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: 007-36/2021/2
Datum: 1. 9. 2021

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) – MNENJE
ZVEZA: Vaš e-dopis št. IPP 007-39/2021/18 (146-01), z dne 20. 7. 2021

Spoštovani,

na podlagi vašega 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) in 76. člena Zakona o varstvu osebnih podatkov na področju obravnavanja kaznivih dejanj (v nadaljevanju ZVOPOKD) posredujemo pripombe Informacijskega pooblaščenca (v nadaljevanju IP) k predlaganim dopolnitvam in 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 ocenam učinkov predvidenih dejanj obdelave na varstvo osebnih podatkov na podlagi 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 predlagane 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, pri čemer večina teh predlogov ne vsebuje zahtevanih ocen učinkov predvidenih dejanj obdelave na varstvo osebnih podatkov, kot jih zahteva 49. člen ZVOPOKD, oceni učinkov za dva primera širjenja pooblastil, ki sta priloženi, pa sta skopi in zelo pomanjkljivi ter ne zadoščata zahtevam 49. člena ZVOPOKD. Gre za oceno učinkov glede uvedbe sistema Lifeseeker – sistem primerljiv s t.i. IMSI lovilci ter oceno učinkov za uvedbo avtomatiziranega preverjanja registrskih tablic v javnem prometu.

Poleg tega želi 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, posebej izpostaviti:

- predlog za izvajanje stalnega video in avdio nadzora nekaterih javnih površin,
- 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 opozarjal in ki se s spremembami 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;
- neposreden elektronski dostop policije do širokega nabora evidenc,
- 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 predvideva črtanje 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 (razen v določenih primerih) pravico do anonimnosti pri podaji obvestil. IP takšni spremembi nasprotuje in opozarja, da ureditev, da bi po novem 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 zmanjšuje raven varstva pravic posameznikov. Za uveljavljanje pravice s strani posameznika je bistveno, da je ta z njo seznanjen, kar pa bi po novem 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.

Obveznost obveščanja naj bi po navedbah predlagatelja oteževala komunikacijo policistov z ljudmi. Predlagatelj v obrazložitvi ne navaja nobenih prepričljivih razlogov za sprejem take spremembe, ampak argumente podaja povsem na splošno. Tudi primeri, ki jih navaja so povsem splošni in iz njih ni mogoče razbrati, zakaj naj bi obveščanje posameznikov o pravicah do te mere oteževalo izvajanje policijskih nalog, da ga je potrebno opustiti. Namen spremembe pa naj bi bil zgolj v tem, tako obrazložitev, da se policista razbremeni podajanja takšnega obvestila v nekaterih izjemnih situacijah, kjer to resnično ni smiselno. Če je to namen predlagane spremembe, potem mora biti zakonska dikcija takšna, da je ta namen dosežen, da pa niso možne širše interpretacije, kot bi lahko izhajale iz predlaganega besedila. V praksi namreč 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. Če obstajajo primeri, ko tako obveščanje res bistveno otežuje policijsko delo, naj se člen oblikuje na način, da se v takih izjemnih primerih obveščanje lahko opusti, v vseh drugih pa naj ostane. Če se bo obveščaje črtalo, bo pravica v veliki meri ostala gola črka na papirju.

IP pri tem ponovno opozarja na problematično prakso pri pridobivanju podatkov o uporabnikih različnih spletnih storitev, kjer je policija v številnih primerih svoja pisna oz. ustna zaprosila formulirala tako, da je bila zaprošena oseba prepričana, da zaprošene podatke, vključno s prometnimi podatki, mora posredovati. Kot smo že večkrat poudarili v svojih poročilih oz. na medsebojnih sestankih, takšna

praksa ne sme biti dopustna. Obveznost posredovanja podatkov obstoji zgolj v primerih, ko to določa 115. člen ZNPPol ali drug zakon. V teh primerih mora biti dopis tudi ustrezno označen kot obvezen (kot zahtevek, ne zaprosilo), in mora opozoriti na posledice neposredovanja. V ostalih primerih pa mora iz dopisa jasno izhajati, da gre za zbiranje obvestil, ter da je odgovor na dopis prostovoljno ravnanje. To še posebej drži, ker veljavna možnost zbiranja obvestil velja tudi za s.p.-je in pravne osebe.

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 8. členu predloga ZNPPol-C (sprememba 41. člena zakona, načini ugotavljanja identitete)**

Določba predvideva povsem nesorazmerno izvajanje biometrijskih ukrepov pri ugotavljanju identitete posameznikov s strani policije, saj zajemanja biometričnih podatkov z ničemer ne omejuje (ne določa nobenih dodatnih pogojev zanj), ampak ga dopušča v prav vsakem postopku ugotavljanja identitete. Glede na težo posega v informacijsko zasebnost posameznika, ki ga izvajanje takega ukrepa predstavlja, bi ga bilo eventualno dopustno izvajati v izjemnih, posebej utemeljenih in v zakonu določenih primerih, ne pa dopustiti na splošno, kot to predvideva navedena določba.

IP zato ugotavlja, da je širitev nabora osebnih podatkov, ki se lahko zbirajo od posameznika v zvezi z ugotavljanjem identitete, na vse biometrične podatke osebe nejasna, nedoločna in preširoka, saj ne določa, katere biometrične podatke lahko zbira policija za namen ugotavljanja identitete, pri čemer ločeno na drugih mestih določa zbiranje določenih biometričnih podatkov v posameznih konkretnih primerih. Pojem biometrični podatek je namreč izredno širok, in sicer so glede na določbe 14. točke 4. člena ZVOPOKD to: osebni podatki, ki so rezultat posebne tehnične obdelave v zvezi s fizičnimi, fiziološkimi ali vedenjskimi značilnostmi posameznika, ki omogočajo ali potrjujejo edinstveno identifikacijo tega posameznika, kot so podobe obraza ali daktiloskopski podatki. Predlagatelj torej ni jasno opredelil vrste osebnega podatka, ki naj bi bil predmet zbiranja in s tem ni zadostil načelu pravne varnosti, ki zahteva da morajo biti pravne norme jasne in določne. V konkretnem primeru to pomeni, da bi lahko policist v vsakem posameznem policijskem postopku ugotavljanja identitete prosto izbiral in presojal, katere biometrične podatke bo zbiral in zahteval od posameznika, kar ni dopustno. Besedilo je v tem delu tudi samo s seboj v nasprotju, saj predlagano besedilo 5. odstavka istega člena določa nekatere primere, ko smejo policisti vzeti prstne odtise in fotografirati osebo. Prav tako ne drži navedba predlagatelj v obrazložitvi, da z zajemom biometričnih podatkov ne prihaja do hrambe podatkov in ustvarjanja novih zbirk podatkov oziroma evidenc. Brez vsaj kratkotrajne hrambe namreč primerjava podatkov v drugih zbirkah ne bi bila mogoča.

