

Ljubljana  
telefon 01 300 34 20  
faksimile 01 300 34 32  
e pošta info@odv-zb.si  
www.odv-zb.si

**REPUBLIKA SLOVENIJA**  
**MINISTRSTVO ZA PRAVOSODJE**  
**Direktorat za kaznovalno pravo in človekove pravice**  
**Župančičeva 3**  
**1000 Ljubljana**

Št. 533/2019  
Ljubljana, 25.3.2019

Vaša št.: IPP 007-87/2019

**ZADEVA: Predlog Zakona o varstvu osebnih podatkov (ZVOP-2)- strokovno usklajevanje (EVA 2018-2030-0045)**

Spoštovani,

skladno z vašim dopisom z dne 6.3.2019 vam v zvezi s predlogom ZVOP-2 pošljamo pripombe in predloge Komisije za varstvo osebnih podatkov pri Odvetniški zbornici Slovenije, s katerimi se Odvetniška zbornica Slovenije v celoti strinja.

Lepo pozdravljeni,

Predsednik zbornice  
mag. Roman Završek



Priloga:

- pripombe Komisije za varstvo osebnih podatkov pri OZS z dne 21.3.2019

## Komisija za varstvo osebnih podatkov

Ljubljana, 21.3.2019

Komisija za varstvo osebnih podatkov:

Dr. Nataša Pirc Musar, predsednica

Dr. Rok Čeferin, član

Luka Gaberščik, član

Zdenka Pavlovič, članica

**Zadeva: Pripombe na predlog ZVOP-2 z dne 6.3.2019, ki ga je Odvetniška zbornica Slovenije prejela v postopku javne obravnave v mnenje dne 7.3.2019**

### Splošne pripombe

Predlagamo, da se celotno besedilo predloga ZVOP-2, ki ureja isto materijo, kot GDPR, popolnoma izpusti iz predloga, saj besedilo pogosto napačno povzema določila GDPR in bo zakon, če bi obveljal v trenutni obliki, ustvaril pravno negotovost med upravljavci in obdelovalci, saj bosta dva splošna pravna akta isto vprašanje urejala na drugačen način, predvsem pa zaradi te redundance zakon postaja zelo nepregleden.

To bo za upravljavce pomenilo, da se bodo morali po tem, ko so se že prilagodili zahtevam GDPR, ponovno prilagajati drugačnim zahtevam ZVOP-2. Pristop »vse na enem mestu«, ki ga zasleduje Ministrstvo za pravosodje, lahko po naši oceni vzdrži samo, če so določila obeh aktov v celoti usklajena. Četudi želi zakonodajalec zasledovati to načelo (kar se nam, kot omenjeno, zdi nepotrebno), menimo, da naj bo v enem aktu potem navedeno vse skupaj, ne pa, da besedilo na veliko mestih nekonsistentno napotuje nazaj na določila GDPR.

Nadalje menimo, da implementacija t. i. policijske direktive<sup>1</sup> absolutno ne sodi v splošni zakon, ki ureja varstvo osebnih podatkov.

Ocenjujemo tudi, da je predlagatelj na nekaterih mestih spregledal pravilno definicijo nekaterih izrazov iz GDPR, kar ima za posledico zmanjšanje pravic posameznikov ali (po drugi strani)

---

<sup>1</sup> Direktiva (EU) 2016/680 Evropskega parlamenta in Sveta z dne 27. aprila 2016 o varstvu posameznikov pri obdelavi osebnih podatkov, ki jih pristojni organi obdelujejo za namene preprečevanja, preiskovanja, odkrivanja ali pregona kaznivih dejanj ali izvrševanja kazenskih sankcij, in o prostem pretoku takih podatkov ter o razveljavitvi Okvirnega sklepa Sveta 2008/977/PNZ, *OJ L 119, 4.5.2016, p. 89–131*.

nepotrebno omejevanje oziroma obremenjevanje upravljavcev, Vse to lahko na koncu pomeni tudi neenotno ureditev področja varstva osebnih podatkov znotraj EU (kar pa je bil sicer eden glavnih motivov za sprejem uredbe in ne več direktive). Kot primer naj navedemo besedi »varstvo« in »varnost«, ki sta v predlogu uporabljeni nekonsistentno, imata pa po GDPR povsem drugačen pomen: beseda *varstvo* osebnih podatkov se namreč nanaša na celotno področje, ki ga zakonodajalec želi urediti, medtem, ko GDPR v 32. členu termin *varnost* uporablja za varnost obdelave – angleško »*data security*« (po ZVOP-1, torej po starem, se to imenuje zavarovanje – glej 24. in 25. člen ZVOP-1). Ob tej priložnosti opozarjamo še na nekonsistentne popravke besedila samega GDPR (termin »varstvo« je bil s popravki spremenjen le v 33. členu, ne pa tudi v 34. členu in sami definiciji iz 12. točke člena 4 GDPR, pri čemer gre za enako vsebino (ang. »*personal data breach*«). Posledično so rešitve, predlagane v predlogu, v nasprotju z zahtevami GDPR.

Predlog zakona po naši oceni tudi napačno uporablja terminologijo iz drugih pravnih področij. Tako denimo besedo »tajno« uporablja v smislu zaupnosti osebnih podatkov, medtem, ko Zakon o tajnih podatkih za ta termin določa natančne pogoje rabe in uporabe. Na več mestih predlog uporablja namesto »podatki« termin »dokumenti«. Namesto nove terminologije 15. člena GDPR »pravica dostopa« uporablja še »staro« terminologijo ZVOP-1 »seznanitev z lastnimi osebnimi podatki«.

Poudarjamo, da se je z začetkom veljavnosti GDPR začela uporabljati tudi nekoliko drugačna logika varstva osebnih podatkov, ki v predlogu ZVOP-2 ni upoštevana. Po GDPR so tako pravne podlage za obdelavo osebnih podatkov enakovredne, osebna privolitve posameznika ne more biti omejena z zakonom, poudarek je na procesih obdelave in ne (več) na zbirkah. Po branju predloga pa ugotavljamo, da besedilo predloga še vedno temelji na logiki ZVOP-1, zlasti na hierarhičnosti pravnih podlag za obdelavo, ki je 6. člen GDPR ne pozna.

