Pirc Musar & Lemut Strle
ODVETNIŠKA DRUŽBA

Predlog GZS za spremembo posameznih določb predloga ZVOP-2

Študija predloga

Naročnik:
Gospodarska zbornica Slovenije
Združenje za informatiko in telekomunikacije
Dimičeva 13
1000 Ljubljana

Naša številka: 250/2022
Ljubljana, 26.9.2022

Odvetniška družba Pirc Musar & Lemut Strle o.p., d.o.o., Likozarjeva 14, 1000 Ljubljana,
odvetnice: dr. Nataša Pirc Musar, mag. Rosana Lemut Strle, Ines Rostohar,
Alja Poljšak, Manca Trček, Ula Tomaduz, Katarina Emeršič Polić
telefonska številka: 01 235 50 30, davčna številka SI77958420,
matična številka 6743404000 (Okrožno sodišče v Ljubljani), TRR IBAN: SI56 0201 0026 1275 189, NLB d.d.,
osnovni kapital: 7.500 EUR, **www.pirc-musar.si**

Spoštovani,

na podlagi vašega zaprosila smo izdelali študijo o primernosti predlagane ureditve, kot je bilo zaprošeno, specifično k členom 21., 22., 23., 40., 42., 67., 68., 69., 75. do 79., 80., 82., 92., 93. ter kazenske določbe (97. do 112. člen) predloga ZVOP-2.

Za izhodišče smo vzeli:

- predlog ZVOP-2 z dne 14.7.2022[1],
- predlog sprememb ZVOP-2 Sekcije operaterjev elektronskih komunikacij (8.8.2022), posredovan ob zaprosilu za podajo ponudbe.

Pri izdelavi študije smo se oprli na:

- Splošno uredbo o varstvu podatkov[2],
- ZVOP-1[3],
- področne predpise (kot v besedilu),
- dostopno prakso Informacijskega pooblaščenca (kot v besedilu),
- dostopna mnenja in smernice WP 29 oziroma EDPB (kot v besedilu).

[1] Dostopen prek spletnih strani Državnega zbora: https://www.dz-rs.si/wps/portal/Home/zakonodaja/izbran/!ut/p/z1/04_Sj9CPykssy0xPLMnMz0vMAfIjo8zivSy9Hb283Q0N3E3dLQwCQ7z9g7w8nAwsnMz1w9EUGAWZGgS6GDn5BhsYGwQHG-pHEaPfAAdwNCBOPx4FUfiNL8gNDQ11VFQEAAXcoa4!/dz/d5/L2dBISEvZ0FBIS9nQSEh/?uid=8ABB51F7A7736745C12588800046D644&db=pre_zak&mandat=IX&tip=doc

[2] Uredba (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 o razveljavitvi Direktive 95/46/ES (Splošna uredba)

[3] Zakon o varstvu osebnih podatkov (Uradni list RS, št. 94/07 – uradno prečiščeno besedilo in 177/20); ZVOP-1.

Kazalo vsebine

I. Uvodno o urejanju varstva osebnih podatkov na nacionalni ravni

Splošna uredba o varstvu podatkov postavlja enotna pravila za varstvo osebnih podatkov v EU, nekatera vsebinska in postopkovna vprašanja pa lahko posebej uredijo države članice. ZVOP-2 lahko torej ureja **določena vsebinska področja**, kot so uporaba zdravstvenih, biometrijskih in genetskih podatkov, **nekatere postopkovne vidike** (npr. postopek izrekanja sankcij in pravna sredstva) ter **relacijo do drugih področij in pravic** (npr. dostop do javnih informacij, uporaba osebnih podatkov v znanstvene in statistične namene). ZVOP-2 pa ne sme spreminjati določb Splošne uredbe, saj se ta uporablja neposredno[4]. Eden glavnih ciljev Splošne uredbe je bil »harmonizirati« oziroma uskladiti predpise o varstvu osebnih podatkov držav članic Evropske Unije. Iz tega razloga je bila kot pravni instrument izbrana uredba, neposredno uporabljiva v vseh državah članicah[5].
Države članice so se po začetku uporabe Splošne uredbe o varstvu podatkov regulacije na nacionalni ravni lotevale na različne načine. Primer relativno enostavnega pristopa je hrvaški Zakon o provedbi Opće uredbe o zaštiti podataka[6] z vsega 57. členi, na drugi strani pa lahko najdemo tudi precej obsežnejši poljski zakon o varstvu osebnih podatkov s 176. členi[7].

Različni pristopi držav članic k urejanju varstva osebnih podatkov na nacionalni ravni tudi po začetku uporabe Splošne uredbe o varstvu podatkov lahko ogrozijo doseganje cilja harmonizacije in s tem izjalovijo prizadevanja institucij Evropske Unije v smeri olajšanja doseganja skladnosti s predpisi upravljavcem na njenem območju, še posebej tistim, ki svoje poslovne aktivnosti izvajajo v več državah članicah. Upravljavci se tako žal tudi v prihodnje ne morejo povsem zanesti na to, da bodo v vseh jurisdikcijah znotraj Evropske Unije, v katerih poslujejo, skladnost na področju varstva osebnih podatkov dosegali na enoten način. V primerih, v katerih bi nacionalna ureditev posegla v ureditev iz Splošne uredbe, ne da bi šlo za vsebine, ki jih država članica lahko podrobneje ali samostojno uredi, bo upravljavcu ostala možnost zatrjevanja nedopustnega odstopanja nacionalne ureditve od Splošne uredbe. Pravna pot pa bo slejkoprej časovno (vse do Sodišča Evropske Unije) in finančno zahtevna. Dejstvo pa je, da nacionalna ureditev ne sme biti drugačna,

[4] Enako tudi Informacijski pooblaščenec na svoji spletni strani: https://www.ip-rs.si/zakonodaja/reforma-evropskega-zakonodajnega-okvira-za-varstvo-osebnih-podatkov/najpogostejsa-vprasanja-in-odgovori

[5] Z Uredbo (EU) 2016/679 je bila nadomeščena Direktive 95/46/ES, ki so jo države članice v svoje nacionalne pravne rede prenesle ob pomembnem upoštevanju parcialnih pogledov in že ustaljene ureditve na področju varstva osebnih podatkov, navedeno pa je pripeljalo do bistvenih odstopanj tudi pri osnovnih vprašanjih obdelave osebnih podatkov (kot so pravne podlage za obdelavo osebnih podatkov). Takšna so tudi pojasnila Evropske komisija, dostopna na povezavi: https://ec.europa.eu/commission/presscorner/detail/et/MEMO_15_6385

[6] Narodne novine 42/2018 (dostopen na povezavi: **https://narodne-novine.nn.hr/clanci/sluzbeni/2018_05_42_805.html**).

[7] V angleškem prevodu je dostopen je na povezavi: https://uodo.gov.pl/en/594

milejša ali strožja od ureditve v Splošni uredbi, z izjemo vsebin, ki jih lahko države po pooblastilu iz Splošne uredbe uredijo samostojno (ali podrobneje). Predlog ZVOP-2 po naši oceni v nekaterih določbah odstopa od začrtane ureditve s Splošno uredbo o varstvu podatkov, tudi pooblastila, ki so dana nacionalnim državam, so po našem mnenju v določenih primerih presežena. V študiji se omejujemo zgolj na vsebino predloga ZVOP-2, ki je bila izpostavljena s strani naročnika (GZS).

II. Študija predlaganih sprememb

V Študiji obravnavamo besedilo predloga ZVOP-2 in predloga GZS. Predlagani amandmaji k posameznim določbam so priloga študije.

21. člen (vodenje dnevnikov obdelav), 1. in 2. odstavek

Besedilo predloga ZVOP-2:

(1) Zaradi učinkovitejšega izvajanja 2. in 3. oddelka IV. poglavja Splošne uredbe upravljavci po tem zakonu vodijo dnevnik obdelave, kadar se v avtomatiziranih sistemih obdelave osebnih podatkov izvajajo obsežne obdelave posebnih vrst osebnih podatkov, ali kadar gre za redno in sistematično spremljanje posameznikov, ali kadar je z oceno učinka ugotovljeno tveganje, ki ga je mogoče učinkovito upravljati z vodenjem dnevnika obdelave, ali če tako določa zakon, o naslednjih dejanjih obdelave osebnih podatkov:
1. zbiranje;
2. spreminjanje;
3. vpogled;
4. razkritje, vključno s prenosi;
5. povezovanje;
6. izbris;
7. druga dejanja obdelave, ki jih določa zakon.

(2) Dnevnik obdelave iz prejšnjega odstavka mora za dejanja vpogleda in razkritja osebnih podatkov vsebovati vrsto dejanja obdelave, datum in čas obdelave, identifikacijo osebe, ki je izvedla dejanje obdelave, ter identifikacijo uporabnikov osebnih podatkov, da je mogoče naknadno ugotoviti točno identiteto teh oseb. Dodatne vsebine dnevnika obdelave lahko določi upravljavec ob upoštevanju ocene učinka.

Argumentacija k predlogu GZS:

Splošna uredba v uvodni določbi št. 78. določa, da je treba zaradi varstva pravic in svoboščin posameznikov v zvezi z obdelavo osebnih podatkov sprejeti ustrezne tehnične in organizacijske ukrepe, da bi zagotovili izpolnitev zahtev iz te uredbe. Da bi upravljavec lahko dokazal skladnost s to direktivo, bi moral sprejeti notranjo ureditev in izvesti ukrepe, ki spoštujejo zlasti načeli vgrajenega in privzetega varstva podatkov. Ti ukrepi bi med drugim lahko vključevali

minimizacijo obdelave osebnih podatkov, čimprejšnjo psevdonimizacijo osebnih podatkov, preglednost pri nalogah in obdelavi osebnih podatkov, omogočanje posameznikom, na katere se nanašajo osebni podatki, da spremljajo obdelavo podatkov, in omogočanje upravljavcu, da vzpostavi in izboljša varnostne ukrepe. Pri razvoju, oblikovanju, izboru in uporabi aplikacij, storitev in produktov, ki temeljijo na obdelavi osebnih podatkov ali ki pri opravljanju svoje funkcije obdelujejo osebne podatke, bi bilo treba proizvajalce produktov, storitev in aplikacij spodbujati, da pri razvoju in oblikovanju takih produktov, storitev in aplikacij upoštevajo pravico do varstva podatkov ter ob ustreznem upoštevanju najnovejšega tehnološkega razvoja, zagotovijo, da so upravljavci in obdelovalci zmožni izpolnjevati svoje obveznosti varstva podatkov. Načeli vgrajenega in privzetega varstva podatkov bi morali biti upoštevani tudi pri javnih razpisih.

Iz citirane določne je razvidno, da je breme zagotavljanja varnosti podatkov vselej in v celoti na upravljavcu, ki mora oceniti tveganja v zvezi z dejanji obdelave osebnih podatkov. V Splošni uredbi tudi nismo našli določb, ki bi državo članico pooblaščale k uzakonitvi zapovedi izvajanja prav specifičnih ukrepov za varnost osebnih podatkov v povezavi z na splošno opisanimi vrstami obdelave – ne da bi bila implementacija ukrepa pogojena z oceno tveganja konkretne obdelave, ki jo izdela upravljavec (ali eventualno obdelovalec) osebnih podatkov. Dejansko gre za novo breme, ki je upravljavcem naloženo z nacionalnim predpisom, ne da bi bili po naši oceni izpolnjeni pogoji iz Splošne uredbe – predhodna ocena tveganja konkretne obdelave s strani upravljavca / obdelovalca, ki terja zmanjšanje tveganja na prav določen način (na primer z vodenjem t.i. dnevnika obdelav).

Zdi se, kot da so konkretni ukrepi za varnost podatkov predlagani v 21/I in II členu predloga ZVOP-2 bolj kot v dejansko zmanjšanje tveganja konkretnih obdelav osebnih podatkov usmerjeni v lažje (pa tudi bolj administrativno in manj vsebinsko) izvajanje nadzora nad upravljavci. Delujejo kot nadgradnja ukrepov iz 24. oziroma 25. člena ZVOP-1, pri čemer se morda preveč zanemarja okoliščina, da so ukrepi iz 24. in 25. člena ZVOP-1 uzakonjeni v času, ko je varstvo osebnih podatkov na ravni Evropske Unije urejala direktiva[8] in so države članice imele bistveno več svobode za postavitev specifičnih zahtev na nacionalni ravni. Kot že poudarjeno v uvodu je bil zelo različen pristop držav članic pri prenosu direktive tudi eden od vzrokov za nadgradnjo pravne ureditve na ravni Evropske Unije z uredbo.

Predlog GZS po naši oceni pravilno izpostavlja, da je vodenje dnevnikov obdelav le en od možnih ukrepov za varnost podatkov, predvsem pa, da morajo biti ukrepi za varnost prilagojeni ugotovljenim tveganjem konkretnih obdelav osebnih podatkov. Ukrep, kot je zapovedan s

[8] Direktiva Evropskega parlamenta in Sveta 95/46/ES z dne 24. oktobra 1995 o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem pretoku takih podatkov.

kritizirano določbo niti ni pretehtan z vidika tveganja konkretne obdelave, saj ne upošteva ključnih okoliščin kot so velikost upravljavca, število pooblaščenih delavcev, ki imajo dostop do podatkov, namene obdelave, intenzivnost obdelave ipd.

T.i. sledljivost obdelav osebnih podatkov je v Sloveniji že dolgo več kot dobra praksa, saj so določbe ZVOP-1 skupaj s Smernicami Informacijskega pooblaščenca[9] postavile jasna pravila o tem, katero raven sledljivosti naj bi zagotavljali upravljavci v določenih situacijah[10]. Vsekakor je sledljivost tudi vključena v obdelave podatkov upravljavcev, ki so zavezani različnim standardom informacijske varnosti (na primer ISO 27001), pri čemer gre še vedno za dobro prakso na strani upravljavca. Predlagani dnevniki obdelav pa bistveno odstopajo od ustaljenega razumevanja potreb po zagotavljanju sledljivosti obdelav v praksi, tako glede tipov upravljavcev kot glede vsebine sledi, ki naj bi se obvezno beležila. Za takšno odstopanje predlagatelj ne ponudi nobenega vsebinskega pojasnila. Kot že poudarjeno pa Splošna uredba o varstvu podatkov državam članicam tudi ne daje pooblastila za zapovedovanje oziroma regulacijo konkretnih ukrepov za varnost podatkov – z izjemo primera iz 89/I člena Splošne uredbe o varstvu podatkov (ko gre za obdelavo osebnih podatkov za znanstveno-raziskovalne namene). Takšna regulacija bi bila po naši oceni tudi v škodo razvoju področja varstva osebnih podatkov, saj bi namesto ocenjevanja tveganj upravljavcem vsiljevala z dejanskimi tveganji nepovezana administrativna bremena, prav tako bi Informacijski pooblaščenec namesto presojanja pravilnosti ocene tveganj s strani upravljavca, nadziral zgolj izpolnitev administrativnih bremen. Na ta način je razvoj in razumevanje področja varstva osebnih podatkov obsojen na stagnacijo, na daljši rok pa na nazadovanje.

