Gospodarska zbornica Slovenije

Združenje za informatiko in telekomunikacije
Dimičeva 13, 1504 Ljubljana, 01 5898 102, www.gzs.si/zit, zit@gzs.si

zit
Združenje za informatiko in telekomunikacije

DRŽAVNI ZBOR

Predsednica Državnega zbora, mag. Urška Klakočar Zupančič
Zakonodajno-pravna služba
Poslanske skupine

Šubičeva 4
1000 Ljubljana

gp@dz-rs.si

Ljubljana, 5. 10. 2022

Zadeva: **Pripombe na osnutek predloga Zakona o varstvu osebnih podatkov (EPA: 189-IX) – predlog amandmajev**

Spoštovani.

Sekcija operaterjev elektronskih komunikacij[1] (v nadaljevanju SOEK), ki deluje pod okriljem Združenja za informatiko in telekomunikacije v okviru Gospodarske zbornice Slovenije **vam v nadaljevanju posreduje predlog amandmajev na zadnjo besedilo predloga Zakona o varstvu osebnih podatkov** (EPA: 189-IX). Predlagani amandmaji predstavljajo poenoteno skupno stališče članov SOEK.

Naj uvodoma pojasnimo, da je SOEK od prvega osnutka zakona v letu 2017 v celotnem postopku sprejemanja ZVOP-2 aktivno sodeloval in na vsako verzijo osnutka predloga zakona podajal strokovno argumentirane predloge in pripombe. Žal je od prvega osnutka do današnjega dne minilo kar 5 let, v vmesnem času smo operaterji naše poslovanje uspešno prilagodili vsem zahtevam Splošne uredbe o varstvu osebnih podatkov (GDPR), prihajajoči zakon pa mestoma v nasprotju z GDPR spreminja in zaostruje ureditev, pri kateri ne zaznavamo prav nobenih potreb po takšni popolni spremembi in zasuku ureditve. Žal predlagatelj zakona ne utemelji razlogov za te popravke, niti žal ne odgovori zakaj predlogov SOEK ne sprejema.

Glede na trenutni predlog zakona, ki se obravnava v Državnem zboru RS, člani SOEK še vedno ugotavljamo, da so nujno potrebne spremembe besedila zakona, predvsem tam, kjer nam predlagatelj zakona ni ugodil in kot rečeno tudi ni pojasnil zakaj našim predlogom ni mogoče slediti. Predlagane spremembe ne poslabšujejo ali omejujejo pravic in svoboščin posameznikov (končnih uporabnikov), kvečjemu izboljšujejo z bolj jasnim predlaganim besedilom, s čimer se je moč ogniti različnim tolmačenjem (npr. na področju biometrije ter obdelave osebnih podatkov iz identifikacijskega dokumenta), hkrati pa operaterje razbremenjujejo povsem nepotrebnih administrativnih opravil – vodenje dnevnikov. Predlagane spremembe upoštevajo tudi, da so določena področja z GDPR že ustrezno urejena, posledično pa podrobnejše urejanje z zakonom ni potrebno (npr. 69. in 92. člen), bolj zaostreno urejanje pa niti ni dopustno (ocena učinka, varnost osebnih podatkov na področju posebnih obdelav, posredovanje podatkov za raziskovalne in statistične namene, ožanje pravnih podlag v primeru video-nadzora). V predmetnem dokumentu

[1] Člani SOEK: A1 Slovenija, d.d., Telekom Slovenije, d.d., Telemach, d.o.o., HOT mobil, d.o.o., T-2, d.o.o.

izpostavljamo tudi neustreznost zahtev pri obdelavi osebnih podatkov, ki izhajajo iz predloga zakona, vezanih na informacijsko varnost in upoštevanje posledic za varnost države, vključno z njenimi političnimi in gospodarskimi koristmi, saj navedena materija ne spada v zakon o varstvu osebnih podatkov[2], ampak je predmet urejanja v drugih zakonih (Zakon o informacijski varnosti[3], Zakon o tajnih podatkih[4]). S tem, ko predlog zakona na več delih presega okvir pooblastila, ki je dan z GDPR, upravljavce, ki so registrirani v Republiki Sloveniji, napram drugim upravljavcem v EU postavlja v neenakopraven položaj. Posledično takšna zaostrena ureditev onemogoča prost pretok podatkov v Uniji, kar ima negativen vpliv na konkurenčnost slovenskega gospodarstva. GDPR določa enotna pravila za varstvo osebnih podatkov v EU, zato določbe, ki posegajo v siceršnja splošna pravila upravljavce iz zasebnega sektorja v Republiki Sloveniji nedopustno dodatno omejujejo oziroma posegajo v njihovo svobodno gospodarsko pobudo.

