



REPUBLIKA SLOVENIJA

INFORMACIJSKI
POOBLAŠČENEC

Dunajska cesta 22, 1000 Ljubljana

T: 01 230 9730

www.ip-rs.si

gp.ip@ip-rs.si

Številka: 007-14/2023/14

Datum: 29. 6. 2023

Državni zbor
Šubičeva 4, 1000 Ljubljana

Kolegij predsednice Državnega zbora RS
Vse poslanske skupine
Odbor za zdravstvo
Zakonodajno-pravna služba
Gp@dz-rs.si

ZADEVA: Predlog Zakona o digitalizaciji zdravstva – EPA 872-IX (EVA 2023-2711-0078) – MNENJE

Zveza: objava na portalu Državnega zbora RS

Spoštovani,

Informacijski pooblaščenec (v nadaljevanju IP) se je seznanil s Predlogom Zakona o digitalizaciji zdravstva – EPA: 872 – IX (EVA 2023-2711-0078), v nadaljevanju predlog ZDigZ, ki je objavljen na spletni strani Državnega zbora RS, kot ga je dne 8. 6. 2023 določila Vlada RS na svoji 53. redni seji.

IP uvodoma izpostavlja, da ni dvoma o tem, da je treba obdelave osebnih podatkov v zdravstvu ustrezno prenoviti in izboljšati s ciljem zagotavljanja učinkovitosti zdravstvenih obravnav, s čimer je povezana tudi prenova zakonodaje na tem področju. Hkrati IP svari pred pomanjkanjem resnih strokovnih premislekov pri pripravi predpisov, ki urejajo enega najbolj občutljivih informacijskih sistemov z resnimi posledicami ne le za zasebnost, ampak za širši spekter pravic posameznikov. **IP opozarja, da predlog zakona prinaša preveč tveganj za posameznike, kar potrjujejo spodaj navedene pripombe k predlaganemu besedilu in številne nekonsistentnosti, ki kljub dopolnitvam ostajajo v besedilu predloga zakona.**

IP je tekom priprav predloga ZDigZ ves čas sodeloval s svojimi mnenji predlagatelju (vsa so objavljena na spletni strani IP¹), ki pa jih je predlagatelj le deloma upošteval. IP ugotavlja, da **ostaja predlog zakona v številnih bistvenih delih pomanjkljiv in nejasen, pri čemer predlagatelj izpostavljenih skrbi IP v pomembnem delu ni ustrezno naslovil, z novimi predlogi rešitev pa se pojavljajo tudi nove skrbi in tveganja.**

V številnih pogledih pa je pomanjkljiva tudi priložena ocena učinkov v zvezi z varstvom osebnih podatkov, ki je v tem primeru na podlagi 24. člena ZVOP-2 obvezni sestavni del predloga zakona, in s katero se je IP seznanil šele z objavo na spletni strani Državnega zbora RS. Hkrati predlagatelj pomembnih tveganj in pomanjkljivosti predloga zakona, ki so v oceni učinkov izpostavljeni v besedilu predloga zakona ni naslovil.

IP poudarja, da je namen zakonodajne ocene učinka prispevati k boljšemu oblikovanju zakonskih predlogov s pravočasno identifikacijo in ukrepi za obvladovanje tveganja v zvezi z varstvom osebnih podatkov in bi **praviloma morala biti narejena pred oblikovanjem zakonskih določb** ter po potrebi ažurirana tudi glede na nato predlagane zakonske določbe. Poudarjamo, da namen priprave ocene učinka ni zgolj formalno zadostiti zahtevam Splošne uredbe in ZVOP-2, temveč identificirati tveganja in

¹ <https://www.ip-rs.si/zakonodaja/pripombe-informacijskega-pooblaščenca-na-predloge-predpisov/2023>

predvideti ustrezne ukrepe v predlogu zakona, torej je namenjena primarno predlagatelju – če se zaključki ocene učinka ne upoštevajo pri oblikovanju zakonskih predlogov ocena učinka nima smisla. Ugotovitve, stališča in priporočila iz ocene učinka bi se morali odražati v opisu ciljev in rešitev, v predlaganih določbah in obrazložitvah, žal pa temu ni tako, saj se – sicer korektne **ugotovitve iz ocene učinka – ne odražajo v samem predlogu zakona.**

Navedeno se odraža glede:

- primerjave z ureditvami v tujini,
- upoštevanja narave, obsega, okoliščine in namenov obdelave,
- opredeljenosti naborov podatkov, upravljavcev in uporabnikov ter rokov hrambe,
- opisa podatkovnih tokov in udeleženih subjektov,
- upoštevanje temeljnih načela varstva osebnih podatkov,
- upoštevanja pravic posameznika in
- obvladovanja tveganj za pravice in svoboščine posameznika.

V oceni učinka je na več mestih navedeno: »*DPIA v takšnem obsegu ni izvedena. Treba je izvesti oceno učinka, ki bo vsebovala ukrepe in mehanizme za obvladovanje in ublažitev tveganj, ki se pojavljajo pri predlogu zakona po temeljnih načelih varstva osebnih podatkov.*«. Glede na to, da se takšna dikcija ponavlja že iz prejšnjih verzij prejetih ocen učinka, se utemeljeno postavlja vprašanje, **ali oziroma ali bo sploh kdaj takšna ocena učinka izvedena?** Kot smo že prej izpostavili sicer pričujoča **ocena učinka na več mestih podaja konkretne in utemeljene predloge za izboljšavo predloga zakona z vidika varstva osebnih podatkov, do katerih pa se predlagatelj ne opredeli in jih pri oblikovanju zakonskega besedila iz neznanega razloga konstantno zapostavlja.**

IP v nadaljevanju na podlagi 3. točke prvega odstavka 55. člena Zakona o varstvu osebnih podatkov (ZVOP-2) ter 57. člena 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 (Splošna uredba) posreduje zakonodajalcu svoje mnenje k predlogu Zakona o digitalizaciji, ki naj bi nadomestil Zakon o zbirkah podatkov s področja zdravstvenega varstva (ZZPPZ) in ga poziva, da predlogu zakona posveti ustrezno pozornost.

