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: 007-36/2021/6
Datum: 2. 11. 2021

Ministrstvo za notranje zadeve
Naslov e-pošte: gp.mnz@gov.si

ZADEVA: dopolnjen Predlog Zakona o spremembah in dopolnitvah Zakona o nalogah in pooblastilih policije (EVA 2020-1711-0001) – DODATNO MNENJE
ZVEZA: Vaš e-dopis št. IPP 007-39/2021/49 (146-01) z dne 12. 10. 2021 in IPP 007-39/2021/51 (146-01) z dne 12. 10. 2021 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) posredujemo pripombe Informacijskega pooblaščenca (v nadaljevanju IP) k predlaganim dopolnjenim spremembam Zakona o nalogah in pooblastilih policije (predlog ZNPPol-C), ki se nanašajo na številne vidike množičnih in sistematičnih obdelav osebnih podatkov posameznikov.

Prav tako v tem mnenju podajamo pripombe k predloženim dopolnjenim ocenam učinkov predvidenih dejanj obdelave na varstvo osebnih podatkov na podlagi 35. člena Splošne uredbe oziroma oziroma 49. člena ZVOPOKD glede predlagane uvedbe tehničnega sredstva za iskanje pogrešanih oseb Lifeseeker (povezano s predlaganimi spremembami 43. člena ZNPPol) ter glede predlagane uvedbe novih policijskih pooblastil za avtomatizirano preverjanje registrskih tablic pri nadzoru cestnega prometa (povezano s predlaganimi spremembami 113.a člena ZNPPol).

IP želi uvodoma izpostaviti, da vsebujejo kljub določenim izboljšavam tudi predlagane nove spremembe številne zaskrbljujoče, nejasne in skopo utemeljene predloge glede bistvenega širjenja policijskih pooblastil in resnih posegov v ustavno varovano pravico do zasebnosti ter varstva osebnih podatkov.

IP med novimi oz. razširjenimi pooblastili, ki jih vsebuje predlog ZNPPol-C in ki pomenijo najhujše ter predvsem neutemeljene posege v zasebnost brez ustreznih zakonskih varovalk za pravice posameznikov, tokrat posebej izpostavlja:

- predlog zgoraj omenjene uvedbe tehničnih sredstev za lociranje mobilnih naprav,
- v ZNPPol ostajajo zaskrbljujoče nejasnosti glede široke uporabe biometričnih podatkov, na katere je IP že večkrat opozarjal in ki se s spremembami kljub dopolnitvam še slabšajo (tudi z uporabo avtomatizirane obdelave in preko tehničnih sredstev, med katere bi lahko štela t.i *face recognition* – tehnologija avtomatizirane prepoznave obrazov) brez vezave na konkretne okoliščine in opredelitve ustreznih varovalk;

- nejasno opredeljen predlog za stalen poimenski nadzor obdelav osebnih podatkov določenih varovanih oseb v tako rekoč vseh zbirkah organov javnega sektorja in s tem posredno možnost stalnega nadzora državnih organov, ki so upravljavci teh zbirk.

Pri tem gre med drugim tudi za nekatere sporne vidike oz. zakonske spremembe ZNPPol, ki so bile uvedene z novelo zakona (ZNPPol-A), in na katere je IP tekom zakonodajnega postopka že večkrat opozoril predlagatelja zakona, vendar pa ta pripomb ni upošteval.

V nadaljevanju podajamo konkretne pripombe IP po posameznih členih.

- **K 6. členu predloga ZNPPol-C (sprememba 34. člena zakona, zbiranje obvestil)**

Predlog na nejasen način opredeljuje zelo široke izjeme glede policistove izrecne obveznosti iz 2. odstavka 34. člena ZNPPol, da vsako osebo, od katere zbira obvestila, predhodno pouči, da je dajanje obvestil prostovoljno oz. da ima posameznik (razen v določenih primerih) pravico do anonimnosti pri podaji obvestil. IP takšni spremembi kljub dopolnitvam nasprotuje in opozarja, da ureditev, ki bi glede na izredno široko določeno možnost izjem po novem dopuščala možnost, da bi policisti smeli zadevni osebi dajati vtis, da je podaja obvestil obvezna, ni ustrezna. V praksi je namreč bojazen, da se dogaja prav to.

Določba je zato sporna, saj zaradi nejasnosti ne zadošča načelu pravne varnosti in s tem zmanjšuje raven varstva pravic posameznikov. Za uveljavljanje pravice s strani posameznika je bistveno, da je ta z njo seznanjen, kar pa bi po novem v velikem delu primerov odpadlo. V praksi ni življenjsko od posameznikov pričakovati, da vedo, da je njihovo sodelovanje pri zbiranju obvestil po tem členu prostovoljno in da lahko ostanejo anonimni (zlasti, ker gre za pridobivanje informacij s strani represivnega organa), zato je pomembno, da jih policist s tem seznani. Zlasti se zastavlja vprašanje izjeme, da se določbe glede obveznosti obveščanja ne uporabljajo, ko je zbiranje obvestil sestavni del drugega policijskega obvestila ali ko policisti zbirajo obvestila na podlagi zakona, ki ureja postopek o prekrških. To kaže na dejansko nejasnost tega policijskega pooblastila, ki v nobenem primeru ne obstaja samo za sebe oziroma ni samo sebi namen, ampak je vedno del nekega policijskega postopka. V praksi pa posamezniki glede na podrejen položaj v razmerju do policista kot organa kazenskega pregona pogosto dojemajo odgovor na vprašanja policista kot obveznost.

Obvestilo o prostovoljnem podajanju informacij je zelo pomembno za zagotovitev načela prostovoljnosti in anonimnosti, zato morajo biti izjeme, ko takega obvestila ni potrebno predhodno podati, podane dovolj ozko, da ne dopuščajo preširokih možnosti različnih tolmačenj. Na problematičnost odprave obveznosti obveščanja je poleg IP opozoril tudi Varuh človekovih pravic in drugi strokovnjaki, dopolnitve, kot jih predlaga predlagatelj ter obrazložitev teh dopolnitev, pa kažejo, da predlagatelj v resnici ni naslovil skrbi izražene v pripombah, ampak je z nejasno novo dikcijo problem le zameglil. Te napake pa ni mogoče, kot zavajajoče izpostavlja predlagatelj, rešiti v podzakonskih aktih.

Če obstajajo primeri, ko tako obveščanje res bistveno otežuje policijsko delo, naj se člen oblikuje jasno in na način, da se v takih izjemnih primerih obveščanje lahko opusti, v vseh drugih pa naj ostane. Omejitve obveščanja, kot jih je predlagal predlagatelj, pa zaradi izjemne nejasnosti pomenijo, da bo pravica v veliki meri ostala gola črka na papirju.

