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

Številka: 07122-1/2023/32
Datum: 16. 5. 2023

MNZ RS
Štefanova ulica 2
1501 Ljubljana

gp.mnz@gov.si

Zadeva: Mnenje glede ocene učinka na varstvo podatkov v zvezi z avtomatiziranim pridobivanjem podatkov o obdelavi podatkov oseb

Zveza: Vaš dokument št.: 007-39/2021/141 (146-01) z dne 19. 4. 2023

Spoštovani,

prejeli smo vaš dopis, s katerim ste nam v mnenje posredovali oceno učinka na varstvo podatkov v zvezi z avtomatiziranim pridobivanjem podatkov o obdelavi podatkov oseb v okviru predloga Zakona o spremembah in dopolnitvah Zakona o nalogah in pooblastilih policije (ZNPPol; EVA 2020-1711-0001).

* * *

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.

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). Poleg tega se mora upravljavec posvetovati z nadzornim organom vedno, kadar je to potrebno v skladu s

[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

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 (peti odstavek 36. člena). 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.

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.

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 58. člena, v povezavi s 35. in 36. členom Splošne uredbe, 5. točko prvega odstavka 55. 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.

* * *

2. Pregled ocene učinka

2.1 Splošne ugotovitve

Predložena ocena učinka se nanaša na obvladovanje tveganj za posamezne kategorije oseb, zajete v 23. členu ZNPPol in 66. členu Zakona o organiziranosti in delu v policiji (v nadaljnjem besedilu: ZODPol), in oseb, ki so na podlagi Zakona o zaščiti prič (v nadaljnjem besedilu: ZZPrič) vključene v program zaščite prič, saj do njihovih osebnih podatkov, na primer podatkov o prebivališču, vozilu, ki ga uporabljajo, ter do slik iz osebnih dokumentov lahko dostopa vedno večje število uporabnikov storitev, ki imajo na podlagi različnih zakonov dovoljenje za obdelovanje osebnih podatkov (na primer nosilci javnih pooblastil).

Kot je pojasnjeno se z dostopi do osebnih podatkov ogroženih uslužbencev policije in oseb, ki pri svojem delu uporabljajo prirejeno identiteto, tako za izdelavo oblikovane identitete (23. člen ZNPPol) kot v fazi uporabe prirejene identitete v skladu s 155.a členom Zakona o kazenskem postopku (v nadaljnjem besedilu: ZKP) ali 6. člena ZZPrič, lahko ogrozi varnost teh oseb, kar je bilo v preteklosti že zaznano. Osebe z dostopom do evidenc upravnih notranjih zadev in drugih evidenc so preverjale osebne podatke tajnih delavcev in te podatke sporočale kriminalnim združbam, s čimer so ogrozile življenja ne le tajnih delavcev, temveč tudi njihovih družin. Policija je zaznala tudi, da so zaposleni na tehničnih pregledih, ki zaradi narave svojega dela lahko dostopajo do evidenc, večkrat neupravičeno vpogledovali v podatke o lastništvu vozil, med drugim tudi vozil, ki so jih za izvajanje prikritih metod dela uporabljali tajni delavci, ali pa vozil, ki so se uporabljala za izvajanje prikritih preiskovalnih ukrepov oziroma za prevoze varovanih oseb na podlagi Uredbe o varovanju določenih oseb, prostorov, objektov in okolišev objektov, ki jih varuje policija.

V skladu s predlagano ureditvijo bi bila policija v trenutku obdelave določenega osebnega podatka ogrožene osebe v posamezni evidenci obveščena o nazivu državnega organa oziroma nosilca javnega pooblastila, času obdelave ter imenu in priimku osebe, ki v določenem trenutku obdeluje podatke ogrožene osebe ali vozila, ki ga ima ta oseba v uporabi, in bi s tem ob sočasnem izvajanju drugih ukrepov lahko nemudoma začela zagotavljati njeno osebno varnost. Predlog zakona uporablja izraz »obdelava«, čeprav bo v praksi šlo za obveščanje o vpogledih v osebne podatke kot delu obdelave. Policija bi bila torej avtomatično obveščena o posameznem vpogledu v osebne podatke ogrožene osebe in ne bi sama vpogledovala v te podatke. Po prejemu posebnega avtomatiziranega obvestila bi policija vpogled preverila z zbiranjem obvestil, tudi pri samem organu, in sicer z izpisom dnevnika obdelav oziroma s pogovorom s predstojnikom posameznega organa, hkrati pa bi začela izvajati preventivne ukrepe, predvidene za zagotavljanje osebne varnosti ogroženih oseb.

Policija torej do same vsebine posameznih evidenc ne bi dostopala oz. do konkretnih osebnih podatkov oziroma vsebine vpogleda organa, ampak bi bila v primeru zadetka le obveščena o tem, da se je vpogledovalo v osebne podatke uporabnika prirejene identitete, ogroženega uslužbenca policije ali zaščitene priče, k čemur pa bodo te osebe dale soglasje.

