REPUBLIKA SLOVENIJA
INFORMACIJSKI POOBLAŠČENEC
Dunajska cesta 22, 1000 Ljubljana
T: 01 230 9730
F: 01 230 9778
gp.ip@ip-rs.si
www.ip-rs.si

Številka: 007-24/2020
Datum: 1. 7. 2020

Kolegij predsednika Državnega zbora RS
Vse poslanske skupine
Gp@dz-rs.si

ZADEVA: Predlog Zakona o interventnih ukrepih za pripravo na drugi val COVID-19 – EVA 2020-2611-0033 - MNENJE

Spoštovani,

Informacijski pooblaščenec (IP) se je včeraj seznanil s predlogom Zakona o interventnih ukrepih za pripravo na drugi val COVID-19[1], katerega poglavitne rešitve se po navedbah predlagatelja nanašajo na: podaljšanje ukrepa čakanja na delo, določitev in plačilo nadomestila za odrejeno karanteno, ukrepe s področja institucionalnega varstva po Zakonu o socialnem varstvu in na mobilno aplikacijo za obveščanje o stikih z okuženimi.

Uvodoma poudarjamo, da se predlagatelj zakona v zvezi s predlaganimi rešitvami z Informacijskim pooblaščencem ni predhodno posvetoval, kljub temu, da gre za zelo občutljivo materijo z vidika varovanja temeljne pravice posameznikov do varstva osebnih podatkov in zasebnosti. Do včerajšnjega dne Informacijski pooblaščenec in javnost nista imela dostopa do predloga zakona, kljub temu, da naj bi bil, glede na sporočila za javnost predlagatelja, usklajen že 24. 6. 2020. Tematika, ki naj bi jo zakon urejal, zahteva dosledno spoštovanje standardov odločanja v demokratični družbi, predvsem transparentnosti zakonodajnih predlogov, ki omogoča, da zainteresirana javnost lahko na predloge zakonodaje poda pripombe in se odpre javna diskusija glede problematike.

V nadaljevanju podajamo podrobnejše mnenje glede določbe 24. člena, ki se nanaša na obdelavo identifikacijskih osebnih podatkov, na določbe 26. do 34. člena, ki se nanašajo na mobilno aplikacijo za obveščanje o stikih z okuženimi z virusom SARS-CoV-2 in osebami, ki jim je bila odrejena karantena ter na kazensko določbo 48. člena.

K 24. členu - Obdelava osebnih podatkov (obdelava identifikacijskih osebnih podatkov)

> *Če je obdelava identifikacijskih osebnih podatkov ter tudi lokacijskih osebnih podatkov s področja elektronskih komunikacij, ki se nanašajo na določenega posameznika, nujno potrebna za varovanje življenja, telesa ali zdravja ljudi, se lahko ti podatki začasno obdelujejo ne glede na to, da za obdelavo njegovih osebnih podatkov ni druge zakonite pravne podlage, vendar le za obdobje, ko je temu posamezniku posamično in začasno omejena osebna svoboda zaradi ukrepov, sprejetih na podlagi zakona, ki ureja nalezljive bolezni.*

Določba glede obdelave identifikacijskih podatkov ter lokacijskih podatkov posameznika s področja elektronskih komunikacij vzpostavlja novo podlago za pridobivanje in uporabo teh podatkov o osebah, ki jim je posamično in začasno omejena osebna svoboda zaradi ukrepov, sprejetih na podlagi zakona, ki ureja nalezljive bolezni (npr. osebe, ki so v karanteni). Informacijski pooblaščenec je nad to določbo izjemno zaskrbljen, saj jo gre brati v smislu pooblastila,

- da lahko nedoločen nabor organov za namen nadzora nad upoštevanjem karantene ali samoizolacije posameznika

[1] https://www.dz-rs.si/wps/portal/Home/deloDZ/zakonodaja/izbranZakonAkt?uid=45A8E2E6C3172A27C125853B0024B1F3&db=pre_zak&mandat=VIII&tip=doc

- od nedoločenega nabora virov podatkov, t. j. različnih ponudnikov s področja elektronskih komunikacij pridobiva
- nedoločen nabor identifikacijskih podatkov in podatkov o lokaciji te osebe, t. j. o lokaciji njenega telefona ali druge naprave.