Prav tako iz predloga ZNPPol-C ne izhaja jasna obrazložitev, zakaj bi morala imeti policija v vsakem primeru ugotavljanja identitete 'po potrebi' možnost zajema vseh biometričnih podatkov, brez opredelitve, da je to npr. skrajni ukrep oz. dopusten ukrep zgolj, če identitete ni mogoče zanesljivo ugotoviti na drug način (npr. z vpogledom v javno listino s fotografijo osebe).

Zato IP predlaga, da se člen ustrezno dopolni ter izčrpno navede primere, katere biometrične podatke je dopustno zbirati ter v katerih primerih ali pa se črta besedilo », *po potrebi zajamejo biometrične podatke osebe*«, da se zagotovi sorazmernost obdelav osebnih podatkov.

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

S spremembo prvega odstavka 41. člena ZNPPol se 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.

Problematična je tudi predvidena sprememba drugega odstavka, saj pojma »neznana oseba« ZNPPol ne definira in ga je zato mogoče interpretirati zelo široko. To izhaja tudi iz obrazložitve, saj predlagatelj pod tem pojmom razume tudi npr. storilce kaznivih dejanj in prekrškov, kar pomeni, da bi policija vse navedene načine obdelave (tudi biometričnih) osebnih podatkov lahko uporabljala ne samo pri storilcih kaznivih dejanj in prekrškov ampak tudi širše, pri vsakemu posamezniku, ki ji ne bi bil znan, v kontekstu katerekoli njene policijske naloge. Sprejetje take določbe bi 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*) in s pomočjo te tehnologije prepoznava ne samo storilce prekrškov, ampak tudi vse druge »neznane osebe«, kar bi potencialno omogočalo zlorabo tako zbranih podatkov v nezakonite, celo politične namene.

V zvezi s tem IP ponovno izpostavlja tudi 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 tudi besedilo 1. odstavka 42. člena ZNPPol ustrezno dopolni na način, da bodo tehnična sredstva opredeljena upoštevajoč načelo sorazmernosti, določnosti obdelav in ne zgolj primeroma.

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 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. 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)**

IP ugotavlja, da predlagana nova sedma alineja četrtega odstavka 43. člena ZNPPol predvideva uporabo tehničnih sredstev za lociranje mobilnih naprav brez kakršnihkoli dodatnih resnih varovalk ali omejitev, kot pojasnjujemo v nadaljevanju.

Poleg tega 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 ob tem predlaga, 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.

V skladu s 147. členom Zakona o elektronskih komunikacijah (ZEKom-1; Uradni list RS, št. 109/12, 110/13, 40/14 – ZIN-B, 54/14 – odl. US, 81/15, 40/17) mora operater varovati zaupnost komunikacij. Ta zaupnost se nanaša na vsebino komunikacij, podatke o prometu in lokacijske podatke, povezane s komunikacijo, ter dejstva in okoliščine v zvezi s prekinitvijo povezave ali s tem, da povezava ni bila vzpostavljena. Informacije o komunikacijah smejo tako pridobiti le v obsegu, ki je nujno potreben za izvajanje določenih javnih komunikacijskih storitev, te informacije pa smejo uporabljati ali posredovati drugim le zaradi izvajanja teh storitev. Peti odstavek istega člena nadalje določa, da so vse oblike nadzora oziroma prestrezanja komunikacij, ki jih izvajajo tretje osebe in te niso uporabniki, udeleženi v komunikaciji, kot so poslušanje, prestrezanje, snemanje, shranjevanje in posredovanje komunikacij iz prvega odstavka tega člena brez soglasja zadevnih uporabnikov, prepovedane, razen če je to dovoljeno v skladu s prejšnjim odstavkom ali v skladu s 153. ter 160. členom tega zakona oziroma če je taka oblika nadzora oziroma prestrezanja nujno potrebna za prenos sporočil (npr. telefaks sporočila, elektronska pošta, elektronski predali, glasovna pošta, storitev SMS). Ob tem IP poudarja, da sme policija na podlagi 153. člena ZEKom-1 zaradi varstva življenjskih interesov posameznika in kadar je to glede na okoliščine konkretnega primera nujno, od operaterja pridobiti določene podatke za ugotovitev zadnje lokacije opreme za mobilno komunikacijo. Gre za podatke o lokacijski oznaki (ID celice) na začetku komunikacije in podatke, ki določajo zemljepisno lego celic z navedbo njihovih lokacijskih oznak (ID celice) med obdobjem, za katero se hranijo, podatke o komunikaciji ter druge podatke, ki jih v zbirkah osebnih in drugih podatkov obdeluje operater in lahko omogočajo natančnejšo ugotovitev zadnje lokacije opreme za mobilno komunikacijo posameznika.

