



REPUBLIKA SLOVENIJA

INFORMACIJSKI
POOBLAŠČENEC

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

Številka: 007-36/2022/

Datum: 8. 12. 2022

Ministrstvo za notranje zadeve

Naslov e-pošte: gp.mnz@gov.si

ZADEVA: Predlog Zakona o spremembah in dopolnitvah Zakona o nalogah in pooblastilih policije (EVA 2020-1711-0001) – DODATNO MNENJE glede predloga sprememb 112.e člena in 57. člena (avtomatizirano pridobivanje podatkov o obdelavi podatkov oseb, ki jim policija mora zagotavljati varnost)

ZVEZA: Vaše elektronsko sporočilo z dne 7. 12. 2022 s priloženimi gradivi

Spoštovani,

na podlagi vašega dodatnega zaprosila in 48. člena Zakona o varstvu osebnih podatkov (v nadaljevanju ZVOP-1), 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 (v nadaljevanju: Splošna uredba) ter 76. člena Zakona o varstvu osebnih podatkov na področju obravnavanja kaznivih dejanj (v nadaljevanju ZVOPOKD) vam posredujemo pripombe Informacijskega pooblaščenca (v nadaljevanju IP) k predlaganim spremembam Zakona o nalogah in pooblastilih policije (predlog ZNPPol-C), ki se nanašajo na predlagane spremembe 112.e ter 57. člena (avtomatizirano pridobivanje podatkov o obdelavi podatkov oseb, ki jim policija mora zagotavljati varnost ter omogočanje izvedbe avtomatiziranega pridobivanja podatkov o obdelavi podatkov oseb, ki jim policija mora zagotavljati varnost).

Nov 112.e člen ZNPPol naj bi določal:

»112.e člen

(avtomatizirano pridobivanje podatkov o obdelavi podatkov oseb, ki jim policija mora zagotavljati varnost)

(1) Policija zaradi:

- *zagotavljanja varnosti uporabnikov prirejene identitete iz 23. člena tega zakona, 155.a člena Zakona o kazenskem postopku (Uradni list RS, št. 176/21 – uradno prečiščeno besedilo in 96/22 – odl. US; v nadaljnjem besedilu: Zakon o kazenskem postopku) in 6. člena Zakona o zaščiti prič (Uradni list RS, št. 81/06 – uradno prečiščeno besedilo, 117/06 – ZDoh-2, 110/07 in 30/18),*
- *zagotavljanja varnosti neposredno življenjsko ogroženih uslužbencev policije iz 66. člena Zakona o organiziranosti in delu v policiji (Uradni list RS, št. 15/13, 11/14, 86/15, 77/16, 77/17, 36/19, 66/19 – ZDZ, 200/20, 172/21, 105/22 – ZZNŠPP in 141/22), za katere je skladno s predpisom, ki ureja varovanje ogroženih uslužbencev policije, ugotovljena visoka stopnja ogroženosti,*

- izvajanja ukrepa nadzora poizvedb o izvirnih podatkih zaščitene osebe po evidencah v skladu z zakonom, ki ureja zaščito prič,

avtomatizirano pridobiva podatke o nazivu državnega organa in nosilca javnega pooblastila ter imenu in priimku osebe, ki obdeluje podatke teh oseb in vozil, ki jih imajo v uporabi, v zbirkah podatkov iz uradnih evidenc iz četrtega odstavka tega člena (v nadaljnjem besedilu: avtomatizirano pridobivanje podatkov).

(2) Za vključitev v avtomatizirano pridobivanje podatkov je potrebno predhodno pisno soglasje osebe iz prejšnjega odstavka. Seznam evidenc, ki so predmet avtomatiziranega pridobivanja podatkov, je sestavni del pisnega soglasja.