Utemeljenost predlaganih amandmajev smo v SOEK preverili tudi pri enem od slovenskih priznanih strokovnjakov na področju varstva osebnih podatkov, Odvetniška družba Pirc Musar & Lamut Strle, ki je potrdil, da se z izhodišči SOEK strinja ter lahko s primerjalno študijo vse predloge SOEK dodatno utemelji. Študijo prilagamo temu predlogu amandmajev.

V nadaljevanju pošiljamo predloge sprememb k posamičnim predlogom členov.

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

Predlagamo da se:

uvodni stavek v 1. odstavku preoblikuje, tako da glasi:

(1) Zaradi učinkovitejšega izvajanja 2. in 3. oddelka IV. poglavja Splošne uredbe upravljavci po tem zakonu vodijo dnevnik obdelave, kadar pri obdelavi osebnih podatkov prepoznajo tveganje, ki ga je mogoče učinkovito upravljati le z vodenjem dnevnika obdelave, ali če tako določa zakon, o naslednjih dejanjih obdelave osebnih podatkov:

zadnji stavek v 2. odstavku spremeni, tako da se na koncu besedna zveza "*ocene učinka*", nadomesti z besedno zvezo "*tveganj obdelave*".

Obrazložitev:

Zahteva po vodenju dnevnikov obdelave iz 21. člena predloga ZVOP-2, je v nasprotju z GDPR, ki predvideva oblikovanje ukrepov za varovanje osebnih podatkov glede na prepoznana tveganja. GDPR s tem namreč dopušča oziroma nalaga obveznost za oblikovanje varnostnih ukrepov upravljavcu, ki mora varnostne ukrepe oblikovati tako, da zagotovi ustrezno varstvo podatkov, vendar pa jih vseeno lahko prilagodi specifični obdelavi podatkov. **Vodenje dnevnikov obdelave je tako le eden izmed možnih ukrepov in ni vedno najprimernejši ali sorazmeren. Obvezna zahteva po vodenju dnevnikov obdelave zato pomeni kršitev pravil enotnega trga, nedopusten poseg v ustavno pravico do svobodne gospodarske pobude ter nesorazmerno breme za slovenska podjetja**. **Obenem predstavlja vodenje dnevnikov obdelave tudi**

[2] Ki tako kot GDPR varuje temeljne pravice in svoboščine posameznikov, zlasti njihovo pravico do varstva osebnih podatkov. Namen GDPR nikakor ni zagotavljanje varnosti in varovanje interesov nacionalnih držav. Navedenemu bi moral slediti tudi ZVOP-2.
3 Zakon o informacijski varnosti (uradni list RS, št. 30/18 in 95/21); ZInfV.
4 Zakon o tajnih podatkih (Uradni list RS, št. 50/06 – uradno prečiščeno besedilo, 9/10, 60/11 in 8/20); ZTP.

tveganje za prekomeren poseg v osebne podatke in zasebnost tistih zaposlenih ali drugih oseb, ki bodo obdelovale osebne podatke in katerih podatki se bodo zapisovali v baze revizijskih sledi. Zahteva po doslednem beleženju vsakršne obdelave (vključno z vpogledi, torej dostopanji do baz ali odpiranji datotek, ki vsebujejo osebne podatke) pomeni zahtevo po znatnih dodatnih investicijah v nestandardno programsko opremo ali pa zamudno (in s tem drago) ročno beleženje aktivnosti v zvezi z obdelavo osebnih podatkov. To lahko za sabo potegne ogromne stroške prilagoditve teh sistemov, hkrati pa ta poseg ne prinaša prav nobene bistvene dodatne koristi ne za posameznike, ne za podjetja.

Obenem zahteva po vodenju dnevnikov obdelave nujno pomeni dodatne investicije na področju prostora za hrambo podatkov. Zavedati se je namreč potrebno, da bodo v mnogih primerih baze, v katerih se bo beležila dejavnost obdelave, eksponentno večje od osnovnih baz, ki vsebujejo osebne podatke.