IP ugotavlja, da je ureditev v ZEKom-1 (tu gre poleg 153. člena upoštevati tudi 153.a člen) bolj natančna in podrobna, kot je to primer v ZNPPol-C (to velja tudi ob upoštevanju nekaterih dodatnih določb, ki jih s tem v zvezi vsebuje Pravilnik o policijskih pooblastilih). Glede na to, da predlagana ureditev pomeni dodatni in globlji poseg v zasebnost posameznika, saj širi nabor podatkov, ki jih bo o njegovi komunikaciji smela pridobiti policija, bi bilo treba poskrbeti za dodatne določbe in opredelitev ukrepov za zmanjšanje tveganj, ki obstajajo za varstvo pravic in svoboščin posameznika ob tovrstni obdelavi njegovih osebnih podatkov ter na ta način preprečiti nesorazmerne posege v zasebnost pogrešane osebe oziroma osebe v stiski ali 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 49. člen Zakona o varstvu osebnih podatkov na področju obravnavanja kaznivih dejanj (ZVOPOKD; Uradni list RS, št. 177/20) med drugim določa, da:

»(4) Ocena učinka obsega:
1. splošni opis predvidenih dejanj obdelave;
2. oceno tveganj za človekove pravice in temeljne svoboščine ter zakonite interese posameznikov, na katere se nanašajo osebni podatki, zlasti glede prepovedi diskriminacije iz 2. člena tega zakona;
3. ukrepe, namenjene obvladovanju teh tveganj;
4. zaščitne ukrepe, kot so notranji nadzori;

5. ukrepe za zagotavljanje varnosti obdelave;
6. mehanizme za zagotavljanje varstva osebnih podatkov in za izkazovanje skladnosti z zakonom, pri čemer se upoštevajo pravice in zakoniti interesi posameznikov, na katere se nanašajo osebni podatki, in tretjih oseb.
(5) Pred uvedbo novega sistema za avtomatizirano obdelavo osebnih podatkov za namene iz prvega odstavka 1. člena tega zakona pristojni organ izdela oceno učinka glede ukrepov za zagotavljanje varnosti obdelave po 5. in 6. točki prejšnjega odstavka.«

Predlagatelj je k predlogu sprememb ZNPPol-C priložil oceno učinka (»Presoja vplivov na zasebnost (LIFESEEKER - tehnično sredstvo za iskanje pogrešanih oseb«). **IP ugotavlja, da priložena učinka ne izpolnjuje zahtev po 4.2, 4.3, 4.4, 4.5 in 4.6 točki ter po 5. odstavku 49. člena ZVOPOKD.** Še več, na več mestih v sami oceni učinka je izpostavljeno, da tveganj, povezanih z obdelavo osebnih podatkov posameznikov, (praktično) ni. Ob tem IP izpostavlja, da četudi bi se podatki obdelovali zgolj v realnem času in bi bil namen njihove obdelave varovanje življenja posameznika, to še ne pomeni, da ne obstajajo tveganja za človekove pravice in temeljne svoboščine. IP zato svetuje, da se opravi temeljit premislek glede opredelitve vseh tveganj, ki ob tem lahko obstajajo, zlasti (ne pa zgolj) z vidika razpoložljivosti in zaupnosti podatkov (neupravičeno razkritje ali posredovanje, izguba ali izbris podatkov, prekomerna obdelava podatkov, …), ter opredeli ustrezne ukrepe, namenjene njihovemu obvladovanju. Izpostaviti je treba tudi vidik preglednosti – treba je obravnavati tveganje, da vsem posameznikom, katerih osebni podatki se obdelujejo, ne bodo posredovane vse ali da jim bodo posredovane nepopolne informacije o obdelavi osebnih podatkov. Glede slednjega so zelo pomembni ukrepi za ustrezno obveščenost posameznika o obdelavi (v skladu z zahtevami 13. člena Splošne uredbe), vključno z jasno navedbo namenov uporabe, ukrepov za preprečitev nenamenske uporabe in uveljavljanjem pravic posameznikov. V tej luči IP meni, da določba predlagane spremembe osmega odstavka 43. člena ZNPPol, ki določa 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.

Prav tako iz priložene ocene učinka ni razvidno, ali je bilo v zvezi z njeno izdelavo pridobljeno mnenje pooblaščene osebe za varstvo osebnih podatkov in kakšno je njeno mnenje oziroma ali je le-ta opravila svojo nalogo iz 3. točke prvega odstavka 57. člena ZVOPOKD, kjer je določeno, da je med nalogami pooblaščene osebe za varstvo osebnih podatkov tudi svetovanje glede ocene učinka v zvezi z varstvom osebnih podatkov in spremljanje njenega izvajanja v skladu z ZVOPOKD. IP priporoča, da pooblaščena oseba za varstvo osebnih podatkov torej svetuje pristojnim službam upravljavca glede izvedbe ocene učinka, zlasti glede same metodologije izvedbe in uporabe tehničnih in organizacijskih ukrepov za varstvo pravic posameznika. Svetovanje bi moralo zajemati ves čas izvajanja ocene učinka, od same priprave na izvedbo preko dejanske izvedbe do pregleda izvedene ocene in podaje mnenja. Pooblaščena oseba mora torej sodelovati pri izvedbi ocene učinka, ni pa odgovorna za njeno izvedbo.

IP izpostavlja tudi, 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 deluje po principu IMSI lovilca. Iz katerih razlogov tehničnega sredstva LIFESEEKER ne uporabljajo v oceni učinka navedene (in po vsej verjetnost tudi preostale) države članice EU? Če morda katere od držav članic to tehnično sredstvo uporabljajo, kakšne so njihove (pozitivne in negativne) izkušnje? Kakšna tveganja so bila prepoznana ob njihovi uporabi? Pod katerimi pogoji se lahko (če sploh) uporablja navedeno tehnično sredstvo? Tovrstna in druga podobna vprašanja bi morala biti obravnavana v okviru ocene učinka.

IP ob tem znova izpostavlja, da je iz navedene prakse razvidno, da večina teh tehničnih sredstev deluje po principu IMSI lovilca ter opominja, 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.

IP poudarja, da je v okviru tega mnenja zgolj izpostavil nekatera najbolj izstopajoča tveganja, nikakor pa ne vsa, ki bi jih veljalo obravnavati v okviru ocene učinka. IP zato svetuje, da vsa morebitna tveganja podrobno preučite v luči navedenih pojasnil. Ob tem IP pojasnjuje, da je ustrezna in poštena obravnava tveganj zlasti v interesu upravljavca, ki pripravlja oceno učinka. Na ta način se namreč lahko identificira nabor možnih tveganj, kar omogoča tudi hitro ter ustrezno izvedbo ukrepov za odpravo ali ublažitev identificiranih tveganj. Obsežen nabor možnih tveganj glede varstva osebnih podatkov, ki bi jih ocena učinka morala obravnavati, je naveden v smernicah IP »Smernice o presoji vplivov na zasebnost pri uvajanju novih policijskih pooblastil", še zlasti na str.16-18.
https://www.ip-rs.si/fileadmin/user_upload/Pdf/smernice/
Presoje_vplivov_na_zasebnost_pri_uvajanju_novih_policijskih_pooblastil_Smernice_IP.pdf;

IP želi spomniti predlagatelja, da je že izdelal zelo kakovostne in celovite učene učinka na varstvo osebnih podatkov v primeru PNR sistemov, medtem ko priložena ocena učinkov glede tehničnega sredstva LIFESEEKER niti približno ni takšne kakovosti ali celovitosti. Predlagatelj ima na voljo smernice IP, ki so mu lahko v pomoč pri izdelavi ocene učinka (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).