Iz prejetega gradiva izhaja, da naj bi predlagatelj obstoječi sistem zbiranja in obdelave osebnih podatkov, ki temelji na ZZPPZ na podlagi predloga zakona **nadomestil s centralnim zdravstvenim informacijskim sistemom (CeZIS), katerega dejanski upravljavec bo novoustanovljeno podjetje DigiZdravje, d.o.o.**

Arhitektura sistema ostaja glede na besedilo predloga zakona, kljub dopolnitvam, pomanjkljivo in nekonsistentno opredeljena. Sistem naj bi vseboval 19 temeljnih zbirk osebnih podatkov, ki se med seboj v celoti povezujejo, brez kakršnekoli zakonske opredelitve omejitev povezovanja glede na namene posameznih zbirk:

1. centralni elektronski zdravstveni zapis (CeZZ) – upravljavec ZZZS,
2. vire v zdravstvu (VVZ) – upravljavec ministrstvo za zdravje,
3. državne registre organiziranih presejalnih programov (presejalni programi) – upravljavec koordinator posameznega programa,
4. register raka – upravljavec Onkološki inštitut,
5. register podatkov o nalezljivih boleznih in okužbah, povzročiteljih in njihovih lastnostih – upravljavec NIJZ,
6. register podatkov o umrlih osebah in vzrokih smrti – upravljavec NIJZ,
7. register podatkov o bolnišničnih obravnavah posameznikov v bolnišnicah in drugih stacionarnih ustanovah (s sprejemom v posteljno enoto) – upravljavec NIJZ,
8. register redkih nemalighnih bolezni – upravljavec Univerzitetni klinični center, Pediatrična klinika,
9. register endoprotetike Slovenije (RES) – upravljavec ortopedska klinika Valdoltra,
10. register kroničnih nemalighnih nenalezljivih in prirojenih bolezni – upravljavec NIJZ,
11. register podatkov o reproduktivnem zdravstvenem varstvu – upravljavec NIJZ,
12. register podatkov o zunajbolnišničnih obravnavah – upravljavec NIJZ– upravljavec NIJZ,
13. register s področja zdravja in varstva pri delu – upravljavec NIJZ,
14. register cepljenih oseb in neželenih učinkov po cepljenju – upravljavec NIJZ in

15. centralna baza zdravil – upravljavec nosilec pravic iz obveznega zdravstvenega zavarovanja,
16. zbirke podatkov, ki jih ZZZS vodi na podlagi 79.b člena Zakona o zdravstvenem varstvu in zdravstvenem zavarovanju (evidenca o zavarovanih osebah obveznega zdravstvenega zavarovanja, evidenca o zavezancih za prispevek, evidenca o izvajalcih zdravstvene dejavnosti, evidenca o zavarovanih osebah, ki so upravičene do plačila razlike do polne vrednosti – upravljavec ZZZS).

Poleg tega predlog zakona določa tudi zbirko: osnovna zdravstvena dokumentacija (OZD), ki jo vodijo posamezni izvajalci zdravstvene dejavnosti.

V zvezi s temi zbirkami in centralnim sistemom ostajajo številne bistvene nejasnosti, ki jih predlagatelj ni opredelil dovolj jasno in določno oziroma jih je neustrezno naslovil. Zlasti v predlogu zakona ni jasno opredeljeno:

- upravljavstvo CeZIS in njegovo razmerje do upravljavcev posameznih zbirk, ki so njegov del,
- razmerja, odgovornosti, naloge in obveznosti posameznih deležnikov glede varstva podatkov ter zagotavljanja pravic posameznikov v CeZIS in posameznih zbirkah,
- način uveljavljanja pravic posameznikov v pretežnem delu sploh ni urejen (urejen je zgolj v delu dostopa do sistema, ne pa tudi drugi vidiki),
- nameni povezovanja zbirk podatkov so opredeljeni preširoko in nejasno,
- ni jasno, kateri so lahko dodatni nameni obdelav podatkov,
- ni jasno, kakšno je razmerje med posameznimi zbirkami, ki so del CeZIS in se dejansko glede na vsebino vodijo za različne namene ter bodo skupaj vsebovale tako rekoč vse osebne podatke vseh posameznikov v Sloveniji v zvezi z zdravjem in zdravstvenim zavarovanjem,
- materija opredelitve obdelav (gre za zakonsko materijo), ki deloma z zakonom ni določena, je prepuščena v prevelikem delu v ureditev s podzakonskim aktom – t.j. z enotnimi metodološkimi načeli, ki jih sprejme minister,
- kot odgovorne osebe za obdelavo so določene fizične osebe pri upravljavcih, namesto, da bi bili kot taki določeni sami upravljavci – odgovornost za skladnost obdelav s Splošno uredbo je namreč na upravljavcu in ne njegovih zaposlenih (upravljavec pa mora poskrbeti za ustrežno dodelitev nalog med zaposlenimi in morebitnimi zunanji izvajalci v skladu s predpisi).

IP ponovno izpostavlja, da ni jasno, zakaj je predlagatelj izbral novo in z vidika varstva pravic posameznika bolj tvegano rešitev ustanovitve novega izvajalca centralne digitalizacije, ki bo gospodarska družba – d.o.o. **Nov subjekt naj bi bil pristojen za upravljanje centralne interoperabilnostne hrbtnice** za izmenjavo osebnih podatkov, kar so zelo obsežna pooblastila za poseganje v zasebnost in posledično prinašajo velika tveganja za pravice posameznikov. Nedvomno gre torej najmanj za **prenos pomembnega dela nalog upravljavstva ene najbolj obsežnih in najbolj občutljivih zbirk osebnih podatkov v državi v roke subjekta, za katerega je razbrati, da bi lahko deloval tudi kot subjekt zasebnega sektorja**, za katerega veljajo drugačni pogoji in zahteve glede varstva osebnih podatkov ter zasebnosti, kot za subjekte javnega sektorja, prav tako so s tem povezana drugačna tveganja. Nova gospodarska družba bo namreč lahko izvajala tudi tržne storitve. **Doslej so imeli to vlogo zgolj izvajalci zdravstvenih dejavnosti in Nacionalni inštitut za javno zdravje (NIJZ) oz. glede vsebin zavarovanja ZZZS. V novo predlagani ureditvi razmerja med novim izvajalcem centralne digitalizacije, izvajalci zdravstvenih storitev, ZZZS in NIJZ zakonsko še vedno niso dovolj jasno opredeljena in sorazmerna glede na zakonite cilje obdelave z vidika zahtev 38. člena Ustave. Novost pa je tudi upravljanje centralnega elektronskega zdravstvenega zapisa s strani ZZZS, ki ostaja v marsičem zakonsko nedorečena.**

V nadaljevanju po posameznih bistvenih sklopih podajamo nekatere konkretnije pripombe.