Kolikor bi predlagatelj ZVOP-2 vztrajal pri tako podrobnih zapovedih o zagotavljanju varnosti pri obdelavi osebnih podatkov, četudi bo v tem delu šlo za odstopanje od določil Splošne uredbe, posledično pa za posebnost slovenske ureditve, predlog GZS pomeni vsaj minimalno uskladitev določb 21/I in II člena predloga ZVOP-2 z določili Splošne uredbe (uvodna določba 78 in člen 32), ki terjajo prilagoditev ukrepov ugotovljenim tveganjem.

22. člen (varnost osebnih podatkov na področju posebnih obdelav), 1. (podredno 2.) odstavek

Besedilo predloga ZVOP-2:

Za informacijske sisteme, v katerih se izvajajo obdelave osebnih podatkov:

1. *določenih v zakonih, ki urejajo področja upravnih notranjih zadev, finančne uprave, državljanstva, Slovenske obveščevalno-varnostne agencije, obrambe, zdravstvenega*

[9] Smernice Informacijskega pooblaščenca: Zavarovanje osebnih podatkov, 22.9.2015, dostopne na povezavi: https://www.ip-rs.si/fileadmin/user_upload/Pdf/smernice/Smernice_o_zavarovanju_OP.pdf

[10] Glejte 24. člen ZVOP-1 in Smernice Informacijskega pooblaščenca: Zavarovanje osebnih podatkov (strani 21 - 23).

varstva, obveznega zdravstvenega zavarovanja, uveljavljanja pravic iz javnih sredstev ter kazenskih in prekrškovnih evidenc, ali

2. *kadar se na podlagi zakonov v zbirki osebnih podatkov obdelujejo osebni podatki več kot 100.000 posameznikov, ali*
3. *kadar upravljavec ali obdelovalec v zbirki osebnih podatkov obdeluje predvsem posebne vrste osebnih podatkov, ali*
4. *kadar se v zbirki osebnih podatkov obdeluje posebne vrste osebnih podatkov več kot 10.000 posameznikov ali*
5. *v zasebnem sektorju, kadar se v zbirki osebnih podatkov obdelujejo osebni podatki več kot 200.000 posameznikov,*

se smiselno uporabljajo določbe o varnostnih zahtevah in priglasitvi incidentov zakona, ki ureja informacijsko varnost.

(2) Obdelave iz prejšnjega odstavka se izvajajo tako, da se sistemsko onemogoča razkritje osebnih podatkov ali obdelav nepooblaščenim osebam ali drugim subjektom, ki za njihov dostop nimajo pravne podlage ter s tem stalno preprečuje škodo varnosti in interesom Republike Slovenije.

Argumentacija k predlogu GZS:

Primarno izpostavljamo, da področje informacijske varnosti in ukrepe za doseganje visoke ravni varnosti omrežij in informacijskih sistemov v Republiki Sloveniji, ki so bistvenega pomena za nemoteno delovanje države v vseh varnostnih razmerah ter zagotavljajo bistvene storitve za ohranitev ključnih družbenih in gospodarskih dejavnosti v Republiki Sloveniji (že) ureja ZinfV[11]. Namen ZInfV je ureditev področja informacijske varnosti in zagotovitev visoke ravni varnosti omrežij in informacijskih sistemov v Republiki Sloveniji, ki so bistvenega pomena za nemoteno delovanje države v vseh varnostnih razmerah in zagotavljajo bistvene storitve za ohranitev ključnih družbenih in gospodarskih dejavnosti. Da gre pravzaprav za namen varstva informacijskih sistemov (in ne specifično za varnost osebnih podatkov) izhaja že iz samega uvodnega, napovednega stavka k prvem odstavku 22. člena, ki v predlogu ZVOP-2 glasi: *Za informacijske sisteme, v katerih se izvajajo obdelave osebnih podatkov...*" Gre torej za vsebinska vprašanja, ki jih že ureja ZInfV. Če v tem pogledu ni zadosten, je treba eventualno dopolniti ZInfV.

Urejanje novih kategorij upravljavcev, katerih obdelave so bistvenega pomena za nemoteno delovanje države v ZVOP-2 je tako najmanj nesistemsko, saj takšne potrebe očitno niso bile zaznane ob sprejemu ZInfV, niti ob njegovi spremembi oziroma dopolnitvi v letu 2021[12]. Določbe ZInfV zavezujejo t.i. izvajalce bistvenih storitev, ponudnike digitalnih storitev in organe državne uprave, ki upravljajo z informacijskimi sistemi in deli omrežja oziroma izvajajo informacijske storitve, nujne za nemoteno delovanje države ali za zagotavljanje nacionalne varnosti[13]. Iz

[11] Zakon o informacijski varnosti (Uradni list RS, št. 30/18 in 95/21); ZInfV.
[12] ZInf je bil v letu 2021 noveliran. Novela Zinf-A je bila objavljena v Uradnem listu RS, št. 95/2021.
[13] Glejte 1. in 2. člen ZInfV.

obrazložitve k predlogu ZVOP-2 ni razvidno, zakaj je prišlo do spregleda (če je prišlo do spregleda) pri urejanju informacijske varnosti v Republiki Sloveniji na sistemski ravni, in jo je posledično treba dopolniti z ZVOP-2. Poleg tega se pooblastilo za urejanje na nacionalni ravni, na katerega se sklicuje predlagatelj (6/III[14], 9/IV[15] člen in uvodna določba št. 53[16] Splošne uredbe o varstvu podatkov), po našem mnenju ne nanašajo na pooblastilo za urejanje ukrepov za varnost osebnih podatkov na splošno, pač pa omogočajo državam članicam določitev dodatnih pogojev, tudi omejitev le glede obdelave (zgolj) genetskih, biometričnih ali podatkov v zvezi z zdravjem. Pooblastilo države se torej ne nanaša na vse skupine posebnih vrst osebnih podatkov, pač pa le na genetske, biometrične in podatke v zvezi z zdravjem. V določbah Splošne uredbe o varstvu podatkov tako nismo našli podlage za poseganje države v obdelavo osebnih podatkov s strani upravljavcev v zasebnem sektorju, ki obdelujejo osebne podatke velikega števila posameznikov, pri tem pa zbirke ne vsebujejo genetskih, biometričnih ali podatkov v zvezi z zdravjem. Glede na navedeno so v določbah 22. člena predloga ZVOP-2 po naši oceni presežena pooblastila države članice v delu, ki se ne nanaša na ukrepe, ki bi zadevali zgolj genetske, biometrične ali podatke v zvezi z zdravjem.

Predlog člena uvaja tudi nov termin na področju varstva osebnih podatkov - *področje posebnih obdelav*. Splošna uredba o varstvu podatkov ga ne pozna. V obrazložitvi predlagatelj pojasni, da gre za določitev posebnega sistema varovanja za *določene zbirke, ki so zaradi svoje velikosti, podatkov, ki se v njej obdelujejo ali drugih lastnosti, posebej občutljive*. V splošni uredbi ne najdemo definicije *posebej občutljivih zbirk.* ZVOP-2 torej vzpostavlja nove termine in jih razlaga na nacionalni ravni. Pri tem kot *občutljivih zbirk* ne določa le zbirk, katerih upravljavci so državni organi, in kjer bi eventualno lahko sprejeli tolmačenje, da s takšno ureditvijo ne posega (vsaj ne pomembno) v položaj upravljavcev, ki je enotno urejen na ravni Evropske Unije, pač pa zgolj

---

[14] 3. odstavek 6. člena Splošne uredbe o varstvu podatkov:
Podlaga za obdelavo iz točk (c) in (e) odstavka 1 je določena v skladu s:
(a) pravom Unije; ali
(b) pravom države članice, ki velja za upravljavca.
Namen obdelave se določi v navedeni pravni podlagi ali pa je ta v primeru obdelave iz točke (e) odstavka 1 potrebna za opravljanje naloge, ki se izvaja v javnem interesu, ali pri izvajanju javne oblasti, dodeljene upravljavcu. Navedena pravna podlaga lahko vključuje posebne določbe, s katerimi se prilagodi uporaba pravil iz te uredbe, med drugim: splošne pogoje, ki urejajo zakonitost obdelave podatkov s strani upravljavca; vrste podatkov, ki se obdelujejo; zadevne posameznike, na katere se nanašajo osebni podatki; subjekte, katerim se osebni podatki lahko razkrijejo, in namene, za katere se lahko razkrijejo; omejitve namena; obdobja hrambe; ter dejanja obdelave in postopke obdelave, vključno z ukrepi za zagotovitev zakonite in poštene obdelave, kot tiste za druge posebne primere obdelave iz poglavja IX. Pravo Unije ali pravo države članice izpolnjuje cilj javnega interesa in je sorazmerno z zakonitim ciljem, za katerega si prizadeva.

[15] 4. odstavek 9. člena Splošne uredbe o varstvu podatkov:
Države članice lahko ohranijo ali uvedejo dodatne pogoje, tudi omejitve, glede obdelave genetskih, biometričnih ali podatkov v zvezi z zdravjem.

[16] Uvodna določba št. 53 Splošne uredbe o varstvu podatkov:
Države članice bi morale imeti možnost, da ohranijo ali uvedejo dodatne pogoje, tudi omejitve, glede obdelave genetskih podatkov, biometričnih podatkov ali podatkov o zdravstvenem stanju. To pa ne bi smelo ovirati prostega pretoka osebnih podatkov v Uniji, kadar ti pogoji veljajo za čezmejno obdelavo takih podatkov.

postavlja dodatna pravila upravljavcem, ki so del države. Nenazadnje lahko sprejmemo tolmačenje, po katerem sme država sama sebi, za zbirke, ki jih vodi, postaviti specifična in stroga pravila za zagotavljanje varnosti osebnih podatkov, v smislu, da je kot upravljavec pretehtala tveganja obdelave za svoje zbirke.

Po Splošni uredbi varstvu podatkov pa državi niso dana pooblastila, da pretehta tveganja v povezavi z obdelavo osebnih podatkov v zbirkah, ki jih vodijo upravljavci iz zasebnega sektorja, tudi upravljavci iz širšega javnega sektorja, ki presega sektor države. Argument, da je določba namenjena posebnemu varovanju zbirk, ki vsebujejo podatke o velikem številu posameznikov[17], že na prvi pogled ne zdrži resne presoje. Ni namreč razvidno, zakaj »večje število posameznikov«, ki zbirko dela *posebej občutljivo* v javnem sektorju predstavlja 100.000 posameznikov, v zasebnem pa 200.000 posameznikov[18]. Navedeno napeljuje k zaključku, da je po mnenju predlagatelja ZVOP-2 javni sektor bistveno manj vreden zaupanja, saj je število posameznikov v zbirki, odločilno za njen značaj »občutljivosti« kar 1x manjše od števila, ki enak značaj prinese zbirki v zasebnem sektorju. Dodatno posebni značaj zbirke v javnem sektorju ustvarijo tudi posebne vrste podatki v zbirki (ne nujno genetski, biometrični ali podatki v zvezi z zdravjem), v zasebnem sektorju značaj posebnih vrst osebnih podatkov ni pomemben.

Očitno je torej, da gre za povsem arbitrarno postavljena pravila, ki nimajo opore v dejanski oceni tveganja in iz katerih tudi ni mogoče ugotoviti, zakaj takšna odstopanja.

Bistveno v tem primeru je po naši oceni preseganje pooblastil predlagatelja, ki jih daje Splošna uredba z določanjem posebnega statusa zbirk – "posebej občutljivih zbirk", predvsem pri upravljavcih v zasebnem sektorju in zapovedjo ukrepov za varnost, ki ne temeljijo na oceni tveganja, ki jo je izdelal upravljavec konkretne zbirke iz zasebnega sektorja. Ponavljamo, da je treba, kolikor se je ZInfV pokazal kot pomanjkljiv z vidika varnosti informacijskih sistemov, poseči vanj.

Ohranitev 5. točke ob opustitvi referiranja na zasebni sektor ni smiselna, saj so *občutljive zbirke* v javnem sektorju že definirane (tudi) kot tiste, v katerih so podatki več kot 100.000 posameznikov[19]. Zaradi navedenega naj se 5. točka prvega odstavka 22. člena izpusti. Eventualno lahko ostane, kolikor bi se razlagalo, da se nanaša na zbirke v javnem sektorju, ki se ne vodijo na podlagi zakona, pri čemer pa bi pričakovali, da predlagatelj dodaten napor usmeri v argumentacijo zaznavanja tako

[17] Glejte obrazložitev k členu 22, 1. in 2 odstavek obrazložitve na strani 97 preldoga ZVOP-2.

[18] Opozarjamo na napako v obrazložitvi k 22. členu – zadnji odstavek prvega odstavka obrazložitve na strani 97 predloga ZVOP-2.

[19] Glejte 2. alinejo 22/I člena predloga ZVOP-2.

različnega tveganja in posledično ocene občutljivosti, če gre za zbirko, ki se v javnem sektorju vodi na podlagi zakona in na drugi strani, če se zbirka v javnem sektorju ne naslanja na zakon.

23. člen (ocena učinka glede obdelav osebnih podatkov), 2. in 3. odstavek

Besedilo predloga ZVOP-2:

(2) Ocena učinka glede varstva osebnih podatkov in predhodno posvetovanje z nadzornim organom se izvajata tudi pred obdelavo osebnih podatkov iz prvega odstavka prejšnjega člena. Ocena učinka mora upoštevati okoliščine, določene v tretjem odstavku tega člena in možne škodljive posledice za varnost države, vključno z njenimi političnimi ali gospodarskimi koristmi, če bi bili obdelovani podatki razkriti nepooblaščenim osebam ali subjektom.

(3) Pred začetkom obdelave se ocena učinka ponovno izdela tudi v naslednjih primerih:

1. kadar je bila spremenjena pravna podlaga za obdelavo iz 6. člena tega zakona;
2. kadar je uvajajo nova sredstva obdelave;
3. kadar se uvajajo nova dejanja obdelave, ki lahko pomenijo večje tveganje za varnost osebnih podatkov, ali
4. kadar se spremenijo narava, obseg, okoliščine oziroma namen obdelave osebnih podatkov večjega števila posameznikov, na katere se nanašajo osebni podatki, kar bi lahko povzročilo tveganje za človekove pravice in temeljne svoboščine posameznikov.

Argumentacija k predlogu GZS:

Predlog spremembe GZS je relevanten, kolikor prvi odstavek 22. člena predloga ZVOP-2 ostane nespremenjen. Če se sprejme predlagana sprememba prvega odstavka 22. člena ZVOP-2, določba 23/II člena nalaga izvedbe ocene učinkov izven kriterijev in meril iz določb Splošne uredbe o varstvu podatkov le upravljavcem v javnem sektorju.

Splošna uredba o varstvu podatkov je sicer glede zahtev po izdelavi ocene učinkov povsem jasna. Upravljavci so jo dolžni izdelati, kadar je možno, da bi vrsta obdelave, zlasti z uporabo novih tehnologij, ob upoštevanju narave, obsega, okoliščin in namenov obdelave povzročila veliko tveganje za pravice in svoboščine posameznikov. Pooblastilo za določitev in objavo seznama vrst dejanj obdelave, za katere velja zahteva po oceni učinka v zvezi z varstvom podatkov, je dano nacionalnim nadzornim organom (in ne državam članicam) – 35/IV člen Splošne uredbe o varstvu podatkov. Na spletni strani Informacijskega pooblaščenca je objavljen seznam obdelav[20], pri

[20] Seznam obdelav Informacijskega pooblaščenca (št. 014-1/2018/1 z dne 24.5.2018) pri katerih je obvezna ocena učinkov na varstvo osebnih podatkov, je dostopen na povezavi: https://www.ip-

katerih je izdelava ocene učinka na varstvo osebnih podatkov obvezna, kot tudi komentar Informacijskega pooblaščenca o tem, da konkreten seznam obdelav, pri katerih je ocena učinkov obvezna, sprejme nadzorni organ[21].

