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

Številka: 007-50/2024/14 in 07122-1/2024/76
Datum: 22. 11. 2024

Republika Slovenija
Ministrstvo za zdravje
gp.mz@gov.si

Republika Slovenija
Ministrstvo za pravosodje
gp.mp@gov.si

Zadeva: Mnenje na Predlog Zakona o digitalizaciji zdravstva in na Zakonodajno oceno učinka v zvezi z varstvom podatkov – Obdelava osebnih podatkov na področju zdravstvenega varstva, zdravstvenega zavarovanja in javnega zdravja (Gradivo k predlogu Zakona o digitalizaciji zdravstva)

Zveza: dopis Ministrstva za pravosodje št. 007-63/2024-2030-21 prejet dne 30.10.2024 ter dopis Ministrstva za zdravje št. 007-50/2024/63 prejet dne 29.10.2024 s priloženim dokumentom št. 0070-114/2023, z dne 28. 10. 2024 ter Predlog Zakona o digitalizaciji zdravstva z dne 28. 10. 2024 (EVA 2024-2711-0031)

Spoštovani,

Informacijski pooblaščenec je 29. in 30. 10. 2024 prejel dopise Ministrstva za pravosodje in Ministrstva za zdravje, s katerimi ste nam v mnenje posredovali Predlog Zakona o digitalizaciji zdravstva z dne 28. 10. 2024 – EVA 2024-2711-0031 (predlog zakona) ter Dokument: Zakonodajna ocena učinka v zvezi z varstvom podatkov – Obdelava osebnih podatkov na področju zdravstvenega varstva, zdravstvenega zavarovanja in javnega zdravja – Gradivo k predlogu Zakona o digitalizaciji zdravstva (zakonodajna ocena učinka k predlogu zakona).

I. Uvodni povzetek

IP pozdravlja namero predlagatelja, da celovito uredi področje digitalizacije sistema obdelav osebnih podatkov v zdravstvu s ciljem izboljšave elektronske hrambe in izmenjave podatkov ter zagotavljanja učinkovite zdravstvene oskrbe. Učinkovita digitalizacija na tem področju je nedvomno proces, ki bo v prihodnje moral biti vzpostavljen, vendar pa to nikakor ne sme rezultirati v slabšem varovanju osebnih podatkov posameznikov, prebivalcev Slovenije, pač pa kvečjemu v višji ravni varstva zdravstvenih podatkov oziroma vsaj v ohranitvi obstoječe ravni varstva podatkov.

Predlog zakona predvideva centralno zbirko vseh zdravstvenih podatkov posameznikov, torej zbirko, kot je v Sloveniji še ni bilo, v kateri bodo vsi zdravstveni podatki vseh državljanov. V tem smislu bi to bila največja zbirka občutljivih podatkov v državi. Zanjo morajo tako veljati najstrožji standardi varovanja osebnih podatkov, kot veljajo za ostale državotvorne zbirke v javnem sektorju, npr. zbirke davčnih podatkov, zbirke podatkov na socialnem področju, zbirke v pravosodju, zbirke organov pregona itd. Ne le, da nezakoniti posegi v tako zbirko podatkov lahko pomenijo poseg v zasebnost posameznikov/pacientov, diskriminacijo itd., pač pa izguba podatkov, pomanjkljivosti pri dostopnosti podatkov ali napačni podatki lahko pomenijo

neposredno tveganje za življenje posameznika ob neprimerni zdravstveni obravnavi, ki ne bi temeljila na pravih podatkih.

Kot podrobneje pojasnjujemo v nadaljevanju, je zlasti pomembno, da predlog zakona ustrezno naslovi: (1) vprašanje sorazmernosti obdelave osebnih podatkov za različne namene (ne le za zdravljenje, pač pa tudi kako so podatki v centralnem sistemu dostopni za druge namene, zaračunavanje zdravstvenih storitev, zdravstveno zavarovanje, upravni postopki itd.) ter (2) vprašanje upravljavstva centralne zbirke. **Z vidika ohranjanja trenutne ravni varstva osebnih podatkov je lahko upravljavec osebnih podatkov le pravna oseba javnega prava** s področja zdravstva (kot so osebe javnega prava tudi javni zavodi, ki nudijo javno zdravstvene storitve, katerih podatki bodo v sistemu, ter tudi Nacionalni inštitut za javno zdravje). Pravna oseba zasebnega prava lahko sodeluje pri procesih digitalizacije (kot je tudi praksa na področjih drugih državotvornih zbirk podatkov), vendar z omejeno odgovornostjo pogodbene obdelave osebnih podatkov in ne kot upravljavec podatkov. Tudi druge države v EU, v katerih je bila izvedena centralizacija in digitalizacija zdravstva, so po pridobljenih informacijah vlogo upravljavca podatkov take osrednje zbirke zaupale pravni osebi javnega prava in ne zasebnega prava.