Nejasna opredelitev vlog in pojmov glede odgovornosti za varstvo podatkov (6., 7., 8., 9., 11., 12., 13., 14. in 16. člen)

Predlog zakona še vedno nejasno in premalo določno ter konkretno opredeljuje naloge, odgovornosti in pristojnosti različnih vključenih deležnikov pri delovanju sistema. **Zakon določa posamezne upravljavce zbirk podatkov, ki so del CeZIS (npr. ZZZS, NIJZ, koordinatorji posameznih presejalnih programov, ministrstvo za zdravje, Onkološki inštitut), pri čemer pa niso opredeljena dovolj jasno razmerja in pooblastila za obdelavo med njimi ter njihovo razmerje do izvajalca centralne digitalizacije.**

Gre brez dvoma vsaj deloma za razmerje skupnega upravljanstva, glede na vsebino pa je razbrati, da bo **dejansko glavni med skupnimi upravljavci, ki bo v praksi in vsebinsko, kot podrobneje pojasnjujemo v nadaljevanju, odločal o bistvenih vprašanji varovanja osebnih podatkov t.i. izvajalec centralne digitalizacije, ki bo družba z omejeno odgovornostjo**. Ugotavljamo, da je v tem delu velik del zakonske materije prepuščen podzakonskim aktom.

Ob tem je v zakonu upravljavcem v delu hkrati za iste podatke oz. zbirke podeljena vloga upravljavca in uporabnika, pri čemer razmejitev teh vlog in posledice za varovanje osebnih podatkov iz predloga zakona še vedno ni mogoče v celoti razbrati.

Upoštevajoč vse izpostavljene vidike zakonitosti obdelave izpostavljene v tem mnenju predlagamo, da se z zakonom jasno za vsako zbirko opredeli, kateri od skupnih upravljavcev je odgovoren za posamezne elemente zbiranja in obdelave, za katere vrste osebnih podatkov ter določi razmerja med posameznimi skupnimi upravljavci vezano na posamezne zbirke in zdravstveni informacijski sistem kot celoto, tako glede različnih vidikov obdelave kot glede uveljavljanja pravic posameznikov.

Pravice posameznikov (6., 7., 13., 17. in 39. člen)

Predlog zakona na več mestih ureja ali omejuje pravice posameznikov, kot jih urejajo 12.-23. člen Splošne uredbe, pri čemer je ureditev nekonsistentna, določbe o možnosti uveljavljanja podatkovne samoodločbe posameznika in omejevanju obdelave pa si med seboj celo nasprotujejo. Prav tako postopki uveljavljanja posameznih pravic specifično vezano na centralni informacijski sistem niso določeni, zato bo v praksi v primeru, da ostane besedilo posameznih členov v tem delu nespremenjeno, prihajalo do resnih težav pri ugotavljanju zakonitosti obdelav ter uveljavljanju pravic posameznikov.

Tako 2. odstavek 6. člena med drugim določa, da v primerih posrednega zbiranja osebnih podatkov posameznika ni treba predhodno seznaniti s tem, da se bodo osebni podatki pridobili iz že vzpostavljene zbirke podatkov, pri čemer ne opredeljuje nobenih ukrepov za zaščito zakonitih interesov posameznika, na katerega se nanašajo osebni podatki, kot to zahteva točka c) 5. odstavka 14. člena Splošne uredbe. Predlog zakona tudi ne določa, kako naj bi posameznik v tem delu uveljavljal možnost nasprotovanja taki obdelavi, če zanjo sploh ne ve (več spodaj).

Prav tako predlog zakona na razmeroma dolgo obdobje (3 tedne) v 3. odstavku 7. člena omejuje seznanitev posameznika z lastnimi osebnimi podatki vnesenimi v sistem v primerih, ko naj bi razkritje 'škodovalo zdravstvenemu stanju osebe', kar je pravno povsem nejasen in neopredeljen pojem. Odločanje o razkritju je torej prepuščeno v tem obdobju v vsakokratno presojo zdravstvenim delavcem, ki to presojo izvajajo na podlagi lastnih vrednostnih prepričanj in ne strokovne in pravne opredelitve pojma. Gre za omejitev, ki je deloma še širša od pravno primerljivo sporne in nejasne omejitve vsebovane v 22. členu Zakona o pacientovih pravicah, glede katere je IP podal zahtevo za oceno ustavnosti (<https://www.ip-rs.si/zakonodaja/pripombe-informacijskega-pooblaščenca-na-predloge-predpisov/2023>).

Predlog zakona nejasno določa možnost posameznika, ki je navedena v 3. odstavku 13. člena, da nasprotuje uporabi za namen posodabljanja vseh registrov po predlogu zakona, saj po eni strani to možnost omenja, po drugi strani pa določa avtomatično povezljivost in izmenjavo vseh podatkov med vsemi zbirkami v CeZIS. Zakon pa hkrati bistveno oži (glede na trenutno ureditev) tudi možnost svobodnega odločanja posameznika o obdelavah osebnih podatkov, s tem ko širi nabor osebnih podatkov, ki so dostopni vsem ne glede na voljo pacienta npr. področje medicine dela, prometa in športa (17. člen).

