Ljubljana, 25. 3. 2019

**PREDLOGI K OSNUTKU ZAKONA O VARSTVU OSEBNIH PODATKOV (EVA: 2018-2030-0045)**

K 12. členu:

V točki č) drugega odstavka se za besedo »ustanove« doda vejica in beseda »zavodi«.

Obrazložitev:

Drugi odstavek 12. člena določa pravne podlage za obdelavo t.i. posebnih vrst osebnih podatkov, kot jih predvideva tudi 9. člen Splošne uredbe o varstvu osebnih podatkov (GDPR). Ker omenjena uredba med drugim dovoljuje obdelavo takšnih osebnih podatkov tudi »neprofitnim telesom«, pozdravljamo namero ministrstva, da takšna »telesa« glede na slovenski pravni red v zakonu konkretneje opredeli. Ker pa **osnutek zakona pri tem zajame pravzaprav vse oblike nepridobitnih pravnih oseb** (društva, ustanove, sindikate, verske skupnosti…) **razen zavodov** po Zakonu o zavodih, predlagamo, da se doda tudi slednje. Med zavodi in npr. društvi ali ustanovami, ki jih osnutek že zajema, ni nobenih bistvenih bistveni razlik - oboji že na podlagi zakona ne morejo biti ustanovljeni za namene opravljanja pridobitne dejavnosti in morebitnega presežka tudi ne delijo, zato ne vidimo utemeljenega razloga, da se jih ne bi vključilo v to rešitev.

Tudi praktično gledano (zasebni) zavodi kot npr. *Zavod Emma-Center za pomoč žrtvam nasilja*, *Pravno-informacijski center nevladnih organizacij-PIC*, *Mirovni inštitut* ali *Zavod Pelikan-Karitas* izvajajo povsem enake dejavnosti ali socialnovarstvene programe kot njim sorodna društva, ustanove ali verske organizacije in pri svojem delu na enak način tudi obdelujejo posebne osebne podatke svojih uporabnikov.

K 12. členu:

V prvem stavku tretjega odstavka se črta beseda »pisno«.

Obrazložitev:

Z namenom **zmanjšanja administrativnih obveznosti** za upravljalce osebnih podatkov predlagamo črtanje obveznosti, da morajo ti svoje ukrepe za zaščito posebnih osebnih podatkov tudi pisno opredeliti. Ključno namreč je, da se ustrezni ukrepi za zaščito izvajajo in ne da so nujno tudi pisno opredeljeni. Obvezne pisne opredelitev ukrepov v praksi zelo pogosto pomenijo, da upravljalci uporabljajo vzorčne ali generične akte in pisne opredelitve, ki v resnici bistveno ne prispevajo bistveno k povečanju varnosti osebnih podatkov, temveč hitro postanejo sami sebi namen. Tudi sicer zakon v tem primeru nalaga obveznost, ki je GDPR ne zahteva in tudi zato ne vidimo potrebe, da se slovenskim upravljalcem osebnih podatkov nalaga še dodatne obveznosti.

K 14. členu:

V drugem odstavku se črta drugi stavek.

Obrazložitev:

Člen določa, da vsak upravljalec na svoji spletni strani objavi navodila in obrazce za potrebe uveljavljana pravic posameznikov glede njihovih osebnih podatkov, če »je to mogoče«. Glede na stanje razvoja spleta in obstoja različnih brezplačnih orodij za izdelavo spletni strani, je praktično nemogoče zavzeti stališče, da kaj takšnega ni mogoče, kar pravzaprav pomeni, da določba, čeprav to morda ne izgleda na prvi pogled, **prinaša vsem upravljalcem dodatne obveznosti, ki jih GDRP od njih ne zahteva**. Menimo namreč, da ni nikakršne potrebe, da bi vsako društvo, samostojni podjetnik ali podjetje, ki ima svojo spletno stran, moralo zavoljo tega zakona to stran dopolnjevati z obrazci in informacijami. Od tega ukrepa tudi ni pričakovati kakšnega bistvenega premika na področju varstva osebnih podatkov, saj lahko upravičeno pričakujemo, da bodo upravljalci na svoje spletne strani dodajali generična oziroma vzorčna pojasnila.

K 16. členu:

V drugem odstavku se besedna zveza »petih delovnih« zamenja z besedo »petnajstih«.

