost / skupni upravljavci (čezmejna izmenjava podatkov)	Zahteva Splošne uredbe o varstvu podatkov ni ustrezno izpolnjena	Majhna, ker morajo upravljavci skladno s Sklepom Evropske komisije in 26. členom Splošne uredbe o varstvu podatkov na pregleden način določiti dolžnosti z namenom izpolnjevanja obveznosti v skladu z navedeno uredbo. Poleg tega je določena tudi možnost, da se navedene dolžnosti določijo s pravom EU ali pravom države članice, ki veljajo za upravljavca.	Majhna, ker mora vsak posamezni upravljavec zagotoviti, da ima na nacionalni ravni podlago za obdelavo na združevalni prehod via evropskega centralnega strežnika. Izpolnjevanje pogojev pa preverja Evropska komisija.	Nizka	Dodaten ukrep ni potreben	Nizka
31.	Odgovornost / evidenca dejavnosti obdelave	Zahteva Splošne uredbe o varstvu podatkov ni ustrezno izpolnjena	Majhna, ker imata NIJZ in MJU v svoje delovne procese vgrajeno pripravo	Majhna, saj so vsi vidiki evidence dejavnosti obdelavo obdelani v okviru pričujoče ocene	Nizka	Dodaten ukrep ni potreben	Nizka

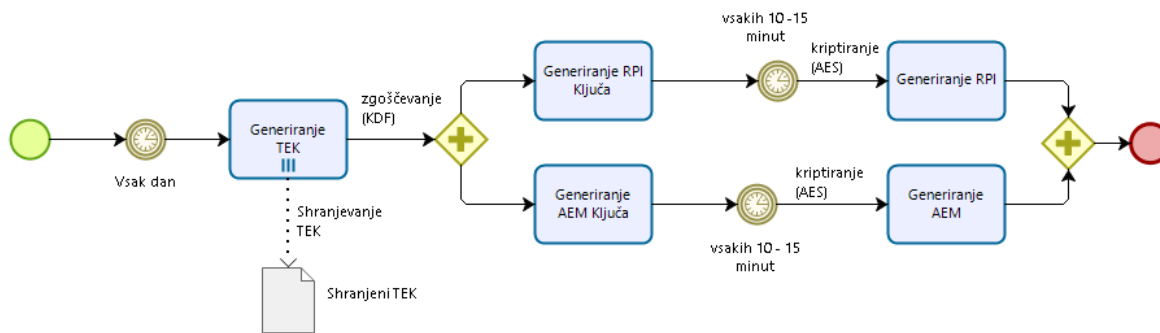
	A	B	C	Č	D	E	D
	Načelo/vsebin a	Tveganje	Verjetnost	Resnost	Raven tveganja	Ukrep	Raven tveganja po upoštevanju ukrepa
			evidence dejavnosti obdelave.	učinkov, torej sta skupna upravljavca domislila vse vidika varstva podatkov, ki jih lahko naslavlja evidenca dejavnosti obdelave. Prav tako pa je pravna podlaga za aplikacijo soglasje, ki pa ga v izvedbi aplikacije posameznik izvede po tem, ko prebere opozorilo v zvezi z varstvom podatkov, torej je posameznik seznanjen, NIJZ in MJU pa lahko evidenco pripravita tudi naknadno.			
32.	Odgovornost / varnostni ukrepi	Zahteva Splošne uredbe o varstvu podatkov ni ustrezno izpolnjena	Majhna, saj so organizacijski varnostni ukrepi domišljeni v okviru pričujoče ocene učinkov, tehnični pa so predmet celotne DRO infrastrukture, ki ima vzpostavljen sistem upravljanja varovanja informacij skladno z internimi akti.	Velika, ker je varnost informacijskega sistema, v okviru katerega se obdelujejo osebni podatki, najpomembnejši vidik, v primeru zlorab pa kršenje človekove pravice	Visoka, zaradi velike resnosti	Ukrepi so bili izvršeni že pred pripravo ocene učinkov, saj z njihovo pomočjo deluje celoten DRO, ki ima vzpostavljen sistem upravljanja varovanja informacij skladno z internimi akti. Obenem je MJU pridobil certifikat ISO27001 za DRO.	Nizka

	A	B	C	Č	D	E	D
	Načelo/vsebin a	Tveganje	Verjetnost	Resnost	Raven tveganja	Ukrep	Raven tveganja po upoštevanju ukrepa
33.	Odgovornost / obveščanje o varnostnih incidentih	Zahteva Splošne uredbe o varstvu podatkov ni ustrezno izpolnjena	Majhna, saj se obveščanje o incidentih del rednega postopka pri delovanju aplikacij na infrastrukturi DRO.	Velika, saj bi v primeru neustreznega obveščanja o varnostnih incidentih prišlo do večje zlorabe osebnih podatkov	Visoka, zaradi velike resnosti	Ukrepi so bili izvršeni že pred pripravo ocene učinkov, saj ima celoten DRO vzpostavljene ustrezne sisteme obveščanja o varnostnih incidentih.	Nizka
34.	Odgovornost / ocena učinkov in predhodno posvetovanje	Zahteva Splošne uredbe o varstvu podatkov ni ustrezno izpolnjena	Majhna, saj je določanje tveganj in ukrepov za njihovo odpravo del ocene učinkov, njeno usklajevanje pa je načrtovano in se v času priprave popravljenе verzije že izvaja	Velika, saj bi se brez ustrezne ocene učinkov lahko spregledalo kakšnega od pomembnih vidikov varstva osebnih podatkov	Visoka, zaradi velike resnosti	Ukrepi se izvajajo v okviru postopka analize tveganj in predlaganja ukrepov za njihovo odpravo	Nizka
35.	Odgovornost / pooblaščen osebe za varstvo podatkov	Zahteva Splošne uredbe o varstvu podatkov ni ustrezno izpolnjena	Nizka, saj so pooblaščen osebe za varstvo podatkov določene v oceni učinkov	Velika, saj so to osebe, ki imajo v zvezi z varstvom osebnih podatkov največ znanja in lahko zelo pripomorejo pri načrtovanju obdelave osebnih podatkov	Visoka, zaradi velike resnosti	Ukrepi se izvajajo v okviru postopka priprave ocene učinkov.	Nizka

6 Priloga 2: Postopki prenosa podatkov med lokalno namestitvijo aplikacije na mobilni telefon in centralno zbirko







Powered by
bizagi
 Modeler

7 Priloga 3: Postopek generiranja in uporabe kode za potrditev statusa okuženosti na strežniku CWA