Področje elektronskih komunikacij je široko in lahko vključuje tako operaterje elektronskih komunikacij kot tudi ponudnike drugih storitev informacijske družbe (npr. različne aplikacije ali druge storitve, ki beležijo lokacije posameznika, kot so nosljive pametne naprave, pametni avtomobili, druge pametne naprave). Vsi tovrstni ponudniki obdelujejo širok krog podatkov o posamezniku, ki bi jih lahko šteli za identifikacijske podatke, najpogosteje beležijo tudi podatke o lokaciji. Delovanje operaterjev elektronskih komunikacij primarno ureja Zakon o elektronskih komunikacijah (Uradni list RS, št. 109/12, 110/13, 40/14 – ZIN-B, 54/14 – odl. US, 81/15 in 40/17, v nadaljevanju ZEKom-1) in predpisuje natančne pogoje, kdaj in komu smejo razkriti identifikacijske ali lokacijske podatke o svojih uporabnikih in naročnikih, med drugim organom pregona, glede na pooblastila iz 149b. člena Zakona o kazenskem postopku (Uradni list RS, št. 32/12, s spremembami in dopolnitvami; ZKP). V primeru podatkov o prometu, katerega del so lahko podatki o lokaciji naprave, se podatki posredujejo le na podlagi sodne odredbe. Ostali ponudniki storitev elektronske družbe, ki zbirajo in beležijo podatke o identifikaciji in lokaciji uporabnika, morajo za to imeti eno od pravnih podlag iz 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 razveljavitvi Direktive 95/46/ES (v nadaljevanju: Splošna uredba) ter upoštevati določbe 157. člena ZEkom-1. Za posredovanje takih podatkov npr. organom za nadzor nad ukrepi po zakonu, ki ureja nalezljive bolezni, pa mora obstajati izrecna pravna podlaga, skladno s 3. odstavkom člena 6 Splošne uredbe.

Pooblastilo, kot ga želi uvesti 24. člen predloga zakona nedvomno pomeni velik poseg v številne ustavno zagotovljene pravice posameznika, pri čemer je utemeljenost, sorazmernost in nujnost takega posega v konkretni situaciji omejevanja širjenja COVID-19 zelo vprašljiva. Krog subjektov, kateremu določba dopušča obdelavo identifikacijskih podatkov in podatkov o lokaciji ni zamejen, brati ga je mogoče tako v smislu,

- da vsem zgoraj navedenim ponudnikom storitev elektronskih komunikacij nudi dodatno pravno podlago, da zbirajo in obdelujejo identifikacijske podatke in podatke o lokacijah, kljub temu, da za to ni druge podlage, da npr. nimajo privolitve posameznika za sledenje njegovi lokaciji, kot jo za predpisuje ZEKom-1 oz. pravnih podlag iz Splošne uredbe. Taka določba izprazni varstvo, kot ga posameznikom zagotavljata Splošna uredba in ZEKom-1, po katerih je privolitev posameznika v zbiranje lokacijskih podatkov eden od standardov varovanja pravic.

- da nedoločenemu naboru organov za namen nadzora nad ukrepi, izrečenimi po zakonu, ki ureja nalezljive bolezni, daje dodatno podlago za pridobivanje teh podatkov od ponudnikov elektronskih komunikacij in za nadaljnjo obdelavo teh podatkov. Še posebej je tako pooblastilo nedoločenim organom zaskrbljujoče ob javnih navedbah, da bo pri nadzoru karantene sodelovala tudi policija.