IP je na različne predloge zakona že podal večje število pripomb in predlogov, vse s ciljem, da novo vzpostavljena centralna zbirka podatkov v zdravstvu zadovolji zgoraj navedene standarde. Žal vse dosedanje pripombe niso bile upoštevane. V nadaljevanju jih podajamo še enkrat, glede na zadnji predlog zakona. Le z upoštevanjem teh pripomb in predlogov lahko nastane sistem in proces digitalizacije v zdravstvu, pri katerem bo zagotovljena raven varstva podatkov, kot jo posamezniki uživamo trenutno. Neupoštevanje spodnjih priporočil in pripomb pa bo neizogibno vodilo k sistemu z velikimi tveganji za posege v pravice posameznikov.

a) Sorazmernost obdelave osebnih podatkov

Glede na navedeno je nujno, da se v okviru zakonskega urejanja centralne informacijsko komunikacijske infrastrukture na področju zdravstva **v skladu z ustavnim načelom sorazmernosti jasno opredeli in razmeji nabor osebnih podatkov in obdelave ter centralizirano hrambo osebnih podatkov v zvezi z zdravjem za namen zdravstvene oskrbe in ukrepov javnega zdravja od obdelav za druge namene (kot npr. za namene upravnih postopkov, zaračunavanja zdravstvenih storitev, izvajanja zdravstvenega zavarovanja, načrtovanja politik in podobne druge upravno-politične namene)**.

Prejeti predlog zakona namreč vzpostavlja eno največjih zbirk v državi na področju javnega zdravstva, v kateri naj bi se za vse te različne namene in neselektivno vodil bistveno preširok nabor osebnih podatkov v zvezi z zdravjem brez razlikovanja med podatki, ki so relevantni za nadaljnjo obravnavo in ostalimi podatki. Kot pojasnjujemo v nadaljevanju, je po mnenju IP z vidika tveganj in posegov v zasebnost neustrezna in premalo dodelana predlagana arhitektura vodenja enotne centralne 'nad-zbirke' – Centralni elektronski zdravstveni zapis (CeZZ), ki naj bi vsebovala popolnoma vse osebne podatke v zvezi z zdravjem, ne glede na to, ali so podatki relevantni za nadaljnje zdravstvene obravnave ali ne. Med drugim naj bi CeZZ vseboval podatke o popolnoma vseh zdravstvenih obravnavah, celotno osebno in družinsko anamnezo pacienta kot tudi podatke o življenjskem slogu in dejavnikih tveganja (npr. kajenje, alkoholizem) neselektivno za vse opisane namene in za namen omogočanja dostopa najrazličnejšim uporabnikom in niti ne zgolj izvajalcem zdravstvene dejavnosti ter NIJZ (kot so npr. ministrstvo, upravne enote, zavarovalnice, izvajalci postopkov dolgotrajne oskrbe). Zaskrbljujoča je nejasna opredelitev vrste in obsega pooblastil za dostopanje, ki naj bi jih določil minister s podzakonskim aktom. IP ob tem glede na uvodno definicijo, da gre za javno centralno informacijsko komunikacijsko infrastrukturo na področju javnega zdravstva ne razbere, kako naj bi bilo urejeno vodenje zbirk osebnih podatkov s strani preostalih izvajalcev zdravstvenih storitev.

Po pregledu prejetega besedila IP ugotavlja, da predlog zakona ostaja v številnih bistvenih delih notranje neusklajen in nedodelan, saj si posamezne določbe notranje med seboj nasprotujejo, med drugim:

- **glede vloge posameznih deležnikov kot upravljavcev različnih centralnih zbirk – vloge bodo razdeljene med izvajalce zdravstvene dejavnosti, zasebnopravni subjekt – družba z omejeno odgovornostjo in NIJZ (20., 22. in 23. člen),**
- **glede določitve namenov (19., 25. in 31. člen),**
- **glede rokov hrambe (24. in 29. člen),**
- **glede določitve nabora osebnih podatkov, ki naj bi jih vsebovala centralna zbirka CeZZ in upravičenj različnih uporabnikov (nujna ločitev osebnih podatkov potrebnih na različnih ravneh obravnave, ločitev zbirk za posamezne namene (npr. za namene zavarovanja).**

V predlogu zakona so tudi številna nesistemska poimenovanja različnih pojmov.