Ugotavljamo tudi, da je v besedilu ogromno slovničnih napak in sklicevanj na očitno napačne člene, zato predlagamo lekturo in vsebinsko uskladitev.

### **Konkretne pripombe**

Člen 3 (prepoved diskriminacije glede obdelave osebnih podatkov)

*Pri izvajanju obdelave osebnih podatkov je vsakemu posamezniku zagotovljeno, da se obdelave njegovih osebnih podatkov ali **osebnih podatkov posameznikov, katerih podatki so povezani z njegovimi osebnimi podatki**, izvajajo na nediskriminatoren način ne glede na narodnost, raso, barvo kože, veroizpoved, etnično pripadnost, spol, jezik, politično ali drugo prepričanje, spolno usmerjenost, spolno identiteto, premoženjsko stanje, kraj rojstva, izobrazbo, družbeni položaj, državljanstvo, kraj oziroma vrsto prebivališča, zdravstveno stanje, genske predispozicije ali katerokoli drugo osebno okoliščino teh posameznikov.*

Besedila tega dela člena 3 ne razumemo.

## Člen 6 (3)/1,4

(3) Naslednji izrazi, uporabljeni v tem zakonu, pomenijo:

*1. »javni sektor« pomeni javne organe, kar vključuje državne organe, organe samoupravnih lokalnih skupnosti, nosilce javnih pooblastil, javne agencije, javne sklade, javne zavode, univerze, samostojne visokošolske zavode in samoupravne narodne skupnosti;*

*4. »zasebni sektor« pomeni pravne in fizične osebe, ki opravljajo dejavnost v skladu z zakonom, ki ureja gospodarske družbe ali gospodarske javne službe ali obrt, in druge osebe zasebnega prava; zasebni sektor so tudi javni gospodarski zavodi, javna podjetja in gospodarske družbe in izvajalci gospodarskih javnih služb, ne glede na delež oziroma vpliv države ali dejstvo, da so **nosilci javnega pooblastila**, samoupravne lokalne skupnosti ali samoupravne narodne skupnosti;*

V točki 4 je definicija v delu, ki govori o nosilcih javnih pooblastil, spremenjena glede na definicijo iz še veljavnega ZVOP – 1, točka 23.

ZVOP – 1, člen 6, točka 23.

*Zasebni sektor – so pravne in fizične osebe, ki opravljajo dejavnost po zakonu, ki ureja gospodarske družbe ali gospodarske javne službe ali obrt, in osebe zasebnega prava; zasebni sektor so javni gospodarski zavodi, javna podjetja in gospodarske družbe, ne glede na delež oziroma vpliv države, samoupravne lokalne skupnosti ali samoupravne narodne skupnosti.*

Besedili obeh točk se izključujeta v delu nosilcev javnih pooblastil (ti so določeni kot »javni sektor« in kot »zasebni sektor«). Poleg tega je definicija upravljavca (člen 6/I(7) predloga) prepisana iz GDPR, v točkah 1 do vključno 4 člena 6/III pa so »subjekti«, ki so definirani kot upravljavec, definirani še nekoliko drugače in nekonsistentno.

Člen 7/(1)/a (temeljna načela varstva osebnih podatkov)

*(1) Osebni podatki:*

*a) se obdelujejo zakonito, tako da so v skladu z 8. ali 9. ali 12. ali 13. členom tega zakona določene pravne podlage za njihovo konkretno obdelavo, ter da se obdelujejo pošteno in na pregleden način za posameznika, tako da se ne obdelujejo za prikrite ali drugače nepošte nenamene, zato da se posamezniki lahko svobodno odločijo, ali bodo sodelovali pri obdelavi njihovih osebnih podatkov oziroma da lahko temu zakonito in učinkovito ugovarjajo (zakonitost, poštenost in preglednost)...*

Posamezniki se lahko svobodno odločajo samo v primeru, kadar je temelj za obdelavo podatkov njihova osebna privolitve (6/I(a) člen GDPR); ugovarjajo lahko samo, kadar je temelj za obdelavo osebnih podatkov zakonit interes (6/I(f) člen GDPR) oziroma je namen obdelave neposredno trženje. Če se obdelava osebnih podatkov izvaja na katerem od drugih

enakovrednih pravnih temeljev iz 6/I člena GDPR, potem svobodna odločitev posameznika oziroma njegov ugovor ne prideta v poštev (če obdelavo določa zakon, potem se posameznik ne more odločati o obdelavi svojih osebnih podatkov (npr. FURS obdeluje osebne podatke za namen davčnih postopkov; odločitev tudi ne bo svobodna ali ugovor možen, kadar je temelj za obdelavo pogodba iz 6/I(b) člena GDPR, ipd.).

#### Člen 7/(2)

*(2) Upravljavca in obdelovalec morata biti vedno zmožna dokazati skladnost svojih obdelav osebnih podatkov z določbami prejšnjega odstavka ter morata v skladu s tem voditi tudi predpisano dokumentacijo.*

*Upravljavca takšno določilo napotuje na prekomerno obdelavo osebnih podatkov, kar ni v skladu s členom 11 GDPR. Poleg tega gre za preveč splošno določbo, ker nikjer ni določene nobene »predpisane dokumentacije«.*

#### Člena 8 in 9

Predlog zakona v teh dveh členih predpostavlja, da je osebna privolitev primarna pravna podlaga, medtem, ko so ostale pravne podlage tej podrejene. Gre za kršitev 6. člena GDPR, kjer so vse pravne podlage med seboj enakovredne (ni pa seveda nujno, da je vedno mogoče uporabiti vsako izmed njih). Predlagamo, da se oba člena zelo natančno prilagodita definicijam iz člena 6 GDPR. Tudi zato, ker posledično niso uravnotežena in skladna druga razmerja oziroma obveznosti, ki jih določa GDPR – na primer, v javnem sektorju bo imel upravljavec težave pri izvajanju neposrednega trženja po 109. členu predloga, kar pa ni namen GDPR. Predvsem je problematična delitev na pravne temelje v javnem in zasebnem sektorju, česar GDPR ne dopušča na tak način. Za javni sektor prideta v poštev primarno točki c) in e) 6. člena GDPR in dodatno še 3. odstavek tega člena, ki natančno pojasni, da mora le obdelavo iz točke e) prvega odstavka določiti pravo Unije ali države članice.

