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

Izdajatelj: Republika Slovenija
Podpisnik: Andrej Tomšič
Potek veljavnosti: 25.11.2028
Ref. št. dokumenta: 07122-1/2025/53
Čas podpisa: 14:01, 31.07.2025
Št. cert: 62 4b 11 71 00 00 00 00 57 2a e9 d5

Številka: 07122-1/2025/53
Datum: 31. 7. 2025

MINISTRSTVO ZA ZUNANJE IN EVROPSKE ZADEVE
DIREKTORAT ZA MEDNARODNO PRAVO IN ZAŠČITO INTERESOV
SEKTOR ZA MEDNARODNO PRAVO
omejevalni-ukrepi.mzez@gov.si

Zadeva: Mnenje glede ocena učinka glede varstva osebnih podatkov v zvezi z Zakonom o omejevalnih ukrepih, ki jih Republika Slovenija uvede ali izvaja skladno s pravnimi akti in odločitvami, sprejetimi v okviru mednarodnih organizacij (Uradni list RS, št. 127/06 in 44/22)

Zveza: Vaš dopis z dne 8. 7. 2025

Spoštovani,

prejeli smo vaš dopis, s katerim ste nam v mnenje posredovali oceno učinkov v zvezi glede varstva osebnih podatkov v zvezi z vzpostavitvijo zbirke podatkov po Zakonu o omejevalnih ukrepih, ki jih Republika Slovenija uvede ali izvaja skladno s pravnimi akti in odločitvami, sprejetimi v okviru mednarodnih organizacij (Uradni list RS, št. 127/06 in 44/22; ZOUPAMO), ter v skladu z Uredbo o zbirki podatkov o omejevalnih ukrepih (Uradni list RS, št. 97/24).

* * *

1. Uvodoma

Informacijski pooblaščenec (v nadaljevanju: IP) pojasnjuje, da je po določbi prvega odstavka 35. 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 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 (sedmi odstavek 35. člena). 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 prvega odstavka 36. člena Splošne uredbe ter uvodnih izjav (84) in (94) obdelava nadaljuje brez posvetovanja z nadzornim organom.

IP pojasnjuje, da je po določbi drugega odstavka 36. člena Splošne uredbe nadzorni organ v roku do osmih tednov po prejemu zahteve za posvetovanje pisno svetuje upravljavcu, kadar je ustrezno, pa tudi obdelovalcu, in lahko uporabi katero koli pooblastilo iz člena 58. To obdobje se lahko ob upoštevanju kompleksnosti predvidene obdelave podaljša za nadaljnjih šest tednov.

* * *

Na podlagi informacij, ki ste nam jih posredovali, vam v nadaljevanju na podlagi točke (a) tretjega odstavka 58. člena, v povezavi s 35. in 36. členom Splošne uredbe, 5. točko prvega odstavka 55. člena Zakona o varstvu osebnih podatkov (Uradni list RS, št. 163/22, 40/25 – ZInfV-1; 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.

* * *

2. Pregled ocene učinka

Kot ste pojasnili se ustanavlja **nova zbirka podatkov o omejevalnih ukrepih** za potrebe vodenja postopkov na podlagi Zakona o omejevalnih ukrepih, ki jih Republika Slovenija uvede ali izvaja skladno s pravnimi akti in odločitvami, sprejetimi v okviru mednarodnih organizacij (Uradni list RS, št. 127/06 in 44/22; v nadaljnjem besedilu: ZOUPAMO) ter mednarodne izmenjave podatkov v zvezi z izvajanjem omejevalnih ukrepov, na podlagi 4. člena ZOUPAMO. V dosedanji praksi se potreba po predpisu za vzpostavitev zbirke v elektronski obliki ni pokazala, saj naj bi bilo tovrstnih podatkov na podlagi predpisov o omejevalnih ukrepih sorazmerno malo, Ministrstvo za zunanje in evropske zadeve (v nadaljnjem besedilu: MZEZ) pa je kot navajate imelo zadostno podlago za zbiranje podatkov v samem ZOUPAMO. Z uvedbo omejevalnih ukrepov EU v zvezi z rusko agresijo na Ukrajino se je obseg podatkov precej povečal, prav tako obseg obveznosti poročanja institucijam EU na podlagi predpisov EU, zato je smiselno zbiranje podatkov sistemsko urediti z elektronsko zbirko podatkov, ki bo omogočila bolj sistematično in pregledno obravnavanje ter uporabo podatkov v zvezi z izvajanjem omejevalnih ukrepov.

