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

Številka: 007-26/2024/3
Datum: 21. 6. 2024

Urad Vlade RS za informacijsko varnost
gp.uiv@gov.si

ZADEVA: Predlog Zakona o informacijski varnosti (EVA 2023-1544-0005) – MNENJE
ZVEZA: vaše zaprosilo št. IPP 007-66/2023/43 prejeto dne 17. 5. 2024 in priloženo gradivo

Spoštovani,

na podlagi vašega zaprosila, 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) v nadaljevanju posredujemo mnenje Informacijskega pooblaščenca (IP) k Predlogu Zakona o informacijski varnosti – EVA 20234-1544-0005 (predlog ZInfV-1), ki se s pristojnostmi IP prepleta na več ravneh, pri čemer pa IP ne komentira širše ureditve področja informacijske varnosti zunaj svojih pristojnosti. Predlog ZInfV-1 se s pristojnostmi IP prepleta na področjih:

1. opredelitve novih izjem glede prostega dostopa do informacij javnega značaja;
2. urejanja obdelav osebnih podatkov zlasti v 4., 7., 12., 16., 17., 22., 28., 29. in 36. členu;
3. ureditve prenosa osebnih podatkov v tretje države;
4. nekaterih vprašanj povezanih z varnostjo osebnih podatkov npr. 21., 64. člen (zlasti z vidika določb 23. člena ZVOP-2);
5. pristojnosti in sankcioniranja kršitev varstva osebnih podatkov, ki so hkrati lahko kršitve informacijske varnosti po predlogu ZInfV-1 in na podlagi Splošne uredbe, ZVOP-2 ter Zakona o varstvu osebnih podatkov na področju obravnavanja kaznivih dejanj (ZVOPOKD) in
6. sodelovanja med različnimi pristojnimi organi po ZInfV-1 ter Splošni uredbi oz. ZVOP-2 in ZVOPOKD.

Uvodoma IP poziva, da predlagatelj v sodelovanju s strokovno javnostjo in vsemi deležniki, zlasti dodatno skrb nameni jasnejši in pravno nedvoumni ter razumljivi opredelitvi obsega področja uporabe predloga ZInfV-1 ter nabora zavezancev po tem zakonu. Glede na izkušnje IP iz prakse namreč ugotavljamo, da na tem področju prihaja do številnih nejasnosti, ki jih tudi predlagano besedilo 3. in 6. člena predloga ZInfV-1 glede na razumevanje IP v celoti ne odpravlja, saj je dikcija besedila zelo kompleksna in mestoma nejasna.

Prav tako na splošni ravni opozarjamo, da morajo biti v skladu z 38. členom Ustave RS in 6. členom ZVOP-2 nabor in namen zbiranja osebnih podatkov ter rok hrambe določeni z zakonom (to je lahko tudi predpis EU, ki ima naravo zakona) in ne zgolj s podzakonskim aktom. Iz določenih določb predloga zakona namreč izhaja, da bi lahko ta predvideval vzpostavitev nekaterih novih zbirk osebnih podatkov (torej poleg podatkov o poslovnih subjektih tudi obdelave podatkov o določljivih oz. določenih fizičnih osebah), katerih vsebine predlog ZInfV-1 ne določa oz. ne določa namena ali roka hrambe. IP zgolj iz previdnosti v zvezi s tem še poudarja, da morata biti vsaka obdelava osebnih podatkov, kot tudi njeno urejanje na zakonski ravni skladna z načelom sorazmernosti.

V nadaljevanju podajamo nekatere pripombe k posameznim členom predloga ZInfV-1.

K 4. členu

Prvi odstavek

IP izpostavlja, da pravne podlage za obdelavo osebnih podatkov načeloma (razen v primeru subjektov, za katere velja zgolj ZVOP-2, kot npr. SOVA) določajo 6. in 9. člen Splošne uredbe, ki se uporabljata neposredno, v povezavi s 6. členom ZVOP-2, oziroma 6., 7. in 8. člen ZVOPOKD, v primerih ko gre za zavezance in namene po ZVOPOKD. Za obdelavo osebnih podatkov na podlagi predloga ZInfV-1 naj bi torej primarno veljala Splošna uredbe (razen ozkih izjem oziroma zgolj v primeru pristojnih organov po ZVOPOKD in za namene po ZVOPOKD tudi zgoraj omenjeni členi tega zakona). To pomeni, da **se pravne podlage za obdelave osebnih podatkov iz točke f prvega odstavka 6. člena Splošne uredbe ne bi smelo ločeno določati z nacionalnim predpisom**, kot to izhaja iz drugega stavka prvega odstavka 4. člena predloga ZInfV-1.