#### Člen 8/(7)

*(7) Obdelava osebnih podatkov za drug namen kot za tistega, za katerega so bili zbrani, v javnem sektorju ni dopustna, razen če to določa ta zakon ali če to zaradi razlogov iz prvega odstavka 23. člena Splošne uredbe in pod pogoji iz prvega odstavka tega člena določa drug zakon.*

Glede na pravne podlage iz člena 6 GDPR je obdelava za drugačen namen dopustna, če upravljavec pridobi ustrezno pravno podlago (npr. osebno privolitev, ko govorimo o neoblastnem delovanju organa – *acta iure gestionis*).

#### Člen 9/(1)

*(1) Osební podatki v zasebnem sektorju se lahko obdelujejo, če obdelavo osebnih podatkov in osebne podatke, ki se obdelujejo, določa zakon ali če je za obdelavo določenih osebnih podatkov podana privolitev posameznika. Če obdelavo osebnih podatkov v zasebnem sektorju določa zakon, mora ta določati namen obdelave osebnih podatkov in vrste osebnih podatkov, ki se obdelujejo, kategorije posameznikov, na katere se nanašajo osebni podatki, če je mogoče tudi rok hrambe osebnih podatkov, uporabnike osebnih podatkov oziroma namene, za katere se jim lahko posreduje osebne podatke, posamezna dejanja obdelave in postopke obdelave ter druge ukrepe za zagotovitev zakonite, poštene in pregledne obdelave. **Z zakonom se lahko določi, da se določeni osebni podatki za enega ali več določenih namenov obdelujejo le na podlagi privolitve posameznika.***

Ta določba je v nasprotju z določilom točke (a) 1. odst. člen 6 GDPR. Zakon ne more določati, da je za določeno obdelavo zahtevana osebna privolitev in je takšno določilo pravzaprav v nasprotju s samim seboj. Toliko bolj, ker je navedeno besedilo zapisano v členu, ki obravnava pravne podlage v zasebnem sektorju. Ta del člena je prepisan iz ZVOP-1, ki pa novim standardom iz GDPR ne ustreza več.

Člen 9/(5)

*Ne glede na prvi odstavek tega člena se lahko v zasebnem sektorju obdelujejo osebni podatki, če je obdelava potrebna zaradi uresničevanja zakonitih interesov ter za katere si prizadeva upravljavec ali tretja oseba, razen kadar nad takimi interesi prevladajo interesi ali človekove pravice in temeljne svoboščine posameznika, na katerega se nanašajo osebni podatki, ki zahtevajo varstvo osebnih podatkov.*

Gre za nesmiseln stavek, ki ga ne razumemo.

Člen 14/(2)

*(2) Upravljavec posamezniku, na katerega se nanašajo osebni podatki, olajša pridobitev informacij oziroma sporočil iz prejšnjega odstavka. Če je mogoče, upravljavec na svoji spletni strani v ta namen objavi navodila ter obrazce za uveljavljanje posameznih pravic po tem zakonu ali Splošni uredbi.*

Menimo, da gre za pretirano obveznost za upravljavce, ki je GDPR ne predvideva ter podcenjevanje posameznikov. Člena 12 in 13 GDPR namreč že dovolj natančno določata, kakšne in katere informacije mora posameznik prejeti ter na kakšen način.

Nadalje navedba, da mora upravljavec navajati navodila in obrazce, ustvarja dodatno birokratsko breme na strani upravljavcev, ki je povsem nepotrebna. Večina večjih upravljavcev se sicer je odločila za izdelavo obrazcev, vendar pa to za manjše upravljavce in upravljavce, ki osebnih podatkov ne obdelujejo v velikem obsegu, predstavlja nepotrebno breme.

#### Člen 23/ (1,2,3 in 4)

*(1) V postopku iz prejšnjega člena ima pooblaščen uradna oseba Informacijskega pooblaščenca, ki mora izpolnjevati pogoje za nadzornika, poleg preiskovalnih pooblastil iz prvega odstavka 60. člena Splošne uredbe oziroma 71. člena tega zakona tudi pooblastila iz zakona, ki ureja inšpekcijski nadzor. Druga postopkovna dejanja v upravnem postopku, vključno z dejanji iz drugega in tretjega odstavka tega člena, lahko opravlja in **v njih dokončno odloči tudi pooblaščen uradna oseba, ki ne izpolnjuje pogojev za nadzornika.***

*(2) V postopkih iz prejšnjega člena lahko pooblaščen uradna oseba Informacijskega pooblaščenca opravlja ogled prostorov, osebnih podatkov in dokumentarnega gradiva ter zaslišuje osebe pri upravljavcu in priče brez prisotnosti pritožnika ter morebitnih stranskih udeležencev. Če zadostuje za odločitev o pritožbi posameznika, lahko pooblaščen uradna oseba Informacijskega pooblaščenca pridobi le pisne izjave o dejstvih ter pisna pojasnila od upravljavca, prič ter drugih oseb. **Pri dajanju pisnih ali ustnih izjav odgovornih oseb upravljavca ali pooblaščenih oseb morajo te osebe govoriti resnico in ne smejo ničesar zamolčati, njihove izjave pa se lahko štejejo kot izjave strank.** Določbe prejšnjega stavka ne vplivajo na odločanje v prekrškovnem postopku.*

Inšpekcijska pooblastila ima lahko samo državni nadzornik, ne pa osebe, ki ne izpolnjujejo pogojev za inšpektorja. Menimo, da gre za preobsežno (in nevarno) določilo zakona. Inšpektor ima namreč potrebna znanja, izkušnje in tudi opravljen inšpektorski izpit, medtem ko oseba, ki tega izpita nima, potencialno lahko upravljavcu povzroči nepopravljivo škodo. Tudi z vidika odgovornosti takšne osebe, gre za nevaren precedens.