Zato predlagamo, da je vodenje dnevnikov obdelave vezano na to ali je pri posamezni obdelavi prepoznano tveganje, ki ga je mogoče učinkovito upravljati le z vodenjem dnevnikov obdelave.

<u>K 22. členu (varnost osebnih podatkov na področju posebnih obdelav), 1. in 2. odstavek</u>

Primarni predlog – k 1. odstavku:

Predlagamo, da se v 1. odstavku spremeni uvodni stavek, tako da glasi:

Za informacijske sisteme v javnem sektorju, v katerih se izvajajo obdelave osebnih podatkov.

Prav tako predlagamo, da se v celoti briše 5. točka prvega odstavka 22. člena.

Podredno, če predlog spremembe k prvemu odstavku 22. člena ZVOP-2 ne bi bil sprejet, bi bil za izločitev upravljavcev iz zasebnega sektorja iz zaveze za ukrepe za sistemsko onemogočanje razkritja osebnih podatkov ali obdelav nepooblaščenim osebam in s tem stalno preprečevanje škode Republiki Sloveniji potreben amandma k drugemu odstavku 22. člena:

Podredni predlog – k 2. odstavku:

Podredno, če se 1. odstavek ne omeji na javni sektor, predlagamo, da se 2. odstavek spremeni tako da se glasi:

Obdelava iz 1. do 4. točke prvega odstavka tega člena, ki jih izvajajo državni organi in organi samoupravnih lokalnih skupnosti, javne agencije in javni zavodi se izvaja tako, da se sistemsko onemogoča razkritje osebnih podatkov ali obdelav nepooblaščenim osebam ali drugim subjektom, ki za njihov dostop nimajo pravne podlage in s tem stalno preprečuje škodo varnosti ter interesom Republike Slovenije.

Obrazložitev k primarnemu predlogu korekcije:

V zvezi s primarnim predlogom spremembe navajamo, da je **določba 22. člena v neskladju z GDPR**. S tem členom se uvaja nov izraz »posebne obdelave« osebnih podatkov. GDPR ne pozna tega termina »posebne obdelave« in ga ne ureja, niti ne predvideva. Iz določbe 22. člena ni jasno, kaj je namen vzpostavitve takšnih vrst obdelave. Zaradi navedenega bi bilo smiselno določbo 22. člena celo brisati.

S tem, ko se v ZVOP-2 vnašajo posebne zahteve in določbe za določene »posebne obdelave« podatkov – določbe, ki jih GDPR ne pozna in ne predvideva – se za tovrstne obdelave v Sloveniji postavljajo drugačne zahteve kot v ostalih državah članicah. To je v nasprotju z enim izmed ciljev GDPR, tj. poenotenjem pravil za obdelavo osebnih podatkov v celotni EU. GDPR sicer dopušča urejanje nekaterih področjih obdelave osebnih podatkov državam članicam, vendar so ta področja in pooblastila državam članicam v GDPR izrecno navedena oziroma podeljena, čemur ta člen ne sledi, kar bo podrobneje pojasnjeno v nadaljevanju.

Predlagamo popravek določbe na način, da le-ta velja le za upravljavce v javnem sektorju.

Navedena namera zakonodajalca, da naj obveznosti iz tega člena veljajo le za javni sektor, izhaja tudi iz samega komentarja predloga zakona k 22. členu obrazložitve, kje je navedeno »Prav tako so občutljive obdelave osebnih podatkov v zbirkah, ki vsebujejo osebne podatke več kot 100.000 posameznikov, posebne osebne podatke več kot 10.000 posameznikov ali več kot 200.000 posameznikov, kadar se obdelujejo podatki v javnem sektorju.". Besedilo samega člena tako določa obveznosti še širše od obrazloženega namena. S predlagano spremembo se besedilo zakona uskladi z obrazložitvijo.

Nadalje izpostavljamo, da je v komentarju k 22. členu pojasnjeno, da je s to določbo implementirano pooblastilo, ki ga daje GDPR v tretjem odstavku 6. člena in četrtem odstavku 9. člena. Navedeno ne drži in pooblastilo ni implementirano pravilno. Namreč tretji odstavek 6. člena GDPR določa, da lahko države članice ohranijo ali uvedejo podrobnejše določbe, da bi prilagodile uporabo pravil te uredbe v zvezi z obdelavo osebnih podatkov za zagotovitev skladnosti s točkama c) in e) prvega odstavka 6. člena GDPR, ki pa se nanašata na obdelavo, ki je potrebna za izpolnitev zakonske obveznosti ter obdelavo, ki je potrebna za opravljanje naloge v javnem interesu ali pri izvajanju javne oblasti, dodeljene upravljavcu. Nadalje tretji odstavek 6. člena določa, da 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, subjekti, 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.