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 *smiselno* skladno s sedmim odstavkom 35. člena Splošne uredbe.

IP ugotavlja, da gre za zakonodajno ocena učinka, ki sicer sledi *Smernicam za presoje vplivov na zasebnost pri uvajanju novih policijskih pooblastil*[2], ki jih je leta 2014 izdal Informacijski pooblaščenec, ne sledi pa novi prilagojeni metodologiji za pripravo zakonodajnih ocen učinka v zvezi varstvom osebnih podatkov za učinkovito izvajanje 24. člena ZVOP-2.

IP pojasnjuje, da je pripravil osnutek **metodologije za pripravo zakonodajnih ocen učinka v zvezi varstvom osebnih podatkov**, ki smo jo posredovali Ministrstvu za javno upravo - po zadnjih informacijah Ministrstva za javno upravo z dne 2. 3. 2023 je bila (nekoliko spremenjena) predlagana metodologija posredovana v medresorsko usklajevanje in v času izdaje tega mnenja po nam razpoložljivih informacijah še ni bila potrjena na Vladi RS. Ministrstvo za notranje zadeve je torej seznanjeno s predlagano metodologijo[3] in priporočamo, da se v bodoče tudi uporablja.

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,

[2] https://www.ip-rs.si/fileadmin/user_upload/Pdf/smernice/Presoje_vplivov_na_zasebnost_pri_uvajanju_novih_policijskih_pooblastil_Smernice_IP.pdf

[3] Med drugim tudi v okviru Mnenja glede ocene učinka na varstvo podatkov v zvezi s Predlogom Zakona o spremembah in dopolnitvah Zakona o nadzoru državne meje (št. 07122-1/2023/24, z dne 18. 4. 2023).

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. Le omejen nabor tveganj (tri) glede varstva osebnih podatkov je naveden na str. 21 prejete ocene učinka. Treba je opredeliti stopnjo (verjetnost in resnost, t.j. težo posledic, ki bi jih imela uresničitev tveganj) vseh relevantnih tveganj.

IP zgolj primeroma našteva relevantna tveganja, ki bi jih morala obravnavati ocena učinka, smiselno urejena in obravnavana po temeljnih načelih varstva osebnih podatkov in z opredelitvijo njihove verjetnosti, resnosti, skupne raveni tveganja in možnih ukrepov za obvladovanje tveganj (seznam ni izčrpen):

- tveganje, da določeni informacijski sistemi ne bodo posredovali potrebnih podatkov, da jih bodo posredovali z zamudo, v napačnem obsegu;
- tveganja v povezavi s slabo kakovostjo podatkov na strani pošiljateljev podatkov (ažurnost, točnost);
- tveganja v povezavi s tehnično izvedljivostjo sistema (npr. različnih sistemov za vodenje dnevnikov obdelav pri zacezancih, formatov podatkov ipd.);
- tveganje, da podatki na strani zavezancev ne bodo ustrezno šifrirani;
- tveganje, da bo zaradi napak v delovanju sistema prihajalo do napačne ali nepopolne uparitve podatkov;
- tveganje v povezavi z lažnimi zadetki (npr. zaradi pogostega a utemeljenega dostopa oseb na strani zavezancev lahko pride do prekomerne porabe policijskih resursov na eni strani ter obremenitev na strani pošiljateljev podatkov);
- tveganje neupravičene uvrstitve določene zbirke podatkov na seznam zbirk, iz katerih se bodo pridobili podatki o obdelavah;
- tveganje prekomerne hrambe uparjenih podatkov (upoštevanje zakonskih rokov v praksi);
- …

Podarjamo, da ne gre za neobvladljiva tveganja, morajo pa biti analizirana in opravljen premislek o možnih in učinkovitih ukrepih za njihovo obvladovanje ter – kjer je smiselno – ukrepe tudi jasno opredeliti (že) v besedilu zakona.

Določena tveganja so že bila analizirana in so predmet predvidenih varovalnih ukrepov - tveganje masovnega neselektivnega dostopa do podatkov iz dnevnikov obdelav pri zavezancih je (deloma) naslovljeno s predvideno določbo, da se shranijo le uparjeni podatki: podatki, kjer ne pride do uparitve pa se takoj nepovratno zavržejo. Prav tako je zelo primerna in potrebna varovalka predhodna seznanitev varovanih oseb ter določbe glede ex-post nadzora.

Glede obravnave tveganj opozarjamo, da gre za zakonodajno oceno učinka, ki torej mora nasloviti **vsa tveganja** in ne zgolj tveganja, ki so relevantna na strani uporabnika (torej policije), temveč tudi na strani pošiljateljev podatkov, saj se s predlagano spremembo ureja sistem, ki naslavlja delovanje obojih in v vseh pogledih lahko pride do tveganj, katerih realizacija bi posegla v pravico do varstva osebnih podatkov oseb, katerih osebni podatki bodo obdelovani (tako varovanih oseb kot oseb, ki so izvajale obdelave osebnih podatkov pri pošiljateljih).

