



REPUBLIKA SLOVENIJA

INFORMACIJSKI
POOBlašČENEC

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

Številka: 07122-1/2023/3
Datum: 1. 3. 2023

Ministrstvo za gospodarstvo, turizem in šport
Kotnikova ulica 5

1000 Ljubljana

gp.mgts@gov.si

Zadeva: Mnenje glede ocene učinka na varstvo podatkov v zvezi z 12. členom Predloga zakona o spremembah in dopolnitvah Zakona o gospodarskih družbah (ZGD-1L; EVA 2023-2180-0001)

Zveza: vaš dopis št. 007-211/2022/94 z dne 13.2.2023

Spoštovani,

prejeli smo vaš dopis, s katerim ste nam v mnenje posredovali ocene učinka na varstvo podatkov v zvezi z 12. členom Predloga zakona o spremembah in dopolnitvah Zakona o gospodarskih družbah (ZGD-1L; EVA 2023-2180-0001).

* * *

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 učinka¹ 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*.

Upravljavec podatkov se mora posvetovati z nadzornim organom vedno, kadar ne najde zadostnih ukrepov za zmanjšanje tveganj na sprejemljivo raven (tj. so preostala tveganja še vedno visoka).

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

Poleg tega se mora upravljavec posvetovati z nadzornim organom vedno, kadar je to potrebno v skladu s pravom države članice in/ali kadar mora v skladu z njim pridobiti predhodno dovoljenje nadzornega organa glede obdelave za izvajanje naloge, ki jo upravljavec izvede v javnem interesu, vključno z obdelavo v zvezi s socialno zaščito in javnim zdravjem (člen 36(5)). EDPB poudarja še, da obveznost hrambe evidence ocene učinka in njenega posodabljanja ostaja, ne glede na to, ali je glede na raven preostalega tveganja posvetovanje z nadzornim organom potrebno ali ne.

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. Drugi odstavek 87. člena ZVOP-2 določa, da mora upravljavec ali obdelovalec **pred začetkom povezovanja zbirk** iz prvega odstavka istega člena izdelati oceno učinka po 35. členu Splošne uredbe in se posvetovati z nadzornim organom po 36. členu Splošne uredbe.

* * *

Na podlagi informacij, ki ste nam jih posredovali, vam v nadaljevanju na podlagi točke (a) člena 58(3), v povezavi s členoma 35 in 36 Splošne uredbe, 5. točko prvega odstavka 55. člena ZVOP-2 ter 2. členom Zakona o informacijskem pooblaščenca (ZInfP; Uradni list RS, št. 113/05, 51/07 – ZUstS-A) posredujemo naše neobvezno mnenje v zvezi s predloženo oceno učinka.

* * *

2. Pregled ocene učinka

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 treba upoštevati smiselno – če in ko jih je primerno doreči že na ravni 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 podatkov, ki bi nato morali izdelovati ločene ocene učinka (10. odstavek 35. člena Splošne uredbe oz. 3. odstavek 49. člena Zakona o varstvu osebnih podatkov na področju obravnavanja kaznivih dejanj - ZVOPOKD).

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 upravljajal, 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.

Izjemnega pomena so 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.

Predložena ocena učinka se nanaša na obdelavo podatkov v povezavi s predlogom sprememb in dopolnitev 255. člena Predloga Zakona o spremembah in dopolnitvah Zakona o gospodarskih družbah (ZGD-1L), EVA št: 2023-2180-0001 (v nadaljnjem besedilu: Predlog ZGD-1L). Kot ste pojasnili se spremembe in dopolnitve omenjenega člena predlagajo zaradi zagotovitve skladnosti z Direktivo (EU) 2019/1151 Evropskega parlamenta in Sveta z dne 20. junija 2019 o spremembi Direktive (EU) 2017/1132 glede uporabe digitalnih orodij in postopkov na področju prava družb (v nadaljnjem besedilu: Direktiva (EU) 2019/1151). Namen predlaganih sprememb in dopolnitev je zagotovitev skladnosti z Direktivo (EU) 2019/1151, splošni cilj katere je zagotoviti več digitalnih rešitev za gospodarske družbe na notranjem trgu in ki določa pravila v zvezi s spletno ustanovitvijo kapitalskih družb, registracijo podružnic in vpisom dokumentov in informacij s strani družb in podružnic.