Opredelitev zbiranja, obdelav in namenov zbiranja ter zbirk osebnih podatkov (13. do 35. člen)

IP opozarja, da **Splošna uredba v točki h 2. odstavka 9. člena** za posebne vrste osebnih podatkov za namene, ki so predmet predloga zakona, **izrecno zahteva, da se lahko obdelujejo, če je obdelava potrebna za namene preventivne medicine ali medicine dela, oceno delovne sposobnosti zaposlenega, zdravstveno diagnozo, zagotovitev zdravstvene ali socialne oskrbe ali zdravljenja ali upravljanje sistemov in storitev zdravstvenega ali socialnega varstva** na podlagi prava Unije ali prava države članice ali v skladu s pogodbo z zdravstvenim delavcem **ter zanjo veljajo pogoji in zaščitni ukrepi iz 3. odstavka 9. člena Splošne uredbe**. Slednji zahteva, da se osebni podatki posebne vrste za namene iz točke h 2. odstavka 9. člena Splošne uredbe **lahko obdelujejo le, kadar jih obdeluje ali je za njihovo**

obdelavo odgovoren strokovnjak, za katerega velja obveznost varovanja poklicne skrivnosti v skladu s pravom EU ali pravom države članice ali pravili, ki jih določijo pristojni nacionalni organi, ali druga oseba, za katero tudi velja obveznost varovanja skrivnosti v skladu s pravom EU ali pravom države članice ali pravili, ki jih določijo pristojni nacionalni organi.

Glede na to, da bo CeZIS dejansko ena 'nadzbirka', ki se bo obdelovala za zelo raznolike namene od zdravstvene oskrbe do ukrepov zdravstvenega zavarovanja, statistike in raziskovanja, IP ocenjuje, da bi bilo nujno jasneje in konsistentno opredeliti in zamejiti posamezna pooblastila za dostopanje in obdelavo osebnih podatkov v CeZIS (in ne le delno v posameznih zbirkah), saj se podatki znotraj zbirk v CeZIS sproti posodablajo in izmenjujejo. Kljub poskusom predlagatelja, da navedeno materijo opredeli jasneje večina bistvenih členov v delu, ko določajo namene zgoraj navedenih 19 zbirk osebnih podatkov, ki bodo del CeZIS, ostajajo preširoki in nejasni.

Dodatno opozarjamo, da je mestoma izbira pojmov, s katerimi so opredeljene posamezne vrste osebnih podatkov in zbirke nejasna. Tako npr. ni jasno, zakaj je opredelitev osnovne zdravstvene dokumentacije dokaj ozka in nedoločena, zakaj je rok hrambe te dokumentacije, ki je lahko za pacienta ključnega pomena, v delu zgolj 15 let od nastanka (v primerjavi z rokom hrambe podatkov iz centralnega elektronskega zdravstvenega zapisa, ki je načeloma 10 let po smrti pacienta) ter kakšno je njeno razmerje do podatkov v elektronskem zdravstvenem zapisu. Prav tako ni jasno glede na sorodne vsebine, kakšna je razmejitev med obema zbirkama. IP iz gradiva ne razbere niti razlogov za razmeroma kratke roke hrambe nekaterih drugih delov dokumentacije.

IP dodatno opozarja, da niso opredeljeni zgoraj omenjeni zaščitni ukrepi, ki jih za tovrstne obdelave zahteva Splošna uredba v 9. členu.

Na podlagi prejetega ni razbrati razlogov in utemeljitve za mestoma (pre)široke dostopne pravice oz. vloge upravljavcev za posamezne zbirke, med drugim:

- ni jasno kako in ali sploh je bila izvedena presoja sorazmernosti obsega dostopa ZZS, ki je upravljavec CeZZ do vseh osebnih podatkov v CeZZ (Centralni elektronski zdravstveni zapis) – kot razberemo – gre za neposredno dostopanje do vseh podatkov v elektronskem zdravstvenem zapisu in ne le do podatkov za posamezni primer in na podlagi posamezne konkretne zahteve upravljavcu oz. zgolj do določenih ozko opredeljenih osebnih podatkov, ki bi bili sorazmerni glede na zasledovane cilje in konkretno nalogo posameznega upravičenca.
- Sama narava upravljavstva pomeni dejansko dostopanje do vseh osebnih podatkov, pri čemer pa ni jasno opredeljeno, katere naloge upravljavstva bo dejansko opravljal ZZS v zvezi s CeZZ.
- Prav tako ni razbrati ukrepov za preprečevanje realnega tveganja, ki v tem primeru obstaja za prekomerno obdelavo osebnih podatkov in obdelavo za druge namene od zakonsko določenih.
- Iz gradiva ni razbrati razlogov in presoje ureditve z vidika načela sorazmernosti v delu omejitev pravic posameznika glede pravice do podatkovne samoodločbe pri odločanju o tem, kdo lahko dostopa do njegovih osebnih podatkov v zvezi z zdravjem, saj je ureditev drugačna, kot velja doslej na podlagi ZZPPZ, Zakona o pacientovih pravicah in Zakona o varnosti in zdravju pri delu.
- IP ne razbere, s katerimi ukrepi se bo zagotovila sorazmernost in zakonitost neposrednega dostopanja upravnih organov do CeZZ.
- Ni jasno, kaj naj bi pomenil in kakšne obdelave naj bi določal podatkovni model, ki je naveden v 35. členu in ki ga bo določil minister.

Obdelava osebnih podatkov za razvojne, raziskovalne in statistične namene (11., 41. do 43. člen)

Kot ugotavlja IP, je v tem delu (v 11. ter 41. členu) **predvidena obdelava osebnih podatkov iz CeZIS za dodatne namene zlasti za raziskovalne namene.**

Ob tem je dodatno zaskrbljujoče, da zakon še vedno posredno in brez jasnih opredelitev podrobnosti posredno predvideva tudi javno objavo podatkov iz zbirk podatkov iz predloga zakona na portalu odprtih podatkov, pri čemer je izbor in vsebina teh podatkov prepuščena izvajalcu centralne digitalizacije, saj predlog zakona ne opredeljuje, kateri zdravstveni podatki oz. informacije izmed vseh osebnih podatkov, ki se zbirajo v 19 zbirkah (te vsebujejo zelo različne podatke) na podlagi predloga zakona, so dejansko anonimizirani, kateri pa psevdonimizirani podatki (torej še vedno varovani osebni podatki). Zgolj sklic na zakon, ki ureja dostop do informacij javnega značaja po mnenju IP v tem primeru ne zadošča, saj so tveganja za (lahko celo nenamerno) javno objavo napačno anonimiziranih osebnih podatkov v zvezi z

zdravjem glede na posebno naravo nekaterih zbirk, kot je Centralni elektronski zdravstveni zapis, prevelika. Pri tem zakon ne razlikuje med različnimi zbirkami, ki so del CeZIS in se vodijo za zelo različne namene (npr. zbirka viri v zdravstvu ima povsem drugačno naravo kot ostale zbirke, ki vsebujejo podatke v zvezi z zdravjem).