(3) Za izvajanje prvega odstavka tega člena lahko policija avtomatizirano pridobiva podatke za naslednje zbirke podatkov, ki vključujejo posamezne podatke o osebah in vozilih, ki jih imajo te osebe v uporabi:

- evidenco prekrškov, evidenco kaznivih dejanj, evidenco optične prepoznave registrskih tablic, evidenco operativnih zaznamkov, evidenco potnikov, prijavljenih na let (API), evidenco potnikov iz sistema rezervacij letalskih vozovnic (PNR) iz tega zakona;
- evidenco registriranih vozil iz zakona, ki ureja motorna vozila;
- evidenco o voznških dovoljenjih iz zakona, ki ureja voznike;
- register stalnega prebivalstva iz zakona, ki ureja prijavo prebivališča;
- matični register iz zakona, ki ureja matični register;
- evidenco izdanih osebnih izkaznic iz zakona, ki ureja osebno izkaznico;
- evidenco izdanih potnih listin iz zakona, ki ureja potne listine;
- centralni register prebivalstva iz zakona, ki ureja centralni register prebivalstva;
- evidenco o dovoljenjih za začasno prebivanje, evidenco o dovoljenjih za stalno prebivanje in evidenco o potnih listih za tujce iz zakona, ki ureja tujce;
- davčni register iz zakona, ki ureja finančno upravo;
- evidenco o zavarovanih osebah obveznega zdravstvenega zavarovanja iz zakona, ki ureja zdravstveno varstvo in zdravstveno zavarovanje;
- centralno evidenco izdanih orožnih listin iz zakona, ki ureja orožje;
- centralni register podatkov o pacientu iz zakona, ki ureja zbirke podatkov s področja zdravstvenega varstva;
- matično evidenco o izplačilih prejemkov, matično evidenco uživalcev pravic iz obveznega pokojninskega in invalidskega zavarovanja ter matično evidenco zavarovancev iz zakona, ki ureja matično evidenco zavarovancev in uživalcev pravic iz obveznega pokojninskega in invalidskega zavarovanja.

(4) Za avtomatizirano pridobivanje podatkov se ne šteje avtomatska obdelava podatkov v zbirkah podatkov iz prejšnjega odstavka.

(5) Upravljalci zbirk podatkov iz prejšnjega odstavka omogočajo avtomatizirano pridobivanje podatkov brezplačno.

(6) Avtomatizirano pridobivanje podatkov se izvede na način, da se policiji podatke pošlje v šifrirani obliki. Pred pošiljanjem se identifikacijskemu podatku doda enoznačen, začasen in naključen polnilni niz, ki se v nadaljevanju v zgoščeni obliki doda k ostalim podatkom za pošiljanje na način, ki zagotavlja neberljivost in nedoločljivost identifikacijskega podatka.

(7) Policija prejete podatke iz prejšnjega odstavka avtomatizirano primerja z identifikacijskimi podatki oseb iz prvega odstavka tega člena. Policija lahko shrani le prejete podatke, ki se ujemajo z

identifikacijskim podatkom. Ostale prejete podatke informacijski sistem ob primerjavi avtomatizirano nepovratno zavrže.

(8) Policija podatke iz prejšnjega odstavka izbriše najkasneje v šestih mesecih od njihovega prejema.

(9) Inšpekcijski nadzor nad obdelavo podatkov iz tega člena opravlja informacijski pooblaščenec najmanj enkrat letno.«.

Nadalje naj bi 57. člen ZNPPol določal:

»57. člen

(omogočanje izvedbe avtomatiziranega pridobivanja podatkov o obdelavi podatkov oseb, ki jim policija mora zagotavljati varnost)

Upravljavci zbirk podatkov iz četrtega odstavka novega 112.e člena zakona vzpostavijo informacijsko rešitev za izvajanje avtomatiziranega pridobivanja podatkov o obdelavi podatkov oseb, ki jim policija mora zagotavljati varnost na način, ki ne ogroža njihove varnosti, v treh letih od uveljavitve tega zakona. Informacijska rešitev iz prejšnjega stavka se dogovori s tehničnim protokolom na podlagi predhodnega mnenja Informacijskega pooblaščenca.«.