Z namenom, da se zagotovi zaščita vseh oseb, ki sodelujejo z družbami in podružnicami ter prepreči goljufivo ravnanje ali druge zlorabe Direktiva (EU) 2019/1151 omogoča pristojnim organom, da lahko zavrnejo imenovanje osebe za opravljanje funkcije direktorja, če ima ta prepoved izrečeno tudi v drugi državi članici. Prav tako se zahteva od držav članic, da nemudoma odgovorijo na zahtevo druge države članice in zagotovijo informacije glede obstoječih prepovedi opravljanja funkcije direktorja na podlagi prava države članice, ki odgovarja na zahtevo. Zahteve za informacije in odgovori nanje se posredujejo elektronsko prek sistema povezovanja poslovnih registrov (v nadaljnjem besedilu: BRIS), ki ga v skladu z 22. členom Direktive (EU) 2017/1132 Evropskega parlamenta in Sveta z dne 14. junija 2017 o določenih vidikih prava družb (kodificirano besedilo) (v nadaljnjem besedilu: Direktiva (EU) 2017/1132) sestavljajo registri držav članic, evropska osrednja platforma in portal kot evropska elektronska točka za dostop. BRIS upravlja Evropska komisija. Upravljavec nacionalnega vozlišča BRIS v Republiki Sloveniji je Agencija Republike Slovenije za javnopravne evidence in storitve (v nadaljnjem besedilu: AJPES). Nacionalno vozlišče BRIS je celota postopkov in informacijskih rešitev, ki omogoča prejem in posredovanje podatkov ter listin in zagotavljanje javnosti določenih podatkov ter listin v okviru BRIS. Pravno podlago in podrobna pravila za delovanje BRIS poleg Direktive (EU) 2017/1132 zagotavlja Izvedbena uredba Komisije (EU) 2021/1042, ki določa pravila v zvezi s tehničnimi specifikacijami in postopki za sistem povezovanja poslovnih registrov (BRIS).

Kot ste pojasnili je bila **ocena učinka v zvezi z varstvom osebnih podatkov opravljena ob pripravi oziroma sprejemanju predloga Direktive (EU) 2019/1151 in Izvedbene uredbe Komisije (EU) 2021/1042**. Evropski nadzornik za varstvo osebnih podatkov je podal mnenje 26. 7 2018 in 10. 3. 2021. Skladno z desetim odstavkom 35. člena Splošne uredbe o varstvu podatkov v povezavi s prvim odstavkom 6. člena ocena učinka za izmenjavo podatkov prek BRIS med organi držav članic ni potrebna, vendar pa je potrebno pripraviti **oceno učinka v delu povezovanja**

nacionalnih registrov oz. pridobivanja podatkov, ki se jih nato posreduje prek BRIS drugim državam članicam. Ocena učinka in mnenje IP na oceno učinka se tako nanašata samo na omenjeni del obdelav osebnih podatkov, t.j. povezovanje zbirk osebnih podatkov v skladu z zahtevo drugega odstavka 87. člena ZVOP-2.

Pregled ocene učinka se v nadaljevanju opravi s formalnega in vsebinskega vidika.

2.2 Formalni pregled celovitosti ocene učinka

IP je najprej pregledal predloženo oceno učinka z vidika njene celovitosti skladno s členom 36(7) Splošne uredbe in priporočili EDPB, kot so navedena v Prilogi 2 smernic o ocenah učinka.

S pomočjo kontrolnega seznama za celovitost ocene učinka iz priloge 2 smernic o ocenah učinka IP ugotavlja:

✓ **Podan je sistematičen opis obdelave (člen 35(7a)):**

- upoštevani so narava, obseg, okoliščine in namen obdelave (uvodna izjava (90));
- opredeljen je nabor podatkov, upravljavci in uporabniki ter roki hrambe;
- podan je opis podatkovnih tokov in udeleženih subjektov;
- opredeljena so sredstva obdelave osebnih podatkov, kolikor je možno ob dejstvu, da tehnična rešitev še ni na voljo ().

V oceni učinka je podan sistematičen opis obdelave (člen 35(7)(a)), kakor tudi ocena nujnosti in sorazmernosti obdelave nabora osebnih podatkov (člen 35(7)(b)).

✓ **Delno so obvladovana tveganja za pravice in svoboščine posameznika:**

- Delno je podana ocena izvora, narave, posebnosti in resnosti tveganj (uvodna določba 84), pri čemer so tveganja deloma ocenjena z vidika posameznika, tako da:
 - so delno upoštevani viri tveganj;
 - so delno opredeljeni ukrepi za obvladovanje tveganj (člen 35(7d) in uvodna določba 90).