Pooblastilo iz 35/IV člena Splošne uredbe o varstvu podatkov je torej dano informacijskemu pooblaščencu, ta pa je svojo nalogo že opravil. V Splošni uredbi o varstvu podatkov nismo našli pooblastila za urejanje vprašanja ocene učinkov državi članici, še posebej ne v delu, v katerem bi se regulacija obveznosti izdelave ocene učinkov na varstvo osebnih podatkov raztezala na upravljavce v zasebnem sektorju. Dodajamo, da po 35/VI členu Splošne uredbe o varstvu podatkov prav zaradi namena harmonizacije področja varstva osebnih podatkov nadzorni organ pred sprejemom seznama obdelav, pri katerih je ocena učinkov obvezna, v primeru, kadar seznam vključuje dejavnosti, povezane z nudenjem blaga ali storitev posameznikom, na katere se nanašajo osebni podatki, ali s spremljanjem njihovega ravnanja v več državah članicah ali pa lahko znatno vplivajo na prosti pretok osebnih podatkov v Uniji, uporabi mehanizem za skladnost iz 63. člena Splošne uredbe o varstvu podatkov. Tudi nadzorni organ, ki mu je s Splošno uredbo dano pooblastilo za določitev seznama vrst dejanj obdelave, za katere velja zahteva po oceni učinka, torej pri svojem odločanju ni povsem prost.

Iz obrazložitve k predlogu določbe ni razvidno, zakaj je predlagatelj upravljavcem odrekel izvedbo samostojne presoje o potrebnosti izdelave ocene učinkov. Zapisano je le, da je treba oceno učinkov napraviti tudi *pred posebnimi obdelavami osebnih podatkov (22. člen). Ker imajo kršitve varnosti za posebne obdelave lahko škodljive posledice za varnost države, je treba v takšnem primeru izdelati tudi oceno učinka obdelav osebnih podatkov na varnost države, vključno z njenimi političnimi ali gospodarskimi koristmi.*

Kot smo že poudarili v argumentaciji pri predlogu 22. člena ZVOP-2 so *posebne obdelave osebnih podatkov* nov izraz na področju varstva osebnih podatkov, ki ga Splošna uredba o varstvu podatkov ne pozna. V Splošni uredbi o varstvu podatkov nismo našli pooblastila državi članici, da na nacionalni ravni uvaja nove pojme na področju varstva osebnih podatkov in jih vsebinsko zapolnjuje. S tem namreč uvaja nove obveznosti za upravljavce, ki s Splošno uredbo o varstvu podatkov niso določene in preprečuje njeno neposredno uporabo. Glede argumenta o potrebnosti izdelave ocene učinkov zaradi potencialnih škodljivih posledic obdelave na varnost države, pa je treba najprej ugotoviti, da te okoliščine niso niti izkazane, niti njihovo urejanje sistemsko ne sodi v zakon, ki ureja varstvo osebnih podatkov. Če gre za podatke, katerih obdelava ima lahko

---

rs.si/fileadmin/user_upload/Pdf/Ocene_ucinkov/Seznam_dejanj_obdelav_osebnih_podatkov__za_katere_velja_zahteva_po_izvedbi_ocene_ucinka_v_zvezi_z_varstvom_osebnih_podatkov.pdf

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

škodljive posledice za varnost države, bodo ti slejkoprej podvrženi pravilom iz ZTP[22]. ZTP kot tajni podatek opredeljuje dejstvo ali sredstvo z delovnega področja organa, ki se nanaša na javno varnost, obrambo, zunanje zadeve ali obveščevalno in varnostno dejavnost države, ki ga je treba zaradi razlogov, določenih v tem zakonu, zavarovati pred nepoklicanimi osebami, in ki je v skladu s tem zakonom določeno in označeno za tajno[23]. Zavezuje pa ne le državnih organov pač pa tudi organe lokalnih skupnosti, nosilce javnih pooblastil ter druge organe, gospodarske družbe in organizacije, ki pri izvajanju zakonsko določenih nalog pridobijo ali razpolagajo s podatki iz prejšnjega odstavka, ter posamezniki v njih, vključno z dobavitelji, izvajalci gradenj ali izvajalci storitev, ki se jim podatki posredujejo zaradi izvršitve naročil organa[24].

Kakšne *škodljive posledice za varnost države* imajo lahko *posebne obdelave osebnih podatkov*, in pri tem ne gre hkrati za tajne podatke, ki jih že sistemsko in celovito ureja ZTP oziroma ne gre hkrati za obdelave izvajalcev bistvenih storitev iz ZInfV in obrazložitve predlagatelja nismo mogli ugotoviti.

Kar smo zapisali zgoraj, v veliki meri velja tudi za obvezno določanje izvedbe posvetovanja z nadzornim organom. Države članice lahko po pooblastilu iz 36/V člena Splošne uredbe o varstvu podatkov od upravljavcev izven določbe 36/I člena Splošne uredbe o varstvu podatkov zahtevajo, naj se posvetujejo z nadzornim organom in od njega prejmejo predhodno dovoljenje v zvezi z obdelavo s strani upravljavca le, ko gre za izvajanje naloge, ki jo upravljavec izvaja v javnem interesu, vključno z obdelavo v zvezi s socialnim varstvom in javnim zdravjem.
Nobenega dvoma tako ni, da država članica v Splošni uredbi nima pooblastila za določanje obveznega predhodnega posvetovanja z nadzornim organom upravljavcem v zasebnem sektorju zgolj zaradi števila podatkov, ki bi jih ti vodili v svojih zbirkah. Ko pa gre za vsebino podatkov, lahko to stori le, če je upravljavcu (tudi upravljavcu iz zasebnega sektorja) obdelava osebnih podatkov naložena v javnem interesu (torej na podlagi zakona oziroma z zakonom).

Če sprejemamo razlago, da sme država eventualno dodatne obveznosti naložiti upravljavcem, ki so državni organi, saj tudi v tem pogledu usmerja njihovo delovanje, pa teh pooblastil nima v odnosu do upravljavcev iz zasebnega sektorja (po našem mnenju tudi ne do upravljavcev v širšem javnem sektorju izven sektorja država). Pooblastil, ki bi državam članicam v nacionalnih predpisih dovolila zapovedovati obvezno izdelavo ocene učinka na varstvo podatkov in obvezno posvetovanje z nadzornim organom pa tudi v Splošni uredbi o varstvu podatkov nismo našli.

---

[22] Zakon o tajnih podatkih (Uradni list RS, št. 50/06 – uradno prečiščeno besedilo, 9/10, 60/11 in 8/20); ZTP.
[23] Glejte prvo alinejo 2. člena ZTP.
[24] Glejte 1/II in III člen ZTP.

40. člen (postopek posredovanja osebnih podatkov), 2. odstavek, predlog za nov 5. odstavek

Besedilo predloga ZVOP-2:

(2) Upravljavec vlagatelju zahteve, če zakon ne določa drugačnega načina, zahtevane osebne podatke posreduje najpozneje v 15 dneh od prejema popolne zahteve ali pa ga v tem roku pisno obvesti o razlogih, zaradi katerih mu zahtevanih osebnih podatkov ne bo posredoval. Upravljavec in vlagatelj zahteve se v roku iz prejšnjega stavka lahko dogovorita za njegovo podaljšanje.

Argumentacija k predlogu GZS:

Vsebinsko 40. člen predloga ZVOP-2 pomeni nadgradnjo 22. člena ZVOP-1[25]. V praksi bo nesorazmerne težave in zaplete najverjetneje povzročalo že izvajanje njegovega prvega odstavka (glede obvezne vsebine zahteve za posredovanje/pridobitev podatkov), saj je subjekt, ki zaproša za podatke poleg namena oziroma razlogov, ki izkazujejo potrebnost in primernost osebnih podatkov za dosego namena pridobitve (4. točka prvega odstavka), dolžan napisati tudi predmet in številko ali drugo identifikacijo zadeve, v zvezi s katero so osebni podatki potrebni, ter navedbo organa ali drugega subjekta, ki obravnava zadevo (5. točka). To pomeni, da bo pridobitev podatkov pogojena s tekom postopka pred pristojnim organom. Seveda pa to še zdaleč niso vsi primeri, v katerih bi bil subjekt, ki zaproša, po določbah Splošne uredbe o varstvu podatkov sicer upravičen (sklicujoč se na pravni temelj in namen obdelave osebnih podatkov) do njihove pridobitve. Namen obdelave se tako z novim 40. členom za pridobitelja po naši oceni v nasprotju z določbami Splošne uredbe o varstvu podatkov skrči na situacije, ko so osebni podatki potrebni zgolj v zvezi z določenim uradnim postopkom.

[25] 22. člen ZVOP-1 določa:
(1) Upravljavec osebnih podatkov mora proti plačilu stroškov posredovanja, če zakon ne določa drugače, posredovati osebne podatke uporabnikom osebnih podatkov.
(2) Upravljavec centralnega registra prebivalstva ali evidenc stalno in začasno prijavljenih prebivalcev mora na način, ki je določen za izdajo potrdila, posredovati upravičencu, ki izkaže pravni interes za uveljavljanje pravic pred osebami javnega sektorja, osebno ime in naslov stalnega ali začasnega prebivališča posameznika, zoper katerega uveljavlja svoje pravice.
(3) Upravljavec osebnih podatkov mora za vsako posredovanje osebnih podatkov zagotoviti, da je mogoče pozneje ugotoviti, kateri osebni podatki so bili posredovani, komu, kdaj in na kakšni podlagi, in sicer za obdobje, ko je mogoče zakonsko varstvo pravice posameznika zaradi nedopustnega posredovanja osebnih podatkov.
(4) Ne glede na prvi odstavek tega člena je upravljavec osebnih podatkov v javnem sektorju dolžan uporabniku osebnih podatkov v javnem sektorju posredovati osebne podatke brez plačila stroškov posredovanja, razen če zakon določa drugače ali če gre za uporabo za zgodovinsko, statistično ali znanstveno-raziskovalne namene.

Drugi odstavek ureja rok za odločitev o posredovanju zaprošenih podatkov. Določa ga na 15 dni od prejema popolne zahteve, kar na primer sovpada z rokom, ki ga ZOdv[26] v 10. členu določa za posredovanje podatkov odvetniku.

Splošna uredba o varstvu podatkov v 12/III. členu določa, da so se upravljavci na zahteve posameznikov za uveljavitev pravic iz naslova varstva osebnih podatkov dolžni odzivati v roku enega meseca po prejemu zahteve, ta rok pa se lahko po potrebi podaljša za največ dva dodatna meseca ob upoštevanju kompleksnosti in števila zahtev.
GZS predlaga, da se zaradi poenostavitve in enotnega vodenja postopkov in zahtev rok za posredovanje podatkov uskladi z rokom za odziv na pravice posameznika. Po določbi drugega odstavka 40. člena predloga ZVOP-2 se upravljavec in vlagatelj zahteve v 15-dnevnem roku iz lahko dogovorita za njegovo podaljšanje, seveda pa je povsem mogoče, da dogovor ne bo dosežen.

Upoštevaje uvodni stavek k 40/II členu predloga ZVOP-2, po katerem je rok za posredovanje osebnih podatkov v ZVOP-2 določen subsidiarno (*če zakon ne določa drugačnega načina)*, in dejstvo, da druge določbe 40. člena upravljavcu ne dajejo možnosti, da sam odloča o podaljšanju roka, vsaj v primeru obsežnejših ali kompleksnejših zahtev, je določitev daljšega roka za posredovanje zahtevanih osebnih podatkov smiselna in primerna.

Dodatno opozarjamo, da v določbah 40. člena nismo zasledili vsebine iz 22. člena ZVOP-1, ki se nanaša na možnost zaračunavanja posredovanja osebnih podatkov. Tako predlagamo še, da se ohrani ta možnost iz ZVOP-1.

42. člen (rok hrambe osebnih podatkov, določitev roka in vezanost na rok), cel člen (podredno 3. odstavek)

Besedilo predloga ZVOP-2:

(1) Rok hrambe osebnih podatkov je omejen na najkrajše možno obdobje in le, dokler je hramba potrebna za dosego namena obdelave, zaradi katerega so se osebni podatki zbirali in nadalje obdelovali, razen če zakon za posamezne obdelave določa rok hrambe.

(2) Upravljavec ob upoštevanju narave obdelovanih podatkov in tveganj občasno in na dokumentiran način preverja, ali se upoštevajo določbe prejšnjega odstavka.

[26] Zakon o odvetništvu (Uradni list RS, št. 18/93, 24/96 – odl. US, 24/01, 54/08, 35/09, 97/14, 8/16 – odl. US, 46/16 in 36/19); ZOdv.

(3) Po izpolnitvi namena obdelave se osebni podatki izbrišejo, uničijo ali anonimizirajo, če zakon za posamezne vrste osebnih podatkov ne določa drugače, zlasti omejevanje dostopa do njih, njihovo blokiranje ali njihovo arhiviranje.

Argumentacija k predlogu GZS:

Predlagatelj v obrazložitvi k določbi pojasni, da se podatki po izpolnitvi namena izbrišejo, uničijo ali anonimizirajo, le zakon pa lahko določa tudi druge načine postopanja (npr. omejevanje dostopa, blokiranje, arhiviranje). Pri tem gre za povsem nepotrebno pa tudi za neobrazloženo oženje načinov prenehanja obdelave osebnih podatkov po izpolnitvi namena glede na določbe Splošne uredbe o varstvu podatkov (t.i. načelo omejitve shranjevanja iz 5. člena).

ZVOP-1 v drugem odstavku 21. člena določa, da se po izpolnitvi namena obdelave osebni podatki zbrišejo, uničijo, blokirajo ali anonimizirajo, če niso na podlagi zakona, ki ureja arhivsko gradivo in arhive, opredeljeni kot arhivsko gradivo, oziroma če zakon za posamezne vrste osebnih podatkov ne določa drugače.

Tako je po ZVOP-1 po izpolnitvi namena osebne podatke dopustno tudi blokirati oziroma arhivirati. Ni najti razloga za spreminjanje ustaljene ureditve in oženje možnosti upravljavca za ravnanje z osebnimi podatki po izpolnitvi namena obdelave glede na načelo omejitve shranjevanja iz Splošne uredbe o varstvu podatkov. Za takšno ravnanje države članice tudi ni najti pooblastila v določbah Splošne uredbe o varstvu podatkov.

Po načelu omejitve shranjevanja iz točke e) 5/I člena Splošne uredbe o varstvu podatkov se podatki hranijo v obliki, ki dopušča identifikacijo posameznikov, na katere se nanašajo, le toliko časa, kolikor je potrebno za namene, za katere se osebni podatki obdelujejo. Za daljše obdobje se osebni podatki lahko shranjujejo, če bodo obdelani zgolj za namene arhiviranja v javnem interesu, za znanstveno- ali zgodovinsko-raziskovalne namene ali statistične namene v skladu s členom 89/I Splošne uredbe o varstvu podatkov, pri čemer je treba izvajati ustrezne tehnične in organizacijske ukrepe iz te uredbe, da se zaščitijo pravice in svoboščine posameznika.