IP uvodoma ugotavlja, da je v predlogu sprememb 112.e člena glede na prejšnje verzije bistveno zožan nabor oseb, za katere bi se avtomatsko obdelovalo podatke o dostopih do njihovih osebnih podatkov in sicer na (v nadaljevanju mnenja: varovane osebe):

- uporabnike prirejene identitete,
- neposredno življenjsko ogrožene uslužbencev policije, za katere je skladno s predpisom, ki ureja varovanje ogroženih uslužbencev policije, ugotovljena visoka stopnja ogroženosti in
- za izvajanja ukrepa nadzora poizvedb o izvirnih podatkih zaščitene osebe po evidencah v skladu z zakonom, ki ureja zaščito prič.

Prav tako pozdravljamo natančno definiran nabor evidenc, na katerih bi se tovrstne obdelave izvajalo ter vključitev varovalke z zahtevo po predhodnem pisnem soglasju zadevnih oseb, kakor tudi predlog rednega nadzora s strani IP.

Opozarjamo pa, da ostaja izredno širok nabor evidenc, v katerih se preverja podatke, med drugim tudi posebne vrste osebnih podatkov, kot so podatki v zvezi z zdravjem. IP se sprašuje o sorazmernosti in nujnosti tako širokega nabora zbirk, med katerimi je tudi register podatkov o pacientih.

Ne glede na navedeno pa moramo poudariti tudi naslednje:

- glede ne predvideno obsežno obdelavo osebnih podatkov bi bilo že v fazi priprave zakonske materije - če ne obvezno - pa priporočljivo izdelati predhodno oceno učinka glede varstva osebnih podatkov, saj je to najprimernejše orodje za celovito naslovitev vseh relevantnih tveganj kakor tudi za celovito presojo izvedbenih opcij (glede na predlog ZVOP-2, ki je v fazi sprejemanja, bodo tovrstne ocene učinke tudi obvezne ob pripravi zakonodajnih predlogov);
- glede na tveganja in naravo ter množičnost obdelave je izvedba predhodne ocene učinkov vsekakor nujna in obvezna pred začetkom s predlaganimi spremembami ZNPPol predvidene množične obdelave osebnih podatkov;
- IP se sprašuje, zakaj je glede na izredno velik obseg osebnih podatkov o vseh vpogledih v izredno veliko število zbirk potrebna 6-mesečna hramba vseh tako obdelanih osebnih podatkov

kot izhaja iz 8. odstavka novega 112.e člena. Ocenjujemo, da bi bilo treba vse ostale podatke, razen zadetkov brisati bistveno prej in iz prejetega gradiva ne razberemo razlogov, ki taki ureditvi nasprotovali. Prav tako predlagamo, da se ustrezno določi kratek rok hrambe zadetkov, ki niso potrebni za morebitne konkretne postopke;

- predlagana ureditev ne določa konkretne zbirke, kjer se bodo na podlagi 112.e člena pridobljeni osebni podatki hranili, morebitnih omejitev pravic posameznika in preohlapno določa režim izbrisa oz. blokiranja (vsebina bi verjetno zahtevala tudi dopolnitve 123.-129.a člena ZNPPol);
- nameni predlagatelja so, kot izhaja iz obrazložitev, legitimni in razumljivi, treba pa se je zavedati, da gre za resen poseg v zasebnost posameznikov in da ima vsaka izvedbena opcija, ki na nek način vpliva tudi na samo dikcijo pravnih podlag, svoje prednosti in slabosti ter s tem povezana resna tveganja, ki jih je treba že v fazi priprave predpisa nasloviti zlasti z vidika zagotavljanja spoštovanja ustavnega načela sorazmernosti, ki zahteva, da je vsak z zakonom predviden poseg v zasebnost jasno opredeljen zgolj v obsegu, ki je nujen, potreben in učinkovit ter sorazmeren za doseg zakonitega cilja, ki ga zasleduje;
- IP v okviru mnenja ne more preferirati, potrjevati ali se kakor koli drugače opredeljevati za določeno izvedbeno opcijo, temveč je to naloga predlagatelja, IP pa vas v nadaljevanju opozarja, katere bistvene sestavine predlaganih določb bi morale biti upoštevane.