2.1 Splošne ugotovitve

IP ugotavlja, da gre za **projektno** oceno učinka in ne za zakonodajno oceno učinka. Gre namreč za zbirko, ki je že določena v zakonodaji in ne za določanje pravne podlage v zakonu

[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

za novo zbirko. Razlike med t.i. zakonodajnimi in projektnimi ocenami učinka glede varstva osebnih podatkov smo pojasnili na posebni podstrani o ocenah učinka, ki je je dostopna na:

https://www.ip-rs.si/zakonodaja/reforma-evropskega-zakonodajnega-okvira-za-varstvo-osebnih-podatkov/klju%C4%8Dna-podro%C4%8Dja-uredbe/ocena-u%C4%8Dinka-v-zvezi-z-varstvom-podatkov/#a4.

Na navedeni spletni strani so dostopne tudi **smernice IP o ocenah učinka**[2], za katere priporočamo, da jih upoštevate pri izdelavi ocen učinka.

Projektne ocene učinka niso obvezne za vsako obdelavo osebnih podatkov, kakor tudi ne posvetovanje z nadzornim organom za varstvo osebnih podatkov, zato bi MZEZ kot upravljavec zbirke moral **najprej presoditi, ali je ocena učinka obvezna ali ne**, česar v prejeti oceni učinka nismo zasledili.

Pri ugotavljanju, **ali je ocena učinka obvezna** ali ne, mora upravljavec preveriti izpolnjevanje kriterijev po 35. členu Splošne uredbe ter glede **na seznam dejanj, ki terjajo izvedbo učinka** in ga je na podlagi četrtega odstavka 35. člena Splošne uredbe sprejel IP[3] ter potrdil Evropski odbor za varstvo podatkov.

Kot smo pojasnili se lahko v določenih primerih obdelava nadaljuje brez posvetovanja z nadzornim organom. Ne glede na navedeno podajamo mnenje na prejeto oceno učinka.

***

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 sedmim odstavkom 36. člena Splošne uredbe in priporočili EDPB, kot so navedena v Prilogi 2 smernic o ocenah učinka.

S pomočjo navedenega seznama ugotavljamo, da **niso izpolnjene naslednje zahteve glede celovitosti ocene** učinkov, kot izhajajo iz Priloge 2 smernic o ocenah učinka:

- Opredeljenost ukrepov za zagotavljanje skladnosti, ki vključujejo:
  - ukrepe, ki prispevajo k varstvu pravic posameznika:
    - informiranje posameznika o obdelavi podatkov (členi 12, 13 in 14);

[2] https://www.ip-rs.si/publikacije/priro%C4%8Dniki-in-smernice/smernice-po-splo%C5%A1ni-uredbi-o-varstvu-podatkov-gdpr/smernice-ocene-u%C4%8Dinkov-na-varstvo-osebnih-podatkov

[3] https://www.ip-rs.si/fileadmin/user_upload/Pdf/Ocene_ucinkov/Seznam_dejanj_obdelav_osebnih_podatkov__za_katere_velja_zahteva_po_izvedbi_ocene_ucinka_v_zvezi_z_varstvom_osebnih_podatkov.pdf

- pravica do seznanitve in prenosljivosti podatkov (člena 15 in 20);
- pravica do popravka in izbrisa podatkov (člena 16, 17 in 19);
- pravica do ugovora in omejitve obdelave (členi 18, 19 in 21).