  Organi pregona lahko po veljavnih pravilih podatek o lokaciji posameznika od operaterja elektronskih komunikacij ali drugega ponudnika pridobijo le ob upoštevanju pogojev kazenske procesne zakonodaje (če je lokacija del podatkov o prometu, z odredbo sodišča). V tem kontekstu je nedopustno, da se za pridobivanje enakega podatka izven namenov pregona kaznivih dejanj, t. j. npr. za namen nadzora nad karanteno posameznika ustvarja nižji standard za pridobivanje podatkov, brez varoval za pravice posameznika in brez upoštevanja, da je v določenih primerih za pridobivanja podatka o lokaciji posameznika od operaterja potrebna odredba sodišča. Tak nižji standard lahko pomeni tudi pot za obvod strožjih določb za pridobivanje podatkov o lokaciji posameznika, ki jih morajo upoštevati organi pregona.

- da omogoča dodatno pravno podlago za zbiranje podatkov o lokacijah uporabnikov predlagane aplikacije za slednje stikov iz poglavja 4 predloga zakona, kljub temu, da 30. člen predloga zakona pravi, da aplikacija ne sme pa omogočati identifikacije uporabnika, zbiranja podatkov o njegovi lokaciji in njegovih drugih osebnih podatkov. Informacijski pooblaščenec opozarja, da bi taka pravna podlaga pomenila možnost nadzora lokacije okuženih in tistih, za katere velja ukrep glede na zakon, ki ureja nalezljive bolezni, še posebej, če bi bila raba aplikacije zanje obvezna, kot to predvideva 2. odstavek 29. člena predloga zakona. Glede

take možnosti nadzora smo negativno mnenje podali že ob uvajanju te tematike v 104. členu prvega interventnega zakona v času COVID-19 ukrepov[2].

Določba 24. člena je tako po našem mnenju izrazito sporna z vidika varovanja temeljne pravice do varstva osebnih podatkov iz 38. člena Ustave RS, saj podaja blanketno pooblastilo ne-zamejenemu krogu subjektov, da lahko obdelujejo podatke o identifikaciji in lokaciji posameznikov, če je to povezano z ukrepom po zakonu, ki ureja nalezljive bolezni. Informacijski pooblaščenec poudarja, da tak ukrep v času poletnih počitnic in pogostih prehodov meje v sosednje države z manj ugodno epidemiološko sliko lahko zadeva potencialno veliko število posameznikov, državljanov Slovenije, katerih podatke o lokaciji bi bilo mogoče spremljati.

Določba je v nasprotju in nejasni relaciji z določbami Splošne uredbe o varstvu podatkov in ZEKom-1 ter nedopustno niža standarde za pridobivanje podatka o lokaciji posameznika za namen nadzora nad ukrepi, izrečenimi po zakonu, ki ureja nalezljive bolezni (ki naj bi ga izvajala tudi policija, ne le zdravstveni organi), celo pod standard, ki velja za pridobivanje enakovrstnega podatka v kazenskem postopku, brez varoval za pravice posameznika in brez upoštevanja, da je običajno za pridobivanje podatka o lokaciji posameznika iz elektronskih komunikacij potrebna odredba sodišča. Tak nižji standard lahko pomeni tudi pot za obvod strožjih določb za pridobivanje podatkov o lokaciji posameznika, ki jih morajo upoštevati organi pregona.