IP zato predlaga črtanje 6. člena predloga ZNPPol-C, saj ocenjuje, da je besedilo 2. odstavka 34. člena ZNPPol, kot je bilo spremenjeno z ZNPPol-B, zadostno. Možnost izključitve obveščanja namreč

že veljavni 34. člen ZNPPol izključuje zgolj v posebnih primerih, ko gre za preventivne dejavnosti in če je do zbiranja obvestil prišlo na pobudo osebe.

- **K 9. členu predloga ZNPPol-C (sprememba 42. člena zakona, identifikacijski postopek)**

S spremembo prvega odstavka 41. člena ZNPPol se kljub izključitvi prvotno predlaganega pojma »*neznana oseba*« ugotavljanje identitete iz navedenega člena vsebinsko skoraj popolnoma izenači z identifikacijskim postopkom iz prvega odstavka 42. člena tega zakona. Ni jasno, kaj je namen take izenačitve, tega predlagatelj ne pojasni niti v obrazložitvi.

IP izraža resno skrb, da bi sprejetje take določbe policiji omogočalo, da v primerih različnih oblik javnega zbiranja, protestov, ki so predmet inšpekcijskih postopkov pri IP, posnetke shodov zakonito analizira s tehnologijo avtomatizirane prepoznave obrazov z uporabo digitalnih tehnologij (ang. *face recognition*).

V zvezi s tem IP ponovno izpostavlja neustreznost besedila »*drugih operativnih in kriminalistično-tehničnih opravil*« v 1. odstavku 42. člena ZNPPol, ki pušča popolnoma odprte možnosti glede uporabe tehničnih sredstev za namen izvedbe identifikacijskega postopka. Predlagamo, da se posledično besedilo 1. odstavka 42. člena ZNPPol tudi v tem delu ustrezno dopolni na način, da bodo tehnična sredstva opredeljena upoštevajoč načelo sorazmernosti, določnosti obdelav in ne zgolj primeroma. Glede na tveganja, ki jih navedeni posegi lahko predstavljajo za varstvo osebnih podatkov, bi bilo v tem delu smiselno izvesti tudi predhodno oceno učinkov za posamezna tehnična sredstva, s katerimi se zbira in/ali obdeluje osebne podatke, vsekakor bi bilo to nujno za primere množičnih obdelav biometričnih podatkov.

IP zato (tudi na podlagi inšpekcijskih postopkov ter odzivov posameznikov) ugotavlja, da bi bilo treba 42. člen ZNPPol ustrezno dopolniti, saj bi moral zakon (in ne predpis, ki ga izda minister) točno in nedvoumno določati, kdaj lahko policisti izvedejo identifikacijski postopek, ki zajema odvzem in preverjanje tako rekoč vseh osebnih podatkov, vključno z biometričnimi podatki posameznika, v vseh zbirkah, ki obstajajo. Trenutna določba s predlaganimi spremembami pa še vedno ne vsebuje namena dopustnosti tovrstnih obdelav, ampak prepušča opredelitev načina izvajanja tega policijskega pooblastila v prosto presojo ministru, kar pomeni, da se materija, ki bi jo moral opredeliti zakon prepušča v prosto politično opredelitev izvršilni veji oblasti. Zakon bi moral torej točno določati, katere podatke in v katerih primerih se lahko obdeluje v takem postopku. Prav tako pa tak postopek ne bi smel omogočati izvedbe nedoločenega in neomejenega nabora kriminalističnotehničnih opravil s strani policije, ampak bi morala biti ta jasno zamejena, npr. ne bi smela obsegati splošne in neomejene obdelave biometričnih podatkov. V nasprotnem primeru je policijsko pooblastilo po mnenju IP nedoločno, nesorazmerno in pomeni pretiran poseg policije v zasebnost in varstvo osebnih podatkov posameznikov v neskladju z 38. členom Ustave RS.

- **K 10. členu predloga ZNPPol-C (sprememba 43. člena zakona, iskanje oseb – uporaba tehničnih sredstev za lociranje mobilnih naprav)**

Nova prva alineja četrtega odstavka 43. člena ZNPPol v odnosu na obstoječo ureditev širi nabor podatkov, ki jih sme policija pridobiti od operaterja, in sicer se podatkom o času in telefonski številki klicane ali kličoče osebe ter podatkom o naročniku številke s predlogom ZNPPol-C dodajajo tudi podatki o sporočilih v SMS in MMS obliki, kraju, iz katerega je bila komunikacija opravljena, ter podatki o telefonski številki, vezani na internetno dostopno točko. Prav tako sme policija v skladu s predlogom ZNPPol-C od ponudnika storitev informacijske družbe pridobiti podatke o internetni dostopni točki in naročniku internetne dostopne točke.

IP vztraja, da se ustrezno dopolni tudi sedmi odstavek obstoječega 43. člena ZNPPol in se tako jasno zapiše, da se tudi pridobivanje vseh zgoraj navedenih podatkov izvede šele po pridobitvi sodne odredbe in če je to nujno za razjasnitev okoliščin pogrešitve ali za izsledite iskane osebe oziroma osebe v stiski. Gre namreč za zelo široke ukrepe, saj poleg komunikacije pogrešane osebe oziroma osebe v stiski posredno zajemajo tudi komunikacije tretjih oseb.

Glede predlagane nove sedme alineje četrtega odstavka, ki določa, da sme policija »uporabiti tehnična sredstva za lociranje mobilnih naprav«, IP uvodoma ugotavlja, da je predlagatelj k predlogu sprememb ZNPPol-C priložil oceno učinka (»Tehnična sredstva policije za ciljno usmerjeno iskanje pogrešanih oseb, Presoja vplivov na zasebnost«), ki jo je pripravil na podlagi 35. člena Splošne uredbe. V zvezi s tem izpostavljamo, da v oceni učinka manjka primerjalno pravna analiza tveganj. Naveden je zgolj kratek pregled prakse nekaterih držav (4), iz katerih niti niso razvidni podatki o uporabi tehničnega sredstva LIFESEEKER, ampak podobnih tehničnih sredstev, večini katerih je skupno, da delujejo po principu IMSI lovilca. Ni razvidno, iz katerih razlogov tehničnega sredstva LIFESEEKER ne uporabljajo v oceni učinka navedene (in po vsej verjetnost tudi preostale) države članice EU. Prav tako ni razbrati, kakšne so morebitne pozitivne in negativne izkušnje, prepoznana tveganja in ukrepi za njihovo naslovitev držav članic EU, ki morda tako sredstvo uporabljajo. Še vedno torej ni praktično nobenih informacij o morebitni uporabi in delovanju predlaganega tehničnega sredstva v drugih državah. Argumentacija predlagatelja, da gre za »posebno tehnično opremo, ki ni predmet široke potrošnje in s tem možnosti nakupa v tehničnih trgovinah« in da gre za »posebno opremo, pri kateri ni mogoče napisati podrobnih pojasnil iz več držav in pravnih podlag za njeno uporabo«, ni prepričljiva, saj se nedvomno vsaka policija pri svojem delu srečuje tudi z iskanjem pogrešanih oseb, pri čemer so za takšno analizo pri pripravi zakona relevantne prav ureditev in izkušnje policije drugih držav članic EU in ne izkušnje posameznikov. Postavlja se torej vprašanje, kako da ob tej samoumevnosti (kot je mogoče sklepati iz prejetega gradiva) nobena država članica EU ne uporablja predlaganega tehničnega sredstva?