Ocena učinka glede na kontrolni seznam za celovitost ocene učinka iz priloge 2 smernic o ocenah učinka ne vsebuje:

- ukrepov, ki prispevajo k varstvu pravic posameznika:
 - pravica do seznanitve podatkov (člena 15 in 20);
 - pravica do popravka in izbrisa podatkov (členi 16, 17 in 19);
 - pravica do omejitve obdelave (členi 18, 19 in 21).

Ocena učinka ne obravnava ukrepov, ki prispevajo k informiranju posameznika o obdelavi podatkov (členi 12, 13 in 14).

Skladno z določbami člena 35 Splošne uredbe upravljavec pri izvedbi ocene učinka v zvezi z varstvom podatkov za mnenje zaprosi pooblaščen osebo za varstvo podatkov, kjer je ta imenovana. Po potrebi upravljavec glede predvidene obdelave zaprosi za mnenje posameznikov, na katere se nanašajo osebni podatki, ali njihovih predstavnikov, brez poseganja v zaščito komercialnega ali javnega interesa ali varnost dejanj obdelave.

Iz predložene ocene učinka ni razvidno, ali je bilo pridobljeno mnenje pooblaščen osebe za varstvo podatkov (ang. DPO) in kakšno je bilo njeno mnenje. Ob tem IP poudarja, da je primarno

za izvedbo ocene učinka in njeno ustreznost odgovoren lastnik ali skrbnik zadevnega procesa obdelave osebnih podatkov oziroma predlagatelj predpisa, ne pa pooblaščen osebna za varstvo podatkov. Slednja ima namreč druge naloge, med katerimi je tudi svetovanje, kadar je to zahtevano, glede izvedbe ocene učinka in pa spremljanje njenega izvajanja. IP priporoča, da pooblaščen osebna torej svetuje pristojnim službam upravljavca glede izvedbe ocene učinka, zlasti glede same metodologije izvedbe in uporabe tehničnih in organizacijskih ukrepov za varstvo pravic posameznika. Svetovanje bi moralo zajemati ves čas izvajanja ocene učinka, od same priprave na izvedbo preko dejanske izvedbe do pregleda izvedene ocene in podaje mnenja. Pooblaščen osebna mora torej sodelovati pri izvedbi ocene učinka, ni pa odgovorna za njeno izvedbo.

2.3 Vsebinski pregled ocene učinka

Pregled ocene tveganj in ukrepov za njihovo obvladovanje se izvede po temeljnih načelih varstva osebnih podatkov:

1. zakonitost, poštenost in preglednost,
2. omejitev namena,
3. najmanjši obseg podatkov,
4. točnost,
5. omejitev shranjevanja,
6. celovitost in zaupnost,
7. odgovornost.

V predloženi oceni učinka so identificirana številna tveganja, kar je vsekakor pomembno, vendar pa tveganja niso obravnavana po temeljnih načelih varstva osebnih podatkov, **kot je priporočljivo zaradi celovitosti in konsistentnosti**. Razdelitev tveganja po temeljnih načelih pripomore k temu, da se določena tveganja ne zapostavijo oz. spregledajo, prav tako velja upoštevati vse zahteve in dolžnosti, ki jih določa Splošna uredba (npr. glede evidentiranja dejavnosti, informiranja in pravic posameznikov, pogodbene obdelave ipd.). IP v nadaljevanju zato podaja pojasnila v zvezi s posameznimi temeljnimi načeli.

Glede ocene tveganj IP ugotavlja, da je v oceni učinka opredeljena metodologija ocene tveganj, ki so ovrednotena po kriteriju verjetnost in resnosti (oz. posledic), kot se tudi zahteva.

IP meni, da bi morala biti obravnavana tudi tveganja, ki so povezana z uveljavljanjem pravic posameznika (členi 15 do 22 Splošne uredbe). Tako je treba obravnavati npr. tveganje, da posamezniku ne bo mogoče omogočiti izvajanja pravice do dostopa ali izbrisa podatkov ali da to ne bo možno zagotoviti v predpisanem roku. IP ocenjuje, da bi predlagana ureditev tudi na tem področju lahko vodila v dodatna tveganja, zato svetuje, da se v oceni učinka opredelite do tega.

IP svetuje, da tveganja podrobno preučite v luči navedenih pojasnil.