V zvezi s posegom v ustavne pravice posameznika in obdelavo podatkov o lokaciji njihovih naprav smo, kot navedeno, podali svoje negativno mnenje že ob prvem interventnem zakonu v času COVID-19 ukrepov, negativno se je do tega izrazila tudi Zakonodajnopravna služba Državnega zbora, za katero verjamemo, da bo pozorno pretehtala tudi rešitve, predvidene v tem predlogu in opozorila na morebitna neskladja z Ustavo RS. Sporni 104. člen v DZ posledično ni bil sprejet. **Zaradi navedenega IP predlaga Državnemu zboru RS, da člena ne podpre.** Če je urejanje obdelave identifikacijskih podatkov in podatkov o lokaciji nujno in sorazmerno z vidika ciljev omejevanja širjenja virusa, ki jih zakonodajalec zasleduje, pa naj materijo uredi v okviru ustavno dopustnih mej in standardov, ki za obdelavo tovrstnih podatkov že veljajo v okviru drugih postopkov nadzora in pregona. Določba je nejasna in ne dosega ravni *lex certa*, ki bi bil za take posege v osebne podatke posameznikov nujen, še posebej ob upoštevanju, da so ti podatki vezani na občutljive osebne podatke posameznika, ki je mu je zaradi zdravstvenih razlogov omejeno svobodno gibanje.

K 26. do 34. členu ter 48. členu

Ker nam niso znane podrobnosti delovanja in tehnične zasnove aplikacije, na katero se zakon nanaša, Informacijski pooblaščenec ne more podati celovitega mnenja. Zato na tej točki predvsem znova opozarjamo na nekaj ključnih točk v zvezi z aplikacijami za sledenje stikov iz naših mnenj[3], iz mnenja Evropskega odbora za varstvo podatkov[4], stališč, ki jih je poudarila Evropska komisija v svojem okviru orodij za razvoj aplikacij[5] in stališč Sveta Evrope[6]

1. Glede obdelave osebnih podatkov oziroma anonimnih podatkov

Aplikacije za sledenje kontaktov nedvomno pomenijo obdelavo osebnih podatkov državljanov, količina in narava osebnih podatkov, ki se obdelujejo, pa je odvisna od tehnične izvedbe (npr. ime, priimek, telefonska številka, drugi identifikatorji terminalne opreme, lokacija, ipd.) ter občutljivih podatkov o zdravstvenem stanju, izrečenem ukrepu za izolacijo/karanteno, ipd., zato je nujno upoštevanje določb Splošne uredbe ter ZVOP-1, ki predpisujeta pogoje za zakonito obdelavo tovrstnih osebnih podatkov ter obveznosti upravljavca osebnih podatkov in drugih subjektov.

Četudi aplikacija obdeluje le podatke o stikih, bližini oseb, in ti podatki uporabnikom ne bi bili razkriti na način, da bi določena oseba izvedela, s kom natanko je bila v rizičnem stiku, **to ne pomeni, da gre**

[2] https://www.ip-rs.si/fileadmin/user_upload/Pdf/pripombe/2020/DZ_interventni_zakon_MNENJE_30032020_koncno.pdf
[3] https://www.ip-rs.si/vop/?tx_jzgdprdecisions_pi1[showUid]=1504
[4] https://www.ip-rs.si/fileadmin/user_upload/Pdf/Covid19/EDPB_Guidelines_04_2020_novicka_za_objavo_na_spletni_strani.pdf
[5] https://eur-lex.europa.eu/eli/reco/2020/518/oj
[6] https://rm.coe.int/covid19-joint-statement-28-april/16809e3fd7

za anonimne podatke. Podatek o imenu in priimku osebe – uporabnika – le nadomešča neki drugi identifikator (npr. številka), po katerem ga sicer ni mogoče enostavno prepoznati, vendar so podatki o stikih kljub temu osebni podatki in varovani po zakonu in Ustavi RS. Četudi je zagotovljeno, da en uporabnik drugega ne more prepoznati preko obvestil o rizičnih stikih, v sami aplikaciji in na uporabnikovem telefonu ter (odvisno od načina izvedbe) tudi na nekem centralnem mestu, pod nadzorom upravljavca aplikacije ali drugih subjektov, ki imajo dostope, nedvomno nastaja zbirka podatkov. Ta lahko vključuje različne podatke, odvisno od izvedbe aplikacije, npr. identifikatorje uporabnikov, podatke o stikih, podatke o telefonski številki za kontaktiranje uporabnika, podatke o simptomih, če jih vnese uporabnik, podatke o odrejenih ukrepih, o okužbi, itd. Glede na določbo 29. člena, da naj bi bila uporaba aplikacije obvezna za okužene in tiste, zoper katere je izrečen ukrep omejitve gibanja, v ozadju vsekakor nastajala zbirka osebnih podatkov s temi – občutljivimi – podatki, do katerih bo imel dostop določen krog organov, uporabnikov.