b) Upravljavstvo centralne zbirke podatkov

Ponovno izpostavljamo skrb glede **predlagane neustrezne ureditve upravljavstva javne centralne zdravstvene informacijsko komunikacijske infrastrukture, ki naj bi se izvajala kot obvezna javna služba v obliki družbe z omejeno odgovornostjo, ki jo bi ustanovila Republika Slovenija in ki bi v skladu s predlogom zakona z opravljanjem te gospodarske javne službe ustvarjala primeren dobiček.** Vlada RS pa bi z njo sklenila pogodbo o opravljanju gospodarske javne službe za nedoločen čas ter sprejela akt o ustanovitvi družbe, s katerim bi uredila vsa vprašanja glede delovanja družbe, ki niso urejena s predlogom zakona. IP po analizi prejetega gradiva in pridobivanju informacij o ureditvah primerljivih sistemov v drugih državah članicah EU ugotavlja, da v državah članicah EU upravljavstvo osrednje nacionalne centralne zbirke vse zdravstvene dokumentacije, ki bi bila obvezna in zakonsko predpisana za vse prebivalce Slovenije, **ni zaupano** subjektu zasebnega sektorja s ciljem ustvarjanja dobička, temveč vlogo upravljavca take centralne zbirke osebnih podatkov – če ta sploh obstaja na nacionalni ravni – opravljajo subjekti javnega prava.

Subjekt javnega prava je v vlogi upravljavca osebnih podatkov bistveno bolj omejen kot subjekt zasebnega prava, saj ga prvenstveno omejuje sektorska zakonodaja, ki ureja specifično področje – zdravstvo. Pravne podlage za obdelavo podatkov tako lahko določa le zakon, sprejet v demokratičnem procesu. To omogoča politično neodvisnost in neodvisnost od vsakokratne oblasti, ki je bistveno višja, kot v primeru subjekta zasebnega prava. Zasebnopravni subjekt ima namreč večjo diskrecijsko možnost, da se samostojno odloča glede uporabe pravnih podlag za obdelavo osebnih podatkov, kot jih določa Splošna uredba o varstvu podatkov. Prav zato so vse državotvorne zbirke v državi umeščene v krog subjektov javnega prava in ne v zasebnopravne subjekte. Tudi za centralno zbirko podatkov v zdravstvu bi moralo veljati enako zaradi tveganj za pravice posameznikov. Zasebno pravni subjekt poleg tega upravlja ustanovitelj, torej v primeru trenutnega predloga zakona vsakokratna Vlada RS, s katero bi imela družba sklenjen dogovor. Na tak način bi bil upravljavec največje zbirke zdravstvenih podatkov tudi pod vplivom vsakokratne politike.

Dodatno želimo izpostaviti tudi **problematiko nedostopnosti zdravstvenih podatkov, ki so hranjeni v centraliziranih zbirkah, bodisi zaradi tehničnih težav ali različnih kibernetskih napadov** (na primer izsiljevalski virusi in podobno), ki ima lahko hude posledice za posameznike, vključno z nezmožnostjo opravljanja zdravstvenih storitev ali napačnim zdravljenjem. S tovrstnimi težavami se na primer soočajo na Hrvaškem, ki ima vzpostavljen centraliziran sistem za shranjevanje zdravstvenih podatkov (CEZIH), ki pa pogosto ne deluje. Čeprav noben informacijski sistem ni imun pred tovrstnimi napadi ali napakami v delovanju, pa so v primeru, da so zdravstveni podatki hranjeni centralizirano, posledice lahko mnogo hujše, obenem pa je

dostop do teh podatkov običajno nujen v situacijah, ko so posamezniki zaradi svojega zdravstvenega stanja v ranljivem položaju.

V zvezi s tem uvodoma še ugotavljamo, da **se besedilo predloga zakona, ki je bilo poslano v mnenje Informacijskemu pooblaščencu (IP) bistveno razlikuje od besedila predloga zakona, ki je bilo dne 29. 10. 2024 s strani Ministrstva za zdravje objavljeno na portalu e-Demokracija** (na spletni strani https://e-uprava.gov.si/si/drzava-in-druzba/e-demokracija/predlogi-predpisov/predlog-predpisa.html?id=16672). Širša strokovna javnost je tako vabljena k razpravi o besedilu predloga zakona iz aprila 2024, ki je bistveno drugačno kot besedilo, o katerem v resnici teče razprava na ravni strokovnega usklajevanja predlagatelja.

V nadaljevanju podajamo mnenje na predlog zakona po sklopih ter podrobnejše mnenje na oceno učinkov.

II. Mnenje na predlog Zakona o digitalizaciji zdravstva

Nekatere najbolj bistvene pomanjkljivosti predloga zakona po posameznih sklopih so:

- **Ureditev zbirk podatkov in razmejitev vlog skupnih upravljavcev (19. do 31. člen in 40. ter 41. člen)**

IP opozarja, da predlog zakona ne opredeljuje izrecno in dovolj jasno upravljavstva in vlog pri skupnem upravljanju temeljne centralne zbirke – centralni elektronski zdravstveni zapis (CeZZ) in razmerja do zbirke osnovne zdravstvene dokumentacije (OZD). Predlog zakona tudi ne določa jasno in nedvoumno odgovornosti upravljavstva in vsebine za zbirke osnovne zdravstvene dokumentacije (OZD) – umešča jo namreč v CeZZ in dopušča, da se OZD vodi neposredno v CeZZ, kot njegov del, hkrati pa določa, da gre za zbirko na lokalnem zdravstvenem informacijskem sistemu pri izvajalcu zdravstvene dejavnosti. Z vidika sorazmernosti tudi ne more biti utemeljeno, potrebno in sorazmerno, da je celotna vsebina vse OZD brez omejitev in strokovne presoje zdravnika kopirana v CeZZ.