Pomanjkljiva ocena učinkov se odraža tudi v predlaganem zakonskem besedilu, kjer razen relativno splošne določbe osmega odstavka predlaganega 10. člena, po kateri se zbranih podatkov ne sme uporabiti v druge namene, policisti pa morajo s podatki, ki jih pridobijo na podlagi četrtega odstavka tega člena, ravnati še posebno skrbno in jih uporabiti na način in v obsegu, ki so nujno potrebni za ugotavljanje okoliščin pri iskanju pogrešane osebe, **ni konkretnih in bistvenih varovalk**. Iz navedenega po mnenju IP očitno izhaja, da predlagatelj ni niti prepoznal, kaj šele obravnaval vseh možnih tveganj in predvidel primernih varovalk, zato je praktično nemogoče govoriti o sorazmernosti takšnega predvidenega ukrepa oziroma pooblastila.

IP zato predlaga, da se predlagana določba 10. člena predloga ZNPPol-C bodisi bistveno dopolni bodisi črta.

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

IP ugotavlja, da predlagan nov 1. odstavek 45. člena ZNPPol ni skladen z nameni razpisa prikrite, poizvedovalne ali namenske kontrole, kot jih določa Uredba 2018/1862/EU, saj je poleg namenov preprečevanja, odkrivanja, preiskovanja in pregona kaznivih dejanj, izvrševanja kazenske sodbe in preprečevanja ogrožanja varnosti (pri slednji bi kljub vsemu morali napisati javna varnost, ne zgolj varnost) dodan še namen izvrševanja odredbe sodišča. Uredba 2018/1862/EU namreč v 3. odstavku 36. člena določa, da se razpisi ukrepov za osebe zaradi prikrite, poizvedovalne ali namenske kontrole lahko vnesejo za namene preprečevanja, odkrivanja, preiskovanja ali pregona kaznivih dejanj, izvrševanja kazenske sodbe in preprečevanja ogrožanja javne varnosti, kadar gre za v uredbi opredeljene okoliščine, ki so povzete v predlaganih treh alinejah 1. odstavka 45. člena. Poleg tega se lahko na zahtevo organov, pristojnih za nacionalno varnost, v skladu z nacionalnim pravom vnesejo razpisi ukrepov za osebe zaradi prikrite, poizvedovalne ali namenske kontrole, kadar obstajajo

konkretni indici, da so informacije iz prvega odstavka 37. člena Uredbe 2018/1862/EU potrebne za preprečitev resne grožnje, ki jo predstavlja zadevna oseba, ali drugih resnih groženj za notranjo ali zunanjo nacionalno varnost.

Pri dodanem namenu »izvrševanja odredbe sodišča« gre torej za precej širok pojem in širjenje namena razpisa brez pravne podlage v Uredbi 2018/1862/EU in brez kakršnekoli obrazložitve, saj predlagatelj tudi v obrazložitvi ta namen povsem spregleda.

Prav tako IP ugotavlja, da sta predlagana 5. in 6. odstavek 45. člena preskopa glede na določbe Uredbe 2018/1862/EU, saj bi morala biti jasno določena (vsaj) obveznost izbrisa, poleg obveznosti prenehanja izvajanja ukrepa, ki pa pomeni vsebinsko nekaj povsem drugega in nujno ne vključuje tudi izbrisa razpisa vključno z osebnimi podatki. Poleg tega sta predlagani 5. in 6. odstavek 45. člena ostala precej podobna dosedanji ureditvi v ZNPPol. V času, ko se je ta pisal, pa je še veljal Sklep 2007/533/PNZ, ki je bil v primerjavi z Uredbo 2018/1862/EU manj jasen, saj slednja vsebuje poseben člen o izbrisu (55. člen), kar pri sklepu ni bil primer, zato bi bilo treba ob spremembi ZNPPol to upoštevati.

IP zato predlaga, da se besedilo 11. člena predloga ZNPPol uskladi z Uredbo 2018/1862/EU ter določi jasno obveznost izbrisa razpisa in z razpisom povezanih osebnih podatkov po poteku zakonsko ter v Uredbi 2018/1862/EU določenih rokov.

- **K 12. členu predloga ZNPPol-C (sprememba 48. člena zakona, poligrafski postopek)**

Predlagatelj s spremembo prvega odstavka 48. člena ZNPPol želi širiti uporabo poligrafskega postopka iz preiskovanja kaznivih dejanj tudi na zagotavljanje notranje varnosti v policiji.

Kot navaja predlagatelj v obrazložitvi, naj bi po novem policija poligraf uporabljala kot pripomoček pri zbiranju obvestil in kot preventivni ukrep, s katerim bi preverila podatke o odklonskem ravnanju uslužbenca. Gre za resen poseg v zasebnost, ki kljub temu, da je zanj predviden pogoj soglasja posameznika, že kot predlog sam po sebi pomeni poseg v osebnostne pravice posameznika. Posameznik, ki bo namreč predlog poligrafskega postopka zavrnil, bi zaradi tega bil lahko deležen drugačne obravnave. IP opozarja, da gre za nevaren precedens obravnave javnih uslužbencev in se sprašuje, kaj to pomeni za vse druge javne uslužbence, ki so prav tako dolžni spoštovati zakonitost, strokovnost, integriteto pri svojem delu in

- **K 13. 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 21. členu predloga ZNPPol-C (sprememba 91. člena zakona, uporaba po odredbi in po lastni presoji)**

Predlagatelj s predlogom sprememb 5. odstavka 91. člena ZNPPol predvideva, da **bi policisti (torej katerikoli) smeli brez odredbe pristojne osebe in brez poprejšnjega ukaza in opozorila**, če utemeljeno pričakujejo oboroženi odpor, zaradi katerega bi lahko bilo neposredno ogroženo življenje policista ali druge osebe, **uporabiti tudi radarske sisteme za detekcijo navzočnosti oziroma premikov skozi stene in za nujno potreben čas naprave za motenje radiofrekvenčnega spektra (t.i. jammerji ali motilci radijskega signala)**. Kot navaja predlagatelj v obrazložitvi, naj bi šlo npr. za zaključne realizacije mobilnih kriminalističnih oddelkov ali Specialne enote zaradi prijetja nevarnih storilcev kaznivih dejanj, ogleda kraja kaznivega dejanja, hišne preiskave, v primerih, ko je glede na okoliščine mogoče pričakovati, da bi lahko bila ogrožena varnost policistov z eksplozivom ali drugimi nevarnimi sredstvi.