Že sama Splošna uredba o varstvu podatkov torej dopušča daljšo hrambo osebnih podatkov, če bodo kasneje obdelani zgolj za namene arhiviranja v javnem interesu, za znanstveno ali zgodovinsko-raziskovalne namene ali statistične namene. Hkrati posebej ureja tudi obdelavo, ki ne zahteva identifikacije (11. člen Splošne uredbe o varstvu podatkov[27]).

[27] 11. člen Splošne uredbe o varstvu podatkov:
(1) Če upravljavec za namene, za katere obdeluje osebne podatke, ne potrebuje ali ne potrebuje več identifikacije posameznika, na katerega se nanašajo osebni podatki, upravljavec ni zavezan ohraniti, pridobiti ali obdelati dodatnih informacij, da bi identificiral posameznika, na katerega se nanašajo osebni podatki, samo zaradi zagotavljanja skladnosti s to uredbo.

Tako ni nobenega dvoma o tem, da je po izpolnitvi namena obdelave oziroma izteku roka hrambe osebnih podatkov upravljavec svoboden v izbiri mehanizmov, ki bodo zagotovili, da pravica posameznikov do varstva osebnih podatkov ni prizadeta, in ni omejen le na izbris, uničenje ali anonimizacijo – kot je predlagano v tretjem odstavku 42. člena predloga ZVOP-2. Splošna uredba nacionalni državi ne daje pooblastila za regulacijo ravnanja upravljavcev z osebnimi podatki po izpolnitvi namena obdelave.

67. člen (obdelava osebnih podatkov za raziskovalne namene), 1. odstavek

Besedilo predloga ZVOP-2:

(1) Obdelava osebnih podatkov za znanstvenoraziskovalne, zgodovinskoraziskovalne in statistične namene (v nadaljnjem besedilu: raziskovanje) je dovoljena organizacijam in posameznikom, ki pri svojem delovanju uporabljajo etična načela in metodologijo s področja raziskovanja ter pravila glede varstva osebnih podatkov iz tega poglavja.

Argumentacija k predlogu GZS:

Argumentacija glede primernosti dopolnitve prvega odstavka na način, da je organizacija oziroma posameznik vpisan v Evidence izvajalcev raziskovalne in razvojne dejavnosti pri Javni agenciji za raziskovalno dejavnost Republike Slovenije, izhaja iz devetega odstavka argumetacije k predlogu GZS k 68. členu.

68. člen (pogoji obdelave osebnih podatkov za raziskovalne namene), 1., 2. (podredno glede na predlog spremembe 67/1 člena) in 4. odstavek

Besedilo predloga ZVOP-2:

(1) Ne glede na prvotni namen obdelave lahko upravljavec osebne podatke, vključno s posebnimi vrstami osebnih podatkov, nadalje obdeluje za namen raziskovanja, če tako obdelavo dovoljuje drug zakon ali če:

---

(2) Kadar lahko upravljavec v primerih iz odstavka 1 tega člena dokaže, da ne more identificirati posameznika, na katerega se nanašajo osebni podatki, upravljavec o tem po možnosti ustrezno obvesti posameznika, na katerega se nanašajo osebni podatki. V takih primerih se členi 15 do 20 ne uporabljajo, razen kadar posameznik, na katerega se nanašajo osebni podatki, za uresničevanje svojih pravic na podlagi teh členov zagotovi dodatne informacije, s katerimi ga je mogoče identificirati.

1. posameznik, na katerega se ti podatki nanašajo, ni prepovedal obdelave svojih osebnih podatkov za namen raziskovanja ali prepovedal obdelave svojih osebnih podatkov na določenem raziskovalnem področju, ki vključuje tudi namene raziskave, ali
2. je posameznik, na katerega se nanašajo osebni podatki, ki pomenijo poklicno skrivnost, za obdelavo dal pisno soglasje.

(2) Raziskovalne organizacije ter raziskovalci, ki so pri raziskovanju vezani na etična načela in metodologijo iz prvega odstavka prejšnjega člena, lahko za namene iz prvega odstavka prejšnjega člena od upravljavca pridobijo osebne podatke, vključno s posebnimi vrstami osebnih podatkov, če predložijo opis raziskave, ki vključuje:
1. naslov raziskave in navedbo nosilcev raziskave (za fizične osebe osebno ime, naziv in prebivališče, za pravno osebo pa firma, matična številka in sedež);
2. podatke o neposrednih izvajalcih raziskave (osebno ime, naziv, prebivališče, razmerje do nosilca raziskave in morebitna šifra raziskovalca);
3. namene oziroma cilje raziskave;
4. predvidena sredstva in dejanja obdelave osebnih podatkov, vključno z navedbo etičnih načel in metodologije iz prejšnjega člena in ukrepi za varnost osebnih podatkov;
5. vrste osebnih podatkov, ki bi jih želeli pridobiti od upravljavca, in kategorije posameznikov, na katere se nanašajo ti podatki;
6. obliko, v kateri želijo prejeti osebne podatke (izvorni osebni podatki, psevdonimizirani osebni podatki, osebni podatki v obliki, ki ne zahteva identifikacije, anonimizirani podatki), in navedbo razloga za določeno obliko podatkov;
7. način objave ali drugačne dostopnosti raziskave.

(4) Upravljavec zavrne posredovanje osebnih podatkov:
1. če niso izpolnjeni pogoji iz drugega in tretjega odstavka tega člena;
2. če oceni, da zahtevani osebni podatki niso primerni za izvedbo raziskave;
3. če oceni, da nameni oziroma cilji raziskave ne upravičujejo posega v pravice posameznikov, na katere se nanašajo osebni podatki;
4. če oceni, da ukrepi za varnost osebnih podatkov niso ustrezni, ali
5. če gre za tajne podatke v skladu z zakonom o tajnih podatkih.

Argumentacija k predlogu GZS:

Osnovno vodilo pri obdelavi osebnih podatkov v znanstveno raziskovalne namene je zapisano v uvodni določbi št. 159[28]. Po njem je treba obdelavo osebnih podatkov v znanstveno-raziskovalne

[28] *Ta uredba bi se morala uporabljati tudi za obdelavo osebnih podatkov v znanstveno-raziskovalne namene. Za namene te uredbe bi bilo treba obdelavo osebnih podatkov v znanstveno-raziskovalne namene razlagati široko, tako*

namene razlagati široko, tako da vključuje tudi na primer tehnološki razvoj, predstavitvene dejavnosti, temeljne raziskave, uporabne raziskave in zasebno financirane raziskave in upoštevati cilj Unije iz člena 179(1) PDEU glede oblikovanja evropskega raziskovalnega prostora. Veljati bi morali posebni pogoji, zlasti v zvezi z objavo ali drugim razkritjem osebnih podatkov v okviru znanstveno-raziskovalnih namenov. Sicer pa obdelavo osebnih podatkov v znanstveno raziskovalne namene urejajo še uvodne določbe št. 33, 50, 52, 53, 62, 65, 113, 156 in 157.

Državam članicam je dana možnost, da pri obdelavi osebnih podatkov v znanstvene in zgodovinsko-raziskovalne namene ali statistične namene pod določenimi pogoji in ob zagotovitvi ustreznih zaščitnih ukrepov za posameznike, na katere se nanašajo osebni podatki, določijo natančnejšo ureditev in odstopanja v zvezi z zahtevami po informacijah ter pravice do popravka, do izbrisa, do pozabe, do omejitve obdelave, do prenosljivosti podatkov in do ugovora (uvodna določba št. 156 Splošne uredbe o varstvu podatkov). Tako 89/II člen Splošne uredbe o varstvu podatkov izrecno določa, da se lahko, kadar se osebni podatki obdelujejo v znanstveno ali zgodovinsko-raziskovalne namene, v pravu države članice določijo odstopanja od pravic posameznikov iz členov 15, 16, 18 in 21 Splošne uredbe o varstvu podatkov, če so za obdelavo določeni zaščitni ukrepi iz prvega odstavka 89. člena, kolikor je verjetno, da bi takšne pravice onemogočile ali resno ovirale doseganje posebnih namenov in kolikor so takšna odstopanja nujna za uresničitev teh namenov.

Državam članicam tako ni dano pooblastilo, da drugače, izven določb 6. člena Splošne uredbe o varstvu podatkov urejajo pravne podlage za obdelavo osebnih podatkov v znanstveno-raziskovalne namene. Tako v določbah Splošne uredbe o varstvu podatkov ni najti osnove za drugačno določanje pravnih podlag, kot so urejene v 6. členu Splošne uredbe o varstvu podatkov. V določbah Splošne uredbe o varstvu podatkov tako tudi ni najti pooblastila državi članici, da obdelavo uredi na t.i. domnevni privolitvi, kot je to predlagano v 68. členu predloga ZVOP-2 – če posameznik ni prepovedal, oziroma je dal pisno privolitev, če so osebni podatki poklicna skrivnost. V tem delu manjka tudi definicija osebnih podatkov kot poklicne skrivnosti. ZVOP-2 namreč ne definira, kdaj gre za osebne podatke, ki pomenijo poslovno skrivnost.

---

da vključuje tudi na primer tehnološki razvoj, predstavitvene dejavnosti, temeljne raziskave, uporabne raziskave in zasebno financirane raziskave. Poleg tega bi bilo treba upoštevati cilj Unije iz člena 179(1) PDEU glede oblikovanja evropskega raziskovalnega prostora. Znanstveno-raziskovalni nameni bi morali zajemati tudi študije, izvedene v javnem interesu na področju javnega zdravja. Da bi upoštevali posebnosti obdelave osebnih podatkov v znanstveno-raziskovalne namene, bi morali veljati posebni pogoji, zlasti v zvezi z objavo ali drugim razkritjem osebnih podatkov v okviru znanstveno-raziskovalnih namenov. Če so na podlagi rezultatov znanstvenih raziskav, zlasti na področju zdravja, potrebni nadaljnji ukrepi v interesu posameznika, na katerega se nanašajo osebni podatki, bi se v zvezi s takšnimi ukrepi morala uporabljati splošna pravila iz te uredbe.

Sledeč določbam Splošne uredbe o varstvu podatkov o načelu "omejitve namenov" je nadaljnja obdelava osebnih podatkov v znanstveno ali zgodovinsko-raziskovalne namene združljiva z nameni, za katere so bili osebni podatki prvotno zbrani in s tem dovoljena (uvodna določba št. 50 in točka b) 5/I člena Splošne uredbe o varstvu podatkov). Predvidene niso nobene omejitve in državam članicam ni dano pooblastilo za uzakonitev dodatnih pogojev za združljivost znanstveno-raziskovalnih namenov s prvotnimi. Kot izjemo vidimo le možnost, ki naj bi bila dana posamezniku v primeru, ko obdelava osebnih podatkov za znanstveno raziskovalne namene temelji na privolitvi, da da privolitev le za nekatera znanstveno-raziskovalna področja, ali le za dele raziskovalnih projektov (uvodna določba št. 33 Splošne uredbe o varstvu podatkov). Vsekakor pa je privolitev kot pravni temelj primerna in dopustna le, če je v skladu z zahtevami Splošne uredbe o varstvu podatkov (dana z jasnim pritrdilnim ravnanjem, informirana, svobodna in specifična - dana za konkreten namen).

Države članice sicer imajo možnost da ohranijo ali uvedejo dodatne pogoje, tudi omejitve, glede obdelave genetskih podatkov, biometričnih podatkov ali podatkov o zdravstvenem stanju (uvodna določba št. 53 Splošne uredbe o varstvu podatkov), vendar je očitno da se omejitve v zvezi z obdelavo osebnih podatkov za znanstveno-raziskovalne namene iz 68. člena predloga ZVOP-2 ne nanašajo na te vrste podatkov.

Predlagamo uskladitev določbe prvega odstavka 68. člena predloga ZVOP-2 z določili Splošne uredbe o varstvu podatkov, kar bi pomenilo, da se obdelava osebnih podatkov, prvotno zbranih za druge namene, vselej šteje za združljivo s prvotnim namenom. Drugi odstavek 67. člena predloga ZVOP-2 sicer določa: *Šteje se, da namen obdelave osebnih podatkov za raziskovanje ni v nasprotju z namenom njihovega zbiranja.* Pri tem ne gre za ustaljeno terminologijo iz Splošne uredbe o varstvu podatkov, saj ta primarno govori o *združljivosti namenov* in ne o tem, da si nameni ne nasprotujejo. Gre torej za institut iz Splošne uredbe o varstvu podatkov, ki ga je treba uporabiti, kot je reguliran (uvodna določba št. 50).

Znanstveno raziskovalni namen obdelave je ob zagotovitvi ustreznih zaščitnih ukrepov vselej združljiv s prvotnim (točka b) 5/I in 89/I člen Splošne uredbe o varstvu podatkov). V primeru združljivosti namenov ni potrebna ločena pravna podlaga od tiste, na podlagi katere so bili osebni podatki zbrani (uvodna določba št. 50 Splošne uredbe o varstvu podatkov). S tem odpade odgovornost upravljavcev pri posredovanju osebnih podatkov za znanstveno raziskovalne namene glede pravnega temelja prosilca. Upravljavci se bodo osredotočili na vprašanje, ali prosilec izpolnjuje pogoje za izvajalca raziskovanja.

V nadaljevanju podajamo še naše mnenje in argumente glede predlagane spremembe četrtega odstavka 68. člena predloga ZVOP-2. Določba določa okoliščine, v katerih sme upravljavec prosilcu zavrniti posredovanje osebnih podatkov za namen izvedbe raziskave.

Sami imamo pomisleke že glede okoliščin, ki jih je nanizal predlagatelj, kot na primer, ali je res v domeni upravljavca presoja o tem, ali so zahtevani osebni podatki primerni za izvedbo raziskave in ocena, da nameni raziskave ne opravičujejo posega v pravice posameznikov. Breme vsebinske presoje ne bi smelo biti na upravljavcu. Ta vsaj praviloma ne bo strokovnjak za področje, na katerem se bo izvajala raziskava, čaka pa ga zahtevna naloga že v prvem koraku – pri presoji, ali je zaprosilo vložil upravičen prejemnik – *organizacija ali posameznik, ki pri svojem delovanju uporablja etična načela in metodologijo s področja raziskovanja ter pravila glede varstva osebnih podatkov tega poglavja zakona* (prvi odstavek 67. člena predloga ZVOP-2). Opredelitev upravičencev je zelo splošna. Iz obrazložitve k 67. členu predloga ZVOP-2 izhaja, da se za raziskovalce in raziskovalne organizacije ne zahteva, da so registrirani skladno z zakonodajo s področja raziskovanja, edini pogoj je, da pri svojem delovanju uporabljajo etična pravila in metodologijo. V izogib dvomov upravljavcev o tem, katere so po drugem odstavku 68. člena predloga ZVOP-2 *raziskovalne organizacije ter raziskovalci, ki so pri raziskovanju vezani na etična načela in metodologijo iz prvega odstavka prejšnjega člena,* ter potencialnih nehotenih kršitev iz tega naslova, predlagamo natančnejšo opredelitev upravičenih raziskovalcev. Kot najbolj enostavna možnost se ponuja navezava na Evidenco izvajalcev raziskovalne in razvojne dejavnosti, ki jo vodi ARRS, sprejemljiva pa bi bila tudi drugačna referenca, če upravljavcem omogoča enostavno preverjanje statusa oziroma upravičenosti prosilca. V tem delu je predlagam amandma k prvem odstavku 67. člena predloga ZVOP-2.
Če ne pride do navezave na obstoječe evidence in sezname, bo upravljavec ta pogoj po naši oceni težko preverjal drugače kot, da se bo zanesel na izjavo prosilca podatkov. Predlagamo, da se, kolikor ne pride do spremembe prvega odstavka 67. člena s sklicem na Evidenco pri ARRS, na ta način dopolni drugi odstavek 68. člena predloga ZVOP-2. Med dokazila o opisu raziskave, ki so jih dolžni raziskovalci predložiti upravljavcu, bi dodali tudi izjavo raziskovalca oziroma raziskovalne organizacije, da pri svojem delovanju uporabljajo etična pravila in metodologijo s sklicem na konkretna pravila etike in metodologijo, ki ji sledi pri predmetni raziskavi.