Predlog zakona izrecno določa, da naj bi bili uporabniki podatkov v CeZZ tudi upravni organi za namene izvedb upravnih postopkov s področja zdravstvenega, pokojninskega ali invalidskega zavarovanja ali s področja uveljavljanja pravic po drugih zakonih v celoti. Ob tem pa predlog zakona niti med upravljavce niti med uporabnike ne uvršča NIJZ, hkrati pa NIJZ dodeljuje nalogo, da podatke posreduje drugim uporabnikom.

Predlog zakona določa presplošno, deloma nejasno in preširoko nabor osebnih podatkov, ki naj bi jih vseboval centralni elektronski zdravstveni zapis (CeZZ), do katerega naj bi lahko dostopal izredno širok krog tako rekoč vseh zdravstvenih delavcev kot tudi zunanji uporabniki; pri čemer bo vrste in obseg pooblastil določil minister s podzakonskim aktom. IP opozarja, da je treba ločiti posamezne centralne zbirke in glede na to določiti nabor osebnih podatkov, ki bodo v njih hranjeni (ločeno za OZD, za CeZZ, za zbirko ZZZS ipd.). V skladu s 15. in 38. členom Ustave namreč ni sprejemljivo vodenje vseh v predlogu zakona navedenih osebnih podatkov v eni enotni centralni nacionalni zbirki za najrazličnejše namene – torej v CeZZ, saj nabor podatkov bistveno presega namene zdravstvenega varstva in javnega zdravja.

Predlog zakona hkrati določa preširok namen CeZZ, saj tega širi povsem izven namena zdravstvenega varstva in ukrepov javnega zdravja tudi npr. na področje zagotavljanja podatkov za upravne postopke, za namene zdravstvenega zavarovanja, postopkov dolgotrajne oskrbe. Ob tem IP izpostavlja na nujnost razlikovanja med primarnimi nameni CeZZ in opredelitvijo področnih pravnih podlag za dostop do posameznih ozko opredeljenih vrst osebnih podatkov za ločene namene, ki niso povezani z zdravstveno oskrbo.

Prav tako predlog zakona ne določa jasno in nedvoumno vloge, nalog in odgovornosti NIJZ oz. si posamezne določbe med seboj vsebinsko nasprotujejo.

Predlog zakona določa premalo konkretno tudi povezovanje različnih zbirk (v določenih deli niso določene konkretne vrste podatkov) in na nejasen način to prepušča v urejanje z enotnimi metodološkimi načeli.

Predlog zakona določa notranje nekonsistentne (npr. nejasno razlikovanje glede rokov hrambe OZD v primerih, ko se OZD hrani v CeZZ) in premalo segmentirane ter posledično v nekaterih primerih zelo dolge, v drugih pa prekratke roke hrambe za posamezne vrste osebnih podatkov. Tako je za vse zbirke javnega zdravja predvidena v celoti trajna hramba, po drugi strani pa se podatki iz OZD (ki so bistveni za pacientovo obravnavo in ki so vir preverjanja v primeru uveljavljanja pravic posameznikov do izbrisa oz. popravka) brišejo že 5 let po pacientovi smrti oz. celo 15 let od nastanka, če je dokumentacija posredovana v CeZZ, kar pomeni, da uveljavljanje pravic v takem primeru ne bo mogoče.

Predlog zakona še vedno premalo jasno in preširoko določa dostopne pravice in pooblastila za dostopanje in obdelavo osebnih podatkov iz CeZZ. Pri tem ni jasna tudi vloga NIJZ z zvezi s posameznimi posredovanji drugim uporabnikom.

Predlog zakona premalo jasno in neučinkovito določa možnost posameznika, da omeji dostop do nekaterih najbolj občutljivih osebnih podatkov v zvezi z zdravjem, kar bi posledično lahko vplivalo na to, da posameznik ne bo poiskal ustrezne zdravstvene oskrbe v strahu pred popolnim nadzorom nad njegovo zdravstveno zasebnostjo (npr. s strani zdravnikov medicine dela, ki bodo lahko dostopali tudi do podatkov o obravnavah pri kliničnem psihologu), ki z delom nimajo nobene zveze. V zvezi s tem se zakonska pooblastila glede opredelitve omejitev s predlogom zakona podeljuje ministru.