Gre za tehnična sredstva za lociranja mobilnih naprav, ki temeljijo na tehnologiji t.i. IMSI lovilcev, ki načeloma delujejo na dva načina:

a) **ciljno iskanje določene naprave** - da mora policija bodisi razpolagati z vnaprej znano številko mobilne naprave (IMSI, IMEI), ki jo želi najti na določenem omejenem geografskem področju ali
b) **da gre za zajem vseh mobilnih številk, ki se znajdejo v dometu IMSI lovilca**, kjer se poskuša ugotoviti prisotnosti določenih naprav, ugotavljanje povezav med njimi in nato naknadno pridobivanje prometnih podatkov ali vsebine komunikacij zaradi iskanja storilcev kaznivih dejanj (princip »lažne bazne postaje«).

Predlagatelj je predvidel naslednje varovalke:

Za petim odstavkom se doda nov šesti odstavek, ki se glasi:

»*(6) Tehnična sredstva iz druge alineje četrtega odstavka tega člena smejo policisti uporabiti, če lokacijski podatki, ki jih policisti pridobijo od operaterja mobilne telefonije ali ponudnika storitev informacijske družbe na podlagi zakona, ki ureja elektronske komunikacije, niso pripomogli ali, če glede na okoliščine konkretnega primera ne bi pripomogli k hitri izsleditvi pogrešane osebe. S tehničnimi sredstvi je dovoljeno vzpostaviti samostojno radijsko komunikacijo z napravo za mobilno komuniciranje pogrešane osebe. Ne smejo se uporabljati tehnična sredstva, ki omogočajo ali bi lahko omogočala vstop v komunikacije tretjih oseb ter hrambo podatkov za kasnejšo uporabo*.«

Glede na to, da je namen predlaganih določb **ciljno iskanje pogrešanih oseb** mora biti z izrecno zakonsko varovalko natančno onemogočena uporaba v načinu delovanja lažnih baznih postaj – opominjamo, da je Ustavno sodišče RS leta 2019 začasno zadržalo izvajanje 150.a člena Zakona o kazenskem postopku, ki ustvarja pravno podlago za uporabo IMSI lovilcev, saj bi po oceni US lahko izvrševanje tega člena oziroma uporaba lovilca IMSI lahko imelo težko popravljive škodljive posledice. **Za uspešno iskanje pogrešanih oseb, s tem, da so obvladovana tveganja za morebitne zlorabe z ustreznimi varovalkami menimo, da morajo zakonske določbe vsebovati naslednje varovalke**:

- tehnična sredstva ne smejo omogočati hrambe podatkov ali prestrezanja komunikacije tretjih oseb,
- tehnično sredstva ne smejo biti uporabljeno na način lažnih baznih postaj za zajem mobilnih številk (klasični IMSI catcher),
- uporaba je lahko dopustna zgolj za iskanje pogrešanih oseb in ne za preiskovanje ali druga policijska opravila v zvezi s pregonom kaznivih dejanj,
- uporaba dopustna le na podlagi vnaprej znane zakonito pridobljene telefonske številke pogrešane osebe,
- zunanji nadzor s strani Informacijskega pooblaščenca.

Glede na navedeno IP predlaga, da se določba 10. člena najmanj dopolni, kot navajamo:

a) poleg že predvidene varovalke: »*Ne smejo se uporabljati tehnična sredstva, ki omogočajo ali bi lahko omogočala vstop v komunikacije tretjih oseb ter hrambo podatkov za kasnejšo uporabo.*«, ki jo pozdravljamo, **bi uporaba »tehnična sredstva za lociranje mobilnih naprav« z namenom reševanja pogrešanih oseb morala tako biti vezana na predpogoj, da policija razpolaga z vnaprej znano in zakonito pridobljeno številko mobilne naprave (IMSI, IMEI) pogrešane osebe, da se tako izključi možnost uporabe zadevne tehnologije v smislu zajema vseh mobilnih številk**, ki se znajdejo v dometu IMSI lovilca.

b) Prav tako predlagamo, da se v stavek »*S tehničnimi sredstvi je dovoljeno vzpostaviti samostojno radijsko komunikacijo z napravo za mobilno komuniciranje pogrešane osebe.*« **doda besedo »samo«**, da je torej nedvomno jasno, da zakon dopušča vzpostavitev **komunikacije le z napravo za mobilno komuniciranje pogrešane osebe**.

c) Določba predlagane spremembe osmega odstavka 43. člena ZNPPol, ki določa zgolj ustno seznanitev najdene osebe o obdelavi njenih podatkov na podlagi pooblastil iz četrtega odstavka, glede na stopnjo posega v njeno zasebnost ni zadostna in **bi bilo treba osebo vselej, ne pa zgolj na njeno zahtevo, pisno seznaniti z zbranimi podatki**. IP v tem smislu ne sprejema kot utemeljenega razloga za neustrezno seznanitev osebe o tako resnem posegu v njeno zasebnost načela odprave administrativnih ovir in nepotrebnih birokratskih del in nalog, kar naj bi po navedbah predlagatelja po nepotrebnem obremenjevalo policijo. Obveščanje posameznika o tovrstnem posegu, ne more biti razumljeno kot administrativna ovira, saj je transparentnost obdelav eno temeljnih načel varstva osebnih podatkov, zato IP glede na stopnjo posega v zasebnost posameznika ocenjuje, da bi bilo treba besedilo v tem delu dopolniti.

- **K 11. členu (novo besedilo 44. in 45. člen, prikrita, poizvedovalna ali namenska kontrola)**

Dopolnjen predlog ZNPPol-C prinaša spremembo roka hrambe za evidenco prikritih, poizvedovalnih ali namenskih kontrol, in sicer v 37. členu predloga ZNPPol-C določa, da se podatki v tej evidenci hranijo »*dokler traja razpis ukrepa*.«. Nov koncept določitve roka hrambe podatkov v tej evidenci IP pozdravlja, menimo pa, da sama terminologija ni ustrezna, saj Uredba 2018/1862/EU ne uporablja izraza trajanje ukrepa, zato predlagamo, da se terminologija uskladi z omenjeno uredbo in se navede, da se podatki hranijo »**do izteka veljavnosti razpisa ukrepa**«.