Nadalje opozarjamo tudi na termin »pooblaščen uradna oseba«, ki se uporablja v prekrškovnem pravu in v upravnem postopku.

Besedilo pooblaščen oseb za varstvo podatkov postavlja v položaj stranke, kar je v izrecnem nasprotju s členom 38 GDPR, ki določa (povzeto), da mora biti pooblaščen oseba za varstvo podatkov neodvisna pri svojem delu (torej neodvisna tudi in zlasti od upravljavca). Pooblaščen oseba za varstvo podatkov po GDPR ni in ne more (ne sme) biti stranka v postopku, to je le upravljavec.

#### Člen 29/(3)

*V postopku z zahtevo in pritožbo po 41., 42. in 45. členu zakona, ki ureja pacientove pravice se smiselno uporabljajo določbe 15., 16., 17., 19., 20., 21., 22., 23., 24., 25. in 26. člena tega zakona.*

ZPacP ne more biti del urejanja po ZVOP-2, zato predlagamo črtanje (sklic na splošni zakon sodi v ZPacP).

## Člen 30/(2)

*(2) Upravljavec, ki izvaja obsežno obdelavo posebnih vrst osebnih podatkov ali osebnih podatkov v zvezi s kazenskimi obsodbami ali kaznovanji za prekrške, ali ki izvaja obdelave, pri katerih bi glede na naravo, obseg, okoliščine in namene obdelave lahko nastalo veliko tveganje za pravice in svoboščine posameznikov, poleg ukrepov izprejšnjega odstavka **vzpostavi in izvaja še splošno politiko varstva osebnih podatkov.***

Ta določba predstavlja dodatno, povsem nepotrebno, pa tudi vsebinsko nerazumljivo breme za upravljavce. Določila so o varnosti navedena že v GDPR, in na drugih mestih v ZVOP-2 in seveda v internih aktih o varnosti obdelave upravljavca in ne vidimo popolnoma nobene potrebe, da bi bilo treba poleg vseh z zakonom predpisanih internih aktov delati še enega. Gre za podvajanje zahtev.

## Člen 30/(3)

*(3) Upravljavec mora biti sposoben dokazati, da obdelava potekav skladu s Splošno uredbo, tem zakonom oziroma drugimi predpisi, ki urejajo varstvo osebnih podatkov. To dokazuje še zlasti z vodenjem ustrezne dokumentacije glede izvajanja obveznosti v skladu s tem poglavjem, s seznanitvijo zaposlenih s pravno ureditvijo varstva osebnih podatkov,  **vključno s podpisanimi izjavami zaposlenih glede seznanitve.***

Kaj pa, če posameznik izjave ne želi podpisati? Menimo, da mora biti dokazovanje skladnosti prepuščeno upravljavcu in ga je povsem nepotrebno z dodatno administracijo bremeniti še bolj. Naj spomnimo na 5. člen GDPR, ki določa le zmožnost dokazati skladnost, ne pa tudi oblike oziroma vrste dokaza:

*Upravljavec je odgovoren za skladnost z odstavkom 1 in je to skladnost tudi zmožen dokazati („odgovornost“).*

## Člen 31

*Upravljavec že tekom načrtovanja nove obdelave predvidi ustrezne tehnične in organizacijske ukrepe ter varovalke za zagotovitev, da bo obdelava potekala v skladu s temeljnimi načeli varstva osebnih podatkov iz 7. člena tega zakona, še zlasti pa z načelom sorazmernosti. Ukrepi morajo biti primerni glede na stanje najnovejšega tehnološkega razvoja na tem področju, naravo, obseg, okoliščine in namene obdelave ter tveganja za poseg v človekove pravice in temeljne svoboščine posameznikov, ki nastajajo pri obdelavi, lahko pa se upošteva tudi stroške njihovega izvajanja. Z izvajanjem teh ukrepov se pod pogoji iz prejšnjega člena nadaljuje tudi po začetku obdelave. **Pri izvajanju ukrepov se upošteva tudi tehnologijo, ki je dejansko na razpolago upravljavcu.** Upravljavec izvede ustrezne tehnične in organizacijske ukrepe, s katerimi zagotovi, da se privzeto obdelajo samo osebni podatki, ki so potrebni za vsak poseben namen obdelave. Ta obveznost velja za količino zbranih osebnih podatkov, obseg njihove*



*obdelave, obdobje njihove hrambe in njihovo dostopnost. S takšnimi ukrepi se zagotovi zlasti, da osebni podatki niso samodejno dostopni nedoločenemu številu posameznikov brez posredovanja zadevnega posameznika.*

Menimo, da mora upravljavec upoštevati razvoj tehnologije na splošno, ne le tehnologije, ki mu je v danem trenutku »na razpolago«. Če denimo upravljavec ne bo imel zadostnih finančnih sredstev, bo lahko trdil, da mu določena tehnologija ni na razpolago.

#### Člen 32/4(9)

*... Pogodba ali dogovor zlasti določa, da obdelovalec:*

*... vedno pravočasno obvesti upravljavca, če meni, da je določeno navodilo iz pogodbe ali dogovora ali na njuni podlagi v nasprotju z določbami tega zakona.*

Določba je napačno povzeta po drugem pododstavku 28/III člena GDPR, ki se nanaša zgolj na točko (h) prvega pododstavka 28/III člena GDPR:

*(h) da upravljavcu na voljo vse informacije, potrebne za dokazovanje izpolnjevanja obveznosti iz tega člena, ter upravljavcu ali drugemu revizorju, ki ga pooblasti upravljavec, omogoči izvajanje revizij, tudi pregledov, in pri njih sodeluje.*

*V zvezi s točko (h) prvega pododstavka obdelovalec nemudoma obvesti upravljavca, če po njegovem mnenju navodilo krši to uredbo ali druge določbe Unije ali predpisov držav članic o varstvu podatkov.*

#### Člen 33/(3)

*Obveznost iz prvega odstavka se ne uporablja za zasebni sektor glede osebnih podatkov o evidencah s področja dela, kot jih določajo zakoni, ki določajo evidence s področja dela.*

Ne vidimo razloga, zakaj se to določilo ne bi uporabljalo tudi v javnem sektorju. GDPR takšne izjeme ne dopušča.