V tem delu tudi niso dovolj jasno opredeljene in omejene vloga in odgovornosti izvajalca centralne digitalizacije (ki bo glede na opisano nastopal v vlogi skupnega upravljavca, kot podrobneje pojasnjujemo v nadaljevanju).

Nejasna vloga izvajalca centralne digitalizacije (34. in 44. do 54. člen)

Predlog zakona, kot je zgoraj omenjeno, predvideva ustanovitev novega poslovnega subjekta – d.o.o. v lasti države, ki naj bi mu bile zaupane pomembne naloge povezane z zbiranjem in obdelavo vseh osebnih podatkov v zvezi z zdravjem v Centralnem zdravstvenem informacijskem sistemu. Kot je omenjeno zgoraj, naj bi bil ta subjekt – organiziran kot gospodarska družba v organizacijski obliki družbe z omejeno odgovornostjo – pristojen za širok nabor nalog povezanih z obdelavo osebnih podatkov na področju digitalizacije zdravstva, med drugim za:

- upravljanje centralne interoperabilnostne hrbtnice za izmenjavo osebnih podatkov in dokumentov;
- za pripravo elektronskih zdravstvenih podatkov za ponovno uporabo in za državno statistiko – to pomeni obdelavo in dostop do vseh zdravstvenih osebnih podatkov vseh prebivalcev Slovenije za ta namen;
- načrtovanje, vzpostavitev, razvoj, zagotavljanje, spremljanje in vzdrževanje centralnega zdravstvenega informacijskega sistema (CeZIS), ki podpira zbiranje in izmenjavo zdravstvenih podatkov in zdravstvene dokumentacije ter kazalnikov javnega zdravja,
- zagotavljanje enotnosti razvoja CeZIS v Republiki Sloveniji,
- skrb za kibernetsko varnost CeZIS in lokalnih informacijskih sistemov,
- zagotavljanje tehnične podpore uporabnikom CeZIS in lokalnih informacijskih sistemov,
- načrtovanje, koordinacijo razvoja in spremljanje delovanja informacijskih sistemov, ki podpirajo zbiranje in izmenjavo zdravstvenih podatkov in zdravstvene dokumentacije ter kazalnikov javnega zdravja,
- izvajanje skupnega javnega naročanja informacijskih sredstev za izvajalce zdravstvene dejavnosti v mreži javne zdravstvene službe ter njihovega vzdrževanja in delovanja povezanih storitev;
- vodenje projektov in razpisov (so)financiranih iz državnega proračuna in EU skladov na področju informacijsko komunikacijske tehnologije,
- zagotavljanje statističnih in drugih javno dostopnih podatkov s področja zdravstvenega varstva za ponovno uporabo v skladu s predpisi s področja državne statistike in ZDIJZ,
- zagotavljanje strokovne podpore ministrstvu in inšpektoratu, pristojnemu za zdravje s področja digitalizacije,
- sodelovanje v delovnih telesih uradnih inštitucij na nacionalni ravni, na ravni Evropske unije in na mednarodni ravni, na zahtevo ministra,
- strokovne in druge naloge v okviru svoje pristojnosti.

Navedeno pomeni, da bo novo javno podjetje tudi po dopolnitvah predloga zakona vsaj v delu ključni (skupni)upravljavac vseh zbirk osebnih podatkov v zvezi z zdravjem. Še vedno pa ni jasno, kakšna bodo razmerja med tem novim subjektom in drugimi upravljavci. Razbrati je mogoče, da gre za razmerja skupnega upravljanja, pri čemer bo dejansko o večini vsebin in nalog razen vnosa osebnih podatkov odločala izključno nova gospodarska družba, brez vzpostavitve kakršnihkoli varovalk pred zlorabami.

Mnenje glede predložene ocene učinka

ZVOP-2 v tretjem odstavku 24. člena določa, da kadar se z zakonom določa obdelava osebnih podatkov, za katero je treba izdelati oceno učinka, predlagatelj predlogu zakona priloži oceno učinka v skladu s 35. členom Splošne uredbe. Po proučitvi ocene učinka nadzorni organ poda mnenje glede obdelave osebnih podatkov, glede katerega se mora predlagatelj zakona opredeliti.

* * *

IP uvodoma pojasnjuje, da gre za **t.i. zakonodajno oceno učinka** (po tretjem odstavku 24. člen ZVOP-2) in ne za oceno učinka, ki jo je dolžan pripraviti upravljavec osebnih podatkov (35. člen Splošne uredbe), zato je zahteve 35. člena Splošne uredbe treba upoštevati smiselno – če in ko jih je primerno upoštevati in doreči že na ravni (priprave) zakona.

Poleg ocene učinkov v zvezi z varstvom osebnih podatkov, ki jih pripravljajo upravljavci osebnih podatkov, so posebej pomembne ocene učinka glede varstva osebnih podatkov pri pripravi predpisov. Glede na to, da mora obdelavo osebnih podatkov določati zakon (kakor tudi upravljavce, namene, roke hrambe, evidence, morebitno povezovanje zbirk ipd.), je **bistveno, da se tveganja glede varstva osebnih podatkov analizirajo že v času priprave predpisa, saj jih upravljavci kasneje, ko so bistveni elementi že določeni v predpisu, ne morejo spremeniti in njihove ocene učinka nimajo več takšnega pomena**. Kakovostno in celovito izdelana ocena učinka na ravni predpisa lahko bistveno razbremeni upravljavce osebnih podatkov, ki bi nato morali izdelovati ločene ocene učinka (deseti odstavek 35. člena Splošne uredbe oziroma tretji odstavek 49. člena Zakona o varstvu osebnih podatkov na področju obravnavanja kaznivih dejanj - ZVOPOKD). V tem smislu je zakonodajna ocena učinkov pomembno orodje tudi za ustrezno presojo obdelav z vidika zagotavljanja skladnosti predpisa z Ustavo.