- **Določitev enotnih metodoloških načel (2., 5., 7., 8., 24. in 29. člen)**

Enotna metodološka načela, ki jih sprejme minister, zajemajo širok nabor vsebin, med njimi so tudi take, ki so zakonska materija glede na 38. člen Ustave in s tem glede na predlagano ureditev bistveno vplivajo
na vse zbirke osebnih podatkov na podlagi predlog zakona. Predlog zakona pa niti ne vsebuje določb glede metodoloških načel zbirk javnega zdravja.

To pomeni, da je po eni strani pomemben del zakonske materije (npr. vsebine glede opredelitve nabora osebnih podatkov z vidika določitve psevdonimiziranih oz. anonimiziranih podatkov, pravila glede povezovanja zbirk) prepuščen v urejanja podzakonskemu aktu, hkrati pa je v delu glede javnega zdravja podnormiran in tako predstavlja tveganja za ustrezno vzpostavitev in razvoj zbirk javnega zdravja. Zato je nujna dopolnitev zakona, ki bo jasneje omejila materijo urejanja enotnih metodoloških načel, ter ustrezno uredila določanje in spreminjanje tako enotnih metodoloških načel kot metodoloških načel posamezne zbirke javnega zdravja.

- **Nosilec centralne informatizacije v zdravstvu**

CeZZ in vse zbirke na področju zdravstva, v katerih se bodo podatki obdelovali ob podpori informacijskih rešitev, ki jih bo zagotavljala novo ustanovljena gospodarska družba v lasti države – t.i. nosilec centralne informatizacije v zdravstvu – naj bi glede na določbe predloga zakona soupravljala gospodarska družba kot subjekt zasebnega sektorja. Navedena gospodarska družba bo v skladu s predlogom zakona poleg opravljanja gospodarske javne službe, opravljala tudi tržno dejavnost, ki v novem predlogu zakona niti ni več omejena na »manjše spremljevalne dejavnosti«, kot je to določal prejšnji predlog zakona, temveč bo opravljanje tržne dejavnosti omejeno zgolj glede na vrsto nalog, ki jih bo gospodarska družba lahko izvajala kot tržno dejavnost. Ob tem velja opozoriti, da je CeZZ centralna zbirka zdravstvene dokumentacije za vse prebivalce Republike Slovenije – gre torej za 'nadzbirko' osebnih podatkov v zdravstvu, ki bo ob predlagani ureditvi, kljub nekaterim zakonskim omejitvam, podvržena vsem tveganjem obdelav v zasebnem sektorju, družba pa bo delovala na trgu in ne kot subjekt javnega sektorja kot npr. javni zavod, državni organ ipd., ki je podvržen drugačnim zahtevam in tveganjem. Tudi naša preliminarna analiza primerljivih sistemov v EU kaže na to, da v ostalih državah članicah EU praviloma vlogo upravljavca centralizirane zbirke zdravstvenih podatkov opravljajo subjekti javnega prava.

- **Obdelava osebnih podatkov za sekundarne namene – razvojne, raziskovalne, izobraževalne in statistične**

Opozarjamo, da predlog zakona kljub nekaterim dobrodošlim dopolnitvam predloga zakona, kot je opredelitev možnosti ugovora posameznika k obdelavi, še vedno premalo jasen in preveč ohlapno določa pogoje za sekundarne obdelave osebnih podatkov. V zvezi s tem izpostavljamo, da je neustrezna predlagana ureditev, ki IP dodeljuje pristojnosti za izdelavo mnenja glede učinka nameravane raziskave na varstvo osebnih podatkov. Taka ocena mora biti namreč predmet ocene učinkov, ki jo mora za namen pridobivanja podatkov na podlagi 69. člena ZVOP-2 pripraviti raziskovalec oz. raziskovalna organizacija, ki želi izvesti raziskavo in v ta namen pridobiti osebne podatke, lahko pa je tudi predmet presoje različnih neodvisnih etičnih komisij. Glede na pristojnosti IP kot neodvisnega nadzornega organa je nesprejemljivo to odgovornost dodeliti IP, saj se s tem ogroža neodvisnost in nepristranskost postopkov IP, ki lahko o ustreznosti ukrepov varovanja osebnih podatkov presoja dokončno zgolj v nadzornih postopkih.

III. Mnenje na predlog Zakonodajne ocene učinka v zvezi z varstvom podatkov – Obdelava osebnih podatkov na področju zdravstvenega varstva, zdravstvenega zavarovanja in javnega zdravja

1. Uvodoma

Informacijski pooblaščenec (v nadaljevanju: IP) uvodoma pojasnjuje, da je po določbi člena 35(1) 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 o varstvu podatkov; v nadaljevanju: Splošna uredba) ocena učinka v zvezi z varstvom osebnih podatkov (v nadaljevanju: ocena učinka) potrebna, kadar „je možno, da bi [dejanje obdelave] lahko povzročil[o] veliko tveganje za pravice in svoboščine posameznikov“. Upravljavec podatkov mora nato oceniti tveganja za pravice in svoboščine posameznikov, na katere se nanašajo osebni podatki, in opredeliti ukrepe, predvidene za zmanjšanje navedenih tveganj na sprejemljivo raven, ter dokazati skladnost s Splošno uredbo (člen 35(7)). Skladno s priporočili Evropskega odbora za varstvo podatkov (v nadaljevanju: EDPB), kot so navedena v smernicah o ocenah učinka[1] velja, da če je upravljavec podatkov štel, da so tveganja zadosti zmanjšana, se lahko glede na razlago člena 36(1) Splošne uredbe ter uvodnih izjav (84) in (94) obdelava nadaljuje brez posvetovanja z nadzornim organom.