Glede mnenja posameznikov oziroma predstavnikov posameznikov, kjer je to primerno, ste pojasnili, da od posameznikov oz. posameznic niste pridobivali mnenj, saj gre zgolj za izvedbo že sprejetega in usklajenega zakona ter za učinkovito izvajanje omejevalnih ukrepov, zato ste ocenili, da pridobitev ostalih mnenj v tem primeru ni potrebna.

IP dalje ugotavlja, da je ocenjena verjetnost in resnost identificiranih tveganj, **ni pa opredeljena metodologija za izračun skupnega tveganja**, kar je pomemben formalni del ocene učinka na varstvo osebnih podatkov. Prav tako priporočamo, da se oceni raven tveganj *po izvedenih ukrepih*.

Več informacij o metodologiji za obravnavo tveganj je na voljo v smernicah IP o ocenah učinka (str. 20).

Iz prejete ocene učinka ni razvidno **mnenje pooblaščene osebe za varstvo osebnih podatkov**, kar mora prav tako biti sestavni del ocene učinka, ko je pri zavezancu takšna pooblaščena oseba imenovana. V spremnem dopisu, s katerim ste nam posredovali oceno učinka, je sicer navedeno, da je oceno učinkov pregledala tudi DPO na MZEZ, ki vam je podala pripombe, ki ste jih upoštevali. Priporočamo, da mnenja pooblaščene osebe v bodoče priložite ocenam učinka, ki nam jih pošiljate v mnenje.

V oceni učinka so opredeljena tveganja (skupaj 4) in opisani ukrepi za njihovo obvladovanje, pri čemer pa opozarjamo predvsem na:

a. strukturiranje in obravnavo tveganj po temeljnih načelih varstva osebnih podatkov ter na
b. čim bolj konkretizirane opredelitve tveganj.

Ocena tveganja se priporočljivo izvede po temeljnih načelih varstva osebnih podatkov. Ključni deli ocene tveganj naj bi sledili (vsem) temeljnim načelom varstva osebnih podatkov, kot jih določa 5. člen Splošne uredbe, zato je priporočljivo, da pri vsakem tveganju presodite, s katerim temeljnim načelom varstva osebnih podatkov je posamezno tveganje povezano. Več priporočil v zvezi s tem podajamo v vsebinskem pregledu ocene učinka v nadaljevanju.

Glede **konkretizacije tveganj** pa opozarjamo, da so v prejeti oceni učinka **tveganja preveč široko opredeljena** (npr. »izbris podatkov«, »razkritje podatkov«), da bi lahko natančno opredelili, kakšna je resnost uresničitve tveganja in kakšne bodo posledice za posameznike ali upravljavca, s tem pa tudi ovirajo natančno in učinkovito opredelitev ukrepov za obvladovanje tveganj. Izbris ali razkritje podatkov lahko povzročijo različni dejavniki (bodisi da gre za človeško napako, za namerno dejanje, za tehnično okvaro, za varnostno pomanjkljivost itd.), zato so tudi ukrepi, s katerimi obvladujejo tveganja lahko različni. **Konkretizacija in razdelitev tveganj pripomore k boljšemu zavedanju tveganj in k boljšemu obvladovanju tveganj**. V zvezi s tem vas napotujemo na **infografiko IP**, ki vsebuje določena **priporočila glede obravnave tveganj**:

https://www.ip-rs.si/fileadmin/user_upload/Pdf/infografike/Infografika%20-%20Ustreznost%20DPIA%20in%20priporo%C4%8Dila.pdf.

Podrobnejša priporočila za ocenjevanje resnosti tveganj podajamo v nadaljevanju v razdelku 2.3.4.

IP priporoča doslednejše upoštevanje smernic in mnenj IP in EDBP ter uporabo kontrolnega seznama za celovitost ocene učinkov.