2.3.1 Zakonitost, poštenost in preglednost

Z vidika upoštevanja načela zakonitosti in s tem povezanih tveganj nimamo posebnih pripomb, pri čemer poudarjamo, da nismo prejeli samega besedila predlaganega 12. člena, zato se do same vsebine zakonske določbe ne moremo opredeliti. Posebej opozarjamo na zahteve drugega odstavka 6. člena ZVOP-2, ki določa vsebine, ki naj bi jih zakon, ki predvideva obdelavo osebnih podatkov, vseboval in sicer: obdelavo osebnih podatkov, vrste osebnih podatkov, ki naj se obdelujejo, kategorije posameznikov, na katere se ti osebni podatki nanašajo, namen njihove obdelave in rok hrambe osebnih podatkov ali rok za redni pregled potrebe po hrambi določa zakon.

Če je mogoče, se v zakonu določijo tudi uporabniki osebnih podatkov, posamezna dejanja obdelave in postopki obdelave ter drugi ukrepi za zagotovitev zakonite, poštene in pregledne obdelave.

Še bolj izrecno zahtevo pa vsebuje drugi odstavek 10. člena ZVOP-2 glede varstva in obdelave osebnih podatkov o odločitvah o kazenskih obsodbah ter o kaznovanjih za prekrške in sicer mora zakon določiti namen obdelave, vključno s povezovanjem, ki mora biti v javnem interesu, vrste podatkov, ki se obdelujejo, posameznike, na katere se nanašajo osebni podatki, subjekte, katerim se osebni podatki lahko razkrijejo, namene, za katere se lahko razkrijejo, omejitve namena ter rok hrambe, vključno z ukrepi za zagotovitev zakonite in poštene obdelave.

Z vidika povezovanja zbirk je opredeljen povezovalni znak, sam zakon bo moral natančno navesti tudi zbirke osebnih podatkov, ki se bodo povezovale in sam namen povezovanja ter druge zrogarj navedene elemente.

Glede načela preglednosti pa IP opozarja predvsem, da bodo morali *upravljalci* ob izvajanju predvidenih obdelav zadevnih obdelav osebnih podatkov posameznike ustrezno obvestiti o obdelavi osebnih podatkov skladno z zahtevami 13. oz. 14. člena Splošne uredbe, kar pa najverjetneje ni potrebno posebej zakonsko urediti, ker gre za splošno zahtevo za upravljalce osebnih podatkov že po Splošni uredbi, vendar pa jo želimo posebej izpostaviti.

2.3.2 Omejitev namena

Identificirali ste številna tveganja v povezavi z načelom namenskosti (npr. zlorabe uslužbencev pri vpogledu v podatke) in tudi identificirani ukrepi so primerni.

2.3.3 Najmanjši obseg podatkov

Glede najmanjšega nabora podatkov IP ugotavlja, da so bili opravljeni ustrezni razmisleki za omejitev nabora osebnih podatkov na najmanjšega, ki je potreben. Nabor podatkov je jasno naveden in obsega točno določen nabor osebnih podatkov, prav tako je iz ocene učinkov razviden premislek o možnih drugih rešitvah, kot npr. vzpostavitev nove enotne evidence, za katero pa se niste odločili.

2.3.4 Točnost

Glede načela točnosti IP ugotavlja, da ste identificirali relevantna tveganja, zelo pomembna varovalka je tudi zahteva po uporabi tako imena in priimka kot EMŠO, kar lahko bistveno zmanjša tveganja za obdelavo napačnih osebnih podatkov ter napačne identifikacije osebe. V povezavi s tem **opozarjamo na določbo tretjega odstavka 10. člena ZVOP-2** in sicer se za izvedbo povezovanja po drugem odstavku 10. člena ZVOP-2 za državljana Republike Slovenije ali osebo s prebivališčem v Republiki Sloveniji kot identifikacijski znak uporabi enotna matična številka občana *iz kazenske ali prekrškovne evidence*.

2.3.5 Omejitev shranjevanja

Glede rokov hrambe IP meni, da so dovolj natančno opisani in ni vidi posebnih dodatnih tveganj.

2.3.6 Celovitost in zaupnost (informacijska varnost)

Glede zagotavljanja informacijske varnosti (celovitosti, zaupnosti in razpoložljivosti) predložena ocena učinka navaja določen nabor tveganj, ki se nanašajo tako na tehnične kot organizacijske vidike tveganj in predvidenih ukrepov, katerih implementacija pa se zagotavlja predvsem na ravni internih aktov posameznih udeleženih subjektov in ne na ravni zakona.