Ob tem pozdravljamo predlagano določbo 38. člena predloga ZNPPol-C, ki sedaj določa, da se po preteku rokov hrambe iz prejšnjega člena podatki v evidenci prikritih, poizvedovalnih in namenskih kontrol brišejo (v nasprotju z obstoječo ureditvijo, v skladu s katero se v blokirani obliki hranijo še nadaljnjih 30 let).

- **K 12. členu predloga ZNPPol-C (sprememba 55. člena zakona, protiteroristični pregled prostorov, objektov, naprav in območij)**

IP glede določbe 6. odstavka 55. člena ZNPPol, ki predvideva uporabo tehničnih sredstev za motenje radiofrekvenčnega spektra, odkrivanje pasivnih in aktivnih prisluškovalnih naprav ter naprav za odkrivanje lažnih baznih postaj, glede na nejasnost določbe in v izogib nedopustnemu širjenju uporabe tovrstnih naprav tudi za druge namene ter morebitne posege v zasebnost glede na razvoj modernih tehnologij, predlaga, da se v besedilu 6. odstavka 55. člena ZNPPol doda, da policisti z aktivnostmi in uporabo naprav na podlagi 6. odstavka 55. člena ZNPPol ne smejo zbirati ali obdelovati osebnih podatkov.

- **K 24. členu predloga ZNPPol-C (sprememba 112. člena zakona, zbiranje podatkov – nejasna ureditev zbiranja biometričnih podatkov)**

IP se strinja, da je določbo treba novelirati, vendar ne na način, kot to predlaga predlagatelj, ampak tako, da bo v njej povsem jasno in nedvoumno določeno, v katerih primerih in pod kakšnimi pogoji smejo policisti obdelovati biometrične podatke in katere.

Določbe 112. člena ZNPPol skupaj s predlaganimi spremembami ZNPPol omogočajo, da bo lahko policist, ki bo npr. legitimiral posameznika na ulici ali ga želel prepoznati na nekem posnetku, nad njim praktično brez omejitev izvajal katerekoli biometrijske ukrepe, medtem ko bo izvajanje takih ukrepov nad posameznikom, zoper katerega vodijo kazenski postopek dovoljeno samo pod strogo določenimi pogoji. Določba namreč omogoča tudi izvajanje biometrijskih ukrepov v identifikacijskih postopkih in jo je treba brati v povezavi s spremembami 42. člena ZNPPol.

IP ponavlja svoje stališče, izraženo že v mnenju k predlogu ZNPPol-A, da **ne vidi potrebe, da se v 1. odstavek 112. člena zapisuje splošna in neomejena podlaga za zbiranje biometrijskih podatkov**. V skladu s 7. členom ZVOPOKD je obdelava posebnih vrst osebnih podatkov prepovedana, razen, če:

- je obdelava skladna z določbami 6. člena ZVOPOKD in
- so v zakonu določeni pogoji in ukrepi, s katerimi je zagotovljeno ustrezno varstvo človekovih pravic ali temeljnih svoboščin posameznika, na katerega se nanašajo osebni podatki, in
- je nujno potrebna za opravljanje nalog pristojnih organov, določenih z zakonom, ali jih je posameznik očitno naredil javno dostopne ali objavil, razen če gre za komunikacijo znotraj dejansko ožjega kroga oseb.

IP zato ponovno opozarja na neustreznost takega nejasnega besedila 1. odstavka 112. člena ZNPPol in vztraja, da se raba biometrije opredeli konkretno in vezano na konkretne okoliščine in da se ustrezno opredeli ter omeji na primere opredeljene v posameznih členih ZNPPol, ki urejajo specifična policijska pooblastila oz. v drugih takšnih zakonih (npr. kriminalistično-tehnična obdelava ob odvzemu prostosti po ZKP).

Zakon bi moral jasno določati, da je avtomatizirana obdelava in zbiranje biometričnih podatkov dopustna zgolj v ozko določenih primerih sicer pa le v okviru preiskovanja in odkrivanja kaznivih

dejanj. **Predlagane dopolnitve 112. člena pa interpretacijo nevarno širijo na vsak identifikacijski postopek v celoti. Predlagana dikcija po mnenju IP ni skladna z Ustavo RS.**

- **K 25. členu ZNPPol-C (nov 112.e člen, avtomatizirano pridobivanje podatkov o obdelavi podatkov varovanih oseb)**

Predlog zakona predvideva, da lahko Policija za namen učinkovitega in pravočasnega opravljanja policijskih nalog in izvajanja policijskih pooblastil za zagotavljanje varnosti varovanih oseb avtomatizirano pridobiva podatke o nazivu organa javnega sektorja ter imenu in priimku osebe, ki obdeluje podatke varovanih oseb in vozil, ki jih imajo varovane osebe v uporabi, v zbirkah podatkov iz uradnih evidenc, ki jih upravljajo organi javnega sektorja. Policija bi torej lahko teoretično na tak način nadzorovala vsako obdelavo osebnih podatkov varovanih oseb, v vseh evidencah različnih upravljavcev, ki so organi javnega sektorja. Dejansko bi glede na nejasno besedilo predlaganega prvega in drugega odstavka tega člena to lahko pomenilo splošno in odprto pooblastilo za popoln nadzor Policije nad delom drugih organov, tudi npr. Varuha človekovih pravic, Računskega sodišča, Komisije za preprečevanje korupcije, morda celo sodišč, saj zakon ne določa definicije 'organa javnega sektorja' ipd.? Vse navedeno naj bi potekalo avtomatizirano, torej za vse vpoglede in obdelave za določeno varovano osebo, in poleg pooblastil, ki jih sicer določa ZNPPol za obdelavo osebnih podatkov in so vezana na konkretne posamične primere. Gre za obliko stalnega nadzora Policije nad delom vseh organov javnega sektorja, kar glede na veljavno ustavno ureditev ni skladno z načelom ustavno varovane delitve med izvršno, zakonodajno in sodno vejo oblasti.

Četudi bi se dikcija predlaganega novega 112.e člena spremenila na način, kot pojasnjuje predlagatelj v obrazložitvi, da bi bil navedeni nadzor nad obdelavami osebnih podatkov varovanih oseb predviden zgolj za v tretjem odstavku navedene evidence, IP še vedno ugotavlja, da gre za izredno širok nabor zbirk drugih upravljavcev (torej ne gre niti za zbirke katerih upravljavec bi bila Policija in celo niti za zbirke katerih upravljavec bi bilo ministrstvo za notranje zadeve), med drugim za matično evidenco o izplačilih prejemkov, matično evidenco uživalcev pravic iz obveznega pokojninskega in invalidskega zavarovanja, davčni register, evidenco prekrškov, evidenco o zavarovanih osebah obveznega zdravstvenega zavarovanja.