Iz navedenega v prejšnjem odstavku izhaja, da je **prvi odstavek 22. člena predloga ter posledično nadaljnji členi, iz katerih izhajajo obveznosti na podlagi prvega odstavka 22. člena predloga, v nasprotju s pooblastili, ki jih državam članicam daje GDPR. V predlogu 22. člena so kot kriterij upoštevani upravljavec podatkov, neodvisno od pravne podlage za obdelavo podatkov, ter število posameznikov, katerih osebne podatke obdeluje upravljavec, neodvisno od vrst podatkov.**

Določba četrtega odstavka 9. člena GDPR se nanaša na uvedbo dodatnih pogojev glede obdelave genetskih, biometričnih ali podatkov v zvezi z zdravjem.

Iz določb GDPR, iz katere izhaja sklic za dodelitev pooblastila, ne izhaja pooblastilo, ki bi bilo državam članicam dano, da države članice uvedejo podrobnejše določbe za »upravljavce v zasebnem sektorju, ki obdeluje osebne podatke več kot 200.000 posameznikov«. Točka 5 prvega odstavka 22. člena je vezana na zasebni sektor in sploh ne na pravne podlage za obdelavo osebnih podatkov ali posebne vrste osebnih podatkov, kot to določa GDPR (pri zasebnem sektorju velja za vse pravne podlage obdelave, pri čemer je kriterij zasebni sektor in število posameznikov, katerih osebni podatki se obdelujejo). Zakonodajalec je s tem presegel okvir pooblastila, ki ga daje GDPR oziroma je dodatne obveznosti določil povsem izven okvira in pooblastil, ki jih daje GDPR. Podlage za takšno ureditev v GDPR ni. V kolikor je bil namen takšne ureditve v nacionalnem predpisu, da se sistemsko onemogoča dostop do podatkov nepooblaščenim osebam, poudarjamo, da tovrstne obveznosti upravljavcev določa 25. člen GDPR – Vgrajeno in privzeto varstvo osebnih podatkov.

V nacionalnem zakonu se tako v nasprotju s GDPR uvajajo nove zahteve, ki nalagajo upravljavcem nepotrebne dodatne obveznosti in nas napram drugim upravljavcem v EU postavljajo v neenakopraven položaj, otežujejo pa tudi razvoj meddržavnih storitev. Zahteve glede varovanja osebnih podatkov, kot so predvidene v tem členu, pa veljajo enako za vse osebne podatke, ne glede na vrsto in obseg obdelave, z izjemo posebnih vrst osebnih podatkov, kot to določa GDPR.

S predlaganimi dodatnimi obveznostmi se s tem in s členi, ki za tovrstne obdelave določajo dodatne obveznosti (npr. 23. člen predloga) upravljavcem v zasebnem sektorju nalagajo dodatne obveznosti in omejitve, ki veljajo posebej le za v Sloveniji registrirane upravljavce, ne pa za upravljavce registrirane v drugih državah članicah EU. **Tako navedene določbe posegajo v siceršnja splošna pravila in v primerjavi z upravljavci v drugih državah članicah EU upravljavce iz zasebnega sektorja v Sloveniji dodatno omejujejo oziroma posegajo v svobodno gospodarsko pobudo.**

Nenazadnje niti ni jasno, zakaj je v drugi točki prvega odstavka število posameznikov, ki je mejnik te vrste obdelave (100.000), nižji od mejnika v peti točki tega odstavka (200.000). V kolikor se obdelava izvaja že na podlagi zakona, kot to izhaja iz druge točke prvega odstavka, bi bilo smiselno, da je mejnik določen pri veliko višji številki posameznikov, glede na mejnik, ki je določen v peti točki tega odstavka. Vidik varnosti obdelave osebnih podatkov posameznikov je namreč že upoštevan pri samem sprejemu zakona, ki je podlaga obdelave (posledično je izdelana tudi ocena učinka že v fazi samega sprejema zakona).