V četrtem odstavku je smiselno dodatno možnost upravljavcev za zavrnitev posredovanja osebnih podatkov nasloniti na izostanek plačila posredovanja podatkov (razen, če bi drug zakon zapovedoval brezplačno posredovanje) in organizacijske ali tehnične ovire za zagotovitev želenih podatkov.

Upravljavec bi moral imeti možnost, da se sam odloči, ali bo posredovanje osebnih podatkov zaračunal, kot tudi, ali mu obstoječi kadrovski in tehnični viri omogočajo posredovanje podatkov brez posebnega vpliva na njegovo redno poslovanje. Nenazadnje priprava zaprošenih podatkov, tudi upoštevanje zaščitnih ukrepov, vodenje eventualnih revizijskih sledi pri posredovanju osebnih podatkov (v odvisnosti od vrste podatkov), obveščanje posameznikov o obdelavi, izvrševanje njihovih pravic v zvezi z obdelavo osebnih podatkov za znanstveno-raziskovalne namene, ipd upravljavcu povzročajo dodatno delo in stroške.

Predlagana dopolnitev tako prvega kot drugega in četrtega odstavka 68. člena Splošne uredbe o varstvu podatkov je smiselna.

69. člen (kontaktiranje posameznikov), cel člen, podredno 2. odstavek

Besedilo predloga ZVOP-2:

(1) V okviru obdelave osebnih podatkov za raziskovanje upravljavec izjemoma lahko obdeluje tudi osebne podatke ciljne skupine posameznikov zaradi pridobitve privolitev za obdelavo njihovih osebnih podatkov ali zaradi pridobitve dodatnih podatkov ali pojasnil za namene raziskovanja.

(2) Upravljavec lahko na podlagi zbirk, s katerimi razpolaga v okviru zakonitega opravljanja dejavnosti, proti plačilu stroškov obdelave osebnih podatkov kontaktira posameznike z namenom pridobivanja privolitev za izvrševanje namenov iz prejšnjega odstavka.

(3) Za namen kontaktiranja se lahko obdelujejo naslednji osebni podatki: osebno ime, naslov stalnega ali začasnega prebivališča, telefonska številka in naslov elektronske pošte.

Argumentacija k predlogu GZS:

Kot smo obširno pisali v argumentaciji k 68. členu predloga ZVOP-2 se osebni podatki za znanstveno-raziskovalne namene obdelujejo po mehanizmu združljivosti namenov in ni potrebna ločena pravna podlaga od tiste, na podlagi katere so bili osebni podatki zbrani (uvodna določba št. 50 Splošne uredbe o varstvu podatkov). Tako je težko razumeti, zakaj se v prvem odstavku 69. člena ustvarja zakonski pravni temelj – v smislu pravnega temelja obdelave osebnih podatkov v javnem interesu iz točke e) 6/I člena Splošne uredbe o varstvu podatkov za kontaktiranje posameznikov za namen pridobitve njihove privolitve v obdelavo osebnih podatkov. Kolikor sledimo namenu Splošne uredbe o varstvu podatkov o tem, da so znanstveno raziskovalni nameni obdelave osebnih podatkov vedno združljivi s prvotnimi nameni, za katere so bili osebni podatki pridobljeni, ni jasno, v katere namene bi upravljavec kontaktiral posameznike, katerih osebni

podatki bodo vključeni v raziskavo. Dopustiti je možnost, da bi potreba po "dodatnih pojasnilih" s strani v raziskavo vključenega posameznika nastopila na strani izvajalca raziskave. V tem primeru bi morala biti možnost kontaktiranja posameznika dana njemu.
Več kot očitno gre za zamisli, ki so se porodile v zatečeni ureditvi obdelave osebnih podatkov za znanstveno raziskovalne namene po določbah ZVOP-1, ki je dopuščal le posredovanje anonimiziranih podatkov, osebnih pa le če je tako določal zakon ali če je posameznik, na katerega se nanašajo osebni podatki, predhodno podal pisno privolitve, da se lahko njegovi osebni podatki za znanstveno-raziskovalne namene obdelujejo brez anonimiziranja (drugi odstavek 17. člena ZVOP-1).

Poudarjamo še, da so raziskave na posebnih področjih, kot so na primer klinične raziskave posebej regulirane, in se bodo za njihovo izvajanje še naprej uporabljale določbe področnih predpisov (na primer določbe Uredbe (EU) št. 536/2014 Evropskega parlamenta in Sveta[29] in ZZdr-2[30]).

Po Splošni uredbi o varstvu podatkov, ki je glede obdelave osebnih podatkov za znanstveno-raziskovalne namene jasna (in je obdelavo odprla; uvodna določba št. 50, točka b) 5/I in 89/I člen Splošne uredbe o varstvu podatkov) dopustitev kontaktiranja za namen pridobivanja privolitve v udeležbo v raziskavi, ni potrebna. 69. člen predloga ZVOP-2 je tako nepotreben in naj se izpusti.

Res zgolj podredno, kolikor bi ob povsem drugačni regulaciji obdelave osebnih podatkov za znanstveno-raziskovalne namene eventualno obstajali razumni razlogi za omogočanje obdelave osebnih podatkov posameznikov, katerih osebni podatki bodo uporabljeni v raziskavi, upravljavcu, naj se spremeni drugi odstavek 69. člena predloga ZVOP-2. Pri oblikovanju predloga amandmaja je pomembno, da 69. člen predloga ZVOP-2 že sedaj uporablja besedo "lahko". Besedilo predloga je že sedaj treba razumeti kot možnost upravljavca in ne kot njegovo dolžnost, kljub morebitnemu zaprosilu izvajalca raziskave.

75. člen (splošne določbe o videonadzoru in varstvu osebnih podatkov), 1. odstavek

Besedilo predloga ZVOP-2:

(1) Določbe tega poglavja se uporabljajo za izvajanje videonadzora, če drug zakon ne določa drugače.

[29] Uredba (EU) št. 536/2014 Evropskega parlamenta in Sveta z dne 16. aprila 2014 o kliničnem preskušanju zdravil za uporabo v humani medicini in razveljavitvi Direktive 2001/20/ES
[30] Zakon o zdravilih (Uradni list RS, št. 17/14 in 66/19).

Argumentacija k predlogu GZS:

Simseln je amandma k prvemu odstavku 75. člena v zvezi z inteligentno video-analitiko. Obrazložitev argumetacije izhaja iz šestega odstavka argumentacije k predlogu GZS, vezane na 79. člen.

76. – 79. člen (določbe za posebne primere videonadzora)

V tem delu je dana splošna pripomba GZS, da določbe o izvajanju video-nadzora omejujejo krog dopustnih namenov video-nadzora. Takšno omejevanje pa po oceni GZS ni v skladu s Splošno uredbo o varstvu podatkov. Za video-nadzor naj bi po Splošni uredbi veljala splošna pravila obdelave osebnih podatkov, državam članicam ni dano pooblastilo za specifično urejanje. Pri tem GZS opozarja, da lahko izvajanje video-nadzora, ki je sicer skladen z dopustnimi nameni (na primer za zagotavljanje varnosti) predstavlja večji poseg v zasebnost kot pa na primer izvajanje video-nadzora za potrebe video-analitike za štetje obiskovalcev. Pretirano omejevanje dopustnih namenov video-nadzora onemogoča razvoj tehnologij in uporabo novih rešitev in storitev, ki ne podpirajo dopustnih namenov video-nadzora.

Argumentacija k razmišljanju GZS:

Delimo mnenje GZS, da je obdelava osebnih podatkov s sredstvi za snemanje, torej tudi video-nadzor, le ena od potencialnih oblik obdelave osebnih podatkov (podobno kot obdelava osebnih podatkov z napravami za zvočno snemanje, obdelava osebnih podatkov v oblaku ipd).

Po Smernicah EDPB[31] št. 3/2019 o obdelavi osebnih podatkov z video napravami (z dne 29.1.2020[32]), ki jih izpostavlja tudi GZS, ni dvoma, da je izvajanje video-nadzora mogoče nasloniti na vsakega od pravnih temeljev za obdelavo osebnih podatkov iz 6/I člena Splošne uredbe o varstvu podatkov. Na strani 8 Smernic, pod točko 3 so usmeritve glede zakonitosti obdelave osebnih podatkov z video-nadzorom. Med drugim je EDPB v tem delu zapisal: *" Video nadzor se lahko uporablja za številne namene, npr. pomoč pri varstva lastnine in drugega premoženja, pomoč pri varovanju življenja in telesne celovitosti posameznikov ter zbiranje dokazov za civilne tožbe...Načeloma lahko vsak pravni razlog iz člena 6(1) zagotavlja pravno podlago za obdelavo podatkov, pridobljenih z video nadzorom. Na primer, člen 6(1)(c) se uporablja, kadar nacionalno*

[31] EDPB je Evropski odbor za varstvo podatkov je neodvisni evropski organ, ki prispeva k dosledni uporabi pravil o varstvu podatkov v Evropski uniji in spodbuja sodelovanje med organi EU za varstvo podatkov. S sprejemanjem Smernic za podrobnejšo opredelitev pogojev evropske zakonodaje o varstvu podatkov zagotavljajo dosledno razlago Splošne uredbe o varstvu podatkov in enako uporabo – enake pravice in obveznosti posameznikov in upravljavcev (več na povezavi: https://edpb.europa.eu/about-edpb/about-edpb/who-we-are_sl).

[32] Smernice št. 3/2019 so v slovenskem prevodu dostopne na povezavi: https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201903_video_devices_sl_0.pdf

pravo določa obveznost izvajanja video nadzora. Vendar se bosta v praksi najverjetneje uporabljali naslednji določbi:

- *člen 6(1)(f) (zakoniti interes);*
- *člen 6(1)(e) (potreba po opravljanju naloge v javnem interesu ali pri izvajanju javne oblasti).*

V izjemnih primerih lahko upravljavec kot pravno podlago uporabi člen 6(1)(a) (privolitev).«[33]

Pri tem glede zakonitih interesov, ki jih upravljavec lahko zasleduje z video-nadzorom EDPB zapiše: *"Zakoniti interesi, za katere si prizadeva upravljavec ali tretja oseba, so lahko pravni, gospodarski ali nematerialni interesi*[34]*«*. Kroga zakonitih interesov za izvajanje video-nadzora ne le, da ne omejuje Splošna uredba o varstvu podatkov, pač pa tudi skupne usmeritve EDPB-ja ne gredo v tej smeri.

Tako ne more biti nobenega dvoma o tem, da Splošna uredba državam članicam ne daje pooblastila za prepoved naslonitve obdelave osebnih podatkov z video napravami (video-nadzora) na katerikoli pravni temelj iz 6/I člena Splošne uredbe o varstvu podatkov, s tem v povezavi pa tudi ne pooblastila za določitev le ozkega nabora namenov uporabe video-nadzora, četudi tudi EDPB v Smernicah št. 3/2019 dodaja, da države članice lahko ohranijo ali uvedejo posebno nacionalno zakonodajo za video-nadzor, da prilagodijo uporabo pravil iz Splošne uredbe o varstvu podatkov z natančnejšo določitvijo posebnih zahtev za obdelavo, če je to v skladu z načeli, določenimi v Splošni uredbi o varstvu podatkov (npr. omejitev hrambe, sorazmernost)[35]. Ta »natančnejša določitev posebnih zahtev« pa ne more pomeniti omejitve pravnih podlag niti ne namenov oziroma zakonitih interesov upravljavca. Lahko pa država članica določi posebne zahteve glede izkazovanja in/ali dokumentiranja utemeljitev o pravnem temelju za izvajanje video-nadzora in za njegovo skladnost z načeli iz 5. člena Splošne uredbe o varstvu podatkov kot je omejitev hrambe, minimalni obseg podatkov, informiranje posameznikov.

Tudi v tem primeru se tako zdi, da gre v določbah predloga ZVOP-2 o video-nadzoru preprosto za prenos in nadgradnjo ureditve izvajanja video-nadzora iz ZVOP-1, ki pa je bil sprejet v drugačnih pravnih okoliščinah (ob veljavnosti Direktive 46/95). Menimo, da je predlagatelj preprosto spregledal spremenjene pravne okoliščine in s tem presegel pooblastila, ki so državam članicam s Splošno uredbo o varstvu podatkov dana za urejanje obdelave osebnih podatkov na nacionalni ravni.

---

[33] Glejte točki 14 in 15 na strani 8 Smernic št. 3/2019.
[34] Glejte točko 18 na strani 9 Smernic št. 3/2019.
[35] Točka 42 na strani 12 Smernic št. 3/2019.

79. člen (videonadzor na javnih površinah), cel člen, podredno 1. in 10. odstavek

Besedilo predloga ZVOP-2:

(1) Videonadzor na javnih površinah, kot jih določa zakon, ki ureja urejanje prostora, je dovoljen le, kadar je to potrebno zaradi obstoja resne in utemeljene nevarnosti za življenje, osebno svobodo, telo ali zdravje ljudi, varnost premoženja upravljavca ali varovanje tajnih podatkov upravljavca ali obdelovalca v prenosu in teh namenov ni mogoče doseči z drugimi sredstvi, ki manj posegajo v pravice iz prvega odstavka 1. člena tega zakona. Videonadzor na javnih površinah je dovoljen tudi za namene varovanja varovanih oseb ter posebnih objektov in okolišev objektov, ki jih varuje policija, Slovenska vojska, pristojni organi za področje varnosti države, pravosodna policija, oziroma varovanja drugih prostorov, zgradb ali območij, ki jih je treba varovati na podlagi zakona, in sicer samo v obsegu in trajanju, potrebnem za doseganje namena. Vpogled, uporaba ali posredovanje posnetkov so dopustni le za te namene, če drug zakon ne določa drugače.

(2) Videonadzor se lahko izvaja le glede tistih delov javne površine in v obsegu, kjer je treba varovati interese iz prejšnjega odstavka.