IP pozdravlja vključitev varovalka pogoja soglasja varovane osebe, vendar pa to ne odpravi skrbi in tveganj, ki jih tak stalen nadzor prinaša. Gre za zbiranje osebnih podatkov povsem na zalogo in ko je tako zbiranje enkrat odrejeno, naknadno zagotoviti varovanje temeljnih človekovih pravic ni več učinkovito. Med navedene varovane osebe, ki bi lahko bile na ta način pod neomejenim in stalnim tovrstnim nadzorom sodijo npr. predsednik Republike Slovenije, predsednik Vlade Republike Slovenije, predsednik Državnega zbora Republike Slovenije, podpredsednik Vlade Republike Slovenije, minister, pristojen za zunanje zadeve, minister, pristojen za obrambo, minister, pristojen za notranje zadeve, kandidat za predsednika Republike Slovenije, ki je izvoljen za funkcijo predsednika republike, v času od uradne razglasitve izida volitev do prevzema funkcije predsednika republike, bivši predsednik Republike Slovenije še tri mesec po prenehanju opravljanja funkcije predsednika republike, bivši predsednik Vlade Republike Slovenije še tri mesec po prenehanju opravljanja funkcije predsednika vlade, bivši podpredsednik Vlade Republike Slovenije še tri mesece po prenehanju opravljanja funkcije podpredsednika vlade. Tako pridobljeni podatki lahko pomenijo hud poseg v zasebnost vseh varovanih oseb (npr. razkrivanje začetka postopkov nadzora s strani FURS, razkrivanje obiska zdravnika) in bi lahko ob uporabi izven zakonsko določenih namenom pomenili zelo resna tveganja za hude kršitve zasebnosti teh oseb. Prav tako pa gre za hud poseg v vodenje postopkov in samostojnost vodenja posameznih postopkov organov, ki so upravljavci zbirk, ki bodo na tak način predmet stalnega nadzora, vsekakor pri tem ne gre zanemariti resnih tveganj za zlorabe tako zbranih podatkov v morebitne politične ali druge nezakonite namene.

- **K 27. členu ZNPPol-C (sprememba 113.a člena, avtomatizirano preverjanje registrskih tablic v javnem prometu)**

Predlagani dopolnjeni novi 113.a člen, ki opredeljuje avtomatizirano preverjanje registrskih tablic v javnem prometu (ANPR), se glasi:

»*113.a člen*
(avtomatizirano preverjanje registrskih tablic v javnem prometu)

(1) Pri nadzoru cestnega prometa na javnih cestah in nekategoriziranih cestah, ki so dane v uporabo za javni promet, smejo policisti uporabljati tehnična sredstva za optično prepoznavo registrskih tablic in samodejno (avtomatizirano) obdelavo ter primerjanje tako zabeleženih podatkov z evidencami iz četrtega odstavka tega člena.

(2) Ukrep iz prejšnjega odstavka zajema zbiranje podatkov, dostop do osebnih podatkov v evidencah, ki so povezane z odčitano registrsko tablico, analizo, obdelavo in primerjavo podatkov med evidencami z namenom ugotovitve ali je potrebno na tako ugotovljeni primerjavi nadaljnje ukrepanje policije glede nalog, določenih v tretjem odstavku tega člena.

(3) Policisti smejo avtomatizirano preverjanje registrskih tablic v javnem prometu in obdelavo osebnih podatkov po tem členu uporabljati:
pri iskanju oseb,
pri iskanju ukradenih vozil in registrskih tablic,
za izvajanje odrejenih ukrepov s strani sodišč,
za preverjanje, če ima voznik vozila veljavno vozniško dovoljenje,
za preverjanje, če je vozilo na javni cesti in nekategorizirani cesti, ki je dana v uporabo za javni promet, registrirano in tehnično ustrezno za vožnjo,
za preverjanje, če vozilo do 3.500 kg največje dovoljene mase izpolnjuje pogoje za uporabo cestninske ceste ali cestninskega cestnega objekta.

(4) Za potrebe izvajanja tega ukrepa lahko policija primerja osebne podatke pridobljene na podlagi optične prepoznave registrske tablice z:
evidenco iskanih oseb, evidenco iskanih in najdenih predmetov, evidenco odrejenih ukrepov sodišč in evidenco pogrešanih oseb iz tega zakona,
evidenco o vozniških dovoljenjih iz zakona, ki ureja voznike,
evidenco registriranih vozil in evidenco homologiranih vozil iz zakona, ki ureja motorna vozila,
evidenco prodanih elektronskih vinjet, evidenco registrskih označb vozil, oproščenih plačila cestnine, evidenco izmerjenih vozil z višino manj kot 1,3 metra nad prvo osjo in evidenco registrskih označb vozil z neplačano cestnino iz zakona, ki ureja cestninjenje.

(5) Policisti tehničnih sredstev za optično prepoznavo registrskih tablic ne smejo uporabljati za vsesplošen preventivni nadzor cestnega prometa, temveč le za opravljanje nalog po tretjem odstavku tega člena.«.

Predlagatelj je glede avtomatizirano preverjanje registrskih tablic v javnem prometu pripravil oceno učinka, ki je zahtevana z 49. členom ZVOPOKD.

Eden izmed ključnih pomislekov pri delovanju ANPR sistemov je, da omogoča množično zbiranje lokacijskih podatkov vseh udeležencev v prometu, zato **je treba zagotoviti strogo upoštevanje**

načela minimizacije obdelave osebnih podatkov in načela namenskosti. Takojšen izbris tistih zajetih podatkov registrske tablice, ki ne bi bili uporabljeni za izvedbo nalog oziroma katerih primerjanje z drugimi evidencami podatkov ne bi privedlo do ujemanja (zadetka), lahko tudi po mnenju Varuha človekovih pravic onemogoči množični nadzor (zahteva za presojo ustavnosti in odločba Ustavnega sodišča RS št. U-I-152, 4. 7. 2019).

Po pregledu priložene ocene učinka IP ugotavlja, da predlagatelj v priloženi oceni učinka navaja, da se bodo v primeru, da ne bo zadetka, **podatki brisali takoj, v nasprotnem primeru pa takoj po zaključku policijskega postopka, ki se bo nanašal na zadetek iz tretjega odstavka novega 113.a člena, vendar najkasneje v 48 urah**. Navedeno varovalko, ki je po oceni IP ena bistvenih, vsebuje predlagana sprememba prvega odstavka 128. člena ZNPPol):

»– *v evidenci iz 33. točke se podatki izbrišejo nemudoma po sami izvedbi ukrepa, razen v primeru, če primerjava z drugimi evidencami pokaže, da je potrebno nadaljnje ukrepanje policije. V tem primeru se podatki hranijo do zaključka policijskega postopka oziroma nadaljnjega ukrepa policije, vendar največ 48 ur.*«

Menimo pa, da je **nujno potrebna dodatna varovalka, s katero se zameji tudi nabor prikazanih podatkov na samem zaslonu naprave, ki jo uporabljajo policisti na terenu** – tudi v tem primeru je bistveno upoštevati načelo minimizacije obdelave osebnih podatkov – **v primeru, da ni zadetka se na zaslonu naprave ne bi smelo pokazati nobenih drugih podatkov kot podatek o preverjeni registrski tablici in eventualno podatek o uspešno opravljeni poizvedbi oziroma tehnični podatki o pravilnem delovanju sistema**. Prav gotovo se, ko ni zadetka, ne bi smelo pokazati več podatkov, kot npr. podatki o lastniku vozila ali drugi osebni podatki iz povezanih evidenc ipd., kar pa mora biti izrecno zakonsko določeno, sicer bi lahko sistem v praksi deloval drugače in bi tudi v primeru 'ne-zadetkov' prikazoval nesorazmeren nabor podatkov. Gre za bistven ukrep, s katerim se lahko zmanjša možnost uporabe osebnih podatkov za druge namene in t.i. pojav »function creep« ter učinek vsesplošnega nadzora mimo vozečih vozil.