Ocena učinka v zvezi z varstvom osebnih podatkov lahko v fazi snovanja predpisa zagotovi upoštevanje temeljnih načel varstva osebnih podatkov: poštenosti, preglednosti in zakonitosti, minimizacije obdelave, namenskosti, ažurnosti, rokov hrambe ter določitev ustreznih zaščitnih ukrepov in varovalk – njen cilj je celovit premislek o tem, katere podatke se bo zbiralo in za katere namene, kakšne so možnosti minimizacije nabora in obsega obdelave, katere evidence bodo vsebovale katere podatke in kdo bo z njimi upravljal, ali gre pri tem morda za skupno upravljanje, ali je predvideno povezovanje evidenc, kakšne so relevantne pravice posameznika, kateri so najkrajši možni roki hrambe, komu se bodo določeni podatki posredovali, ali prihaja do prenosa osebnih podatkov v tretje države ipd.

Ocene učinka v zvezi z varstvom osebnih podatkov so izjemnega pomena zlasti pri uvajanju sistematičnih novih obsežnih nacionalnih zbirk osebnih podatkov, novih policijskih pooblastil in pristojnosti, na področju obdelave posebej občutljivih podatkov (kot npr. podatki o zdravstvenem stanju, podatki o kazenskih in prekrškovnih postopkih, genski, biometrijski podatki ipd.), pri opredeljevanju ukrepov, ki zadevajo široko populacijo ali specifične družbene segmente, saj z analizo tveganj in učinkov na posameznika in družbo omogočajo javni diskurz o sprejemljivosti, primernosti, učinkovitosti ter nujnosti določenih ukrepov v demokratični družbi.

* * *

IP poudarja, da je namen zakonodajne ocene učinka prispevati k boljšemu oblikovanju zakonskih predlogov in bi praviloma morala biti narejena **pred** oblikovanjem zakonskih določb ter po potrebi ažurirana tudi glede na nato predlagane zakonske določbe. V nadaljevanju podajamo ugotovitve IP po ključnih delih predložene ocene učinka.

Primerjava z ureditvami v tujini

Glede na metodološki predlog IP je priporočljivo izvesti primerjavo z ureditvami v tujini, namen te primerjave pa primarno ni v opisovanju podobnih ureditev v drugih državah temveč – skladno s cilji ocene učinka – v identifikaciji tveganj in ustreznosti rešitev v drugih državah z vidika varstva osebnih podatkov. V tej primerjalni analizi je treba ugotoviti, s kakšnimi težavami so se soočale druge države, kako dobre/slabe so se pokazale njihove rešitve, ali imajo primerne in učinkovite varovalke ipd. Cilj tovrstne analize je predvsem ugotoviti, katerih napak ni dobro ponavljati, katere rešitve so se izkazale

kot delujoče in katere ne ter tako izkoristiti izkušnje drugih držav za oblikovanje boljših zakonskih rešitev².

Na strani 2. predložene ocene učinke je navedeno: *»Izoblikovane in utemeljene pravne omejitve, pozitivne ali negativne izkušnje, ki so se pojavile v tujih pravnih ureditvah, in navedbe o oblikovanju rešitev glede na negativne izkušnje pa so v celoti izostale. Menimo, da bi bila analiza navedenega koristna pri oblikovanju ustreznih rešitev v našem pravnem redu. Na tem mestu izpostavljamo, da bi morda upoštevali izzive, ki so nastali na podlagi obstoječega ZZPPZ in ki bi pripomogli k učinkovitejšemu urejanju v novem predlogu zakona.«* **Iz besedila predloga zakona ter obrazložitvev ni videti, da bi predlagatelj upošteval ta predlog iz ocene učinka.**

Upoštevanje narave, obsega, okoliščine in namenov obdelave

Narava, obseg, okoliščine in nameni obdelavi so upoštevali možnosti velikih tveganj za pravice in svoboščine posameznika glede na ugotovitve ocene učinka pri pripravi predpisa zmerno upoštevanj. V oceni učinka je ugotovljeno, da obseg obdelave pri denimo zbirki presejalnih programov nima dovolj določne vsebine o obsegu obdelave (npr. 2. odstavek 21. člena) – ni jasno, kateri so podatki, ki nastanejo pri izvajanju presejalnega programa. Glede na to, da je ta register glede na ostale registre nekoliko specifičen, je v oceni učinka predlagano, da se v nadaljnjih postopkih obseg obdelave bolj jasno definira, s čimer se strinjamo.

Na strani 2. predložene ocene učinke je navedeno: *»Glede na celotno besedilo zakona menimo, da celoten podatkovni tok obdelave od zbiranja do vseh faz obdelave, morebitne nadaljnje obdelave in hrambe ni v celoti razviden...«*.

Opredeljenost naborov podatkov, upravljavcev in uporabnikov ter rokov hrambe

V zvezi z naborom podatkov je v oceni učinka izpostavljeno, da je pri nekaterih registrih (npr. register podatkov o reproduktivnem zdravstvenem varstvu) obseg podatkov zelo širok ter, da je v 1. odst. 29. člena določeno, da register govori o zdravju žensk, nato pa v namenih vključuje zdravje parov, kar tudi po našem mnenju ni dosledno oz. dovolj jasno opredeljeno, saj nejasnosti in nedoslednosti v poimenovanjih namreč znižujejo standard učinkovitega varstvu osebnih podatkov.

Glede rokov hrambe obstaja nenaslovljeno vprašanje, kot je podrobneje opredeljeno zgoraj v mnenju, o razlogih za odločitve glede relativno kratkega roka hrambe osnovne zdravstvene dokumentacije, ki je lahko za pacienta ključnega pomena (zgolj 15 let od nastanka) ter kakšno je njeno razmerje do podatkov v elektronskem zdravstvenem zapisu.