Zakon o varstvu osebnih podatkov (Uradni list RS, št. 163/22; v nadaljevanju: 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. Kadar ocene učinka ni treba izdelati, predlagatelj zakona opravi samo predhodno posvetovanje z nadzornim organom v skladu s 36. členom Splošne uredbe.

* * *

Na podlagi informacij, ki ste nam jih posredovali, vam v nadaljevanju na podlagi točke (a) tretjega odstavka člena 58. člena, v povezavi s 35 in 36. členom 35 Splošne uredbe, 5. točke prvega odstavka 55. člena in tretjega odstavka 24. člena ZVOP-2 ter 2. členom Zakona o informacijskem pooblaščencu (ZInfP; Uradni list RS, št. 113/05, 51/07 – ZUstS-A) posredujemo naše neobvezno mnenje v zvezi s predloženo oceno učinka.

* * *

[1] 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, 17/SL, DS 248 rev.01; dostopno na: https://www.ip-rs.si/fileadmin/user_upload/Pdf/Mednarodno_delovanje/wp248_rev.01_sl.pdf

2. Pregled ocene učinka

IP je v procesu sprejemanja Zakona o digitalizaciji zdravstva že izdal mnenje na oceno učinka št. 07122-1/2023/23 z dne 24. 4. 2023 ter mnenje na oceno učinka v sklopu mnenja IP št. 007-14/2023/14 z dne 29. 6. 2023 na Predlog Zakona o digitalizaciji zdravstva – EPA 872-IX (EVA 2023-2711-0078).

2.1 Splošne ugotovitve

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 glede izdelave ocene učinka 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 **določena 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.

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.

Kot pogosto poudarjamo so ocene učinka v zvezi z varstvom osebnih podatkov 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. Digitalizacija zdravstva prav gotovo predstavlja primer, ko je zakonodajna ocena učinka glede varstva osebnih podatkov ne samo obvezna, temveč tudi bistvenega pomena za pravočasno naslovitev tveganj.

2.2 Formalni pregled celovitosti ocene učinka

Kot navajate ste pri izdelavi ocene učinka upoštevali metodologijo Informacijskega pooblaščenca za oceno učinkov predpisov (v nadaljevanju metodologija), ki je bila privzeta v Vladno metodologijo za oceno učinkov predpisov na različna družbena področja, iz avgusta 2023. Ob splošnem pregledu ugotavljamo, da ocena učinka sicer sledi predlagani strukturi, vendar pa je v nekaterih delih **pomanjkljiva** in sicer:

- primerjava z ureditvami v tujini (poglavje 1.3),

- opredeljenost nabora podatkov, upravljavcev in uporabnikov ter rokov hrambe (poglavje 2.2.),
- obvladovanje tveganj za pravice in svoboščine posameznika (poglavje 5),
- mnenje relevantnih pooblaščenih oseb za varstvo osebnih podatkov (poglavje 6.1).

Iz vsake ocene učinka bi moralo biti jasno, kdo jo je pripravil, na katero verzijo predpisa oziroma projekta se nanaša in kdaj je bila opravljena, kakor tudi kakšno je bilo mnenje pooblaščene osebe za varstvo osebnih podatkov pri zavezancu.

Prejeta ocena učinka v zelo pomembnem delu (obvladovanje tveganj za pravice in svoboščine posameznika) – dejansko analizo tveganj prepušča projektni oceni učinka, ki naj bi jo izvedla družba, kateri bo poverjena digitalizacija zdravstva. Opozarjamo, da je s tem izpuščeno pomembno poglavje zakonodajne ocene učinka, zato je ta v pomembnem delu **pomanjkljiva**. Kot smo zapisali v metodologiji, je že tudi pri pripravi predpisa **identifikacija tveganj bistvenega pomena** – tveganja, ki jih predlagatelj ob pripravi predloga predpisa morebiti ne bi identificiral, utegnejo kasneje izpostaviti splošna in/ali strokovna javnost oziroma sodna presoja. Rezultat nepravočasno ali nepopolno identificiranih in naslovljenih tveganj je lahko odpor strokovne in splošne javnosti – in to kljub temu, da bi bil ob ustrezni analizi tveganj ukrep sicer povsem sprejemljiv. V interesu predlagatelja je zato, da vsa tveganja pravočasno identificira in obravnava. Tveganja je priporočljivo **strukturirano obravnavati po temeljnih načelih varstva osebnih podatkov** (zakonitost, sorazmernost, namenskost…) ter jih oceniti glede na **verjetnost** in **resnost** ter tako ugotoviti **skupno raven tveganja**, pri čemer mora biti jasna tudi metodologija za določitev skupne ravni tveganja.