- **K 28. členu ZNPPol-C (sprememba 114.a člena, način uporabe tehničnih sredstev pri zbiranju podatkov zaradi opravljanja policijskih nalog)**

Predlagatelj z dopolnitvijo drugega odstavka 114.a člena ZNPPol širi obseg situacij, ko je dopustno zbiranje osebnih podatkov z uporabo brezpilotnih zrakoplovov (dronov) tudi na nadzor cestnega prometa na javnih cestah in na drugih javnih površinah (tretji odstavek 113. člena ZNPPol), če je nadzor načrtovan na kritičnem odseku javne ceste ali zaradi učinkovitejšega ukrepanja policije ob zgostitvah prometa ali drugih interventnih dogodkih. Na ta način še vedno ni zagotovljena skladnost z razlago Ustavnega sodišča v odločbi št. U-I-152/17 z dne 4. 7. 2019.

Predlagatelj je iz predhodnega predloga spremembe 114.a člena (nova četrta alineja v drugem odstavku) na podlagi mnenja IP namreč odstranil le prvi del nove predlagane četrte alineje, ki se je glasil:
»– *pri nadzoru cestnega prometa na javnih cestah in na drugih javnih površinah (tretji odstavek 113. člena tega zakona), če je nadzor načrtovan na kritičnem odseku javne ceste*«, kar pozdravljamo.

Trenutno predlog tako predvideva, da se v 114.a členu v drugem odstavku za tretjo alinejo doda nova četrta alineja, ki se glasi:
»– *za učinkovitejše ukrepanje policije ob prometnih zastojih ali drugih interventnih dogodkih,*«.

Predlagatelj je tako ohranil možnost uporabe brezpilotnikov »*za učinkovitejše ukrepanje policije ob prometnih zastojih ali drugih interventnih dogodkih*«. IP ob tem opozarja, da gre za nejasno določbo, saj poseg v pravico do varstva osebnih podatkov ni jasno opredeljen, na kar je že opozorilo Ustavno sodišče v presoji drugih določb (glej primer ANPR). Iz predlaganih določb tako npr. ni jasno, ali bo policija brezpilotnike za učinkovitejše ukrepanje policije ob prometnih zastojih ali drugih interventnih dogodkih uporabljala zgolj na način pogleda iz zraka ali bo to vključevalo snemanje, morebitne ANPR in druge sisteme itd. Poseg je namreč v pretežni meri odvisen od sistemov, ki bodo nameščeni na brezpilotnike, in senzorjev za zajem podatkov. Brezpilotnik kot tak je namreč le plovilo, ki samo po sebi ne posega v človekove pravice, ključni so sistemi, ki so nanje nameščeni, pri čemer pa je teoretično in praktično njihov nabor neomejen, saj se lahko nanje namesti širok nabor tehničnih sredstev, od ANPR sistemov, IMSI lovilcev, navadnih in termovizijskih kamer, radarskih sistemov, sistemov za merjenje hitrosti, sistemov za biometrijsko prepoznavo itd. Posledično menimo, da:

- bi morala biti predlagana določba **neprimerno bolj konkretizirana z vidika obsega in intenzivnosti posega v pravico do varstva osebnih podatkov – jasno bi moralo biti, kateri podatki naj bi se pri tem zbirali, za katere namene, v katerih evidencah naj bi se hrani, koliko časa** itd., da je omenjeni poseg sploh mogoče presojati z vidika sorazmernosti in ostalih temeljnih načel varstva osebnih podatkov; pri tem opozarjamo, da gre za **zakonsko materijo** in ne za materijo, ki bi se lahko urejala s pravilniki oziroma drugimi podzakonskimi akti;
- bi moral zakon vsebovati **jasno zakonsko določbo, da se glede na zasledovane namene dopustnost uporabe brezpilotnikov nanaša samo na tehnična sredstva, za uporabo katerih ima policija izrecno zakonsko podlago**.

Predlog Pravilnika o uporabi brezpilotnih pravilnikov v policiji v tretjem odstavku določa. »*Policija hrani zapise o opravljenih poletih z brezpilotnimi zrakoplovi 2 leti in vodi evidenco posnetkov skladno s predpisi, ki urejajo varstvo osebnih podatkov*«. **V 123. členu ZNPPol, ki določa, katere evidence policija vodi in vzdržuje v zvezi z izvajanjem policijskih pooblastil, taka evidenca ni predvidena**. Tudi predlog sprememb ZNPPol, ki ga trenutno obravnavamo, ne predvideva take evidence. **Tako temeljna vprašanja v zvezi z obdelavami osebnih podatkov niso urejena** (kakšen nabor podatkov vsebuje ta evidenca, kaj se zgodi s podatki po preteku predvidenega roka hrambe, kdo in pod kakšnimi pogoji ima dostop do te evidence, pravica posameznika do seznanitve, …), kar ni skladno z 38. členom Ustave RS.

IP zato predlaga, da se besedilo sprememb 114.a člena, ki se nanaša na novo četrto alinejo drugega odstavka 114.a člena ZNPPol, bodisi črta bodisi konkretizira ter ocenjuje, da predlagano besedilo v nasprotnem primeru kljub spremembi ni skladno z Ustavo RS. Prav tako ocenjujemo, da bi kakršnekoli nove evidence Policije, kot je navedena evidenca posnetkov, v zvezi z uporabo brezpilotnih letalnikov moral določati zakon in ne podzakonski predpis.

- **K 29. členu ZNPPol-C (sprememba 115. člena)**

Predlagani novi tretji odstavek 115. člena ZNPPol določa splošno in arbitrarno opredeljeno omejitev pravice posameznika, na katerega se nanašajo osebni podatki, do seznanitve s temi podatki, kadar policija pridobiva podatke od drugih upravljavcev. S tem ko določa, da se bo posameznik pri drugem upravljavcu o posredovanju podatkov, ki se nanašajo nanj, policiji seznanil le na podlagi soglasja policije, bistveno otežuje vse postopke seznanitve pri vseh upravljavcih, čeprav je dejansko omejitev po 127. členu ZNPPol in 24. ter 25. členu ZVOPOKD relativno malo. Bistveno primerneje bi bilo, če bi morala policija proaktivno v primerih, ko gre za izjemo upravljavca obvestiti, da obstaja omejitev in o roku omejitve.