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 **tveganja niso obravnavana po temeljnih načelih, kot je priporočljivo zaradi celovitosti in konsistentnosti**. Razdelitev tveganj po temeljnih načelih pripomore k temu, da se določena tveganja ne zapostavijo oziroma spregledajo, prav tako velja upoštevati vse zahteve in dolžnosti, ki jih določata Splošna uredba (npr. glede evidentiranja dejavnosti, informiranja in pravic posameznikov, pogodbene obdelave ipd.) in ZVOP-2. IP v nadaljevanju zato podaja pojasnila v zvezi s posameznimi temeljnimi načeli.

2.3.1 Zakonitost, poštenost in preglednost

Z vidika načela zakonitosti niste identificirali posebnih tveganj, kar je razumljivo glede na to, da ZOUPAMO precej natančno opredeljuje ključne elemente obdelave osebnih podatkov.

Glede načela **preglednosti** ste navedli, da so v 4. členu ZOUPAMO »*določeni načini zbiranja podatkov, natančneje, določeno je, da MZEZ pridobiva podatke neposredno od posameznika ali pravne osebe, od oseb z dostopom ali iz zbirk upravljavcev, pri čemer posameznikov ali pravnih oseb, na katere se podatki nanašajo, ni treba predhodno seznaniti z obdelavo njihovih podatkov*«, pri čemer določbe, da posameznikov ali pravnih oseb, na katere se podatki nanašajo, ni treba predhodno seznaniti z obdelavo njihovih podatkov sami ne zasledimo v ZOUPAMO, temveč drugi odstavek 5. člena določa, da **je treba fizično osebo**, o kateri so bili podatki zbrani brez njene vednosti in niso bili izbrisani, **o pravici do seznanitve z lastnimi osebnimi podatki obvestiti** v treh mesecih od prenehanja veljavnosti omejevalnih ukrepov skladno s 3. členom tega zakona.

Posledično menimo, da bi morali **obravnavati tveganje ustreznosti in celovitosti informacij za posameznike** po 12., 13. in 14. členu Splošne uredbe, glede same opredelitve tveganj pa obravnavati vsaj naslednja tveganja:

- tveganje, da informacije za posameznike ne bodo podane v jedrnati, pregledni, razumljivi in lahko dostopni obliki ter jasnem in preprostem jeziku in skladno z zahtevami 12. člena Splošne uredbe;
- tveganje, da informacije za posameznike ne bodo celovite skladno z zahtevami 13./14. člena Splošne uredbe.

Opozarjamo tudi, da Splošna uredba od upravljavcev ne zahteva zgolj določenih vsebinskih elementov informiranja posameznika (13. člen), temveč do njih postavlja tudi **zahteve glede načina informiranja** (12. člen); v EU so že primeri izrečenih kazni zaradi kršitev 12. člena Splošne uredbe torej zahtev glede jasnosti, preglednosti in razumljivosti informacij za posameznike.

Več informacij o informiranju posameznikov, vključno z (neobveznim) vzorcem lahko najdete na spletni strani:

https://www.ip-rs.si/zakonodaja/reforma-evropskega-zakonodajnega-okvira-za-varstvo-osebnih-podatkov/klju%C4%8Dna-podro%C4%8Dja-uredbe/obve%C5%A1%C4%8Danje-posameznikov-o-obdelavi-osebnih-podatkov.

2.3.2 Omejitev namena

Glede tega načela IP meni, da bi bilo poleg ukrepov, ki ste jih že predvideli, kot so omejevanje in beleženje dostopov, predvideti tudi druge možne ukrepe, kot so navedeni na infografiki IP glede obvladovanja neupravičenih vpogledov v osebne podatke:

https://www.ip-rs.si/fileadmin/user_upload/Pdf/infografike/INFOGRAFIKA_Kako_prepreciti_neupravicene_vpoglede_v_osebne_podatke.pdf.

2.3.3 Najmanjši obseg podatkov

Glede načela najmanjšega obsega podatkov nimamo posebnih pripomb, glede na to, da nabor osebnih podatkov določa ZOUPAMO.