Pri pripravi predpisa je treba opraviti premislek tudi o možnih ukrepih za obvladovanje tveganj - identificirana tveganja se upravlja z ustreznimi varovalkami (kavtelami), kot so npr. kratki roki hrambe, anonimizacija, psevdonimizacija, minimizacijski postopki, sledljivost obdelave, logične in fizične kontrole pri vnosu podatkov, organizacijski in tehnični ukrepi za varnost podatkov, redni notranji nadzor ipd. Ponovno poudarjamo, da gre za ukrepe za obvladovanje tveganj, ki jih je **potrebno in primerno nasloviti že na ravni priprave predpisa (zakona) in ne za ukrepe, ki se jih lahko prepusti upravljavcu**.

2.3 Vsebinski pregled ocene učinka

Kot smo navedli je predložena ocena učinka v določenih delih pomanjkljiva, kot pojasnjujemo v nadaljevanju.

Primerjava z ureditvami v tujini

V oceni učinka je navedeno (le), da je bila primerjava z ureditvami v tujini izvedena za štiri države, ni pa nobene navedbe, kakšne so ugotovitve. Primerjava z ureditvami v tujini je sicer podana v obrazložitvi k predlogu zakona, vendar pa gre tudi za sestavni del zakonodajne ocene učinka – poleg prikaza ureditev v izbranih državah pogrešamo **kritično analizo teh ureditev**. Eno od bistvenih področij, ki ga pogrešamo v oceni učinka, bi tako bila objektivna analiza umeščenosti organizacije, ki skrbi za centralne digitalne zbirke na področju zdravstva, prednosti in slabosti tamkajšnjih organizacijskih oblik in pravne subjektivitete, saj ima tudi to bistven vpliv na zagotavljanje varstva osebnih podatkov.

Kot smo pojasnili v metodologij je pri pravno-primerjalni analizi rešitev ključno, da se iz tuje prakse prenesejo ne le ideje o tem, kaj vse je mogoče, ampak tudi že izoblikovane in utemeljene pravne omejitve ter dejanske izkušnje pri uporabi določene tehnologije, rešitev oziroma ukrepov. Pri tem je bistvenega pomena, da se pridobijo tudi informacije o morebitnih negativnih učinkih uporabe določenih tehnologij ali oblik zbiranja in obdelave osebnih podatkov ter načinih naslavljanja teh učinkov.

Opredeljenost nabora podatkov, upravljavcev in uporabnikov ter rokov hrambe

V oceni učinka je navedeno zgolj, da so opredeljeni nabor podatkov, upravljavcev in uporabnikov ter roki hrambe. Četudi se te vsebine nahajajo v besedilu predloga zakona **gre za sestavni del zakonodajne ocene učinka, ki mora biti vsebovan v oceni učinka**.

Kot pojasnjujemo v metodologiji je namen tega poglavja, da se opravi ustrezne premisleke in jih evidentira s ciljem, da predpis natančno določa upravljavce ali skupne upravljavce osebnih podatkov (slednje glej 26. člen Splošne uredbe), kolikor je mogoče izčrpno nabor osebnih podatkov, uporabnike, ki se jim posredujejo osebni podatki ter roke hrambe. Jasno morajo biti opredeljene različne vloge posameznih deležnikov, ki so vključeni v postopke zbiranja in obdelave, zlasti v primeru skupnega upravljanja. Morebitno povezovanje zbirk osebnih podatkov mora opredeljevati zbirke, ki se povezujejo, uporabljen povezovalni znak in namene povezovanja.

Mnenje relevantnih pooblaščenih oseb za varstvo osebnih podatkov

Iz vsake ocene učinka bi moralo biti jasno, kdo jo je pripravil, na katero verzijo predpisa oziroma projekta se nanaša in kdaj je bila opravljena, kakor tudi kakšno je bilo mnenje pooblaščene osebe za varstvo osebnih podatkov pri zavezancu. Kot smo navedli v metodologiji morajo po določbi 37. člena Splošne uredbe morajo javni organ ali telesa, razen sodišč, kadar delujejo kot sodni organ, imenovati pooblaščeno osebo za varstvo osebnih podatkov (DPO), katere naloga je med drugim svetovanje, kadar je to zahtevano, glede ocene učinka v zvezi z varstvom podatkov in spremljanje njenega izvajanja (točka c prvega odstavka 39. člena Splošne uredbe). Pridobiti in predložiti je torej treba **mnenje pooblaščene osebe na Ministrstvu za zdravje.**

Obvladovanje tveganj za pravice in svoboščine posameznika (5. poglavje)