Opis podatkovnih tokov in udeleženih subjektov

Ocena učinka korektno opozarja, da iz 4. odstavka 7. člena predloga zakona ni jasno, kaj se npr. zgodi, če zavezanec podatka ne popravi, v kakšni obliki oz. na kakšen način mora biti posredovano obvestilo o napaki ipd.) ter da je treba uskladiti pojme (npr. »zavezanec za vnos podatkov«, »oseba, ki je dolžna posredovati podatke v zbirke podatkov«). IP dodaja tudi, da je po oceni **IP premalo pozornosti namenjene kakovosti podatkov (točnosti, ažurnosti in popolnosti)**, ki se prenašajo v centralni sistem v smislu opredelitve učinkovitih postopkov, zahtev in varovalk za zagotovitev točnosti, ažurnosti in popolnosti podatkov, saj je odveč opozarjati, da gre za zelo pomembne podatke tako za zdravje kot

² Portugalska, Estonija in Finska imajo prav gotovo že določene dobre in slabe izkušnje z zakonsko ureditvijo digitalizacije zdravstva glede varstva osebnih podatkov in te bi morale biti upoštewane, v opisu predlaganih rešitev pa je podana zgolj ureditev v omenjenih državah.

za ostale pravice posameznika. Ob primernih ukrepih (kot je npr. dolžnost rednega preverjanja točnosti, ažurnosti in popolnosti podatkov, morebitni notranji in zunanji nadzor ipd.) bi bilo koristno opredeliti tudi odgovornosti za kakovost podatkov.

Osnovni opis sredstev obdelave (strojne in programske opreme, omrežij, človeških virov in uporabljenih komunikacijskih sredstev)

IP se strinja z ugotovitvami ocene učinka, da je potrebno zagotoviti ustrezno vključenost IT stroke:

- IT strokovnjaki naj se vključijo že v fazi oblikovanja zbirk oz. njihovega združevanja,
- določi naj se skupina IT strokovnjakov (projektni team), ki bodo podali oceno tveganja pri prenosu oz. vnosu podatkov,
- v primeru, da se pojavi potreba po zunanjih svetovalcih s področja IKT, da se sklenejo z njimi pogodbe z ustreznimi varovalkami, tako glede same izvedbe projekta, kot tudi glede obveznosti varstva podatkov.

Navedeno je po mnenju IP potrebno poleg tega, da bi bilo **zelo priporočljivo**, da **nad digitalizacijo z vidika IKT stalno bdi ustrezno umeščeno strokovno telo**, zato menimo, da bi predlagatelj moral opraviti premislek kako in v kakšni meri to tudi zakonsko zagotoviti oziroma zagotoviti osnovno ustrezno zakonsko podlago za to, podrobnosti glede umestitve, nalog in delovanja pa se lahko oblikujejo kasneje. Pomembno je tudi, da takšno strokovno telo lahko izvaja neodvisen strokovni nadzor med drugim oz. zlasti nad izvajalcem centralne digitalizacije.

V predlog zakona namreč pogrešamo določbe o zagotovitvi ustreznega strokovnega nadzora nad odločitvami, ki se bodo sprejemale v procesu digitalizacije zdravstva. Kot je navedeno v opisu rešitev npr. na Finskem Findata skrbi za anonimizacijo podatkov, kadar je to potrebno, posebej v zvezi z nadaljnjo obdelavo, nad zakonitostjo obdelave osebnih podatkov pa bdi poseben odbor pri Ministrstvu za socialne zadeve in zdravje (kar ne izključuje zunanjega nadzora s strani pristojnega nadzornega organa za varstvo osebnih podatkov).

IP predlaga tudi, da se **na zakonski ravni okrepi notranji nadzor pri izvajalcu centralne digitalizacije**, in sicer predlagamo, da se vključi zahtevo, da mora pooblaščen oseba za varstvo osebnih podatkov pri izvajalcu centralne digitalizacije izvajati redni letni notranji nadzor na obdelavi osebnih podatkov in o tem poročati Informacijskemu pooblaščenču – tovrstne rešitve so se že izkazale kot učinkovite (prim. 220. člen Zakona o elektronskih komunikacijah in Pravilnik o načinu izvajanja 220. člena Zakona o elektronskih komunikacijah).

Upoštevanje temeljnih načela varstva osebnih podatkov

V oceni učinka je navedeno stališče, da so določbe zakona o ustreznih varovalkah za preprečevanje uporabe v druge namene nezadostne. Določba 3. odstavka 14. člena predloga zakona (*»Podatki se anonimizirajo na način, da so dostopni samo v agregatni obliki.«*) po mnenju IP po eni strani omejuje možne načine in tehnike za anonimizacijo podatkov, po drugi strani pa preveč teže daje agregaciji podatkov, pri čemer velja izpostaviti, da niso nujno (vsi) agregirani podatki že sami po sebi tudi anonimni³, zato predlagamo, da se omenjena določba umakne, saj ne prispeva k jasnosti in učinkovitosti zakona. Ustreznost postopkov za anonimizacijo podatkov bi lahko (med drugim) nadziralo zgoraj omenjeno neodvisno strokovno telo.

V oceni učinka je zapisano, da je v določenih točkah naveden nabor podatkov, ki je precej splošen in širok (npr. podatki o delu lekarn ali delu reševalne službe) in kot takšen lahko povzroči precejšnjo pravno nepredvidljivost pravic, obveznosti in razmerij, ki izhajajo iz takšne normativne ureditve. Strinjamo se,

³ Več o metodah in tehnikah za anonimizacijo podatkov v smernicah Evropskega odbora za varstvo podatkov: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_sl.pdf.

da gre za zelo širok pojem, ki lahko ustvarja nejasnost o naboru podatkov, in da je treba konkretizirati nabor podatkov oz. se sklicevati na drug predpis na zdravstvenem področju, ki takšen opis ali definicije vsebuje.

Glede rokov hrambe pritrujemo zaključku ocene učinka, da so izostale utemeljitve o razlogih za trajno hranjenje podatkov pri večini registrov. V povezavi s tem izpostavljamo vprašanje morebitnega skupnega upravljanja in razdelitev nalog in odgovornosti v zvezi s tem, kot smo podrobneje navedli zgoraj v mnenju.