V okviru dosedanjih razprav je bilo ugotovljeno, da se kot ključni izvedbeni možnosti kažeta naslednji opciji:

- centralizirana obdelava (podatki iz dnevnikov obdelav posameznih upravljavcev evidenc se posredujejo na policijo, kjer se izvede uparjanje s seznamom varovanih oseb);
- decentralizirana obdelava (podatki iz dnevnikov obdelav posameznih upravljavcev evidenc se pri samem upravljavcu uparijo s seznamom varovanih oseb, policiji se posredujejo samo zadetki).

Vsaka od navedenih možnosti ima svoje prednosti, slabosti in tveganja, tako z vidika potrebnih stroškov, časa in drugih izvedbenih vidikov, kot seveda tudi z vidika tveganj za človekove pravice. Kot smo izpostavili, IP v svojem mnenju ne more potrjevati ene ali druge, temveč lahko opozorimo na naslednje:

- predlagatelj mora podrobno analizirati prednosti in slabosti ter tveganja vsake od preučevanih rešitev;
- predlog zakonskih določb mora v vsakem primeru poleg že vsebovanih varovalk (kot navedeno uvodoma), vsebovati tudi **natančen nabor osebnih podatkov, ki se bodo primerjali, posredovali in drugače obdelovali, pri tem pa mora biti strogo upoštevano načelo minimizacije obdelave osebnih podatkov in nabor osebnih podatkov reduciran na najmanjši možen, ki omogoča doseganje cilja** – trenutno predlagana določba ne opredeljuje natančno nabora obdelovanih osebnih podatkov. Načeloma za doseganja cilja zadostuje podatek o enolični identifikaciji uporabnika pri upravljavcu, podatek o upravljavcu (organu) ter podatek za enolično identifikacijo varovane osebe – kateri podatki so to, mora biti natančno opredeljeno. V ta namen bi bila verjetno potrebna dopolnitev 123.-129.a člena ZNPPol;
- obdelava osebnih podatkov mora biti v predlogu zakona dovolj natančno opisana – jasno mora biti, ali gre za centralizirano ali decentralizirano obdelavo;
- tveganja morajo biti celovito identificirana in naslovljena s primernimi ukrepi; med neidentificiranimi tveganji je npr. (v primeru centralizirane obdelave) tveganje, da do uparjanja podatkov pride (iz različnih razlogov, npr. tehnične narave) z zamikom, kar posledično pomeni, da se tudi podatki, ki niso relevantni, za določen čas hranijo v sistemu policije. Navedeno tveganje bi moralo biti naslovljeno s primerno varovalko, kot recimo testiranje pred in med delovanjem sistema. Med možne varovalke sodi tudi izrecna prepoved vsakršne uporabe

pridobljenih podatkov za druge namene, omejenost pravic dostopa samo na določene osebe oziroma notranje enote, izvajanje rednega notranjega nadzora (npr. s strani DPO);

- v vsakem primeru pa mora biti upoštevano izhodišče, ki izhaja iz načela sorazmernosti, t.j. da policija ne sme hraniti podatkov v primerih, ko ne pride do uparitve podatkov – te podatke, bi morala policija brisati takoj po uparitvi in ne šele po 6 mesecih;
- Tudi za podatke, ki predstavljajo zadetek, mora biti jasno opredeljen rok hrambe, pri čemer bi bilo smiselno določiti, kdaj se izbrišejo osebni podatki, ki niso relevantni za nadaljnje postopke in jasneje določiti absolutni rok hrambe osebnih podatkov v taki novo nastali zbirki.

Hvala za sodelovanje in lep pozdrav,

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

Pripravila:

mag. Andrej Tomšič,
namestnik informacijske pooblaščenke

Alenka Jerše,
namestnica informacijske pooblaščenke

Poslati:

- po e-pošti naslovniku;
- v vednost: po e-pošti: Ministrstvo za pravosodje, gp.mp@gov.si;
- v vednost: Varuh človekovih pravic RS, info@varuh-rs.si;
- zbirka dokumentarnega gradiva pri IP.