Kot smo že izpostavili v oceni učinka izostane njen praktično najpomembnejši del - identifikacija in analiza tveganj. Razumljivo je sicer - kot navajate - da vprašanje obvladovanja tveganj (še) ni naslovljeno v celoti, saj je odgovor nanj v veliki meri odvisen od konkretnih tehničnih ukrepov javnega podjetja in njegove ocene vpliva na varstvo osebnih podatkov, vendar pa mora zakonodajna ocena učinka nasloviti tista tveganja, ki jih lahko obravnava le predlagatelj predpisa in katerih ni mogoče niti primerno prepuščati kasnejšim odločitvam in analizam bodočega izvajalca. Med takšna tveganja in ukrepe, ki bi morala biti analizirana v zakonodajni oceni učinka v konkretnem primeru sodijo vsaj naslednje točke:

- Prednosti in slabosti odločitve za predlagano organizacijsko obliko in pravno subjektiviteto predvidenega izvajalca digitalizacije zdravstva, upoštevanje izkušnje iz drugih držav;
- Tveganja povezana s hrambo podatkov na enem mestu (ki ne prinaša samo prednosti, temveč tudi nevarnosti; pomembno je opredeliti odgovornosti za kakovost podatkov in nadzorne ukrepe);
- Ustreznost predvidenih varovalk in ukrepov – ali in zakaj so predvideni ukrepi ustrezni, npr. kakšne so utemeljitve za predvidene roke hrambe, zunanji nadzor, ali je na ravni zakona mogoče predvideti logične in fizične kontrole pri vnosu podatkov, vsaj minimalne organizacijske in tehnične ukrepi za varnost podatkov, redno izvajanje notranjega nadzora ipd. (zaščitni ukrepi, ki jih za tovrstne obdelave zahteva Splošna uredba v 9. členu).

Kot smo že nekajkrat izpostavili, se nekatera od teh vsebin obravnavajo v predlogu zakona (številne ukrepe kot so psevdonimizacija, standardi zapisa podatkov itd. naj bi denimo opredelila enotna

metodološka načela), bi pa tudi te vsebine sodile v samo oceno učinka v smislu katere vsebine je primerno in katerih ni primerno prepuščati nadaljnjim oz. podzakonskim aktom.

Kot smo izpostavili v že podanih mnenjih na ocene učinka je po mnenju IP **zelo priporočljivo,** da **nad digitalizacijo zdravstva 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 oceni učinka med ukrepi pogrešamo tudi določbe o zagotovitvi ustreznega strokovnega nadzora nad odločitvami, ki se bodo sprejemale v procesu digitalizacije zdravstva. Kot je navedeno v primerjalnem pogledu 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 **v oceni učinka analizira potrebo po notranjem nadzoru pri izvajalcu centralne digitalizacije,** in sicer predlagamo, da se vključi zahtevo, da mora pooblaščena oseba za varstvo osebnih podatkov pri izvajalcu centralne digitalizacije izvajati redni letni notranji nadzor na obdelavami osebnih podatkov in o tem poročati Informacijskemu pooblaščencu – 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).

3. Zaključno

IP zaključno ugotavlja, da je priložena ocena učinka na varstvo osebnih podatkov **pomanjkljiva**, saj ne obravnava vseh področij, kjer bodo imele predlagane spremembe vpliv na raven zagotavljanja varstva osebnih podatkov. Četudi so določena vprašanja obravnavana v samem predlogu zakona, bi moralo biti v oceni učinka jasno navedeno, zakaj so bile izbrane določene rešitve in kako so bile analizirane z vidika varstva osebnih podatkov, npr. zakaj so bili izbrani takšni roki hrambe, kakšne so slabosti predlaganih rešitev in podobno. Kot smo večkrat izpostavili je namen zakonodajnih ocen učinka, da se določena tveganja in odločitve predlagatelja glede varstva osebnih podatkov objektivno analizirajo in utemeljijo že v času priprave predpisa.

Glede na številne skrbi predlagamo, da se v okviru nadaljnje priprave predloga zakona najprej bistveno dopolni ocena učinkov ob vključitvi relevantne strokovne javnosti in drugih deležnikov s področja zdravstva. Zasnova sistema centralizirane zbirke podatkov in njenega upravljavstva pa mora ustrezno nasloviti zgoraj izpostavljene pomanjkljivosti. Le z upoštevanjem teh pripomb in predlogov lahko nastane sistem in proces digitalizacije v zdravstvu, pri katerem bo zagotovljena raven varstva podatkov, kot jo posamezniki uživamo trenutno. Za nadaljnje posvetovanje smo na voljo.

S spoštovanjem,

dr. Jelena Virant Burnik,
informacijska pooblaščenka

Poslati:
- Ministrstvo za zdravje (gp.mz@gov.si);
- Ministrstvo za pravosodje (gp.mp@gov.si).