IP predlaga, da se navedene spremembe 115. člena ZNPPol bistveno dopolnijo, v nasprotnem primeru pa IP predlaga njihovo črtanje.

- **K 31. členu predloga ZNPPol-C (sprememba 121. člena, posebna pravila o ustreznosti osebnih podatkov)**

IP v inšpekcijskih postopkih ugotavlja, da Policija ne zagotavlja točnosti in ažurnosti osebnih podatkov, ki jih vodi v svojih zbirkah, saj ne skrbi v zadostni meri za to, da bi bili roki hrambe ustrezno spoštovani (kot upravljavec niso dovolj proaktivni pri pridobivanju informacij s strani tožilstva in sodišč in drugih organov o oprostilnih sodbah ipd). Po informacijah IP je državno tožilstvo sicer naknadno že uredilo to obveščanje, sodišča pa še vedno ne, o ureditvi z drugimi organi IP nima informacij. Po mnenju IP ne more biti sprejemljiva predlagana rešitev, s katero se Policija še naprej izogiba odgovornosti za zagotavljanje učinkovitega izvajanja načela točnosti in ažurnosti in to neposredno prenaša na sodišča in druge organe. IP namreč ugotavlja, da Policija kljub temu, da je problem že več let jasno identificiran, še ni zagotovila ustrezne informacijske rešitve, ki bi zagotavljala pravočasno brisanje vseh podatkov, za katere je potekel rok hrambe. To od upravljavca zahteva tudi 5. člen ZVOPOKD, ki med drugim določa odgovornost upravljavca, da poskrbi, da so osebni podatki točni in, kadar je to potrebno, posodobljeni; pri čemer mora sprejeti vse razumne ukrepe za zagotovitev, da se netočni osebni podatki brez odlašanja izbrišejo ali popravijo ob upoštevanju namenov, za katere se obdelujejo (točnost in posodobljenost). Pri tem morajo upravljavci oz. pristojni organi po ZVOPOKD v skladu z 9. in 10. členom ZVOPOKD pri obdelavi v največji možni meri in z uporabo razumnih ukrepov razlikovati med osebnimi podatki različnih kategorij posameznikov, na katere se nanašajo osebni podatki, kot so: osumljenci; obdolženci; obtoženci; obsojenci; žrtve kaznivega dejanja ali osebe, pri katerih določena dejstva upravičujejo domnevo, da so ali bi lahko bile žrtve kaznivega dejanja; druge osebe, povezane s kaznivim dejanjem, zlasti osebe, ki bi lahko nastopale kot priče, osebe, ki lahko podajo informacije o kaznivem dejanju, ali osebe, ki so ali so bile v stiku ali povezane z osebami iz 1. do 5. točke 9. člena ZVOPOKD. Prav tako morajo pristojni organ pri obdelavi v največji možni meri razlikovati med osebnimi podatki, ki temeljijo na dejstvih, in osebnimi podatki, ki temeljijo na osebnih ocenah. Pristojni organ bi moral izvajati redno notranje preverjanje skladnosti teh obdelav in to dokumentirati. Pri tem osebne podatke, ki temeljijo na osebnih ocenah, v največji možni meri ustrezno označi in utemelji na način, ki omogoča naknadno preverjanje teh ocen.

Določba 121. člena ZNPPol, kot je predlagana, izpostavljene težave ne rešuje in ne naslavlja obveznosti po ZVOPOKD, saj ostaja v delu nejasna, v delu pa nepotrebna. IP predlaga, da se določbo v celoti črta, saj bo v nasprotnem primeru v praksi še naprej povzročala precej zmede.

- **K 34. členu (sprememba 125. člena – v evidenci prikritih, poizvedovalnih in namenskih kontrol dodano zbiranje fotografij in prstnih odtisov)**

IP ugotavlja, da je predlagatelj v evidenci prikritih, poizvedovalnih in namenskih kontrol po 19. točki 125. člena ZNPPol dodal zbiranje fotografij in prstnih odtisov, pri čemer pa predlog ZNPPol-C niti veljavne določbe ZNPPol nikjer (npr. v 44. ali 45. členu) ne določajo nobenih ukrepov za zaščito pravic posameznikov v zvezi z zbiranjem in vnosom fotografij (kot npr. predhodno presojanje, kdaj se fotografija ali prstni odtis vnese, kako dolgo se glede na konkretne namene hrani ipd.), kot so zahtevane z Uredbo 2018/1862/EU. Ta med drugim določa, da bi vsak vnos fotografij, podob obraza ali daktiloskopskih podatkov in vsaka uporaba takih podatkov v Schengenskem informacijskem sistemu morala biti omejena na to, kar je potrebno za doseganje zadanih ciljev, bi morala biti dovoljena v skladu s pravom EU, bi morala spoštovati temeljne pravice, vključno z največjo koristjo otroka. Tem zahtevam bi v luči načela sorazmernosti po mnenju IP glede na določbe slovenske ustave morali zadostiti tudi nacionalni predpisi. IP se zato sprašuje, na čem predlagatelj utemeljuje potrebo po

avtomatičnem vnosu (na zalogo) fotografij v vseh primerih in predlaga, da se določbe v tem delu ustrezno dopolnijo s ciljem zagotavljanja zgoraj navedenih zahtev po izvajanju načela sorazmernosti v praksi.

- **K 35. členu predloga ZNPPol-C (sprememba 126. člena, posebna pravila za vpisovanje podatkov v evidence)**

V 126. členu se v prvem odstavku črta besedilo »ali ugotovitve identitete osebe«. Predlog spreminja pravila glede obdelave DNK in prstnih odtisov v primeru ugotavljanja identitete osebe, saj je doslej veljalo, da se ta podatek v takem primeru sploh ne vpisuje v evidenco, po novem pa naj bi se vpisoval, vendar naj bi se v njej hranil samo do ugotovitve identitete neznane osebe. S tem je povezana nedoslednost pri urejanju brisanja podatkov, saj za ta primer brisanje v 45 dneh ni predvideno.

IP zato ocenjuje, da bi bilo treba v četrti alineji drugega odstavka 129. člena dodati tudi dostavek »od ugotovitve identitete neznane osebe«, ali pa še bolje določiti, da se podatek takoj po ugotovitvi identitete v celoti briše in ne samo blokira.