Gre za širitev uporabe tovrstnih naprav poleg primerov določenih v šestem odstavku 55. člena ZNPPol, ki so že sami po sebi določeni razmeroma široko in ne predvidevajo nobenih varovalk oz. določb, da na njihovi podlagi ne bi smelo priti do zbiranja ali obdelave osebnih podatkov.

IP ugotavlja, da je besedilo predloga sprememb bistveno širše, kot ga pojasnjuje obrazložitev, saj ne navaja vezanosti na ogrožanja varnosti z nevarnimi sredstvi, ampak zgolj milejši pogoj, t.j. utemeljeno pričakovanje oboroženega odpora, pri čemer je treba poudariti, da gre za uporabo izredno invazivnega omejevanja pravic brez odredbe in ukaza pristojne osebe in brez naknadnega nadzora sodišča ali drugega pristojnega organa ali drugih varovalk za zagotavljanje zakonite in sorazmerne uporabe teh ukrepov (kot npr. naknadna presoja zakonitosti, izdelava poročila sodišču ipd.), ki bi zagotavljale njihovo zakonito in sorazmerno uporabo.

IP zato predlaga, da se v besedilu 5. odstavka 91. člena ZNPPol doda, da policisti z aktivnostmi in uporabo naprav na podlagi 5. odstavka 91. člena ZNPPol ne smejo zbirati ali obdelovati osebnih podatkov.

- **K 25. členu predloga ZNPPol-C (sprememba 112. člena zakona, zbiranje podatkov – nejasna ureditev zbiranja biometričnih podatkov)**

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 41. in 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 26. 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.

Gre za zbiranje osebnih podatkov povsem na zalogo in ko je tako zbiranje enkrat odrejeno, brez kakršnekoli posebne omejitve, naknadno zagotoviti varovanje temeljnih človekovih pravic ni več učinkovito. Med navedene varovane osebe, ki bi lahko bile na ta način brez lastnega soglasja posredno 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. člena, uporaba tehničnih sredstev pri zbiranju podatkov)**

IP ugotavlja, da se s predlaganimi spremembami 113. člena ZNPPol predlaga uvedba splošne in nejasne pravne podlage za video in avdio snemanje območij kritične infrastrukture in varnostno tveganih območij, pri tem pa določba ne postavljajo nobenih dodatnih pogojev oziroma omejitev (razen soglasja občine pri drugem območju) in predvideva snemanje in posege v temeljne ustavne pravice posameznikov na zalogo.

Dodatno se predlaga podaljšanje roka hrambe posnetkov, ki jih policija ne bo uporabila za dokazovanje kaznivih dejanj in kaznivih dejanj ter identifikacijo kršitev oz. storilcev. Iz obrazložitve predlagatelja ne izhajajo vsebinski razlogi za tako podaljševanje roka hrambe posnetkov, ampak se predlagatelj sklicuje zgolj na uskladitev roka hrambe v evidenci posnetkov policijskih postopkov in določenih javnih zbiranj. S stališča varstva osebnih podatkov bi bilo uskladitev bolj smiselno in sorazmerno izvesti tako, da se rok hrambe poenoti na krajše, 30 dnevno obdobje, saj za daljši rok ni videti jasne utemeljitve.

IP prav tako opozarja na nesorazmernost določb predlaganega novega 5. in 6. odstavka 113. člena ZNPPol, saj želi policija, podobno kot pri javnih zbiranjih (pri čemer so tam pogoji bistveno bolj zamejeni), zdaj stacionalrno in stalno video in avdio snemati tudi območja kritične infrastrukture in varnostno tvegana območja, pri tem pa določba ne postavlja nobenih dodatnih pogojev oziroma omejitev (razen soglasja občine pri drugem območju). Poleg tega vsaj za varnostno tvegana območja nikjer ni najti zakonske definicije tega pojma, kar **pomeni, da ima policija pri določanju takih območij povsem proste roke in se s tem postavlja veliko vprašanje nevarnosti arbitrarnega odločanja o stalnem in popolnem nadzoru določenih območij.** Glede na to, da pod taka območja spadajo (tudi) tista, kjer se zbira večje število ljudi (npr. glavni trgi in ulice v nekem mestu) bi policija z izvajanjem takega 24-urnega vsakodnevnega (zlasti tudi avdio!) snemanja, resno posegala v informacijsko zasebnost pa tudi v druge ustavne pravice posameznikov (npr. pravico do svobodnega in neoviranega zbiranja in združevanja, pravice do tajnosti komunikacij). Tudi obveščanje o snemanju na spletni strani ni primerno, saj bi moral biti posameznik o snemanju obveščen na kraju samem – kot je to glede obvestila o videonadzoru urejeno po ZVOP-1.

Po mnenju IP bi Policija morala glede na resnost možnih posegov in glede na to, da bo šlo za izvajanje stalnega videonadzora in avdionadzora s snemanjem, v ta namen najprej izvesti predhodno oceno učinka predvidenih dejanj obdelave na varstvo osebnih podatkov v skladu z 49. členom ZVOPOKD. Gre namreč za primer obdelave, ki zahteva obvezno predhodno izvedbo ocene učinkov pred začetkom take obdelave s ciljem ustrezne naslovitve vseh tveganj predlaganih sprememb na zasebnost. V predlaganem besedilu ni opredeljen noben ukrep za naslovitev teh tveganj, niti ni mogoče razbrati ali so bila ta tveganja sploh analizirana in prepoznana ter kako bo Policija zagotovila skladnost z načelom sorazmernosti ter ali in v katerih primerih je takšno stalno video in avdio v takšnem obsegu, kot je predlagano, sploh učinkovito, nujno in potrebni za doseganje zasledovanih zakonitih ciljev. Brez ocene učinkov tega tudi ni mogoče oceniti.