(3) Videonadzor na javnih površinah lahko izvaja oseba javnega ali zasebnega sektorja, ki upravlja z javno površino ali na njej zakonito opravlja dejavnost. Videonadzor smejo za javni sektor izvajati le uradne osebe ali pooblaščeno varnostno osebje, za zasebni sektor pa pooblaščeno varnostno osebje. Osebe ali osebje iz prejšnjega stavka mora biti izrecno pooblaščeno za izvajanje videonadzora.

(4) Videonadzor se lahko izvaja tudi na način, da se ob snemanju izvaja spremljanje dogajanja v živo.

(5) Videonadzor iz prvega odstavka tega člena se za namen varovanja oseb, tajnih podatkov v prenosu, poslovnih skrivnosti ali premoženja večje vrednosti lahko opravlja tudi z uporabo telesne kamere, če jo uporablja za to posebej usposobljena oseba.

(6) Posnetki videonadzora na javnih površinah se lahko ob upoštevanju splošnih načel iz 5. člena Splošne uredbe hranijo največ šest mesecev od trenutka nastanka posnetka, če zakon ne določa drugače.

(7) Upravljavec videonadzornega sistema, ki izvaja videonadzor javnih površin, mora v primeru, ko videonadzorni sistem posname dogodek, ki ogroža zdravje ali življenje posameznika, o tem nemudoma obvestiti policijo ali drug pristojni subjekt.

(8) Na področju videonadzora cestnega prometa sme upravljavec izvajati videonadzor le na vnaprej določenih odsekih cest v svojem upravljanju, tako da se ne izvaja sistemsko nadzorovanje gibanja posameznikov ali poseganje v zasebnost posameznikov. Upravljavec mora v skladu z zakonom določiti tiste odseke ceste v svojem upravljanju, kjer z drugimi sredstvi ni mogoče doseči nujnega in učinkovitega varovanja cestnega prometa ali njegovega upravljanja.

(9) Upravljavec videonadzornega sistema iz prejšnjega odstavka mora pred dokončno določitvijo lokacij iz prejšnjega odstavka izdelati oceno učinka, ki vsebuje lokacijo odsekov cest, in joposredovati v predhodno mnenje nadzornemu organu.

(10) Na javnih površinah je prepovedana uporaba sistemov za avtomatsko prepoznavo registrskih tablic in sistemov, s katerimi se obdelujejo biometrični osebni podatki, razen če zakon izrecno določa drugače.

Argumentacija k predlogu GZS:

Obrazložitev predlagatelja ZVOP-2 k 79. členu je vsebinsko zgolj prepis določil predlaganega člena in ne vsebuje razlogov, ki so predlagatelja vodili pri oblikovanju besedila.

Kot smo zapisali že zgoraj v Splošni uredbi o varstvu podatkov ni najti pooblastila državi za specifično urejanje video-nadzora z oženjem možnih pravnih temeljev in/ali zakonitih interesov upravljavcev zgolj na primere, ki jih "v zakonitem interesu upravljavca" prepozna zakonodajalec, lahko pa zakonodajalec na nacionalni ravni določi natančnejša pravila za izkazovanje skladnosti obdelave z načeli kot so omejitev hrambe, minimalni obseg podatkov, informiranje posameznikov.

Iz že omenjenih Smernic EDPB št. 3/2019 je razvidno, da je sicer treba težiti k skrbni in prepričljivi utemeljitvi upravičenosti video-nadzora. Tako se na primer pravni temelj zakonitega interesa upravljavca izkazuje na način, da se presoja konkretna situacija (ne hipotetična, splošna) in tveganja za poseganje v pravice posameznika, pri čemer je odločilno merilo intenzivnost poseganja v pravice in svoboščine posameznika[36], da pa vnaprejšnjih omejitev za upravljavce v Splošni uredbi o varstvu podatkov ni. Kot primer video-nadzora na javnih površinah je na strani 11 Smernic 3/2019 naveden primer video-nadzora na zasebnem parkirišču[37] zaradi težav s ponavljajočimi se tatvinami na parkirišču. Ker v tem primeru ne gre izrecno za varstvo premoženja upravljavca (pač pa za varstvo premoženja posameznikov, ki na parkirišču parkirajo), video-nadzor, ki je dopusten po Smernicah EDPB št. 3/2019, po ZVOP-2 ne bi bil dopusten. Z video-nadzorom sme po predlogu iz 79/I člena upravljavec namreč varovati le svoje premoženje. Navedeno pa je v očitnem nasprotju s samim konceptom zakonitega interesa iz točke f) 6/I člena Splošne uredbe o varstvu podatkov, ki je lahko zakoniti interes upravljavca ali tretjega. Zakoniti interes pa je pravzaprav najbolj tipičen pravni temelj za izvajanje video-nadzora.

Poudariti je treba tudi, da se za obdelavo osebnih podatkov s strani organov kazenskega pregona ne uporablja Splošna uredba o varstvu podatkov (glej člen 2(2)(d)), ampak Direktiva (EU)

---

[36] Glejte točko 32 na strani 11 Smernic 3/2019.

[37] Primer: *Zasebno parkirno podjetje je dokumentiralo ponavljajoče se težave s tatvinami v parkiranih avtomobilih. Parkirišče je odprt prostor in je zlahka vsakomur dostopno, vendar je jasno označeno z oznakami in cestnimi blokatorji, ki obkrožajo prostor. Parkirno podjetje ima zakoniti interes (preprečevanje tatvin v avtomobilih strank), da nadzoruje parkirišče v času dneva, ko se pojavljajo težave. Posameznike, na katere se nanašajo osebni podatki, se nadzoruje v omejenem obdobju, niso v območju za rekreativne namene in tudi v njihovem interesu je, da se tatvine preprečijo. Nad interesom posameznikov, na katere se nanašajo osebni podatki, da se jih ne nadzoruje, v tem primeru prevladuje zakoniti interes upravljavca.*

2016/680 o kazenskem pregonu, v Sloveniji prenesena v ZVOPOKD[38]. Videonadzor na javnih površinah *za namene varovanja varovanih oseb ter posebnih objektov in okolišev objektov, ki jih varuje policija, Slovenska vojska, pristojni organi za področje varnosti države, pravosodna policija, oziroma varovanja drugih prostorov, zgradb ali območij, ki jih je treba varovati na podlagi zakona*, kot ga ureja prvi odstavek 79. člena predloga ZVOP-2 po naši oceni ne sodi v ta predpis, pač pa v ZVOPOKD ali področne zakone, ki urejajo dejavnost posameznega organa.

Glede avtomatske prepoznave registrskih tablic je najprej treba poudariti, da z vidika posegov v varstvo osebnih podatkov ni primerljiva z avtomatsko prepoznavo obrazov ali obdelavo eventualno drugih posameznikovih biometričnih značilnosti. Tako je težko razumeti, zakaj je predlagatelj enako prepovedal obe. Še posebej, ker se tehnologija za avtomatsko prepoznavo registrskih tablic na podlagi Splošne uredbe o varstvu podatkov v praksi že uporablja, tipično na javnih ali zasebnih parkiriščih, utemeljena na pravnem temelju zakonitega interesa upravljavca (točka f 6/I člena Splošne uredbe o varstvu podatkov), neredko tudi na pravnem temelju iz točke b) 6/I člena Splošne uredbe o varstvu podatkov, ko gre za na primer abonente na parkiriščih. Težko je razumeti, da bo nenadoma nezakonito, kar se povsem zakonito izvaja že več let. Argumentov, ki bi izkazovali potrebo po spremembi v obrazložitvi nismo našli.
Ker gre pri avtomatski prepoznavi registrskih tablic za obliko video-nadzora bi lahko na nacionalni ravni določili obveznosti glede omejitev hrambe, minimalnega obsega podatkov, informiranja posameznikov. Država članica pa nima glede obdelave osebnih podatkov – avtomatske prepoznave registrskih tablic enakih pooblastil, kot jih Splošna uredba v četrtem odstavku 9. člena daje državam članicam glede obdelave genetskih, biometričnih podatkov ali podatkov v zvezi z zdravjem. Vsekakor po našem mnenju državam članicam s Splošno uredbo o varstvu podatkov ni dana možnost, da omejijo ali celo prepovedo določen način obdelave osebnih podatkov, če ne gre hkrati za obdelavo genetskih, biometričnih ali podatkov v zvezi z zdravjem.

S strani upravljavcev, ki so tudi lastniki ali najemniki večjih parkirnih površin, je že v uporabi tudi t.i. inteligentna video-analitika (štetje vozil, spremljanje zasedenosti parkirnih mest, gostote prometa...). Informacijski pooblaščenec je o tovrstni obdelavi osebnih podatkov že izdal smernice[39], ki so po podatkih s spletne strani trenutno v prenovi[40]. Tako v tem trenutku ni mogoče ugotoviti, kakšno je veljavno stališče Informacijskega pooblaščenca do vprašanj, ki so bila v preteklosti že odgovorjena. Uporabo inteligentnih video analiz komentirajo tudi Smernice EDPB 3/2019 (točka 3). Te so lahko invazivne za posameznikovo zasebnost ali pa tudi ne (če grena primer zgolj za štetje obiskovalcev). Ob izvajanju svojih pooblastil, da na nacionalni ravni določi

[38] Zakon o varstvu osebnih podatkov na področju obravnavanja kaznivih dejanj (Uradni list RS, št. 177/20).

[39] Smernice o inteligentni videoanalitiki (22.4.2013).
[40] Glejte povezavo: https://www.ip-rs.si/publikacije/smernice-o-inteligentni-videoanalitiki

natančnejša pravila za izkazovanje skladnosti obdelave z načeli kot so omejitev hrambe, minimalni obseg podatkov, informiranje posameznikov, bi lahko zakonodajalec nagovoril tudi izvajanje video-analitike, na primer omejitev hrambe osebnih podatkov, ki se zajemajo zanjo, način informiranja o izvajanju video-analitike v odvisnosti od njene invazivnosti za varstvo osebnih podatkov. Predlagamo, da se za namen razmejitve med enostavno video-analitiko in video-nadzorom naredi razmejitev že v 75. členu, in sicer v prvem odstavku, tako da se določi, kdaj se za enostavno video-analitiko ne uporabljajo določbe o video-nadzoru.

Video-nadzor na javnih površinah naj se izvaja po splošnih pravilih iz 75. člena, ali pa naj se regulacija video-nadzora na javnih površinah omeji na javne površine kot so javna cesta, ulica, pasaža, trg, tržnica, igrišče, pokopališče, park, zelenica, rekreacijska površina ne pa tudi na atrije in parkirišča.

V izogib dvomov ali je na parkiriščih dopusten video-nadzorni sistem za avtomatsko prepoznavo registrskih tablic, je predlagan še poseg v deseti odstavek 79. člena predloga ZVOP-2. Primarno je predlagano, da se izpusti, saj predlagatelj ni navedel nobenih argumentov za popolno prepoved obdelave osebnih podatkov z avtomatsko prepoznavo registrskih tablic. Vselej niti ne bo šlo za osebne podatke, ker bo podatek o registrski tablici vodil do lastnika in/ali imetnika, ki je pravna oseba (zavod, gospodarska družba, slednih primerov je veliko zaradi razširjene prakse leasinga) ali samostojni podjetnik. V primeru avtomatske prepoznave registrskih tablic gre torej za obdelavo osebnih podatkov le v primeru, ko je lastnik in/ali imetnik vozila posameznik. Tudi v tem primeru je ne moremo šteti za invazivno za zasebnost posameznika, saj lastnik in/ali imetnik vozila nikakor ni nujno tudi njegov voznik oziroma uporabnik. Povezovanje branja podatka registrske tablice z lokacijo lastnika in/ali imetnika vozila je preveč poenostavljeno. Običajno je, da vozilo tudi v družini, torej v primerih, ko bo vsaj imetnik, če že ne tudi lastnik vozila posameznik, uporablja več oseb.

Glede popolne prepovedi sistemov za avtomatsko prepoznavo s katerimi se obdelujejo biometrični osebni podatki, pa je treba ugotoviti, da ta ni potrebna, saj je obdelava biometričnih osebnih podatkov posebej regulirana v 4. poglavju predloga ZVOP-2. Če upravljavec pri obdelavi biometričnih osebnih podatkov ne bo zadostil pogojem iz tega dela zakona, bo ta nezakonita.

Glede na navedeno sta predlagani dve možnosti amandmaja k desetemu odstavku 79. člena predloga ZVOP-2.

80. člen (omejitev biometrije), 2. odstavek

Besedilo predloga ZVOP-2:

(2) Obdelava biometričnih osebnih podatkov se lahko določi le z zakonom, ki poleg vsebin iz drugega ali tretjega odstavka 6. člena tega zakona določi tudi pogoje za njeno uporabo in morebitne omejitve uporabe.

Argumentacija k predlogu GZS:

Predlagatelj v obrazložitev navaja, da gre v drugem odstavku za izrecno prepoved uvedbe biometričnih ukrepov brez zakonske podlage. Obrazložitev je najmanj neprepričljiva, saj določba tretjega odstavka 6. člena (eden od sklicev iz drugega odstavka) ureja pravni temelj privolitve v javnem sektorju, tudi v primerih, ko takšna možnost ni izrecno predvidena z zakonom. V drugem odstavku 6. člena (drugi od sklicev v določbi drugega odstavka 8. člena predloga ZVOP-2) je natančneje opredeljena obveznost zakonodajalca v primeru urejanja obdelave osebnih podatkov na zakonskem pravnem temelju oziroma v javnem interesu (točki e in c 6/I člena Splošne uredbe o varstvu podatkov). Četudi se zdi, da predlagatelj zgolj ne razume v celoti koncepta pravnih podlag za obdelavo osebnih podatkov iz Splošne uredbe o varstvu podatkov, takšen drugi odstavek 80. člena predloga ZVOP-2 vzbuja najmanj dvom o tem, ali se lahko v zasebnem sektorju obdelujejo biometrični osebni podatki na podlagi privolitve posameznika. V drugem in tretjem odstavku 82. člena predloga ZVOP-2 so sicer posebej opisani primer, ko je dopustna privolitev in tudi odločba nadzornega organa ni potrebna, oziroma se obdelava biometričnih osebnih podatkov naslanja na pravni temelj pogodbe, pa vendar gre najmanj za nekonsistentnost.

Menimo, da pri regulaciji obdelave biometričnih osebnih podatkov ne gre za določanje zakonskega pravnega temelja, pač pa uporabo pooblastila, ki je dano državam članicam, da ohranijo ali uvedejo dodatne pogoje, tudi omejitve, glede obdelave genetskih, biometričnih ali podatkov v zvezi z zdravjem. Gre torej za zakonsko urejanje obdelave biometričnih podatkov (na za določitev zakonskega pravnega temelja), ki pa se lahko po tej zakonski ureditvi obdelujejo na različnih pravnih temeljih, tudi na podlagi privolitve ali za namen izvajanja pogodbe.

Poleg navedenega najbrž nenamernega oženja pravnih podlag, tudi ni dvoma, da so pravila zakonske regulacije osebnih podatkov že opredeljena v določbah 6. člena in ponovno sklicevanje nanje na tem mestu lahko vzbudi vtis, da pri drugih obdelavah osebnih podatkov (če ti na primer niso biometrični) ni treba slediti zapovedim glede vsebine zakonskega urejanja obdelave osebnih podatkov. Tak sklic je torej povsem nepotreben, tudi v primerih ko bi bil lahko smiseln in pravilen. Kot že navedeno zgoraj, gre v tem primeru najverjetneje za nekoliko napačno razumevanje institutov varstva osebnih podatkov.