Obrazložitev:

Predlagamo podaljšanje roka v katerem mora upravljalec osebnih podatkov zahtevati dopolnitev nepopolne ali nerazumljive zahteve posameznika glede njegovih osebnih podatkov. Osnutek zakona namreč po vzoru, ki velja za upravni postopek in torej za državni aparat v širšem smislu, postavlja zelo kratek, **pet dnevni rok, ki pa za zasebne ali manjše upravljalce ni življenjski in je prestrog**. V npr. manjšem lokalnem društvu upokojencev je lahko povsem običajno, da so »uradne ure« zgolj enkrat ali dvakrat na mesec in da tudi tajnik ali predsednik društva zgolj takrat urejata društvene zadeve, kot je pregled prejete navadne ali elektronske pošte. Povsem običajno tudi je, da je nek amaterski športni klub aktiven zgolj v določenem letnem času in se izven tega na dnevni ravni nihče sploh ne ukvarja z društvenimi zadevami. V takšnih primerih lahko zelo hitro pride do situacije, da posameznik nekemu društvu po pošti pošlje nepopolno vlogo, za katero v petih delovnih dneh sploh nihče ne bo izvedel, kaj šele ugotovil, da gre za nepopolno vlogo, kjer je potrebno napisati nazaj poziv k dopolnitvi. Zakonski rok bo vmes že potekel. Zakon naj se zato prilagodi tudi takšnim manjšim upravljalcem, ki predlaganega roka tudi po najboljših možnih močeh ne bodo zmogli spoštovati in je tako že vnaprej znano, da bi zakon kršili.

Predviden kratek rok je morda smiseln zgolj za »državne« upravljalce, ki razpolagano s strokovnimi službami in ki imajo načeloma javno zagotovljena sredstva za delovanje ter lahko zato takšne obveznosti tudi izpolnjujejo.

K 30. členu:

Drugi odstavek se črta. Dosedanji tretji in četrti odstavek postaneta drugi in tretji odstavek.

Obrazložitev:

Z namenom **zmanjšanja administrativnih obveznosti** za upravljalce osebnih podatkov predlagamo črtanje obveznosti, da morajo upravljalci, ki izvajajo obsežne obdelave osebnih podatkov izvajati še »splošno politiko varstva osebnih podatkov«. Iz določbe sicer težko razberemo, kaj točno se od upravljalcev sploh pričakuje, da bo njihovo izvajanje ukrepov za varovanje osebnih podatkov že postala »politika«. Tudi sicer gre za obveznost, ki je GDPR ne zahteva in ne vidimo potrebe, da se slovenskim upravljalcem osebnih podatkov nalaga še dodatne obveznosti.

K 35. členu (opisna pripomba k drugemu odstavku):

Člen upoštevajoč 24. člen GDPR določa ukrepe za zagotavljanje varstva osebnih podatkov, pri čemer pozdravljamo namero ministrstva, da se te ukrepe tudi konkretizira. Trenutna dikcija zakona, da upravljalci izvajajo »zlasti« z zakonom predpisane ukrepe (psevdonimizacija, vodenje notranjih evidenc obdelave, redno testiranje, itd.) nakazuje na to, da gre torej obvezne ukrepe, ki jih morajo izvajati vsi upravljalci ne glede na velikost in tveganja in da kakšni drugi ukrepi (npr. manj zahtevni ukrepi za manj zahtevna tveganja) pridejo v pošte zgolj izjemoma in poleg zakonsko določenih ukrepov. Zato predlagamo preoblikovanje dikcije tako, da **naj zakon ne nalaga obveznega izvajanja vseh teh ukrepov vsem upravljalcem osebnih podatkov**, temveč naj si ti ukrepe izberejo povsem svobodno, kar pa bo še vedno lahko predmet kasnejšega nadzora.