2.3.4 Točnost

Glede načela točnosti ni identificirano nobeno tveganje, predvideli ste, da bodo pristojni organi, ki bodo imeli dostop do zbirke, opozorjeni, da ob dostopanju do zbirke hkrati tudi pregledajo že vnesene podatke in jih po potrebi popravijo oz. izbrišejo. Prav tako bodo zavezani, da vnesejo spremembe, ki jih zaznajo pri svojem delu, v zbirko podatkov, in o tem obvestijo ostale člane SKSOU. Na te obveznosti opozarjate tudi v dokumentu, ki ste ga pripravili za namen

sledljivosti dostopanja do zbirke podatkov in v katerega se mora vsaka pooblaščena oseba vpisati vsakič, ko dostopa do zbirke.

Kot tudi na splošno ugotavljamo, pa se v prejetih ocenah učinka v grobem **posplošuje vidik resnosti tveganja** kot npr. »kršitev varstva osebnih podatkov« ali pa pogosto le z opredelitvijo ravni brez podrobnejše obrazložitve (npr. majhna/srednja/visoka), zato menimo, da **bi bilo primerno pri vseh tveganjih vidik resnosti natančneje analizirati.** Pri ocenjevanju resnosti je koristno upoštevati tako posledice za posameznike, katerih osebni podatkov bodo obdelovalni, kot posledice za upravljavca, ki ima dolžnosti zagotavljanja ustreznega varstva osebnih podatkov. Eden od bolj oprijemljivih kriterijev, ki se ga lahko posluži pripravljavec ocene učinka, je ocena, ali bi uresničitev tveganja predstavljala kršitev, za katere so po Splošni uredbi predvidene nižje (četrti odstavek 83. člena Splošne uredbe) ali višje kazni (peti odstavek 83. člena Splošne uredbe).

Nižje kazni so predvidene za kršitve:

a) obveznosti upravljavca in obdelovalca v skladu s členi 8, 11, 25 do 39 ter 42 in 43;
b) obveznosti organa za potrjevanje v skladu s členoma 42 in 43;
c) obveznosti organa za spremljanje v skladu s četrtim odstavkom členom 41. člena Splošne uredbe.

Višje kazni pa so predvidene za kršitve:

a) osnovnih načel obdelave, vključno s pogoji za privolitev, v skladu s členi 5, 6, 7 in 9;
b) pravic posameznika, na katerega se nanašajo podatki, v skladu s členi 12 do 22;
c) prenosi osebnih podatkov uporabniku v tretji državi ali mednarodni organizaciji, v skladu s členi 44 do 49;
d) katere koli obveznosti v skladu s pravom države članice, sprejete na podlagi poglavja IX;
e) ki pomenijo neupoštevanje odredbe ali začasne ali dokončne omejitve obdelave ali prekinitve prenosa podatkov, ki jo izda nadzorni organ v skladu z drugim odstavkom 58. člena ali nezagotovitev dostopa, s čimer se krši prvi odstavek 58. člena Splošne uredbe.

Podobno je smiselno upoštevati možne višine kazni, kot jih določa ZVOP-2.

Poleg višin potencialnih kazni pa se lahko pri ocenjevanju resnosti tveganj upošteva še naslednje elemente:

- možnost diskriminatornih posledic za posameznike[4] na podlagi rasnega ali etničnega porekla, političnega mnenja, vere ali prepričanja, članstva v sindikatu, genskega ali zdravstvenega stanja, spolne usmerjenosti ali učinki, ki privedejo do ukrepov, ki imajo takšne posledice (uvodna določba št. 71);
- ocena, ali gre za takšno tveganje za pravice in svoboščine posameznika, ki bi lahko povzročilo fizično, premoženjsko in ali nepremoženjsko škodo, zlasti:
    - kadar obdelava lahko privede do diskriminacije, kraje ali zlorabe identitete, finančne izgube, okrnitve ugleda, izgube zaupnosti osebnih podatkov, zaščitenih s poklicno molčečnostjo, neodobrene reverzije psevdonimizacije ali katere koli druge znatne gospodarske ali socialne škode;

[4] V tem delu je pomembne vidike glede na konkretno obdelavo posebej označil IP.