Popolna opustitev poudarka o upoštevanja dodatnih pogojev za obdelavo osebnih podatkov po 9/II členu Splošne uredbe o varstvu podatkov, pa je lahko zavajajoča in pri sicer (pre)natančnem urejanju lahko pripelje do zmotnega zaključka, da je poglavje samozadostno in sledenje pogojem in Splošne uredbe sploh ni potrebno.

82. člen (biometrični ukrepi v zasebnem sektorju), 1., 2. in 3. odstavek

Besedilo predloga ZVOP-2:

(1) Obdelava biometričnih osebnih podatkov v zasebnem sektorju se lahko izvaja le v skladu z določbami tega člena, če je to nujno potrebno za opravljanje dejavnosti, za varnost ljudi, varnost premoženja, varovanje tajnih podatkov, varovanje poslovnih skrivnosti ali za varstvo točnosti identitete strank. Dejanja obdelave biometričnih osebnih podatkov morajo biti potrjena v skladu z 51. členom tega zakona.

(2) Oseba zasebnega sektorja lahko obdeluje biometrične osebne podatke tudi glede svojih strank. Taka obdelava je dopustna, če to za namene varovanja interesov iz prvega odstavka tega člena določa drug zakon, če to posebej določa pogodba ali so stranke dale izrecno privolitev. Kadar se biometrični osebni podatki obdelujejo na podlagi pogodbe s potrošnikom, mora upravljavec posamezniku, na katerega se nanašajo osebni podatki, omogočiti tudi način identifikacije brez obdelave biometričnih osebnih podatkov.

(3) Obdelava biometričnih osebnih podatkov v zasebnem sektorju se sme izvajati tudi pod pogojem, da so dejanja obdelave teh podatkov stranke pod njenim izključnim nadzorom ali njeno izključno oblastjo, ter omogoča stranki, da izrecno dovoli obdelavo teh podatkov drugim obdelovalcem in upravljavcem za namen dokazovanja točnosti svoje identitete.

Argumentacija k predlogu GZS:
Države članice kot že poudarjeno smejo po pooblastilu iz Splošne uredbe o varstvu podatkov iz četrtega odstavka 9. člena ohraniti ali uvesti dodatne pogoje, tudi omejitve, glede obdelave biometričnih podatkov. Seveda pa je pričakovati, da za omejitve oziroma dodatne pogoje ponudijo tudi tehtne argumente, tako da pojasnijo njihovo potrebnost in utemeljenost. V obrazložitvi k predlogu so dodatni pogoji (v delu gre tudi za omejitev dopustnih namenov oziroma interesov zasebnega sektorja, ki se smejo varovati z obdelavo biometričnih podatkov) le našteti, z ničemer pa niso utemeljeni.

Dejstvo je, da lahko v prihodnosti pričakujemo vse večjo uporabo t.i. umetne inteligence. V ta namen se področje umetne inteligence na ravni Evropske Unije tudi regulira. V postopku sprejemanja je Uredba Evropskega parlamenta in Sveta o določitvi harmoniziranih pravil o umetni inteligenci in spremembi nekaterih zakonodajnih aktov Unije[41]. EDPS[42] in EDPB sta junija 2021 izdala Skupno mnenje 5/2021 o predlogu Uredbe Evropskega parlamenta in Sveta o določitvi harmoniziranih pravil o umetni inteligenci[43]. Mnenje izpostavljamo kot primer natančne in poglobljene argumentacije sprejemljivosti ali nesprejemljivosti tudi umetno inteligenčnih sistemov, ki posameznike prepoznavajo na podlagi biometričnih podatkov. V nasprotju z njim je obrazložitev k predlogi ZVOP-2, iz katere bi bila razvidna vodila predlagatelja za postavljanje različnih omejitev in dodatnih pogojev, povsem izostala. Posledično se predlog kaže kot pavšalen in arbitraren.

Nobenega dvoma ni, da obdelava biometričnih osebnih podatkov predstavlja bolj invaziven poseg v pravico do varstva osebnih podatkov posameznikov kot obdelava »običajnih« osebnih podatkov. Hkrati ni dvoma, da v določenih primerih zakoniti interes upravljavca za identifikacijo posameznika z uporabo biometričnih podatkov lahko pretehta nad pravicami in svoboščinami posameznika. Oženje upravičenih zakonitih interesov upravljavcev na varnost ljudi, varnost premoženja, varovanje tajnih podatkov, varstvo poslovne skrivnosti ali varstvo točnosti identitete strank je videti ne le arbitrarno, pač pa je nelogično in vsaj v delu tudi v nasprotju z nadaljnjimi določbami 82. člena predloga ZVOP-2. Obdelava osebnih podatkov z biometričnimi ukrepi je namreč vselej namenjena enolični identifikaciji posameznika[44]. Tudi ni mogoče ugotoviti, zakaj je v prvem odstavku 82. člena predloga ZVOP-2 kot upravičen interes upravljavca prepoznan le interes *varstva točnosti identitete strank,* ne pa tudi interes varstva točnosti identitete zaposlenih, varstva točnosti identitete pogodbenih sodelavcev, varstva točnosti identitete posameznika v postopku sklepanja pogodbenega razmerja, ko še ne moremo govoriti o stranki upravljavca.

Nenazadnje so biometrični podatki namenjeni izključno enolični identifikaciji posameznika, ki mu pripadajo. Povedano enostavneje, bodo biometrični osebni podatki vselej za uporabljeni za enolično identifikacijo – ne glede na to, ali bo takšna enolična identifikacija potrebna zaradi varstva poslovne skrivnosti, varstva premoženja, varnosti ljudi ali varstva tajnih podatkov. Konceptualno je torej že prvi odstavek 82. člena po naši oceni smiselno preoblikovati, da bo

---

[41] Dostopno besedilo je iz aprila 2021, na povezavi: https://eur-lex.europa.eu/legal-content/SL/TXT/HTML/?uri=CELEX:52021PC0206&from=EN

[42] EDPS – Evropski nadzornik za varstvo podatkov je organ, ki skrbi, da institucije in organi EU pri obdelavi osebnih podatkov spoštujejo pravico državljanov do zasebnosti.

[43] Skupno mnenje št. 5/2021 je dostopno na povezavi: https://edpb.europa.eu/system/files/2021-10/edpb-edps_joint_opinion_ai_regulation_sl.pdf

[44] Biometrični podatki so po definiciji iz 14. točke 4. člena Splošne uredbe o varstvu podatkov podatki, ki so rezultat posebne tehnične obdelave v zvezi s fizičnimi, fiziološkimi ali vedenjskimi značilnostmi posameznika in omogočajo ali potrjujejo edinstveno identifikacijo posameznika.

logičen in bo sledil definiciji biometričnih osebnih podatkov iz Splošne uredbe o varstvu podatkov. Če ostane kot je, je po naši oceni najmanj v nasprotju s 4. odstavkom 82. člena, ki pa predvidena tudi obdelavo biometričnih podatkov zaposlenih (ne le upravljavčevih strank).

Glede na navedeno je primerno, da se najprej spremeni prvi odstavek 82. člena. Poleg preoblikovanja določbe je interes *varstva točnosti identitete strank* pretvorjen v interes sklepanja pravnega posla na daljavo. To so primeri, ko je drugačna identifikacija (na primer le z izpisom določenih osebnih podatkov iz osebnega dokumenta, ali skenom dela osebnega dokumenta) manj zanesljiva. Varovalka pred preveč poenostavljeno uvedbo pravila za identifikacijo z biometričnimi podatki pri vsakem sklepanju pogodb na daljavo je merilo nujnosti njihove uporabe, ki jo vselej pred izdajo odločbe presoja Informacijski pooblaščenec. Najverjetneje je smiselno tolmačenje v smeri, da bo obdelava biometričnih podatkov pri sklepanju pogodb na daljavo nujna le v povezavi z naravo pravnega posla (pravicami in obveznostmi strank), o čemer bo presojal Informacijski pooblaščenec.

Glede na zgoraj že izpostavljene argumente (na primer krog posameznikov, ki jih lahko naslavljajo biometrični ukrepi) je smiseln predlagan amandma tudi k drugem in tretjem odstavku 82. člena.

92. člen (obdelava osebnih podatkov za izvajanje določenih dejavnosti osebe javnega ali zasebnega sektorja), cel člen, podredno naslov in prvi odstavek

Besedilo predloga ZVOP-2:

(1) Oseba iz javnega ali zasebnega sektorja lahko uporablja kontaktne podatke posameznikov, ki jih je zbrala iz javno dostopnih virov ali v okviru izvrševanja svojih javnih nalog ali so ji jih posamezniki, na katere se nanašajo, prostovoljno razkrili ali dali privolitev, za namene organiziranja uradnih srečanj, izobraževanj, usposabljanj in dogodkov, določanja sestav ali delovanje komisij, svetov, delegacij in drugih podobnih dejavnosti javnega sektorja, dajanja izjav za javnost, razen izvajanja neposrednega trženja. Zbirke osebnih podatkov, ki nastanejo na tej podlagi, morajo biti ločene od drugih zbirk osebnih podatkov, ki nastanejo pri izvrševanju zakonitih pristojnosti, nalog ali obveznosti.

(2) Za namene iz prejšnjega odstavka lahko oseba javnega sektorja uporablja le naslednje osebne podatke: osebno ime, telefonsko številko, naslov elektronske pošte ali drugo komunikacijsko številko oziroma oznako, podatke o delodajalcu ali organizaciji ter podatke o področju dela, položaju, funkciji, članstvu v klubu ali hobiju posameznika, na katerega se nanašajo osebni podatki. Na podlagi privolitve posameznika lahko oseba javnega sektorja za iste namene obdeluje

tudi naslov stalnega ali začasnega prebivališča in druge osebne podatke, posebne vrste osebnih podatkov pa le izjemoma in če ima za to izrecno privolitev posameznika.

(3) Za namene obveščanja javnosti sme oseba javnega ali zasebnega sektorja obdelovati, vključno z objavo, osebna imena, nazive, fotografije in videoposnetke posameznikov, pridobljene na dogodkih, ki jih v okviru svojih nalog, pristojnosti ali dejavnosti organizira ta oseba, če posameznik te obdelave ni prepovedal.

Argumentacija k predlogu GZS:

Predlagatelj je v obrazložitvi zapisal, da se v 92 členu predloga ZVOP-2 *ureja posebna pravna podlaga* za obdelavo osebnih podatkov za izvajanje določenih dejavnosti javnega sektorja, zlasti za organiziranje določenih običajnih uradnih dogodkov. Konkretneje gre za ureditev vprašanja, kako pridobiti (in nadalje obdelovati) osebne podatke za udeležbo na državnih proslavah in drugih uradnih dogodkih (tudi medijske konference, izdaje raznih knjig, usposabljanja, izobraževanja ipd.). Obrazložitev odstopa od samega naslova člena kot tudi vsebine prvega odstavka, saj v obrazložitvi predlagatelj izpostavlja le *izvajanje določenih dejavnosti javnega sektorja.*

Sami imamo velike pomisleke glede dopustnosti *urejanja posebne pravne podlage* v nacionalnem predpisu, saj so pravne podlage za obdelavo osebnih podatkov določene v 6/I členu Splošne uredbe o varstvu podatkov in države vanje ne smejo posegati z določanjem *posebnih pravnih podlag.* Menimo še, da ni nobenih ovir, da tudi upravljavec iz javnega sektorja opre obdelavo osebnih podatkov, kot je opisana v prvem odstavku 92. člena predloga ZVOP-2, na pravni temelj zakonitega interesa (točka f 6/I člena Splošne uredbe o varstvu podatkov), saj omejitev iz zadnjega stavka 6/I člena Splošne uredbe o varstvu podatkov velja le za obdelave s strani javnih organov pri opravljanju njihovih (oblastnih) nalog[45]. V drugem odstavku obrazložitve k 92. členu predlagatelj tudi sam poudari, da v primeru obdelav iz tega člena ne gre za izvrševanje oblastnih nalog javnega sektorja. Torej ni nobenih ovir za naslonitev nameravane obdelave osebnih podatkov na pravni temelj zakonitega interesa.

Sklicevanje na zasebni sektor v naslovu in določbi prvega odstavka je lahko posledica parcialnih popravkov besedila predloga ZVOP-2, ki niti niso bili poočitani v obrazložitvi. Predlagatelj v obrazložitvi tudi izrecno zapiše: *Predlagana določba torej pomeni neposredno pravno podlago*

[45] Zadnji stavek 6/I člena Splošne uredbe o varstvu podatkov določa: Točka (f) prvega pododstavka se ne uporablja za obdelavo s strani javnih organov pri opravljanju njihovih nalog.

za obdelavo osebnih podatkov v javnem sektorju. Določba je ti. lex specialis v razmerju do ti. lex generalis predvsem v četrtem odstavku 6. člena ZVOP-2[46].

Ker je očitno razhajanje med vsebino določbe in obrazložitve, je s strani GZS predlagana sprememba prvega odstavka vsekakor smiselna. Sami predlagamo primarno amandma, po katerem bi se 92. člen v celoti izpustil, saj državam članicam ni dano pooblastilo da ustvarjajo nove *posebne pravne podlage* – kot je zapisano v obrazložitvi; *lex specialis pravne podlage*. Obdelavo, kot je opisana, je vsekakor mogoče nasloniti na eno od pravnih podlag iz 6/I člena Splošne uredbe o varstvu podatkov. Nenazadnje jo bodo na enega od pravnih temeljev iz 6/I člena Splošne uredbe o varstvu podatkov naslonili tudi upravljavci iz zasebnega sektorja.

93. člen (obdelava osebnih podatkov iz uradnega identifikacijskega dokumenta); 1. in 2. odstavek

Besedilo predloga ZVOP-2:

(1) Upravljavec, obdelovalec ali uporabnik, ki izvajata z zakonom predpisano nalogo, smeta za namen identifikacije posameznika vpogledati v njegove uradne identifikacijske dokumente. (2) Upravljavec, ki izvaja z zakonom predpisano nalogo, sme za namen identifikacije posameznika tudi prepisati, kopirati ali drugače obdelati podatke iz njegovih uradnih identifikacijskih dokumentov.

Argumentacija k predlogu GZS:

Načelo točnosti (točka d 5/I člena Splošne uredbe o varstvu podatkov) upravljavca zavezuje, da sprejme vse razumne ukrepe za zagotovitev, da se netočni osebni podatki brez odlašanja izbrišejo ali popravijo ter se ohranijo točni in, kadar je to potrebno, posodobljeni. ZVOP-1 je, na kar pravilno opozarja GZS, v določbi 18. člena, ki je urejala točnost podatkov, vseboval tudi možnost upravljavcev, da pred vnosom osebnih podatkov v zbirko preverijo njihovo točnost z vpogledom v osebni dokument ali drugo ustrezno javno listino posameznika, na katerega se nanašajo.