Predlog prvega odstavka 4. člena namreč določa:
»*(1) Obdelava osebnih podatkov na podlagi tega zakona se izvaja skladno s predpisi, ki urejajo varstvo osebnih podatkov, ponudniki javnih elektronskih komunikacijskih omrežij ali ponudniki javno dostopnih elektronskih komunikacijskih storitev pa tudi v skladu s predpisom, ki ureja zasebnost na področju elektronskih komunikacij. Obdelava osebnih podatkov v obsegu, nujno potrebnem in sorazmernem za zagotovitev varnosti omrežij, informacijskih sistemov in informacij pomeni zakoniti interes zadevnega upravljavca podatkov.*«.

V tem smislu je odveč določba drugega stavka prvega odstavka 4. člena oz. ta celo presega pooblastila za zakonsko urejanje določena s Splošno uredbo, zato predlagamo, da se bodi črta ali bistveno dopolni.

Če je namen predlagatelja zakona, da v predlogu ZInfV-1 izrecno opredeli pravno podlago, na kateri bodo zavezanci po ZInfV-1 lahko obdelovali osebne podatke za namen zagotovitve varnosti omrežij, informacijskih sistemov in informacij, mora biti dikcija zakona temu ustrezna. Ni primeren sklic na zakonite interese iz točke f prvega odstavka 6. člena Splošne uredbe, pač pa mora zakon vsebovati določbo o (obvezni) obdelavi osebnih podatkov, skladno s točkama c in e prvega odstavka 6. člena Splošne uredbe, torej, da se osebni podatki po tem zakonu obdelujejo za namen zagotovitve varnosti omrežij, informacijskih sistemov in informacij, v obsegu, ki je nujno potreben in sorazmernem glede na ta namen. Zakon mora določati, kateri podatki se za ta namen obdelujejo in njihov rok hrambe, kot opozarjamo zgoraj.

Tretji odstavek
Predlog tretjega odstavka 4. člena določa:
»*(3) Izmenjava podatkov in informacij, ki so varovani podatek pristojnega nacionalnega organa, mora biti za potrebe izvajanja tega zakona omejena na obseg, ki je ustrezen in sorazmeren glede na namen takšne izmenjave, pri čemer se ohrani zaupnost zadevnih informacij ter zaščiti varnost in poslovni interes zadevnih subjektov. Ne glede na določbe zakona, ki ureja dostop do informacij javnega značaja, se varovani podatki pristojnega nacionalnega organa ne posredujejo javnosti. Predstojnik pristojnega nacionalnega organa podrobneje predpiše organizacijske in logično tehnične postopke ter ukrepe za določanje in varovanje varovanih podatkov pristojnega nacionalnega organa ter vodenja zbirk podatkov katerih upravljavec je pristojni nacionalni organ. Uslužbenec pristojnega nacionalnega organa mora varovati varovane podatke pristojnega nacionalnega organa tudi po prenehanju delovnega razmerja.*«.

Predlog ZInfV-1 v tem delu uvaja dodatno izjemo od prosto dostopnih informacij javnega značaja, izven sistemske ureditve, kot jo ureja ZDIJZ, pri čemer izključuje tudi možnost presoje neodvisnega državnega organa, to je IP, ki sicer v vsakem konkretnem primeru presoja, ali gre res za tovrstne varovane podatke. Določba je formulirana na način *»ne glede na določbe zakona, ki ureja dostop do informacij javnega značaja se varovani podatki pristojnega nacionalnega organa ne posredujejo javnosti«,* kar namreč pomeni, da se dostop do teh podatkov v vsakem primeru *a priori* vedno zavrne (gre torej za tako imenovano absolutno izjemo oziroma izključitev, pri kateri ne pride v poštev niti presoja po drugem odstavku 6. člena ZDIJZ, ki sicer ureja test prevladujočega interesa javnosti). Ob tem je presoja, ali gre res za tovrstne podatke, v celoti prepuščena predstojniku pristojnega nacionalnega organa, v zvezi s tem pa ni nobenega neodvisnega nadzornega mehanizma, npr. Informacijskega pooblaščenca. Predlagana rešitev tako sistemsko odstopa od vseh že doseženih in uveljavljenih standardov na področju dostopa do informacij javnega značaja. Po trenutno veljavni ureditvi narave tako varovanih podatkov (izključitev iz ZDIJZ) nimajo niti tajni podatki (vseh stopenj), niti podatki policije, SOVE in drugih varnostnih organov. Vsi navedeni organi so namreč vključeni v sistem dostopa do informacij javnega značaja.