2.3.7. Odgovornost

Kot IP pojasnjuje v smernicah, načelo odgovornosti pomeni, da je upravljavec odgovoren za skladnost z ostalimi načeli in je to skladnost tudi zmožen dokazati. Načelo odgovornosti torej od upravljavcev zahteva določeno raven proaktivnosti, pripravljenosti in skrbnosti. Med temeljne mehanizme za zagotavljanje tega načela sodijo naslednje zahteve, ki jih pred upravljavce in obdelovalce postavlja Splošna uredba:

- vgrajeno in privzeto varstvo podatkov (člen 25),
- zahteve glede uporabe obdelovalcev (člen 28),
- evidenca dejavnosti obdelave oz. »katalogi« (člen 30),
- varnostni ukrepi (člen 32),
- obveščanje o varnostnih incidentih (člena 33 in 34),
- ocene učinkov v zvezi z varstvom podatkov in predhodno posvetovanje (člena 35 in 36),
- pooblaščen osebe za varstvo podatkov (členi 37, 38 in 39).

Vsi navedeni mehanizmi so preventivnega značaja, z izvedeno oceno učinka pa se preprečuje, da bi spregledali katere od naštetih obveznosti.

Glede na to, da gre za t.i. zakonodajno oceno učinka in ne za oceno učinka, ki jo je dolžan pripraviti upravljavec osebnih podatkov (35. člen Splošne uredbe), je zgoraj navedene zahteve treba upoštevati smiselno – če in ko jih je primerno doreči že na ravni zakona, sicer pa je načelo odgovornosti bolj pomembno pri ocenah učinka, ki jih pripravljajo upravljavci osebnih podatkov in ne pri zakonodajnih ocenah učinka (po tretjem odstavku 24. člen ZVOP-2).

3. Zaključno

IP zaključno poudarja, da mnenje, ki ga IP izda na podlagi 36. člena Splošne uredbe, temelji zgolj na informacijah, ki so mu bile posredovane in **ne more veljati kot zagotovilo ali potrditev nadzornega organa za varstvo osebnih podatkov, da bo zadevna obdelava zakonita**, saj se to lahko ugotovi le v okviru uradnega inšpekcijskega postopka. IP ne razpolaga z vsemi informacijami, ki so bile vhodni podatki za izdelavo ocene učinka, in kot nadzorni organ ne more prevzemati svetovalne vloge upravljavcem, kako izvesti določeno obdelavo osebnih podatkov skladno z zakonodajo, zaradi česar je odgovornost za skladnost z zakonodajo vedno v prvi vrsti na strani upravljavcev.

IP predlaga, da pri dopolnitvah oceno učinka upoštevate zgoraj navedena priporočila.

Zaključno pojasnjujemo, da je IP **pripravil osnutek metodologije za pripravo zakonodajnih ocen učinka v zvezi varstvom osebnih podatkov**, ki smo jo posredovali Ministrstvu za javno upravo, trenutno pa še ne razpolagamo z informacijami, ali je bila predlagana metodologija tudi sprejeta v okviru Izvajanja projekta ePredpisov - Metodologije za oceno učinkov na različna družbena področja.

Predlog metodologije IP je na voljo na povezavi https://www.ip-rs.si/fileadmin/user_upload/Pdf/pripombe/2022/MJU_metodologija%20ocene%20u%C4%8Dinkov_jul2022_AJ_AT_%C4%8Distopis.pdf, do nadaljnjih informacij tako **predlagamo, da pri pripravi bodočih zakonodajnih ocen učinkov v zvezi z varstvom osebnih podatkov uporabljate predlagano metodologijo**, ki je bolj prilagojena zakonodajnim ocenam učinka kot ocenam učinka, ki jih pripravljajo upravljavci osebnih podatkov.

Prav tako opozarjamo, da izdelava mnenja na oceno učinka terja dovolj časa – po določbi drugega odstavka 36. člena Splošne uredbe **nadzorni organ izdela pisno mnenje v roku do osmih tednov po prejemu zahteve za posvetovanje**, kar se lahko ob upoštevanju kompleksnosti predvidene obdelave podaljša za nadaljnjih šest tednov, zato prosimo, da v bodoče upoštevate omenjene omejitve, pri čemer se bomo potrudili mnenja izdajati v krajših rokih in z upoštevanjem nujnosti.

Mnenje pošiljamo v vednost Ministrstvu za pravosodje, s katerim ste sodelovali pri pripravi ocene učinka.

S spoštovanjem,

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

Pripravi:

mag. Andrej Tomšič,
namestnik informacijske pooblaščenke

Poslati:

- naslovniku (e-pošta);
- v vednost: Ministrstvo za pravosodje (gp.mp@gov.si); Peter Pavlin - peter.pavlin@gov.si).