Iz obrazložitve k določbam 93. člena predloga ZVOP-2 ni razvidno, zakaj predlagatelj možnost zagotavljanja točnosti in posodobljenosti podatkov z vpogledom v osebni dokument veže le na primere, ko upravljavec izvaja z zakonom določeno nalogo. Načelo točnosti v enaki meri zavezuje vse upravljavce in ni mogoče ugotoviti, zakaj je dana prednost tistim, ki izvajajo z zakonom

[46] Glejte zadnja dva stavka v drugem odstavku obrazložitve k 92. členu preldoga ZVOP-2.

določene naloge. V obrazložitvi k 93. členu je skopo zapisano le: *V predlaganem 93. členu se določa seznam uradnih identifikacijskih dokumentov in njihova uporaba. Člen je podoben 60. členu ZVOPOKD, ki pa sicer velja le za obdelave po ZVOPOKD.* Tako ni najti argumentov za predlog, še posebej ne argumentov, ki bi narekovali podobno ureditev v ZVOP-2 kot v ZVOPOKD, saj slednji tipično ureja obdelavo osebnih podatkov za namene izvajanja zakonskih nalog – za državne organe, ZVOP-2 pa zadeva vse upravljavce, obdelovalce in uporabnike. Kot že večkrat v ZVOP-2 je tudi v tem primeru težko nizati predlagani rešitvi nasprotne argumente in razloge, saj niti ni mogoče ugotoviti, kateri argumenti in razlogi so sploh vodili predlagatelja.

Ob tem je treba upoštevati, da kopiranje in hrambo osebnih dokumentov urejajo tudi področni zakoni – ZOIzk[47], ZPLD[48], ZVoz-1[49], torej sprememba režima, če je potrebna, sodi v področni zakon in ne v ZVOP-2.
Glede na navedeno predlagamo amandma, ki bi ohranil vsebino iz 18/II člena ZVOP-1. To pa ustreza tudi predlogu GZS.

Dodajamo še, da je v javnosti včasih zaslediti nelogične in strokovno tudi povsem nepodprte navedbe o tem, da vpogled s strani upravljavca v osebni dokument ni dopusten. S takšnimi navedbami smo se v večji meri srečali v času epidemije, ko so bile določene storitve pogojene z izkazovanjem t.i. PCT pogoja s strani konkretnega posameznika. Informacijski pooblaščenec je takrat večkrat javno opozoril, da gre za povsem zmotno stališče in smejo upravljavci preveriti istovetnost, ko je to potrebno, tudi v vpogledom v osebni dokument – in ne samo v primerih, ko izvajajo z zakonom določeno nalogo[50]. Svoje stališče je opiral ravno na 18. člen ZVOP-1.

97. – 112. člen (kazenske določbe), splošna pripomba

Argumentacija k predlogu GZS:

V Uvodni določbi št. 148 Splošna uredba o varstvu podatkov določa, da je za okrepitev izvrševanja te uredbe poleg ustreznih ukrepov, ki jih lahko po tej uredbi naloži nadzorni organ, za vsako kršitev

---

[47] Zakon o osebni izkaznici (Uradni list RS, št. **35/11, 41/21** in **199/21**).
[48] Zakon o potnih listinah (Uradni list RS, št. **29/11** – uradno prečiščeno besedilo).
[49] Zakon o voznikih (Uradni list RS, št. **92/22** – uradno prečiščeno besedilo).
[50] Glejte na primer izjavo za javnost Informacijskega pooblaščenca z dne 1.8.2021 (dostopna na povezavi: **https://www.ip-rs.si/novice/informacijski-poobla%C5%A1%C4%8Denec-ip-z-nobeno-od-domnevno-dveh-verzij-aplikacije-nijz-za-preverjanje-izpolnjevanja-pogojev-pct-sploh-ni-seznanjen**), kot tudi obvestilo Informacijskega pooblaščenca za javnost z dne 8.11.2021 (dostopno je na povezavi: **https://www.ip-rs.si/novice/zakon-o-varstvu-osebnih-podatkov-dopu%C5%A1%C4%8Da-vpogled-v-osebni-dokument-za-namen-preverjanja-to%C4%8Dnosti-podatkov**) tudi mnenje Informacijskega pooblaščenca št. 07121-1/2021/2292 z dne 18.11.2021 (dostopno je na povezavi: https://www.ip-rs.si/mnenja-gdpr/vpogled-v-osebno-izkaznico-ob-preverjanju-pct-pogojev-1638779408).

uredbe uvesti kazni, vključno z upravnimi globami. Upravne globe so torej neizogibno glavna oblika denarnih kazni za kršitev Splošne uredbe o varstvu podatkov. Pri njihovem izreku je treba upoštevati naravo, težo in trajanje kršitve, namernost kršitve, sprejete ukrepe za ublažitev utrpljene škode, stopnjo odgovornosti ali morebitne pomembne predhodne kršitve, način, kako se je s kršitvijo seznanil nadzorni organ, skladnost z ukrepi, odrejenimi zoper upravljavca ali obdelovalca, zavezanost h kodeksu ravnanja in morebitne druge oteževalne ali olajševalne dejavnike. Menimo, da določitev prekrškovnih glob namesto upravnih in dodelitev njihove pristojnosti Informacijskemu pooblaščencu ni skladna s Splošno uredbo o varstvu podatkov[51]. Splošna uredba izrecno ureja primere držav članic Estonije in Danske, ki sta že v postopku njenega sprejemanja sporočila, da ne poznata sistema upravnih glob, za vse ostale primere pa v devetem odstavku 83. člena Splošna uredbe o varstvu podatkov določa, da se v primerih, kadar pravni sistem države članice ne določa upravnih glob, lahko 83. člen uporablja tako, da pristojni nadzorni organ sproži postopek za naložitev globe, pristojna nacionalna sodišča pa jo izrečejo. Pretvarjanje upravnih glob v prekrškovne in poverjanje njihovega izrekanja informacijskemu pooblaščencu po našem mnenju ni skladno s Splošno uredbo o varstvu podatkov.

Prav tako delimo mnenje GZS, da ni skladno s splošno uredbo o varstvu podatkov določanje spodnje meje – najnižje globe, ki se lahko izreče, saj takšna določitev glob onemogoča izvedbo obveznega navodila iz Splošne uredbe, da je treba vsako izrečeno globo prilagoditi okoliščinam konkretne kršitve. Določitev najnižje globe ne omogoča organu, da izrek globe prilagodi konkretnim okoliščinam kršitve, saj ne sme izreči globe, ki je nižja, četudi bi morda okoliščine kršitve kazale, da je potrebno izreči nižjo globo od najnižje predpisane in hkrati ne gre za okoliščine, v katerih bi bilo po ZP-1[52] dopustno izreči opomin namesto globe[53].

Menimo, da bi se morala v poglavju kazenskih določb spremeniti tako pristojnost za izrekanje glob kot tudi način njihovega določanja. V skladu s devetim odstavkom 83. člena Splošne uredbe o varstvu podatkov bi na predlog Informacijskega pooblaščenca globe izrekalo (najprimerneje) upravno sodišče. Sodbe, na katere se sklicuje predlagatelj, se niso nanašale na presojo pravilnosti uporabe določb Splošne uredbe o varstvu podatkov pri izreku glob, saj jih je informacijski pooblaščenec izrekal opirajoč se na ZVOP-1, pač pa na primere kršitev iz časa pred uveljavitvijo

[51] V uvodni določbi št. 115 Splošne uredbe o varstvu podatkov je zapisano, da pravna sistema na Danskem in v Estoniji ne dovoljujeta upravnih glob, kakor so določene v tej uredbi. Pravila o upravnih globah se lahko uporabljajo na tak način, da na Danskem globo naložijo pristojna nacionalna sodišča kot kazensko sankcijo, v Estoniji pa jo nadzorni organi naložijo v okviru prekrškovnega postopka, pod pogojem, da se s takšno uporabo pravil v teh državah članicah zagotovi enak učinek, kot ga imajo upravne globe, ki jih naložijo nadzorni organi. Pristojna nacionalna sodišča bi zato morala upoštevati priporočilo nadzornega organa, ki je sprožil postopek za naložitev globe. V vsakem primeru pa bi morale globe biti učinkovite, sorazmerne in odvračalne.

[52] Zakon o prekrških (Uradni list RS, št. 29/11 – uradno prečiščeno besedilo, 21/13, 111/13, 74/14 – odl. US, 92/14 – odl. US, 32/16, 15/17 – odl. US, 73/19 – odl. US, 175/20 – ZIUOPDVE in 5/21 – odl. US).

[53] Glejte 24. člen ZP-1.

Splošne uredbe. Primarno se je presoja osredotočala na vprašanje, ali Splošna uredba o varstvu podatkov v smislu določb slovenskega kaznovalnega prava predstavlja t.i. milejši predpis in Informacijski pooblaščenec tudi za kršitve, ki so bile zagrešene pred začetkom uporabe Splošne uredbe o varstvu podatkov ne sme uporabiti določb ZVOP-1.

Prav tako menimo, da določanje spodnje meje globe ni skladno z določbami Splošne uredbe o varstvu podatkov, ki jih država članica ne sme uporabiti drugače, kot so urejene v Splošni uredbi o varstvu podatkov, saj gre za vsebinska in ne postopkovna vprašanja.

Ne glede na navedeno bi bil tak poseg v predlog ZVOP-2 po vsebini konceptualen in po obsegu res zajeten. Šlo bi za prenovo celotnega poglavja, ki je vsekakor mogoča, terja pa velik poseg v predlog prepisa.

III Povzetek

Varstvo osebnih podatkov v Republiki Sloveniji je na visoki ravni. Razlog je v natančnih predpisih[54], močnih pristojnostih nadzornega organa in dejstvu, da jih je nadzorni organ dejansko ves čas tudi izvajal. Slovenski nadzorni organ, Informacijski pooblaščenec je v tej vlogi po ZVOP-1, prej je nadzor izvajalo Ministrstvo za pravosodje, že desetletja inšpekcijski organ in ima tudi pristojnost izrekanja sankcij za kršitve – kot prekrškovni organ. Tako velika oziroma močna pooblastila nadzornih organov na področju varstva osebnih podatkov so bila pred začetkom uporabe Splošne uredbe o varstvu podatkov v drugih državah članicah EU redkost. Zato je ena večjih prednosti Splošne uredbe o varstvu podatkov prav enotna določitev pristojnosti nadzornih organov za izrekanje sankcij – upravnih glob.

Moč nadzornega organa v Sloveniji je vsekakor pozitivno vplivala na prizadevanja upravljavcev osebnih podatkov v Republiki Sloveniji za skladnost s pravili. Upravljavci namreč, med njimi tudi operaterji telekomunikacij, ob sodelovanju s partnerji in povezanimi družbami v drugih državah članicah EU vedno znova opažajo, da sami razumejo in izvajajo določila Splošne uredbe o varstvu podatkov bolj zavzeto in dosledno, sledeč praksi, ki jo je s svojim delovanjem ustvaril Informacijski pooblaščenec, prej Ministrstvo za pravosodje. Pogosto prav iz tega razloga naletijo tudi na nerazumevanje na drugi strani, v smislu, da obveznosti iz Splošne uredbe o varstvu

[54] V Republiki Sloveniji je varstvo osebnih podatkov urejeno z zakonom že več kot 30 let. Prvi zakon je bil Zakon o varstvu osebnih podatkov, Uradni list RS, št. 8/90 in 19/91, nasledil ga je ZVOP – Zakon o varstvu podatkov (Uradni list RS, št. 59/99), še vedno veljavni ZVOP-1 pa je bil objavljen Uradnem listu RS št. 86/04.

podatkov razumejo širše in strožje, kot so zastavljene v Splošni uredbi o varstvu podatkov in širše ter strožje kot so jih sledeč svojemu razumevanju in zahtevam svojega nacionalnega nadzornega organa pripravljeni izvajati njihovi partnerji.

Dejstvo je, da se Splošna uredba o varstvu podatkov uporablja od 28.5.2018 naprej in Slovenija več kot štiri leta zamuja z izvedbo danih pooblastil v uredbi, ki bi jih smela oziroma morala realizirati v nacionalnem predpisu. To pomeni, da so upravljavci v Sloveniji svoje ravnanje že v celoti prilagodili določilom Splošne uredbe o varstvu podatkov, bistvena odstopanja, na nekatera opozarja tudi GZS v svojih pripombah, pa bodo ne le povzročila nove stroške prilagoditve, ki bi se jim lahko izognili, če bi bila država pravočasna v izvedbi danih pooblastil, pač pa bodo terjale tudi nove prilagoditve upravljavcev iz držav članic EU – pogodbenih partnerjev oziroma povezanih družb slovenskih upravljavcev osebnih podatkov, na način, ki jim je tuj in ga ne uredba ne njihov nacionalni organ ne zahtevata. Kot že poudarjeno v uvodu takšno ravnanje izničuje izhodiščna prizadevanja za harmonizacijo področja varstva osebnih podatkov znotraj EU.

ZVOP-2 tako po našem mnenju že konceptualno odstopa od Splošne uredbe o varstvu podatkov, ki z določitvijo načel in pravnih temeljev upravljavce sili v tehtanje tveganj za pravice in svoboščine posameznikov, za kar nosijo tudi odgovornost v eventualnem postopku pred nacionalnim organom. Z ZVOP-2 zakonodajalec v več primerih, kot mu je po uredbi dopuščeno, jemlje presojo tveganja v svoje roke, ne da bi lahko z zakonskimi določbami zajel vso pestrost različnih obdelav osebnih podatkov, iz katerih lahko vznika tveganje za pravice in svoboščine posameznikov. Presoja tveganj nikakor ni poenostavljeno vezana le na sektor (javni ali zasebni), ki mu upravljavec pripada, in število posameznikov, na katere se nanašajo osebni podatki v zbirki. Prav zaradi življenjske pestrosti situacij je uredba tehtanje tveganj in dokazovanje skladnosti z načeli obdelave osebnih podatkov prepustila upravljavcu. Državam članicam ni dano pooblastilo za poseganje v opisani osnovni koncept. Določbe o dnevnikih obdelav, t.i. posebnih obdelavah in podobno iz predloga ZVOP-2, nimajo prav nobene opore v Splošni uredbi o varstvu podatkov. Prav tako je video-nadzor le eden od načinov obdelave osebnih podatkov in državi članici ni dano pooblastilo, da oži pravne temelje iz Splošne uredbe o varstvu podatkov, ki bi jih sicer smeli uporabiti upravljavci, za njeno izvajanje.

Upravljavci, tudi operaterji telekomunikacij, ne bežijo pred svojimi obveznostmi po Splošni uredbi o varstvu podatkov. Nasprotno, jemljejo jih resno in jih več kot štiri leta tudi že izvajajo. Posebnih odstopanj oziroma kršitev Informacijski pooblaščenec po naših informacijah v tem obdobju ni ugotovil.

Sledenje predlogom GZS ne pomeni odstopanja od določil Splošne uredbe o varstvu podatkov in po našem prepričanju tudi ne znižanja nivoja varstva pravic posameznikov. Gre preprosto za

sledenje načelom iz 5. člena Splošne uredbe o varstvu podatkov, še posebej načelu iz drugega odstavka 5. člena. Po citirani določbi je upravljavec odgovoren za skladnost z načeli iz prvega odstavka 5. člena Splošne uredbe o varstvu podatkov in je to skladnost tudi zmožen dokazati.

Odvetniška družba Pirc Musar & Lemut Strle o.p., d.o.o.
Rosana Lemut Strle, odvetnica