Prav tako menimo, da ni ustrezno (vsem) upravljalcem nalagati izvajanja ukrepov, ki še za pet let nazaj omogočajo evidenco, kdaj je kakšna oseba obdelovala osebne podatke v zbirki. Takšna **zahteva ni sorazmerna in pomeni preveliko breme za manjše upravljalce**. Ukrepa, kot je predviden sedaj, večina društev ne bo mogla izvajati (npr. vzpostaviti sistema, kdaj je kdo vpisal telefonsko število člana društva v članski imeni ali kdaj je kateri prostovoljec naložil slike na spletno stran društva). Tudi sicer **gre za obveznost, ki je GDPR ne zahteva** in ne vidimo potrebe, da se slovenskim upravljalcem osebnih podatkov nalaga še dodatne obveznosti. Tudi **za petletni rok ne vidimo utemeljenega razloga**, saj prekrški s področja varstva osebnih podatkov zastarajo po Zakonu o prekrških v dveh letih od storitve. Zato morebitno ugotavljanje v teh postopkih, kdaj je nekdo obdeloval osebne podatke v določeni zbirki za toliko več časa nazaj, niti ne bo prišlo v poštev.

K 35. členu (opisna pripomba k četrtemu odstavku):

Osnutek predvideva novo obveznost vsakega upravljalca osebnih podatkov, da sprejme pravilnik (ali drug podoben akt) s katerimi uredi svoje ukrepe za varstvo osebnih podatkov. Takšna **obveznost ni sorazmerna in pomeni prekomerno administrativno breme**, saj nalaga sprejem pravilnika čisto vsaki organizacija, ki ima npr. opravka še s tako majhnim obsegom osebnih podatkov ali pri kateri so možnosti kršitev praktično minimalne (npr. velja tudi za vsako manjše lokalno prostovoljsko kulturno društvo, ki ima javne zbore članov in tako vsi vaščani točno vedo, kdo so njegovi člani, to pa je hkrati tudi edina zbirka podatkov, ki jo društvo ima).

Pri tem ne gre spregledati, da je podobno zahtevo, da imajo vsi upravljalci sprejet poseben pravilnik o varstvu osebnih podatkov, vseboval že Zakon o varstvu osebnih podatkov (ZVOP-1) iz leta 2004, a **je vlada sama že po dveh letih njegovega izvajanja ugotovila, da gre za preveliko administrativno obremenitev**, da črtanje takšne obveznosti za manjše organizacije ne povzroča povečanja nevarnosti zlorabe osebnih podatkov, kot tudi, da takšna (administrativna) obveznost ne pripomore k povečanju varstva osebnih podatkov (tako v predlogu novele ZVOP-1A, Poročevalec DZ RS št. 41/2007). Tudi sami kot krovna mreža nevladnih organizacij lahko iz lastne prakse svetovanj potrdimo, da takšna obveznost pogosto povzroči zgolj to, da se pravilniki sprejemajo povsem nekritično in zgolj zato, ker se pač morajo, bistvenega prispevka k varstvu osebnih podatkov pa tudi po naših izkušnjah ne dosežejo.

Četudi upravljalec pravilnika nima, je tako ali tako dolžan in odgovoren za ustrezno varstva osebnih podatkov, zato je primerneje, da naj pravilnike sprejmejo tisti, ki sami ugotovijo, da to v resnici potrebujejo ali tisti, pri katerih so tveganja večja. **Tudi GDPR upravljalcem ne nalaga sprejema kakršnih koli notranjih aktov, zato je ta predvidena obveznost strožja od tiste, ki jo zahteva EU**, za kar prav tako ne vidimo razloga.

Glede na vse navedeno predlagamo, da se takšna splošna obveznost za vse upravljalce črta in da se, če že, uvede zgolj za tiste, kjer so pričakovana tveganja višja. Primerna rešitev bi lahko bila enaka sedaj veljavni, da to velja samo za upravljalce občutljivih (t.j. posebnih) osebnih podatkov.

K 38. členu (opisna pripomba):

Predlagamo, da se v 2.alineji drugega odstavka določba preoblikuje tako, da bo jasno, da se pogoj »v velikem obsegu« nanaša tudi na »obdelave posebnih vrst osebnih podatkov« in ne zgolj na »osebne podatke v zvezi s kazenskimi obsodbami«. GDRP namreč zahteva izdelavo ocene učinkov samo, če sta izpolnjena dva pogoja: da gre za obdelavo posebnih osebnih podatkov in da je ta obsežna. V izogib drugačni, strožji, interpretaciji slovenskega zakona (da se pogoj velik obseg nanaša samo na osebne podatke o obsodbah in da je torej ocena učinka potrebna že v vsakem primeru, ko se obdelujejo posebni osebni podatki) predlagamo, da se določba redakcijsko popravi.