Kakršne koli navedbe, da bi uporaba aplikacije pomenila uporabo anonimnih podatkov, oziroma sploh ne bi posegala v osebne podatke posameznikov, tako niso ustrezne. Kot izhaja iz vseh zgoraj navedenih virov, podatki so osebni in morajo biti varovani skladno z Splošno uredbo, ZVOP-1 in Ustavo RS.

2. Glede prostovoljnosti namestitve

Informacijski pooblaščenec je glede vprašanja prostovoljnosti namestitve aplikacije pristojnemu ministrstvu že aprila 2020 posredoval svoje mnenje[7], ki ga predlagatelj zakona ni upošteval, in temelji na pravnem okviru, veljavnem v EU, ki ga kot relevantnega izpostavlja tako Evropska komisija, Evropski parlament, kot tudi Evropski odbor za varstvo podatkov. Prostovoljnosti aplikacije vse te institucije postavljajo kot pogoj za pravno skladno delovanje.

Prostovoljnost izhaja iz določb 157. člena ZEKom-1, s katerim je v slovenski pravni red prenesena Direktiva 2020/58/ES, ki postavlja omejitve za obdelavo podatka o lokaciji uporabnika terminalne opreme/pametnega telefona za operaterje elektronskih komunikacij, pa tudi za druge ponudnike storitev informacijske družbe. 157. člen ZEKom-1 določa, da so lahko tehnologije za pridobivanje podatkov s terminalne opreme uporabnikov (kamor sodijo tudi aplikacije, ki s pametnega telefona uporabnika pridobivajo podatke o lokaciji) **uporabljene le, če posameznik v to privoli oziroma v primerih nujnih izjem, če je to potrebno zaradi zagotavljanja storitve.** Direktiva 2002/58/ES v členu 15 dopušča, da države članice sprejmejo zakonske ukrepe, s katerimi omejijo obseg pravic in obveznosti, med drugim določenih v členu, ki se nanaša na pridobivanje podatkov iz terminalne opreme posameznika,vendar le, kadar takšna omejitev pomeni potreben, primeren in ustrezen ukrep v demokratični družbi za zaščito državne varnosti, obrambe, javne varnosti in preprečevanje, preiskovanje, odkrivanje in pregon kriminalnih dejanj ali nedovoljene uporabe elektronskega komunikacijskega sistema iz člena 13(1) Direktive 95/46/ES. Vprašljivo je, do katere mere lahko nove pravne podlage, ki bi nalagale obvezno rabo aplikacije (npr. za potrjeno okužene) razumeli kot skladne z omejitvami navedenega člena.

V vsakem primeru pa bi morali biti v primeru nove pravne podlage za obvezno namestitev aplikacije spoštovani temeljni standardi varstva pravic posameznikov: podlage morajo biti zakonite in ustavne, časovno omejene, morajo biti nujne in sorazmerne glede na zasledovani cilj, torej omejevanje epidemije COVID19 in tega ni mogoče doseči z milejšimi sredstvi. Predvsem sorazmernost in nujnost je v primeru obvezne aplikacije izredno težko utemeljiti, kot smo že poudarili v mnenju pristojnemu ministrstvu, saj si veliko posameznikov, ki bi se izkazali za okužene, aplikacije niti ne bi moglo naložiti, ker nimajo novejšega pametnega telefona. Le na teh namreč aplikacije zanesljiveje delujejo, kot kažejo izkušnje, kar pomeni, da bi bil velik del, tudi najranljivejše populacije, iz tega ukrepa izključen (starejši, vsi ki nimajo najnovejših mobilnih telefonov, otroci, socialno šibkejši). Posebna skrb bi morala biti posvečena vprašanju obvezne rabe pri posameznikih, ki jim je bila odrejena karantena. Ti namreč niso potrjeno okuženi, o čemer bi aplikacija obveščana ostale uporabnike, pač pa je obvezna raba »na zalogo« in s tem zelo vprašljiva z vidika sorazmernosti in nujnosti.