- kadar bi bile posameznikom, na katere se nanašajo osebni podatki, lahko odvzete pravice in svoboščine ali bi jim bilo preprečeno izvajanje nadzora nad njihovimi osebnimi podatki;
- kadar se obdelujejo osebni podatki, ki razkrivajo rasno ali etnično poreklo, politična mnenja, veroizpoved ali filozofsko prepričanje ali članstvo v sindikatu, ter obdelovanje genskih podatkov ali podatkov v zvezi z zdravjem ali podatkov v zvezi s spolnim življenjem ali kazenskimi obsodbami in prekrški ali s tem povezanimi varnostnimi ukrepi,
- kadar se vrednotijo osebni vidiki, zlasti analiziranje ali predvidevanje vidikov, ki zadevajo uspešnost pri delu, ekonomski položaj, zdravje, osebni okus ali interese, zanesljivost ali vedenje, lokacijo ali gibanje, da bi se ustvarili ali uporabljali osebni profili,
- kadar se obdelujejo osebni podatki ranljivih posameznikov, zlasti otrok;

- ali kadar obdelava vključuje veliko število osebnih podatkov in zadeva **veliko število posameznikov**, na katere se nanašajo osebni podatki (uvodna določba št. 75).

Glede na uvodno določbo št. 76 Splošne uredbe bi bilo tako verjetnost kot resnost tveganja za pravice in svoboščine posameznika, na katerega se nanašajo osebni podatki, treba **ugotavljati glede na vrsto, obseg, okoliščine in namene obdelave**. Tveganje bi bilo treba oceniti na podlagi objektivne ocene, s katero se določi, ali dejanja obdelave podatkov pomenijo tveganje ali veliko tveganje.

Kot dodatne možne elemente ocene predlagamo tudi naslednje:

- ali bi uresničitev tveganja za posameznika (in/ali za organizacijo) pomenila trajne/nepopravljive posledice;
- ali bi uresničitev tveganja imela resne posledice ne samo za posameznika temveč tudi za druge, z njim povezane posameznike (npr. sorodnike, partnerje, ostale udeležene v določeni socialno ekonomski skupini ali združenju ipd.);
- z vidika organizacije: ali bi uresničitev tveganja imela visoke posledice z vidika potrebnih popravljalnih ukrepov ter finančnih in nefinančnih posledic za organizacijo (npr. izguba ugleda, zaupanja) ter trajnost takšnih posledic.

Na podlagi izkušenj iz prakse posebej opozarjamo na podrobno opredelitev resnosti tveganj zlasti pri načelu točnosti podatkov, saj se izkaže, da imajo ravno kršitve načela točnosti (poleg načela zakonitosti) za posameznike lahko najtežje posledice. V zadevnem primeru sicer po našem mnenju ne gre za takšne obdelave, kjer so načelo točnosti in z njim povezana tveganja bolj izpostavljena, temveč vas na zgoraj izpostavljeno opozarjamo predvsem **z vidika priprave bodočih ocen učinka**.

2.3.5 Omejitev shranjevanja

Glede omejitve shranjevanja ste navedli, da v zakonu in v uredbi ni predvideno oblikovanje varnostne kopije, kar po naši oceni ni bistveno. V zakonodaji namreč redko zasledimo izrecne določbe glede možnosti ali zahtev po oblikovanju varnostnih kopij, ki pa sodijo med klasične varnostne ukrepe, katerih bi se moral poslužiti upravljavec ne glede na to, da to ni izrecno

urejena v zakonski podlagi. Opredeliti je torej treba kako in kdaj se izvaja varnostno kopiranje, da ne pride do izgube podatkov, kar pa bi bilo najbolj primerno obravnavati pri načelu varnosti podatkov. Varnostno kopiranje naslavlja predvsem tveganje nepooblaščenega brisanja podatkov pred potekom roka za hrambo, nasloviti pa je treba tudi tveganja prepoznega izbrisa oziroma prekoračitve roka hrambe, za kar so možni različni vzroki.