Po mnenju IP bi Policija morala pogoje dopustnega stalnega video in avdio nadzora ustrezno ožje opredeliti (nikakor se ne zdi dopustno na primer izvajanje stalnega video in avdio nadzora že za namen preprečevanja prekrškov), torej na zalogo.

- **K 28. členu ZNPPol-C (sprememba 113.a člena, avtomatizirano preverjanje registrskih tablic v javnem prometu)**

Predlog 28. člena ZNPPOl-C se glasi:

28. člen

Za 113. členom se doda nov 113.a člen, ki se glasi:

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

(1) Pri nadzoru cestnega prometa na javnih cestah in na drugih javnih površinah smejo policisti uporabljati tehnična sredstva za optično prepoznavo registrskih tablic in samodejno (avtomatizirano) obdelavo in primerjanje tako zabeleženih podatkov z evidencami policije, ki so določene v tem zakonu in evidencami do katerih ima policija dostop pri nadzoru in varovanju javnega prometa.

(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:

- *za nadzor in urejanje prometa na javnih cestah in nekategoriziranih cestah, ki so dane v uporabo za javni promet,*
- *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 in v okviru izvajanja pooblastil po zakonu, ki ureja pravila in varnost v cestnem prometu.«.

IP uvodoma ugotavlja, da je z delno odločbo Ustavnega sodišča RS št. U-I-152, 4. 7. 2019 Ustavno sodišče odločilo, da zahteva drugega odstavka 38. člena Ustave, da je obdelovanje osebnih podatkov predmet zakonskega urejanja, pomeni, da mora obstajati zakonska podlaga za vsak korak obdelave osebnih podatkov. Ukrep optične prepoznave tablic je zasnovan tako, da vključuje dva koraka obdelave: najprej zbiranje podatkov registrske tablice in nato primerjanje teh podatkov z evidencami osebnih podatkov. Oba koraka obdelave podatkov pomenita samostojen poseg v pravico do varstva osebnih podatkov in terjata samostojno zakonsko razdelano ureditev obdelave osebnih podatkov. Ker izpodbijana ureditev ni bila skladna s to zahtevo, je Ustavno sodišče ugotovilo, da je v neskladju z drugim odstavkom 38. člena Ustave in jo je razveljavilo. Zahteva, da je obdelovanje osebnih podatkov predmet zakonskega urejanja, po stališču Ustavnega sodišča ne pomeni le golega obstoja zakonske določbe, ki omogoča, da policija lahko obdeluje osebne podatke na določen način, temveč mora biti tudi skladna z načeli pravne države iz 2. člena Ustave. Ustavno sodišče je prav tako razveljavilo 32. točko drugega odstavka 123. člena, 32. točko 125. člena in dvaindvajseto alinejo prvega odstavka 128. člena ZNPPol, ki so neposredno povezane z izpodbijano določbo in nimajo samostojnega pomena. Ustavno sodišče je v postopku za oceno ustavnosti z delno odločbo št. U-I-152/17 z dne 4. 7. 2019 razveljavilo četrti odstavek 113. člena, 32. točko drugega odstavka 123. člena, 32. točko 125. člena in dvaindvajseto alinejo prvega odstavka 128. člena Zakona o nalogah in pooblastilih policije (Uradni list RS, št. 15/13, 23/15 – popr. in 10/17).

Dalje IP ugotavlja, da 11. člen ZVOPOKD glede avtomatiziranega odločanje in oblikovanja profilov določa, da:

(1) Odločanje, ki temelji izključno na avtomatizirani obdelavi osebnih podatkov, vključno z oblikovanjem profilov, ki ima lahko negativne posledice za pravni položaj ali pravice posameznika, na katerega se nanašajo osebni podatki, ali ga lahko bistveno prizadene, je prepovedano, razen če je to določeno z zakonom, ki določa pravico posameznika, da zahteva vsaj ponovni in ročni pregled odločitve s strani fizične osebe pri pristojnem organu in da do odločitve izrazi lastno stališče, ter določa tudi druge ukrepe za zagotavljanje ustreznega varstva človekovih pravic in temeljnih svoboščin, ki jih mora izvesti pristojni organ.

(2) Odločitve iz prejšnjega odstavka ne smejo temeljiti na obdelavah posebnih vrst osebnih podatkov, razen če zakon določa ustrezne ukrepe za varstvo človekovih pravic in temeljnih svoboščin ter zakonitih interesov posameznika, na katerega se nanašajo osebni podatki, kot je privolitev posameznika v tako obdelavo.

(3) Pred sprejetjem zakona, ki določa avtomatizirano odločanje, mora pristojni predlagatelj zakona izvesti oceno učinka iz 49. člena tega zakona.

(4) Oblikovanje profilov v okviru avtomatizirane ali drugačne obdelave posebnih vrst osebnih podatkov, ki ima za posledico diskriminacijo posameznikov, na katere se nanašajo osebni podatki, je prepovedano.

IP meni, da je gre pri uporabi ANPR sistemov za tematiko, ki vsaj v določenih predvidenih primerih uporabe, kot je npr. izvajanje odrejenih ukrepov s strani sodišč in iskanje oseb, sodi na področje, ki ga ureja ZVOPOKD (glej 1. člen ZVOPOKD), sama narava sistema pa pomeni odločanje, ki temelji izključno na avtomatizirani obdelavi osebnih podatkov - sistem namreč avtomatsko zazna, odčita in preveri registrsko tablico z določenimi zbirkami osebnih podatkov ter sproži signal v primeru ujemanja.

Glede na določbe 11. člena ZVOPOKD mora pred sprejetjem zakona, ki določa avtomatizirano odločanje, pristojni predlagatelj zakona izvesti oceno učinka iz 49. člena ZVOPOKD.