Glede na to, da ocena učinka vsebuje tudi predlog zakonske ureditve glede tega podajamo naslednja priporočila glede predloženega osnutka zakonskih določb:

- **7. odstavek predlaganega 112.e člena**: Predlagamo, da pred besedo »prejete« dodate besedo »samo«, da se tako še bolj poudari, da ni podlage za shranjevanje vseh prejetih podatkov, temveč le uperjenih podatkov.

- **7. odstavek predlaganega 112.e člena:** Bistvena varovalka pred ključnim tveganjem, da se policija neselektivno seznani z vsemi podatki, ki jih bodo posredovali zavezanci, je, da se **podatki uparijo pred dešifriranjem, torej na ravni šifriranih (neberljivih podatkov) in da se dešifrirajo podatki šele potem in samo v primeru ko pride do uparitve**. Navedeno varovalko je zaslediti na str. 17 ocene učinka[4], ni pa je videti v samem besedilu predloga zakona. Gre za po oceni IP eno najpomembnejših varovalk za varstvo osebnih podatkov v zadevnem sistemu, ki naslavlja eno ključnih tveganj – nesorazmernega pridobivanje podatkov s strani policije iz širokega nabora zelo obsežnih zbirk osebnih podatkov, zato menimo, da je izrecna vključitev te varovalke v samem besedilu zakona **nujna**. Ne nedopustnost masovnega neselektivnega zbiranja osebnih podatkov podrobno opozarja sodna praksa Evropskega sodišča za človekove pravice (npr. v zadevah Quadrature du Net, Digital Rights Ireland ipd.).

- **8 . odstavek predlaganega 112.e člena**: Predlagamo, da se v ta odstavek doda zahteva, da se na policiji najkasneje do 31.1. vsako leto izvede letni redni notranji nadzor nad izvajanem določb tega člena ter da se poročilo o opravljanjem notranjem nadzoru in ugotovitvami nadzora posreduje Informacijskemu pooblaščencu (z namenom okrepljenega in bolj učinkovitega skupnega nadzora). Primerljivo zakonodajno rešitev, ki se je tudi v praksi izkazala za učinkovito, je moč najti v 220. členu Zakona o elektronskih komunikacijah (posredovanje prometnih in lokacijskih podatkov v primerih varovanja življenja in telesa).

- Navedba iz ocene učinka na strani 17 se ne odraža v predlogu besedila zakona, in sicer[5]: »*Neselektivno zbiranje podatkov se tako prepreči z informacijsko rešitvijo, o kateri je v skladu s 57. členom predloga zakona predvideno tudi predhodno mnenje informacijskega pooblaščenca*«. Glede na to, da so bile opravljene določene razprave o arhitekturi rešitve, da gre za pomembno informacijsko rešitev tako z vidika varovanih oseb kot zaradi obsežnosti obdelav podatkov in njene nacionalne pomembnosti predlagamo, da se v 112.e člen doda na primerno mesto odstavek z naslednjo (ali nomotehnično gledano primerljivo ustrezno) vsebino:

  »*Pred začetkom avtomatizirane obdelave podatkov po prvem odstavku tega člena policija pridobi mnenje Informacijskega pooblaščenca in mnenje pristojnega organa za nacionalno varnost po zakonu, ki ureja informacijsko varnost*.«

  Pojasnjujemo, da pristojni organ za nacionalno varnost po zakonu, ki ureja informacijsko varnost, t.j. Urad Vlade Republike Slovenije za informacijsko varnost (URSIV) glede na svoje poslanstvo in pristojnosti, kot izhajajo iz 3., 4. in 5. točke 27. člena Zakona o informacijski varnosti (Uradni list RS, št. 30/18, 95/21, 130/22 – ZEKom-2, 18/23 – ZDU-1O in 49/23) ter glede na nacionalni pomen predlagane ureditve in izpostavljenih varnostnih tveganjih po mnenju IP lahko s svojim mnenjem pomembno prispeva pri oblikovanju varne in učinkovite rešitve za potrebe izvajanja zadevnega člena.

[4] »Prejeti identifikacijski podatek (v neberljivi in nedoločljivi obliki) in identifikacijski podatek na strežniku policije (prav tako v neberljivi in nedoločljivi obliki) se bosta primerjala.«
[5] Predvidevamo, da je s 57. členom mišljen 57. člen ZVOP-1 in ne predlog sprememb ZNPPol.

3. Zaključno

IP zaključno predlaga, da upoštevate tu podana opozorila in priporočila ter nam končno verzijo predloga zakona pošljete v mnenje, ki ga izdamo na podlagi 3. točke prvega odstavka 55. člena ZVOP-2 ter točke c) prvega odstavka 57. člena Splošne uredbe.

S spoštovanjem,

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

Pripravil:

mag. Andrej Tomšič,
namestnik informacijske pooblaščenke

Poslati:

- naslovniku (e-pošta)
- v vednost: Urad Vlade Republike Slovenije za informacijsko varnost, po e-pošti: gp.uiv@gov.si.