Glede na to, da je aplikacija lahko učinkovita le, če jo naloži več kot polovica populacije, že dejstvo, da velik del populacije niti nima primernih telefonov za to, postavi presojo nujnosti in sorazmernosti pod velik vprašaj. Še posebej ob upoštevanju kazenske določbe iz 48. člena predloga zakona, po kateri je

[7] https://www.ip-rs.si/vop/?tx_jzgdprdecisions_pi1[showUid]=1504

za kršitelje obveze po aplikaciji predvidena globa od 200 do 600 Eur. Glede na evropski pravni red in glede na to, da je v drugih državah EU taka aplikacija zgolj na prostovoljni bazi, Informacijski pooblaščenec meni, da je potrebno slediti ureditvam v drugih državah članicah EU. Tovrstne aplikacije delujejo zanesljivo le na novejših pametnih telefonih in prisilitev, da si jo pod grožnjo globe naložijo vsi, ki jih zakon opredeljuje, četudi na njihovi napravi ne bo zanesljivo delovala, je nesorazmerna in ne prispeva k ciljem, za katere si prizadeva zakonodajalec. **Glede na navedeno Informacijski pooblaščenec predlaga Državnemu zboru RS, da členov, ki določajo obvezno uporabo aplikacije ne podpre.**

3. Pravne podlage za obdelavo podatkov v zvezi z aplikacijo in pristojni organi.

Predlog zakona opredeljuje le osnovne parametre delovanja aplikacije in je predvsem osredotočen na uporabnike ter na relacije med njimi (npr. zagotavljanje nezmožnosti identifikacije). Kot poudarjeno v točki 1, pa pri delovanju aplikacije nastajajo zbirke podatkov, do katerih imajo lahko dostop in glede katerih imajo obveznosti z vidika zakonodaje o varstvu osebnih podatkov različni subjekti, kot upravljavci podatkov, pogodbeni obdelovalci, tudi uporabniki. Iz predloga zakona razmejitev glede teh odgovornosti in pooblastil, kateri organi lahko dostopajo do katerih podatkov, kje se ti hranijo, ne izhaja. Zato opozarjamo, da določbe predloga zakona o aplikaciji nikakor niso zadostne v smislu pravnih podlag za obdelavo osebnih podatkov, ki izhajajo iz aplikacije, s strani pristojnih organov (npr. NIJZ, Ministrstvo za zdravje, Ministrstvo za javno upravo), kot tudi, da iz predloga zakona ne izhaja delitev obveznosti in dolžnosti pristojnih organov v zvezi z zagotavljanjem varnega in ustreznega delovanja aplikacije. Za obdelavo podatkov preko aplikacije mora obstajati jasna pravna podlaga, kjer posebej opozarjamo na podlage, ki jih v členu 6 določa Splošna uredba (v primeru obdelave osebnih podatkov s strani javnih organov točka f člena 6(1) ne pride v poštev) ter na podlage in omejitve, ki jih za obdelavo občutljivih osebnih podatkov določa Splošna uredba v členu 9.