#### Člen 33/(4)

*Izjeme iz drugega odstavka tega člena se ne uporablja za upravljavce in obdelovalce, ki so del javnega sektorja, notarje, odvetnike, detektive, izvršitelje, izvajalce zasebnega varovanja ter za izvajalce zdravstvene dejavnosti, vključno z zasebnimi zdravstvenimi delavci.*

Določba je več kot očitno prepisana iz ZVOP-1 in glede na 30. člen GDPR sploh ni smiselna.

#### Člen 34/(4)

*V dogovoru se določi tudi kontaktna točka ali kontaktne točke za posameznike, na katere se nanašajo osebni podatki.*

GDPR določa, da »se lahko določi«. Predlagamo uskladitev z GDPR.

Člen 41/(5 in 8)

*(5) Če je zahteva za posredovanje osebnih podatkov delno ali v celoti zavrnjena, lahko vlagatelj v primeru, ko se zahteva nanaša na posredovanje osebnih podatkov iz uradnih evidenc ali javnih knjig, zahteva, da o njegovi vlogi najprej odloči organ druge stopnje, če tega ni ali če tudi organ druge stopnje zavrne njegovo zahtevo, pa lahko zahteva sodno varstvo, o katerem odloča pristojno sodišče v skladu z zakonom, ki ureja upravni spor. V primeru zavrnitve zahteve za posredovanje osebnih podatkov iz zbirk, ki niso uradne evidence ali javne knjige, lahko vlagatelj zahteva sodno varstvo, o katerem odloča sodišče s splošno pristojnostjo v skladu z zakonom, ki ureja nepravdni postopek.*

*Revizijsko sled iz prejšnjega odstavka upravljavec hrani pet let, razen če drug zakon za posredovanje posameznih vrst podatkov ne določa drugačnega roka.*

Revizijska sled je termin, ki se uporablja v IT jeziku, je torej del tehnične terminologije. Če to predpostavko upoštevamo, potem osebnih podatkov ni mogoče poslati drugače, kot le v elektronski obliki – konkretno, če bo npr. FURS od upravljavca pisno zahteval, da mu sporoči osebne podatke nekega posameznika, upravljavec pisno ne bo smel odgovoriti, pač pa le v elektronski obliki, da bo lahko zagotovil ustrezno revizijsko sled?! Priporočamo odpravo oziroma ustrezno nadomestitev tega termina – na primer »dokazilo« iz prejšnjega odstavka.

Člen 44/(1, 3)

*(1) Odločitve upravljavcev, ki temeljijo izključno na avtomatizirani obdelavi osebnih podatkov, vključno z oblikovanjem profilov, ki lahko ima za posameznika, na katerega se nanašajo osebni podatki, pravne učinke ali nanj na podoben način znatno vplivajo, **so prepovedane, razen če to izrecno določa zakon**, ki določa tudi ustrezne ukrepe za varstvo človekovih pravic in temeljnih svoboščin ter upravičenih interesov posameznika, zlasti pravico do osebnega posredovanja upravljavca, do izražanja lastnega stališča in izpodbijanja odločitve.*

Besedilo sploh ne upošteva drugih pravnih temeljev po členu 6 in predvsem členu 22 GDPR, ki dopušča izrecno privolitev in je tako povsem v nasprotju z GDPR. Besedilo povsem blokira avtomatizirano odločanje v zasebnem sektorju. Predlagamo uskladitev z GDPR.

*Kadar se osebni podatki obdelujejo v znanstvene ali zgodovinsko-raziskovalne namene ali statistične namene, ima posameznik, na katerega se nanašajo osebni podatki, pravico, da iz razlogov, povezanih z njegovim posebnim položajem, ugovarja obdelavi osebnih podatkov v zvezi z njim, razen če je obdelava potrebna za opravljanje naloge, ki se izvaja zaradi razlogov javnega interesa. Posameznika, na katerega se nanašajo osebni podatki, se na možnost*

*uporabe pravice do ugovora izrecno opozori najpozneje ob prvem komuniciranju z njim in se mu to pravico predstavi jasno in ločeno od vseh drugih informacij.*

Besedilo nima nobene povezave z avtomatiziranim odločanjem in kaže na nerazločevanje med »avtomatizirano obdelavo« in »avtomatiziranim odločanjem«. Predlagamo črtanje odstavka.

Člen 47/(4)

*(4) Upravljavec ali obdelovalec v osmih dneh od določitve pooblaščenih oseb vpiše njene kontaktne podatke v skladu s 30. členom Splošne uredbe v svojo evidenco dejavnosti obdelav iz 33. člena tega zakona in njen **kontakt ter način možnega kontakta** javno objavi na primeren način, zlasti na spletni strani. V istem roku kontaktne podatke pooblaščenih oseb (osebno ime, naziv upravljavca ali obdelovalca, telefonska številka, lahko pa tudi naslov elektronske pošte ter morebitni strokovni ali znanstveni naslov) sporoči Informacijskemu pooblaščenju, ki jih vključi v seznam pooblaščenih oseb.*

Podčrtanega dela določbe ne razumemo.

Člen 48/(4)

*(4) Če je za pooblaščenega osebo upravljavca ali obdelovalca na področju vzgoje in izobraževanja določena oseba, ki izpolnjuje pogoje za strokovnega delavca na področju vzgoje in izobraževanja, se šteje, da izpolnjuje pogoj iz 4. točke prvega odstavka tega člena.*

Menimo, da gre za popolnoma nesmiselen odpustek na področju izkazovanja ustreznih izkušenj za zaposlene v vzgoji in izobraževanju. To določilo je v nasprotju z GDPR, predvsem pa je očitno diskriminatorno do vseh, ki na primer delajo v zdravstvu, socialni ipd. in se pri svojem delu v primerljivem obsegu srečujejo z osebnimi podatki.