Ob tem iz predloga zakona in obrazložitve ni razvidno, zakaj je potrebna tako stroga izjema, glede na to, da je varstvo interesov, ki jih določba zasleduje, v okviru zakonskih izjem po ZDIJZ že urejeno. IP sicer razume namen predlagatelja po varovanju podatkov organa, ki bi lahko razkrivali varnostne ranljivosti in negativno vplivali na delovanje infrastrukture in s tem posameznike. Vendar pa glede na razpoložljive informacije in omejeno obrazložitev glede potrebe po varovanju podatkov pristojnega nacionalnega organa opozarjamo, da so izjeme, na podlagi katerih dokumenti niso predmet prostega dostopa do informacij javnega značaja, že opredeljene v ZDIJZ. Glede na kontekst organ pri konkretni presoji dokumentov upošteva izjemo npr. v 1. točki 1. odstavka 6. člena ZDIJZ, kadar gre za tajne podatke na podlagi zakona, ki ureja tajne podatke; v 2. točki 1. odstavka 6. člena ZDIJZ, kadar gre za podatke, ki so opredeljeni kot poslovna skrivnost v skladu z zakonom; v 3. točki 1. odstavka 6. člena ZDIJZ, kadar gre za varovane osebne podatke; v 5. točki 1. odstavka 6. člena ZDIJZ, kadar gre za podatke, katerih razkritje bi pomenilo kršitev zaupnosti davčnega postopka ali davčne tajnosti; v 6. točki 1. odstavka 6. člena ZDIJZ, kadar gre za podatke, ki so bili pridobljeni ali sestavljeni zaradi kazenskega pregona ali v zvezi z njim, ali postopka s prekrški in bi njegovo razkritje škodovalo njegovi izvedbi; v 9. točki 1. odstavka 6. člena ZDIJZ, kadar gre za podatke iz dokumenta, ki je v postopku izdelave, in je še predmet posvetovanja v organu, njegovo razkritje pa bi povzročilo napačno razumevanje njegove vsebine; in v 11. točki 1. odstavka 6. člena ZDIJZ, kadar gre za podatek iz dokumenta, ki je bil sestavljen v zvezi z notranjim delovanjem oziroma dejavnostjo organov. To potrjuje tudi sodna praksa s tega področja. Predlagamo, da se rešitev uvajanja nove izjeme, če je to res nujno in po oceni predlagatelja v posebnih primerih res utemeljeno, v dogovoru z resornim ministrstvom, to je Ministrstvom za javno upravo, išče v okviru sistemskega zakona, to je ZDIJZ.

Ob tem še opozarjamo, da je Slovenija v letu 2023 ratificirala Konvencijo Sveta Evrope o dostopu do uradnih dokumentov, s katero morajo biti usklajeni vsi zakoni, ki posegajo v področje dostopa javnosti do informacij javnega značaja. Ta konvencija v 3. členu med drugim določa, da morajo biti omejitve pravice dostopa do informacij natančno določene z zakonom, v demokratični družbi nujne in sorazmerne s ciljem varovanja. Dostop do informacij se sicer z namenom varstva tam določenih interesom lahko omeji, vendar se dostop lahko zavrne le, če njihovo razkritje škoduje ali bi verjetno lahko škodovalo katerim koli interesom iz prvega odstavka tega člena, razen če ne prevlada javni interes za razkritje. Konvencija torej absolutnih *a priori* izključitev določenih informacij ne pozna in po naši oceni bi bila rešitev, kot je predlagana, v nasprotju s to določbo.