Zakon bi moral jasno določiti, kdo so upravljavci podatkov v zvezi z uporabo aplikacije, kateri podatki se lahko obdelujejo in za kakšen namen, kakšni so roki hrambe, kdo ima lahko do njih dostop in predvsem, da se podatki izven namena preprečevanja širjenja COVID-19 ne smejo obdelovati. Kot že poudarjeno v mnenju Ministrstvu za zdravje, bi moral zakon poleg ozke opredelitve namena izključno v povezavi z obvladovanjem epidemije vsebovati varovalke – npr. sodno odredbo za izvedbo posredovanja podatkov organom pregona ali drugim uporabnikom – za zagotovitev tega, da bi zbrani osebni podatki resnično ostali v obdelavi v okviru zdravstvene stroke.

4. Upoštevanje premislekov varstva osebnih podatkov, transparentnost in zaupanje javnosti

Aplikacije za sledenje zbujajo izredno veliko vprašanj glede zasebnosti posameznikov in varstva njihovih osebnih podatkov in ta morajo **biti pred uvedbo aplikacije ustrezno naslovljena v transparentnem postopku demokratičnega odločanja.** Iz mnenj nadzornih organov in Evropske komisije izhajajo tudi naslednja izhodišča, za katera verjamemo, da jih boste pri odločanju o predlogu zakona upoštevali.

Aplikacije ne morejo nadomestiti, temveč lahko le podprejo ročno sledenje stikom, ki ga izvaja usposobljeno javnozdravstveno osebje, ki lahko ugotovi, ali je verjetno, da tesni stiki povzročijo prenos virusa, ali ne (npr. interakcija z osebo, ki je zaščitena z ustrezno opremo – blagajniki itd.– ali ki ni zaščitena). Podpora temu procesu s strani aplikacije bi v praksi najverjetneje pomenila tudi povečan pritisk na tako strokovno osebje, epidemiologe, ki bi morali biti sposobni svetovati in pregledati situacijo veliko večje količine posameznikov, ki bi bili obveščeni o rizičnih stikih. Le posvet z epidemiologom oziroma možnost hitrega testiranja bi posamezniku, ki prejme obvestilo o stiku, lahko zagotovilo varno udeležbo v nadaljnjih družbenih interakcijah (npr. odhod v službo, druženje, status oseb, ki živijo v istem gospodinjstvu). Če podpora v smislu hitrega posveta in testiranja ni zagotovljena, aplikacija ne more pokazati učinka.

Sledenje lokacijam posameznikov ni sorazmerno, na evropski ravni je prednost dana sledenjustikom. Ker lahko aplikacije za sledenje stikom delujejo brez neposredne identifikacije posameznikov, bi bilo treba uvesti ustrezne ukrepe za preprečevanje ponovne identifikacije. Zbrane informacije bi bilo treba shranjevati na terminalski opremi uporabnika, zbirati pa bi bilo treba samo relevantne informacije, kadar je to zares nujno potrebno.

Odločitev o uporabi in zakonski uvedbi tovrstnih storitev prav gotovo terja izvedbo ocene učinka na varstvo osebnih podatkov, s pomočjo katere se pravočasno in predhodno naslovijo tveganja glede varstva osebnih podatkov (člen 35 Splošne uredbe) in zgoraj omenjene dileme. Takšna ocena bi glede na naravo opisane aplikacije morala biti izvedena pred končno odločitvijo o uvedbi in oblikovanjem zakonske podlage za uvedbo takšne aplikacije. Namen predhodne ocene učinke je namreč pravočasno ugotoviti in obvladovati tveganja glede varstva osebnih podatkov (npr. glede primerne pravne podlage) kakor tudi izvesti zgoraj omenjene postopke minimizacije obdelave. Evropski odbor za varstvo podatkov močno priporoča, da se ocene učinka v zvezi z varstvom podatkov objavijo