Člen 49/(4)

*Kadar obveznost določitve pooblaščenih oseb veljajo tudi za odvetnike, lahko odvetniki samostojno določijo z dogovorom z Odvetniško zbornico Slovenije skupno pooblaščenega osebo, **ki je zaposlena na Odvetniški zbornici Slovenije.***

Ne vidimo potrebe, da se v tem zakonu za odvetnike določa obveznost zaposlitve pooblaščenih oseb za varstvo podatkov. Odvetniška zbornica je sicer nosilec javnega pooblastila za vodenje imenika odvetnikov in podeljevanja licenc, a za ta del svoje dejavnosti skladno z GDPR ne potrebuje pooblaščenih oseb. V delu, kjer jo morda nekateri odvetniki potrebujejo, v celoti sodi v zasebni sektor. Prav nobenega razloga ni, da strokovno usposobljene osebe OZS ne bi našla na trgu ali med odvetniki samimi, če bi se odločila, da ena pooblaščenih oseb za varstvo podatkov delo opravlja za vse odvetnike ali več njih. Odvetniška zbornica sodi med upravljavce

v zasebnem sektorju. Država nima nobene pristojnosti, da odreja organizacijo njenega dela z zapovedjo o zaposlovanju pooblaščenih oseb.

#### Člen 52 (Položaj pooblaščenih oseb)

Besedilo predloga v celoti izpušča glavni zahtevi GDPR glede položaja pooblaščenih oseb za varstvo podatkov, ki sta določeni v 2. odst. člena 38 GDPR: »Upravljavca in obdelovalca pooblaščenih oseb za varstvo podatkov pomagata pri opravljanju nalog iz člena 39, tako da **zagotovita sredstva**, potrebna za opravljanje teh nalog, in dostop do osebnih podatkov in dejanj obdelave, **ter ohranjanje njenega strokovnega znanja**.«

#### Člen 61/(1)

*Upravljavca ali obdelovalca, ki namerava prenesti osebne podatke v tretjo državo ali mednarodno organizacijo na podlagi zavezujočih poslovnih pravil ali pogodbenih določil, mora za izvedbo prenosa pridobiti dovoljenje Informacijskega pooblaščenca ali drugega pristojnega nadzornega organa države članice Evropske unije, v skladu s pogoji iz 46. in 47. člena Splošne uredbe.*

3. odstavek člena 47 GDPR se po naši oceni nanaša na dovoljenje nadzornega organa za uporabo pogodbenih določil, ne pa na vsak prenos posebej. Če bo razlaga, da morajo upravljalci za vsak prenos posebej pridobiti dovoljenje Informacijskega pooblaščenca, bo to lahko pomenilo ogromen pripad zadev, po drugi strani pa onemogočanje prenosov na strani upravljalcev, kar lahko povzroči tudi veliko gospodarsko škodo in neenako ureditev področja znotraj EU. Ne razumemo tudi, ali se to nanaša tudi na uporabo standardnih pogodbenih klavzul – tu je namreč izjema že v GDPR; 46/IV člen.

#### Člen 71/(1)/2

*... pregleduje poslovne knjige, pogodbe, listine, **poslovno korespondenco**, poslovne evidence in druge podatke, ki se nanašajo na obdelavo osebnih podatkov strani upravljalca ali obdelovalca samega ali druge pravne ali fizične osebe po njunem pooblastilu, oziroma na prenos osebnih podatkov v tretjo državo ali posredovanje uporabnikom osebnih podatkov iz tretjih držav s strani upravljalca ali obdelovalca oziroma druge pravne ali fizične osebe po njunem pooblastilu (v nadaljnjem besedilu: poslovne knjige in druga dokumentacija), ne glede na njihovo tajnost ali drugo vrsto zaupnosti ter ne glede na nosilec, na katerem so zapisani ali shranjeni; ...*

Menimo, da gre za kršitev 2. odst. 37. člena Ustave RS, ki poseg v korespondenco omogoča zgolj na podlagi odločbe sodišča ter če je to nujno za uvedbo ali potek kazenskega postopka ali za varnost države. Za pregled skritih prostorov člen 71/(2) določa predhodno pridobitev

odredbe preiskovalnega sodnika, za poseg v poslovno korespondenco pa ne? Poudarjamo, da se pristojnosti IP še vedno raztezajo tudi na področje kaznovalnega prava, pri čemer v prekrškovnih postopkih uporabi identično dokumentacijo kot v inšpekcijskih. Korespondenca mora tako ostati varovana in morebiten poseg vanjo pridržan le sodiščem.

Člen 71/(2)

*2) Izvedba ukrepov **pregleda skritih predelov prostorov** oziroma opreme iz 3. točke prejšnjega odstavka oziroma zavarovanje in pregled elektronskih naprav in nosilcev iz 4. točke prejšnjega odstavka je dopustna le na podlagi soglasja upravljavca ali obdelovalca oziroma obrazložene pisne odredbe sodišča. Odredbo iz prejšnjega stavka izda preiskovalni sodnik pri Okrožnem sodišču v Ljubljani najpozneje v 48 urah od prejema predloga uradne osebe iz prvega odstavka tega člena.*

Besedilo ne pojasni pojma »skriti predel prostorov«, kar lahko vodi v arbitrarnost.

Člena 82 in 83

Menimo, da gre za pretirano zaostrovanje pogojev in s tem za onemogočanje uporabe podatkov za znanstveno- in zgodovinsko raziskovalni ter statistični namen, v nasprotju z načeli GDPR, ki obdelavo osebnih podatkov za te namene priznava kot v pomembnem javnem interesu.