K 12. členu (prenos osebnih podatkov v tretje države)

IP želi glede na predvidene izmenjave osebnih podatkov, ki vključujejo prenose osebnih podatkov v tretje države izpostaviti zlasti nujnost skladnosti ureditve prenosa osebnih podatkov v tretje države s Splošno uredbo. V tem smislu predlagamo dopolnitev ustreznih določb predloga ZInfV-1 v povezavi s 46. členom Splošne uredbe in izpostavljamo, da bi bilo treba ta člen dopolniti na način, da bo jasno, kateri zaščitni ukrepi se uporabljajo za prenose osebnih podatkov v tretje države in da bo zakon v tem smislu zadostil zahtevam Splošne uredbe v situacijah, ko gre za prenose osebnih podatkov v tretje države, za katere Evropska komisija ni sprejela sklepa o ustreznosti po 45. členu Splošne uredbe.

IP sklepa, da je namera predlagatelja, bodisi uporaba pravne podlage za zagotavljanje varstva podatkov pri prenosu v tretje države z zaščitnimi ukrepi s pravno zavezujočim in izvršljivim instrumentom, ki ga sprejmejo javni organi ali telesa po točki a drugega odstavka 46. člena Splošne uredbe – ta bi moral biti opredeljen z zakonom (za katerega ni potrebno posebno dovoljenje nadzornih organov), bodisi uporaba ustreznih zaščitnih ukrepov z določbami, ki se vstavijo v upravne dogovore med javnimi organi ali telesi in v katere so vključene izvršljive in učinkovite pravice za posameznike, na katere se nanašajo podatki, na podlagi točke b tretjega odstavka 46. člena Splošne uredbe (za tak dogovor pa je potrebno posebno dovoljenje nadzornih organov, torej IP).

IP predlaga, da se upoštevajoč navedeno jasneje opredeli, za katero od situacij gre in ustrezno opredeli zahteve glede posameznih pravnih podlag za prenose v tretje države. V prvem primeru bi moral že sam zakon opredeliti vsebine varstva osebnih podatkov v tretji državi, kar je verjetno težko izvedljivo glede na naravo prenosov in glede na to, da ni vnaprej znano, za katere tretje države gre. V drugem primeru – če so torej ustrezni zaščitni ukrepi zagotovljeni z določbami, ki se vstavijo v upravne dogovore med javnimi organi ali telesi (torej npr. v ustrezen dogovor med organi v tretji državi) pa so te zahteve opredeljene šele v posameznem dogovoru. V obeh primerih pa morajo imeti posamezniki na podlagi takega dogovora na voljo izvršljive pravice in učinkovita pravna sredstva. Ne

glede na to, ali je torej namera ureditev pogojev za sprejem zaščitnih ukrepov na podlagi točke a drugega odstavka ali na podlagi točke b tretjega odstavka 46. člena Splošne uredbe ali kak tretji mehanizem pravne podlage, bi bilo treba besedilo predloga ZInfV-1 dodatno dopolniti, saj morajo taki zaščitni ukrepi zadostiti vsem zahtevam Splošne uredbe.

K 17. členu

IP predlaga, da se glede na delno prepletanje materije oz. pristojnosti dela različnih zavezancev – med zavezance, s katerimi poteka sodelovanje na nacionalni ravni na podlagi 17. člena na način rednega izmenjevanja informacij, tudi o relevantnih incidentih in kibernetskih grožnjah, na podlagi 4. točke prvega odstavka 17. člena predloga ZInfV-1 uvrsti tudi Informacijskega pooblaščenca.

K 48. členu

IP opozarja, da bi moralo biti besedilo 48. člena poleg nekaterih slogovnih popravkov in popravka napačnih sklicev na člene posameznih zakonskih določb deležno v drugem odstavku tudi vsebinskih dopolnitev zaradi pomenske nejasnosti.

48. člen predloga ZInfV-1 določa:

»*48 . člen*
(kršitve, ki pomenijo kršitve varstva osebnih podatkov)

(1) Inšpektor o obravnavi zadev iz prvega odstavka 40. člena tega zakona, katerih posledica je kršitev varstva osebnih podatkov, obvešča Informacijskega pooblaščenca brez nepotrebnega odlašanja. Za namen pravočasnega ukrepanja v smeri zagotavljanja odprave kršitev varstva osebnih podatkov inšpektor Informacijskega pooblaščenca obvešča tudi v primerih suma kršitve varstva osebnih podatkov.
(2) Kadar Informacijski pooblaščenec zaradi kršitve določbe točka (i) drugega odstavka 58. člena Uredbe (EU) 2016/679 naloži globo na podlagi zakona, ki ureja varstvo osebnih podatkov. Inšpektor poleg ukrepov nadzora, določenih določbah 1. do 8. točk prvega odstavka in drugega odstavka 42. člena tega zakona ter določb 1. do 7. točk prvega odstavka 44. člena ne naloži globe za kršitev tega zakona zaradi istega ravnanja, zaradi katerega je Informacijski pooblaščenec naložil grobo zaradi prej navedene kršitve.
(3). Kadar ima nadzorni organ, ki je pristojen v skladu z Uredbo (EU) 2016/679, sedež v drugi državi članici kot inšpektor, inšpektor obvesti Informacijskega pooblaščenca, o možni kršitvi varstva osebnih podatkov iz prvega odstavka tega člena.«.