V tej luči opozarjamo na določbo 43. člena ZVOP-2, ki v drugem odstavku določa, da upravljavec ob upoštevanju narave obdelovanih podatkov in tveganj občasno in na dokumentiran način preverja, ali se upoštevajo določbe prvega odstavka. Posledično predlagamo, da se v oceni učinka kot predvidene ukrepe za zmanjševanje tveganj navede **redno in dokumentirano preverjanje določenosti in upoštevanja rokov hrambe in kdo ta ukrep izvede oziroma izvaja**. Izraz »*dokumentirano*« je treba razumeti, da ob tem nastane pisna sled, kot je zapisnik ali poročilo; ta naloga lahko sodi med naloge pooblaščene osebe za varstvo osebnih podatkov, ni pa to nujno.

2.3.6 Celovitost in zaupnost (informacijska varnost)

Glede postopkov in ukrepov za varnost podatkov ste med drugim pojasnili, da bo zbirka osebnih podatkov vodena kot zbirka tabel v programu Microsoft Office Excel, pri čemer ste navedli, da čeprav neposredno sledenje spremembam v zbirki ni mogoče, sistem omogoča identifikacijo uporabnika, ki dostopa do zbirke, ter evidentiranje časa dostopa (sistem za pregled spletnega prometa). V zvezi s tem pojasnjujemo, da se da tudi v orodju MS Excel zagotoviti osnovno raven sledljivosti, t.j. sledljivost vnosov, sprememb in izbrisov podatkov s klasično funkcionalnostjo »sledi spremembam« (angl. track changes), ki pa seveda mora biti vklopljena in se lahko (morebitni izklop) tudi zaščiti z geslom.

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),
- pooblaščene 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.

Posebno točko ocene učinkov mora predstavlja tudi opredelitev ukrepov, ki prispevajo k varstvu pravic posameznika. Navedena tveganja niso analizirana, zato priporočamo, da natančno preverite, do uveljavljanja katerih pravic je posameznik dejansko upravičen in do katerih ne in analizirate tudi tveganja v povezavi z uresničevanjem pravic posameznika.

Glede tveganj v povezavi s pravicami posameznika predlagamo, da v sklopu možnih ukrepov predvidite tudi natančno opredelitev odgovorne osebe oziroma oseb, ki bodo obravnavale prejete zahtevke posameznikov ter njihovo ustrezno ozaveščenost oziroma poznavanje vsebine pravic in postopkov obravnave zahtevkov za uresničevanje pravic, kot je med drugim ustrezno zavarovanje podatkov, ki so predmet postopka (21. člen ZVOP-2). Pomembno je, da so jasno določene odgovornosti v teh primerih, da osebe, ki bodo reševale zahtevke, poznajo vsebino pravic posameznika in potrebne postopke. Prav tako je pomemben element sama tehnična izvedljivost v ustreznih časovnih okvirih, saj ni nujno, da je zahteva posameznika tudi s tehnično-izvedbenega vidika enostavno in pravočasno izvedljiva.

3. Zaključno

IP ugotavlja, da ima prejeta ocena učinka številne pomanjkljivosti, zato predlagamo, da upoštevate naše mnenje s priporočili in opozorili glede možnih izboljšav.

IP zaključno poudarja, da mnenje, ki ga IP izda na podlagi člena 36 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 učnika, 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.

S spoštovanjem,

dr. Jelena Virant Burnik,
informacijska pooblaščenka

Pripravil:
mag. Andrej Tomšič,
namestnik informacijske pooblaščenke

Poslati:
- naslovniku, po e-pošti.