Člen 109/(2, 3, 4, 5,7) – Neposredno trženje

*(2) Za namene izvajanja neposrednega trženja lahko upravljavec obdeluje le naslednje osebne podatke, ki jih je zbral v skladu s prejšnjim odstavkom: osebno ime, naslov stalnega ali začasnega prebivališča, telefonsko številko, naslov elektronske pošte, številko telefaksa ter podatke, ki jih je posameznik, na katerega se osebni podatki nanašajo, sam objavil brez očitnega namena, da bi omejil njihovo nadaljnjo obdelavo. Na podlagi privolitve posameznika ali druge **zakonske podlage** lahko upravljavec obdeluje tudi druge osebne podatke, posebne vrste osebnih podatkov pa le, če ima za to izrecno privolitev posameznika.*

*(3) Ne glede na določbe prvega in drugega odstavka tega člena, lahko upravljavec obdeluje osebne podatke iz drugega odstavka tega člena za namene izvajanja neposrednega trženja tudi v skladu z drugimi pravnimi podlagami iz Splošne uredbe in zakona.*

»Zakonske« ni enako, kot je uredba EU, zato predlagamo zamenjavo besede zakonske v *ustrezne*. Prav tako se 2. odstavek delno izključuje s 3. odstavkom tega člena, zato priporočamo, da se oba odstavka smiselno združita in pri tem upoštevata, da je po GDPR 6 enakovrednih pravnih podlag.

*(4) Upravljavec neposredno trženje izprvega in drugega odstavka tega člena izvaja tako, da posameznika ob izvajanju neposrednega trženja jasno in ločeno od katerihkoli drugih informacij obvesti z naslednjimi informacijami, ki vsebujejo:*

*–identiteto in kontaktne podatke upravljavca;*

*–ali je upravljavec podatke zbral iz javno dostopnih virov ali v okviru zakonitega opravljanja dejavnosti in–na kakšen način lahko posameznik uveljavlja pravico iz 16. člena in drugega odstavka 21. člena Splošne uredbe ter iz 110. člena tega zakona.*

Menimo, da gre za nepotrebno birokratsko zahtevo, saj je posameznik o tem seznanjen že ob sami podaji privolitve oz. ob posredovanju osebnih podatkov, kadar gre za druge ustrezne pravne podlage. Gre tudi za dodatno »smetenje« z obvestili neposrednega trženja, saj bo posameznik prejemal še večje količine informacij.

*(5) Če namerava upravljavec posredovati osebne podatke iz drugega odstavka tega člena drugim **uporabnikom** za namene neposrednega trženja, o tem obvesti posameznika in pred posredovanjem osebnih podatkov zagotovi drugo pravno podlago za posredovanje podatkov ali pa pridobi njegovo izrecno privolitev. Obvestilo posamezniku o nameravanem posredovanju osebnih podatkov vsebuje informacijo, katere podatke namerava posredovati, komu, kdaj in za kakšen namen. Stroške obvestila krije upravljavec.*

Glede na to, da so po definiciji GDPR uporabniki tudi obdelovalci, bo moral upravljavec od posameznika pridobiti dodatno dovoljenje (npr. upravljavec bo, preden bo osebne podatke posreboval agenciji, ki bo v njegovem imenu izvajala neposredno trženje kot obdelovalec, za to pridobiti soglasja vseh posameznikov), kar ocenjujemo kot popoln nesmisel in omejevanje načel GDPR.

*(7) Glede uporabe osebnih podatkov s področja elektronskih komunikacijskih sredstev za izvajanje neposrednega trženja se uporabljajo tudi določbe zakona, ki ureja elektronske komunikacije.*

Napotitev na drug zakon je zapisna že v prvem odstavku tega člena.

Ker gre pri tem členu za vsebino, ki je GDPR ne ureja podrobno, predlagamo bolj jasno dikcijo tega člena.

*(1) Upravljavec lahko uporablja osebne podatke posameznikov, na katere se nanašajo osebni podatki, ki jih je zbral iz javno dostopnih virov ali v okviru zakonitega opravljanja dejavnosti, tudi za namene ponujanja blaga, storitev, zaposlitev ali začasnega opravljanja del z uporabo poštnih storitev, telefonskih klicev, elektronske pošte ali drugih elektronskih komunikacijskih sredstev (v nadaljnjem besedilu: neposredno trženje) v skladu z določbami tega poglavja, če drug zakon ne določa drugače.*

(2) Za namene izvajanja neposrednega trženja v skladu s prejšnjim odstavkom lahko upravljavec obdeluje le naslednje osebne podatke, : osebno ime, naslov stalnega ali začasnega prebivališča, telefonsko številko, naslov elektronske pošte, ter številko telefaksa ter podatke, ki jih je posameznik, na katerega se osebni podatki nanašajo, sam objavil brez očitnega namena, da bi omejil njihovo uporabo.

(3) Ne glede na določbe prejšnjih dveh odstavkov, lahko upravljavec obdeluje osebne podatke za namene izvajanja neposrednega trženja tudi na drugih pravnih temeljih v skladu s Splošno uredbo in zakonom.

(4) Upravljavec neposredno trženje po prvem odstavku tega člena izvaja tako, da posamezniku ob izvajanju neposrednega trženja posreduje naslednje informacije:

- identiteto in kontaktne podatke upravljavca;
- ali je upravljavec podatke zbral iz javno dostopnih virov, ali v okviru zakonitega opravljanja dejavnosti;
- na kakšen način lahko posameznik uveljavlja pravico iz 16. člena in drugega odstavka 21. člena Splošne uredbe.

(5) Če namerava upravljavec posredovati osebne podatke iz drugega odstavka tega člena tretjim osebam za namene neposrednega trženja, o tem obvesti posameznika in pred posredovanjem osebnih podatkov zagotovi pravno podlago za posredovanje podatkov. Obvestilo posamezniku o nameravanem posredovanju osebnih podatkov vsebuje informacijo, katere podatke namerava posredovati, komu in za kakšen namen. Stroške obvestila krije upravljavec.