Kot kažejo izkušnje držav, ki aplikacijo za sledenje stikom okuženih s SARS-COV2 že poznajo, je njena učinkovitost v veliki meri odvisna od tehnične zanesljivosti take aplikacije in kvalitete njenega delovanja ter zaznavanja rizičnih stikov. Predpogoj za učinkovitost je tudi, da je aplikacija varna, da so občutljivi podatki posameznikov, ki se z njo zbirajo in obdelujejo, ustrezno zavarovani in se ne razkrivajo nepooblaščenim in je za posameznika predvidljiva, v smislu, da je jasno, kateri organi ali drugi subjekti imajo lahko dostop do podatkov in kdaj. Zakonitost in upoštevanje temeljnih človekovih pravic sta tu predpogoj. Ker je lahko aplikacija pri doseganju ciljev omejevanja širjenja SARS-COV2 učinkovita le, če si jo prostovoljno naloži praktično celotna populacija, ki ima primeren pametni telefon, je zaupanje v njeno varnost in dobro delovanje ter upoštevanje temeljnih pravic posameznikov ključna točka spodbude za posameznike.

Netransparentnost predlagatelja glede predloga zakona in podrobnosti v zvezi z obdelavo osebnih podatkov državljanov ter neupoštevanje številnih do sedaj izpostavljanjih spornih točk predlogov ukrepov, ki se tičejo obdelave lokacijskih podatkov posameznika, obvezne rabe aplikacije in širjenja pooblastil organov pregona na področju nadzora ukrepov po zakonu, ki ureja nalezljive bolezni zagotovo ni popotnica, ki bi javnosti lahko vlivala zaupanje v predlagane ukrepe – tudi aplikacijo. Le preglednost in natančne informacije glede delovanja aplikacije ter izrecna urejenost vse potrebnih pravnih podlag za obdelavo tovrstnih podatkov s strani pristojnih institucij v zakonu in striktno upoštevanje ustavno zagotovljenih pravic so lahko temelj za zaupanje posameznikov v aplikacijo in s tem za dovolj široko uporabo, ki bi lahko potencialno prispevala k omejevanju širjenja SARS-COV2.

Kot kažejo izkušnje iz drugih držav članic EU, modeli za implementacijo aplikacije, ki v veliki meri upoštevajo temelje varstva osebnih podatkov obstajajo, obstajajo tudi druge dobre prakse na tem področju, kot je npr. javna objava natančne dokumentacije presoj vplivov na zasebnost in varstvo osebnih podatkov iz člena 35 Splošne uredbe (t. i. DPIA) konkretnih aplikacij še pred njihovo uveljavitvijo, javna objava dokumentacije glede tehnične izvedbe, itd. Bistvena točka vseh modelov, ki se kažejo kot uspešnejši, je preglednost in zaupanje javnosti, da ji bo aplikacija koristila ter da ne zbira nesorazmerne količine osebnih podatkov in so si jo posamezniki pripravljeni zato prostovoljno naložiti, ne pa siljenje posameznikov v obvezno namestitev z zelo dvomljivim učinkom. Velja pa opozorilo, da se do tega trenutka še nobena od uvedenih aplikacij po našem vedenju ni izkazala za zelo učinkovito pri doseganju ciljev omejevanja širjenja virusa, bodisi zaradi majhnega števila uporabnikov ali nezanesljivega tehničnega delovanja, v nekaterih državah (npr. Norveška) so delovanje celo ustavili.

S spoštovanjem,

Mojca Prelesnik, univ. dipl. prav.
informacijska pooblaščenka

Pripravila:

dr. Jelena Burnik,
vodja mednarodnega sodelovanja in nadzora

Poslati:

- naslovnik (po e-pošti);
- v vednost: Državni svet RS: gp@ds-rs.si;
- v vednost: Vlada RS, gp.gs@gov.si;
- v vednost: Varuh človekovih pravic: info@varuh-rs.si;
- v vednost: ministrica za pravosodje, mag. Lilijana Kozlovič, Ministrstvo za pravosodje, gp.mp@gov.si;
- zbirka dokumentarnega gradiva pri IP.