Upoštevanje pravice posameznika

Dolžnost informiranja posameznika po mnenju IP v predlogu zakona ni bila ustrezno upoštevana, posebej problematična je določba 2. odstavka 6. člena predloga zakona, ki določa, da "v primerih posrednega zbiranja osebnih podatkov posameznika ni treba predhodno seznaniti s tem, da se bodo osebni podatki pridobili iz že vzpostavljene zbirke podatkov, v skladu s tem zakonom, če ni s tem zakonom določeno drugače", kar ni v skladu z zahtevami iz 12., 13. in 14. člena Splošne uredbe.

Kot ugotavlja tudi ocena učinka, je treba dodati določbo o informacijah, ki jih mora upravljavec zagotoviti posameznikom, ko se ustvarjajo zdravstveni zapisi, in določiti, kdo in na kakšen način je odgovoren za zagotovitev teh informacij.

Ocena učinka korektno analizira tveganja, ki se nanašajo na pravice posameznika, vendar pa predlog zakona (kot smo podrobneje opredelili zgoraj v mnenju) tega ne upošteva.

Obvladovanje tveganj za pravice in svoboščine posameznika

V oceni učinka je pri tem poglavju na več mestih navedeno: *»DPIA v takšnem obsegu ni izvedena. Treba je izvesti oceno učinka, ki bo vsebovala ukrepe in mehanizme za obvladovanje in ublažitev tveganj, ki se pojavljajo pri predlogu zakona po temeljnih načelih varstva osebnih podatkov.«*.

Glede na to, da se takšna dikcija ponavlja že iz prejšnjih verzij prejetih ocen učinka, je utemeljeno vprašanje, kdaj oziroma ali bo sploh takšna ocena učinka izvedena? Kot smo že prej izpostavili sicer pričujoča ocena učinka na več mestih podaja konkretne in utemeljene predloge za izboljšavo predloga zakona z vidika varstva osebnih podatkov, do katerih pa se predlagatelj ne opredeli in jih pri oblikovanju zakonskega besedila konstantno zapostavlja.

Mnenje relevantnih pooblaščenih oseb za varstvo osebnih podatkov

Ocena učinka napačno navaja ali pa se v tem delu napačno razume metodologijo, da gre za mnenje IP in se sklicuje le na mnenje IP. V tej točki je namreč mišljeno **mnenje relevantnih pooblaščenih oseb za varstvo osebnih podatkov pri relevantnih upravljavcih in drugih organizacijah**, ki so oziroma bi morale sodelovati pri izdelavi ocene učinka (npr. ministrstva za zdravje, NIJZ, ZZS itd.). Tudi na splošno namreč po Splošni uredbi velja, da je naloga pooblaščenih oseb podaja mnenj k ocenam učinka, saj bi morale razpolagati z dovolj strokovnega znanja in izkušenj, da lahko s svojimi stališči pomagajo predlagatelju zakona pri oblikovanju ustrežnejših zakonskih rešitev z vidika varstva osebnih podatkov. Mnenja navedenih oseb iz priložene ocene učinka niso razvidna.

Zaključni test sorazmernosti

Tudi na tem mestu se v oceni učinka ponovi že videna krožna referenca: »Predlagamo, da se izvede ustrežna ocena učinka, ki bo ocenila, ali je ukrep – sprejetje zakona, sorazmeren glede na zadani cilj, ki ga sprejetje takšnega zakona zasleduje oz. izdelava zaključni test sorazmernosti.«.

Namen zadnjega dela predlagane metodologije za izdelavo zakonskih ocen učinka je, da se opravi končna presoja, ali so oziroma bodo predlagane določbe takšne, da lahko prestanejo ustaljeni ustavnosodni test sorazmernosti, t.j.:

- Ali so predlagane rešitve nujne za doseg (ustavno dopustnega) zadanega cilja? Ali je zakonska dikcija jasna in nedvoumna ter je obdelava določena z zakonom?
- Ali so predlagane rešitve primerne za doseg zadanega cilja?
- Ali so predlagane rešitve učinkovite v doseganju zadanega cilja?

* * *

IP na podlagi vsega navedenega opozarja zakonodajalca na daljnosežne posledice in nesorazmerna tveganja predlagane ureditve tako za varstvo osebnih podatkov in zasebnosti, kot za druge pravice posameznikov. Kot izhaja iz predloga zakona naj bi se npr. gospodarska družba, ki bo dejansko bistven (skupni) upravljavec CeZIS, financirala tako iz sredstev proračuna in obveznega zdravstvenega zavarovanja, kot tudi s prihodki pridobljenimi z opravljanjem tržnih storitev. Postavlja se vprašanje, ali to pomeni, da bo država takemu subjektu, ki bo glede na naloge opredeljene v predlogu zakona nedvomno (skupni) upravljavec največje zbirke osebnih podatkov v državi (nikakor namreč ne gre zgolj za pogodbenega obdelovalca) dopustila v sodelovanju z Vlado in s pristojnim ministrstvom, kot oblastnim oz. političnim organom, posredno v izključno presojo morebitna vprašanja odplačnega pridobivanja osebnih podatkov v zvezi z zdravjem s strani tretjih oseb.

Predlagamo, da zakonodajalec **vse navedene resne skrbi, ki so že bile večkrat predstavljene predlagatelju, kot tudi vse dodatne skrbi izpostavljene v tem mnenju, upošteva pri nadaljnji obravnavi te pomembne materije.** IP na podlagi navedenega ocenjuje, da predlog zakona brez bistvenih dopolnitev ni skladen z Ustavo, Splošno uredbo in ZVOP-2. Predvsem pa IP opozarja, da gre za eno največjih in najboljčutljivejših zbirk osebnih podatkov v državi, zato mora zadostiti najvišjim standardom varstva osebnih podatkov.

Hvala za sodelovanje in lep pozdrav,

Mojca Prelesnik, univ. dipl. prav.,
informacijska pooblaščenka

Poslati:

- po e-pošti;
- v vednost: Ministrstvo za pravosodje: gp.mp@gov.si;
- v vednost: Ministrstvo za zdravje: gp.mz@gov.si.