Člen 111/(9, 10)

(9) Upravljavec videonadzora za vsak vpogled ali uporabo posnetkov zagotovi možnost naknadnega ugotavljanja, v katere posnetke je bilo vpogledano, kdaj in kako so bili uporabljeni ali posredovani, kdo je izvedel ta dejanja obdelave, kdaj in s kakšnim namenom ali na kateri pravni podlagi ter **takšno revizijsko sled hrani pet let**, razen če drug zakon določa drugače.

Če predpostavimo, da je revizijska sled pojem iz IT področja, to pomeni, da bodo morali po uveljavitvi ZVOP-2 vsi upravljavci, katerih video-nadzorni sistem ne omogoča revizijske sledi, kupiti nove video-nadzorne sisteme, kar ocenjujemo kot pretiran poseg v poslovanje pravnih oseb v javnem in zasebnem sektorju in nepotrebno višanje stroškov. Predlagamo zamenjavo termina z besedilom »ter takšen podatek«.

(10) Če z zakonom ni drugače določeno, se to poglavje uporablja za vse vrste videonadzora ter tudi v primerih, ko se z videonadzorom zgolj spremlja neposredno dogajanje pred kamerami.

Predlog izenačuje neposredno spremljanje dogajanja z video-nadzorom, pri čemer pa se ne ozira na druge zahteve, ki jih besedilo določa glede video-nadzora, sprašujemo se na primer,

kako bo upravljavec zagotavljal podatek oziroma "revizijsko sled" o tem, da je določena oseba gledala živo sliko – to lahko pomeni, da bo denimo moral receptor, ki spremlja dogajanje pred vhodom v poslopje, vsakokrat, ko bo pogledal na ekran, zabeležiti, kdaj je vpogledal na ekran in kaj natančno je gledal. Predlagamo razmislek o ustrežnejši ureditvi, saj je predlagana določba očitno neizvedljiva v praksi.

#### Člen 117/(9)

*(9) Oseba zasebnega sektorja pred začetkom uporabe biometričnih ukrepov posamezniku, nad katerim se bodo izvajali ti ukrepi, predloži obvestilo o zakonski ureditvi izvajanja biometričnih ukrepov, ki ga izdelava in na svoji spletni strani objavi Informacijski pooblaščenec.*

Ne vidimo razloga, zakaj je potrebno podvajati zakon še v dodatnem obvestilu. Kopiranje in dodatna seznanitev posameznika z zakonom je popolnoma nesmiselna. Pri tem gre besedilo tako daleč, da zakon Informacijski pooblaščenec najprej kopira na svojo spletno stran, upravljavec pa mora nato kopirati besedilo s spletne strani Pooblaščenca in besedilo posredovati posamezniku.

#### Člen 128/(1)

*Informacijski pooblaščenec odloča o predpisanih kršitvah in upravnih globah iz 83. člena Splošne uredbe kot o prekrških v okviru pristojnosti prekrškovnega organa po določbah zakona, ki ureja prekrške, ne glede na določbe o določanju razponov glob iz 17. člena zakona, ki ureja prekrške.*

Glede na to, da v pravnem redu Republike Slovenije ne poznamo upravnih glob, menimo, da je določilo v neposrednem nasprotju z 9. odstavkom člena 83 GDPR in bo takšno določilo onemogočilo izrekanje upravnih glob Informacijskemu pooblaščenču, saj je pri tem treba upoštevati načelo *nullum crimen nulla poena sine lege praevia*. Predlagamo striktno upoštevanje 9. odstavka člena 83 GDPR. Menimo namreč, da v skladu z navedenim določilom GDPR upravne globe v Republiki Sloveniji lahko izreka samo sodišče. GDPR po našem prepričanju ne dopušča odstopanja od določbe 83/IX člena. V slovenski pravni red pa upravne globe z ZVOP-2 niso bile uvedene. Iz citiranih določil GDPR je jasno razvidno, da zgolj »prevod« upravnih glob v prekrškovne ne zadošča. Da bi Informacijski pooblaščenec še naprej lahko izrekal globe, bi te moral biti upravne in ne prekrškovne. Najbrž je odveč poudarjati, kako bistvena je razloga v naravi upravnih in prekrškovnih glob. Slednje so del kaznovalnega prava in za kršitve GDPR niso dopustne.

#### Člen 150/(3)

*Ne glede na pogoja izobrazbe iz 3. točke in vsebine in trajanja delovnih izkušenj iz 4. točke prvega odstavka 48. člena tega zakona se do 25. maja 2021 za pooblaščenca lahko določi osebo, ki ima najmanj eno leto delovnih izkušenj s primerljivih področij informacijske varnosti,*



*varstva poslovne skrivnosti po zakonu, ki ureja gospodarske družbe, ali varstva zaupnih podatkov po zakonu, ki ureja bančništvo.*

Menimo, da je določilo v nasprotju z GDPR, ki imenovanje pooblaščenih oseb za varstvo podatkov zahteva že od 25. 5. 2018. Prav tako je nekoliko nenavadno, da zakon (tudi za druga določila v tem poglavju) uvaja prehodno obdobje, ko pa je GDPR že skoraj leto dni v veljavi in je Informacijski pooblaščenec že celo izvajal inšpekcijske nadzore po GDPR.

Člen 153

*Slovenska akreditacija začne izvajati postopke akreditacije 1. januarja 2022.*

Menimo, da je prehodno obdobje skoraj treh let nesprejemljivo za upravljavce, ki že na ZVOP-2 čakajo skoraj leto dni. Ni videti razloga, zakaj bi se moralo z akreditacijami čakati tako dolgo. S tem Slovenija izgublja, saj se bodo upravljavci, ki to želijo, šli certificirati produkte v države EU, kjer ti postopki že tečejo. Nenazadnje je EDPB že izdal tudi smernice o kriterijih za certificiranje.<sup>2</sup>

---

<sup>2</sup> [https://edpb.europa.eu/our-work-tools/public-consultations/2019/guidelines-12018-certification-and-identifying\\_en](https://edpb.europa.eu/our-work-tools/public-consultations/2019/guidelines-12018-certification-and-identifying_en)