49. člen ZVOPOKD med drugim določa, da

> *(4) Ocena učinka obsega:*
> 1. *splošni opis predvidenih dejanj obdelave;*
> 2. *oceno tveganj za človekove pravice in temeljne svoboščine ter zakonite interese posameznikov, na katere se nanašajo osebni podatki, zlasti glede prepovedi diskriminacije iz 2. člena tega zakona;*
> 3. *ukrepe, namenjene obvladovanju teh tveganj;*
> 4. *zaščitne ukrepe, kot so notranji nadzori;*
> 5. *ukrepe za zagotavljanje varnosti obdelave;*
> 6. *mehanizme za zagotavljanje varstva osebnih podatkov in za izkazovanje skladnosti z zakonom, pri čemer se upoštevajo pravice in zakoniti interesi posameznikov, na katere se nanašajo osebni podatki, in tretjih oseb.*
>
> *(5) Pred uvedbo novega sistema za avtomatizirano obdelavo osebnih podatkov za namene iz prvega odstavka 1. člena tega zakona pristojni organ izdela oceno učinka glede ukrepov za zagotavljanje varnosti obdelave po 5. in 6. točki prejšnjega odstavka.*

Predlagatelj je k predlogu sprememb ZNPPol-C priložil oceno učinka (»Presoja vplivov na zasebnost pri uvajanju novih policijskih pooblastil (avtomatizirano preverjanje registrskih tablic pri nadzoru cestnega prometa«)). **IP ugotavlja, da priložena učinka ne izpolnjuje zahtev po 4.2, 4.3, 4.4, 4.5 in 4.6 točki ter po 5. odstavku 49. člena ZVOPOKD.**

IP želi spomniti predlagatelja, da je že izdelal zelo kakovostne in celovite učene učinka na varstvo osebnih podatkov v primeru PNR sistemov, medtem ko priložena ocena učnikov glede ANPR ni približno in takšne kakovosti ali celovitosti; predlagatelj ima na voljo smernice IP, ki so mu lahko v pomoč pri izdelavi ocene učinka: 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.

Pomanjkljiva ocena učinkov se odraža tudi v predlaganem zakonskem besedilu, kjer razen relativno splošnega 5. odstavka predlaganega 28. člena, **ni konkretnih in bistvenih varovalk**. Med drugim ni opredeljen morebiten rok hrambe oziroma zavrženje in brisanje podatkov v primeru neujemanja, ni opredeljeno, kakšen nabor podatkov se ob delovanju sistema prikaže policistom na terenu (ali gre zgolj za podatek o ujemanju ali delni ali celotni podatki iz povezanih zbirk, kjer je prišlo do ujemanja itd.). Kot smo že večkrat poudarjali gre za množično obdelavo osebnih podatkov, ki temelji na avtomatiziranem odločanju, sistem pa je povezan s številnimi zbirkami osebnih podatkov, **zato gre za številna in pomembna tveganja glede varstva osebnih podatkov, ki jih** mora predlagatelj najprej v oceni učinka pošteno in celovito nasloviti, predvideti ustrezne ukrepe za njihovo obvladovanja, večdelni test sorazmernosti in te ustrezno »preliti« v zakonsko besedilo. **Obsežen nabor možnih tveganj glede varstva osebnih podatkov, ki bi jih ocena učinka morala obravnavati, je naveden v smernicah IP »Smernice o presoji vplivov na zasebnost pri uvajanju novih policijskih pooblastil"** (https://www.ip-rs.si/fileadmin/user_upload/Pdf/smernice/Presoje_vplivov_na_zasebnost_pri_uvajanju_novih_policijskih_pooblastil_Smernice_IP.pdf; glej zlasti str.16-18).

Specifično glede predlagane ureditve IP dodatno meni, da je glede namenov uporabe ANPR sistemov nesorazmeren namen "*za preverjanje, če ima voznik vozila veljavno vozniško dovoljenje*« in s tem

povezana navezava na zbirko podatkov o vozniških dovoljenjih. Jasno namreč je, da registrska številka vozila ni oz. ni vedno v povezavi z voznikom, ki vozilo dejansko vozi. Sistem bo namreč preveril le registrsko številko vozila, voznik je pa lahko kdorkoli, zato je po mnenju IP takšno preverjanje neprimerno in nesorazmerno glede na množičnost obdelave osebnih podatkov.

- **K 29. 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.

Iz obrazložitve predlagatelja k predlaganim spremembam 114.a člena izhaja, da »*Zakonska določba oži področje uporabe brezpilotnih zrakoplovov. S predlagano novo četrto alinejo prvega odstavka 114.a člena ZNPPol se predvideva, da se brezpilotni zrakoplovi lahko uporabljajo le na kritičnih odsekih cest, in sicer v okviru poostrenih nadzorov (uporaba ob rednih kontrolah ni možna) ali interventnih dogodkih, v katere spadajo tudi zgostitve prometa.«,* kar **po mnenju IP ne drži**. Gre nenazadnje za **novo, dodatno določbo in s tem za dodaten namen uporabe brezpilotnikov**, ki pa je navkljub relativni omejenosti, po našem mnenju problematična, saj ni skladna z razlago Ustavnega sodišča v odločbi št. U-I-152/17 z dne 4. 7. 2019.

V tej odločbi je Ustavno sodišče ob presojanju skladnosti uporabe brezpilotnih letalnikov za dokazovanje kaznivih dejanj in prekrškov ter identificiranje kršiteljev oziroma storilcev z Ustavo ocenilo, da ta pravna podlaga (tretja alineja drugega odstavka 114.a člena ZNPPol) za uporabo brezpilotnikov pri opravljanju policijskih nalog v ZNPPol sicer ni neustavna, je pa Ustavno sodišče v zvezi z izpodbijano določbo podalo obširno razlago, iz katere izhaja:

- da je tehnična sredstva za fotografiranje ter video in avdio snemanje na brezpilotnikih dopustno uporabljati **zgolj za dokazovanje kaznivih dejanj in prekrškov ter identificiranje kršiteljev oziroma storilcev oziroma da jih je dopustno uporabiti zgolj na podlagi že zaznanega prekrška ali kaznivega dejanja**,
- da je s tem **izključena uporaba brezpilotnih zrakoplovov za preventivni oziroma nadzorni namen v smislu odkrivanja protipravnih ravnanj, ki izpolnjujejo znake prekrškov in kaznivih dejanj**.