- **K 37. členu predloga ZNPPol-C (sprememba 128. člena, roki hrambe podatkov)**

IP z vidika ustavnih pravic posameznika in dolžnosti upravljavcev glede zagotavljanja točnosti in ažurnosti podatkov ter spoštovanja rokov hrambe podatkov kot nesprejemljivo ocenjuje prenašanje bremena za izbris podatkov iz evidenc policije v celoti na posameznika. Zato predlagamo bistveno dopolnitev besedila predlaganega novega 5. odstavka 128. člena na način, da ne bo nobenega dvoma, da mora policija in/oz. pristojni upravljavec kazenske evidence zagotoviti ustrezno izmenjavo podatkov z namenom pravočasnega izbrisa podatkov iz evidenc ZNPPol iz tega razloga (torej zaradi izbrisa obsodb iz kazenske evidence).

Prav tako IP ponovno predlaga, da se rok hrambe podatkov API in PNR po 30. oz. 31. točki 125. člena ZNPPol v neblokirani obliki skrajša na čas, ki je potreben za izvedbo ocene tveganja, kar naj bo največ 1 mesec od datuma prejema podatkov.

- **K 38. členu predloga ZNPPol-C (sprememba 129. člena, blokiranje podatkov)**

IP opozarja, da ne glede na širjenje kroga podatkov in evidenc, iz katerih se osebni podatki brišejo, ter krajšanje roka hrambe v nekaterih evidencah, še vedno za velik krog evidenc, določbe ZNPPol dejansko predvidevajo izredno dolg rok hrambe, kar ni skladno z načelom sorazmernosti. S tem ko se za številne evidence določa zgolj blokiranje podatkov in razmeroma široko pooblastilo za dostopanje do podatkov, se dejansko ne izvaja zahtevanega izbrisa, ampak gre na praktični ravni zgolj za obliko ukrepa zavarovanja osebnih podatkov. Dostop do vseh blokiranih podatkov je namreč policistom in pristojnim državnim organom še naprej dovoljen zaradi preiskovanja vseh kaznivih dejanj, ki se preganjajo po uradni dolžnosti ter v vseh drugih primerih, ki so določeni z zakonom. Za blokirane podatke so tudi po predlagani dopolnitvi s predlogom ZNPPol-C v drugem odstavku 129. člena ZNPPol določeni izredno dolgi roki hrambe: za evidence iz 1. (evidenca kaznivih dejanj) in 7. (evidenca operativnih informacij) točke drugega odstavka 123. člena ZNPPol 30 let; za evidence iz 8. (evidenca preiskav DNK), 14. (evidenca daktiloskopiranih oseb) in 15. (evidenca fotografiranih oseb) točke drugega odstavka 123. člena ZNPPol v določenih primerih celo 5-30 let; za evidence iz 2. (evidenca prekrškov), 4. (evidenca identifikacij) in 6. (evidenca operativnih informacij) točke drugega odstavka 123. člena ZNPPol 10 let. V praksi to pomeni, da so dejansko ves ta čas osebni podatki v uporabi, četudi niso dostopni popolnoma vsakemu policistu.

Dodaten resen poseg v zasebnost, na katerega je IP že opozarjal, so nejasnosti glede obravnave in nadaljnje hrambe podatkov na podlagi Zakon o varstvu dokumentarnega in arhivskega gradiva ter arhivih (v nadaljevanju ZVDAGA) ter dostopnosti podatkov, ki se na ta način dalje hranijo. Predlagatelj in zakonodajalec te materije, ki je v primeru evidenc in spisov Policije specifična in ni primerljiva s klasičnimi upravnimi spisi, nista naslovila v predlogu ZVOPOKD, zato ponovno opozarjamo, da bi morala država ustrezno nasloviti ureditev arhiviranja in obravnave evidenc z vidika varovanja pravic posameznikov in izbrisa podatkov, ki jih vodi Policija (zlasti gre za evidence iz 123. člena ZNPPol), z vidika varstva osebnih podatkov in dejanskega izbrisa podatkov še posebej glede na težave zlasti z izvajanjem ZVDAGA v praksi. To pomeni, da bi bilo treba opredeliti, kateri osebni podatki iz evidenc in spisov Policije se hranijo trajno na podlagi ZVDAGA in kakšne so varovalke za hrambo in nadaljnjo javno dostopnost tistih podatkov, ki se na podlagi ZVDAGA hranijo trajno. Za te odločitve bi bilo treba izvesti resno strokovno presojo v sodelovanju policijskih strokovnjakov, strokovnjakov za človekove pravice ter Arhiva RS, pri čemer mora biti vodilo tehtanja javnega interesa arhiviranja ter pravic posameznika do zasebnosti in izbrisa tistih osebnih podatkov, za katere ne obstaja več dejanski interes hrambe glede na zakonsko opredeljen namen zbiranja. Direktiva EU 2016/680 v 4. členu namreč določa, da obdelava podatkov s strani istega ali drugega upravljavca lahko vključuje arhiviranje v javnem interesu, znanstveno, statistično ali zgodovinsko uporabo za namene iz prvega odstavka 1. člena Direktive EU 2016/680, če je zagotovljena ustrezna zaščita pravic in svoboščin posameznikov, na katere se osebni podatki nanašajo. Kot je seznanjen IP, bi lahko (ne)prevzem gradiva s strani Arhiva RS, nejasnosti glede vloge blokiranja, anonimizacije in izbrisa osebnih podatkov iz evidenc Policije in *de facto* trajna hramba osebnih podatkov predstavljala resna tveganja za varstvo podatkov in pravice posameznikov.

IP predlaga, da predlagatelj navedeno materijo prouči in ustrezno zakonsko naslovi, saj nastala situacija, ko so dejansko tako rekoč trajno na Policiji teoretično zgolj ob zagotavljanju ukrepov zavarovanja lahko dostopni številni osebni podatki, ni sprejemljiva.

- **K 39. členu predloga ZNPPol-C (129.a člen – depersonalizacija podatkov)**

IP ponovno izpostavlja, da določbe točke f 2. odstavka 12. člena Direktive EU 2016/681 predvidevajo brisanje vseh zbranih podatkov API (torej vseh podatkov iz evidence potnikov, prijavljenih na let (API) po 30. točki člena 125 ZNPPol). Dikcija, kot jo predvideva predlog ZNPPol (brisanje zgolj podatkov, *ki vsebujejo kakršne koli informacije, na podlagi katerih bi bilo mogoče neposredno identificirati potnika*), posledično ni ustrezna in pravno gledano ni jasna, ne pomeni pravne varnosti in ne izpolnjuje zahtev po brisanju podatkov, po izpolnitvi namena, kot to določa Direktiva EU 2016/681. Pomenila bi namreč dejansko lahko trajno 5-letno hrambo vseh tistih osebnih podatkov API, ki omogočajo posredno identifikacijo.

V tem delu torej sporočamo, da zgornji predpis oz. deloma že veljavni ZNPPol kljub nekaterim dopolnitvam predloga ZNPPol-C po mnenju IP ni skladen z zahtevami predpisov s področja varstva osebnih podatkov in določb 38. člena Ustave RS.

Hvala za sodelovanje in lep pozdrav,

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