Predlagamo, da se določba dopolni in se jasneje opredeli tudi postopek sodelovanja (npr. obveščanje s strani IP o začetku prekrškovnega postopka po drugem odstavku), v zvezi z izvajanjem drugega odstavka, in s ciljem zagotavljanja pravne varnosti opredeli z referenco na ustrezne člene nedvoumno nabor kršitev (tako kršitev Splošne uredbe kot ZVOP-2 in ZVOPOKD), ki sodijo pod domet primerov, ko inšpektor po ZInfV-1 ne bo naložil globe.

K 64. členu

Določbe prvega odstavka 23. člena ZVOP-2, na katere se nanaša 64. člen predloga ZInfV-1 se nanašajo na vprašanja širitve uporabe veljavnega Zakona o informacijski varnosti (ZInfV) in dejansko **vsebinsko posegajo v materijo veljavnega ZInfV, pri čemer deloma urejajo materijo neposredno uporabljivih določb Splošne uredbe, in sicer zlasti glede priglasitve varnostnih incidentov, v delu, ki ne predvideva specialne nacionalne ureditve.**

Veljavni prvi odstavek 23. člena ZVOP-2 določa:

»*(1) Za informacijske sisteme, v katerih:*
1. *se izvajajo obdelave osebnih podatkov, določenih v zakonih, ki urejajo področja upravnih notranjih zadev, finančne uprave, državljanstva, Slovenske obveščevalno-varnostne agencije, obrambe, zdravstvenega varstva, obveznega zdravstvenega zavarovanja, uveljavljanja pravic iz javnih sredstev ter kazenskih in prekrškovnih evidenc, ali*

2. *se obdelujejo osebni podatki več kot 100.000 posameznikov na podlagi zakona, razen obdelav osebnih podatkov iz 3. poglavja 2. dela tega zakona, ali*
3. *upravljavec ali obdelovalec kot svojo temeljno dejavnost izvaja obsežne obdelave posebnih vrst osebnih podatkov, ali*
4. *se obdeluje posebne vrste osebnih podatkov več kot 10.000 posameznikov,*

se smiselno uporabljajo določbe o varnostnih zahtevah in priglasitvi incidentov iz zakona, ki ureja informacijsko varnost, ki se nanašajo na izvajalce bistvenih storitev, če upravljavec glede teh obdelav ni dolžan izvajati ukrepov po zakonu, ki ureja informacijsko varnost.«.

64. člen predloga ZInfV-1 pa določa:

»*64. člen*
(sprememba Zakona o varstvu osebnih podatkov)

V Zakonu o varstvu osebnih podatkov (Uradni list RS, št. 163/22) se v 4. točki prvega odstavka 23. člena besedilo »izvajalce bistvenih storitev« nadomesti z besedilom »pomembne subjekte«.«.

IP glede na nabor obveznosti ne razbere, zakaj je predlagana zgolj referenca na pomembne subjekte. Upoštevajoč tudi vse zgoraj navedeno in v izogib nejasnostim glede nadzornih pristojnosti in nedopustnega poseganja v materijo Splošne uredbe IP predlaga, da se v delu, ki ga predlagatelj ocenjuje kot relevantnega, celotna materija prvega odstavka 23. člena ZVOP-2 glede priglasitve varnostnih incidentov uskladi s Splošno uredbo oz. se vsaj besedilo »*in priglasitvi incidentov«* črta iz besedila prvega odstavka 23. člena ZVOP-2.

Zahvaljujemo se vam za sodelovanje, smo na voljo za morebitna dodatna pojasnila in vas lepo pozdravljamo,

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

Pripravila:
Alenka Jerše, univ. dipl. prav.
namestnica informacijske pooblaščenke