Ustavno sodišče je v 12. točki zadevne odločbe jasno zapisalo (poudaril IP): »*Uporaba tehničnih sredstev na podlagi prvega odstavka 113. člena ZNPPol je vezana na opravljanje konkretnih policijskih nalog in* ***ni dopustna v okviru splošne preventivne dejavnosti policije, ki bi lahko šele vodila do odkritja posameznega prekrška ali kaznivega dejanja****.*[12] *Vezana je torej na konkretno izvajanje policijskih nalog dokazovanja prekrškov in kaznivih dejanj ter identificiranja kršiteljev in storilcev.* ***Določba nima generalno preventivnega značaja,*[13] *da bi omogočala tudi preventivne dejavnosti policije oziroma nadzor (na primer cestnega prometa),*** *pri katerem bi policija s tako uporabljenimi tehničnimi sredstvi slučajno zaznala tudi izvršitev prekrška ali kaznivega dejanja, ki bi bila na ta način tudi zabeležena.* ***Tehnično sredstvo je dopustno uporabiti le, ko je kršitev, ki izpolnjuje (zakonske) znake kaznivega dejanja ali prekrška, že zaznana.*«**

IP zato predlaga, da se besedilo sprememb 114.a člena, ki se nanaša na novo četrto alinejo drugega odstavka 114.a člena ZNPPol, črta ter ocenjuje, da predlagano besedilo v nasprotnem primeru ni skladno z Ustavo RS.

- **K 30. členu ZNPPol-C (sprememba 115. člena, obveznost posredovanja podatkov – nov neposreden elektronski dostop policije do širokega nabora evidenc)**

Predlagatelj z dopolnitvijo 115. člena ZNPPol (doda se nov drugi odstavek) predvideva, da bi po novem Policija lahko v vseh v primerih, ko lahko zahteva določene podatke na podlagi ZNPPol ali drugih zakonov, sama pridobivala te podatke (torej brez pisne ali podobne izkazljive zahteve in aktivnega posredovanja upravljavca zbirke, kot je veljalo doslej) preko brezplačnega neposrednega elektronskega dostopa do teh podatkov v katerihkoli uradnih evidencah, ki jih upravljajo organi javnega sektorja ali subjekti javnega prava v informatizirani obliki. Policija bi lahko na podlagi teh dopolnitev v podatke iz zbirk podatkov vpogledala, jih kopirala, prepisala ali izpisala ter jih obdelovala v postopkih, kjer izvršuje svoje zakonsko določene naloge in pristojnosti.

V zvezi s predlaganim drugim odstavkom bi bilo po mnenju IP treba resno razmisliti o sorazmernosti in potrebnosti takega neposrednega dostopa policije do vseh zbirk organov javnega sektorja in subjektov javnega prava, pri čemer predlagatelj o predlagani spremembi ni naredil ocene učinkov in ni pretehtal tveganj, ki so s tem povezani. Po mnenju IP bi bilo v ta namen nujno izdelati predhodno oceno učinkov, s katero bi med drugim analizirali, identificirali in naslovili specifike in dodatna tveganja, ki jih takšen neposreden dostop prinaša. IP se sprašuje ali gre policijo res enačiti s sodišči in tožilstvi, saj je Policija del izvršilne veje oblasti in organ kazenskega pregona, s posebnimi tveganji, ki bi jih tovrstna zakonska sprememba morala nujno nasloviti. Zato IP opozarja, da bi veljalo omogočanje takega neposrednega dostopa Policije do vseh uradnih evidenc, nikakor ne bi smelo biti urejeno na splošno, kot to predlaga predlagatelj, in brez ustreznih varovalk. Če se namreč dostop že omogoči, ga je treba natančneje razdelati, analizirati tveganja, določiti konkretne zbirke, vrste osebnih podatkov ter pogoje in druge varovalke, čemur predlagana določba ne zadosti, saj je presplošna. Predlagatelj se v obrazložitvi sklicuje na Zakon o državnem tožilstvu in Zakon o sodiščih, vendar pa ne omeni, da so določbe teh zakonov bolj dodelane in vsebujejo določene varovalke, ki jih predlagana določba ne.

Ob tem predlagani novi tretji odstavek 115. člena ZNPPol določa izredno splošno in arbitrarno opredeljeno omejitev pravice posameznika, na katerega se nanašajo osebni podatki, ki bodo na ta način predmet obdelave, do seznanitve s temu podatki, saj se bo v tem delu posameznik lahko s podatki, ki se nanašajo nanj, seznanil le na podlagi soglasja policije. Dikcije predlaganega besedila zato ni mogoče brati na način, da možnosti zavrnitve seznanitve omejuje zgolj na primere iz 127. člena ZNPPol in ZVOPOKD.

IP predlaga, da se navedene spremembe 115. člena ZNPPol bistveno dopolnijo in se za ta namen naprej izdela ustrezna ocena učinkov, v nasprotnem primeru pa IP predlaga njihovo črtanje.

- **K 32. 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 36. 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 127. člena, pravica do seznanitve z lastnimi osebnimi podatki)**

IP opozarja, da ni jasno, kako naj bi v praksi potekal sam postopek na prvi in drugi stopnji glede odločanja o izjemi pri uveljavljanju ustavne pravice do seznanitve z lastnimi osebnimi podatki, kot je po novem predlagana v 5. alineji prvega odstavka 127. člena ZNPPol. Glede na naravo postopka seznanitve posameznika s podatki, ki se nanašajo nanj, ter povsem drugačno naravo ter namene določb in postopka po 118. in 119. členu ZNPPol bi v praksi lahko prihajajo do nejasnosti in težav. Zato IP predlaga, da se 37. člen predloga ZNPPol v tem delu bodisi ustrezno dopolni ter jasno opredeli, kakšna je morebitna vloga sodišča v takem postopku oz. se jasneje navede, da gre zgolj za opredelitev pristojne osebe za odločanje bodisi se črta sklic na 118. in 119. člen ZNPPol.

- **K 38. 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 39. 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, 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), 7. (evidenca operativnih informacij) in 19. (evidenca prikritih in namenskih kontrol) 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 10-50 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 40. 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 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