Obrazložitev k podrednemu predlogu korekcije:

Namen GDPR, kot določa v 1. členu, je določitev pravil o varstvu posameznikov pri obdelavi osebnih podatkov in pravila o prostem pretoku osebnih podatkov. GDPR varuje temeljne pravice in svoboščine posameznikov ter zlasti njihovo pravico do varstva osebnih podatkov. Skladno z določbo 1. člena GDPR je nelogična in neskladna določba v drugem odstavku 22. člena, ki določa: *»(2) Obdelave iz prejšnjega odstavka se izvaja tako, da se sistemsko onemogoča razkritje osebnih podatkov ali obdelav nepooblaščenim osebam ali drugim subjektom, ki za njihov dostop nimajo pravne podlage in s tem stalno preprečuje škodo varnosti ter interesom Republike Slovenije.*« **Namen GDPR je varovanje temeljnih pravic in svoboščin posameznikov in nikakor ne varnosti in interesov nacionalnih držav. Presojanje in določanje ukrepov za preprečevanje**

škode varnosti in interesom Republike Slovenije je naloga države ter to ne sodi v pristojnost zasebnega sektorja.

GDPR že določa obveznosti upravljavcev in obdelovalcev pri varovanju podatkov in oblikovanju ukrepov za varovanje podatkov. Pri tem morajo upravljavci in obdelovalci upoštevati tako zahteve po uporabi načel privzetega in vgrajenega varstva osebnih podatkov, kot tudi oblikovati ukrepe za varovanje osebnih podatkov ob upoštevanju tveganj, ki jih obdelava podatkov prinaša. Zahteve glede varovanja osebnih podatkov, ki izhajajo iz GDPR, veljajo za vse upravljavce in obdelovalce, ki delujejo v EU ter so za vse enake. Posebne, specifične zahteve, ki ne izhajajo iz GDPR, kot je predlagana zahteva za »sistemsko onemogoča razkritje osebnih podatkov«, ki veljajo specifično samo za upravljavce iz zasebnega sektorja v Republiki Slovenije, gospodarstvo tako postavljajo v neenakopraven položaj s subjekti iz ostalih držav članic EU in posledično onemogočajo prost pretok podatkov v Uniji. To ima negativen vpliv na konkurenčnost gospodarstva, omejevanje možnih rešitev pri uporabi sredstev za obdelavo osebnih podatkov z dodatnimi zahtevami, ki so specifične samo v Sloveniji in je povezana z dodatnimi stroški in investicijami. Negativno lahko vpliva npr. na uporabo storitev v oblaku, kjer je lahko neka storitev na podlagi GDPR ustrezna v EU (ostalih državah članicah), ne pa v Sloveniji. GDPR že vključuje zahteve glede varstva osebnih podatkov, zato menimo, da je predlagana dodatna ureditev nesorazmerna in neupravičena ter tako tudi neutemeljen poseg v svobodno gospodarsko pobudo.

K 23. členu, 2. in 3. odstavek

Primarni predlog amandmaja k 2. in 3. odstavku (če ni bil predhodno že sprejet predlagani amandma k 22. členu):

Predlagamo, da se v celoti brišeta 2. in 3. odstavek, ostali odstavki se preštevilčijo.

Podredno, če prvo predlagani amandma ne bi bil sprejet, sta predlagana amandmaja k 2. in 3. odstavku:

Predlagamo, da se spremeni prvi stavek 2. odstavka, tako da glasi:

(2) Oceno učinkov glede varstva osebnih podatkov in predhodno posvetovanje z nadzornim organom upravljavci iz javnega sektorja izvajajo tudi pred obdelavo osebnih podatkov iz prvega odstavka prejšnjega člena.

Predlagamo, da se spremeni napovedni stavek 3. odstavka, tako da glasi:

(3) Pred začetkom obdelave upravljavci iz javnega sektorja oceno učinka ponovno izdelajo tudi v naslednjih primerih:

Obrazložitev:

Ta vsebina je natančno določena v 35. in 36. členu GDPR in ni potrebe za dodatno urejanje v nacionalnem zakonu.

Predlog 2. in 3. odstavka 23. člena je celo v izrecnem nasprotju z določbo 35. in 36. člena GDPR, ki določa pogoje in način izvedbe ocene učinka v zvezi z varstvom osebnih podatkov. Določba 35. člena GDPR jasno določa, v katerih primerih je potrebna izdelava ocene učinka v zvezi z varstvom osebnih podatkov, obveznost nadzornemu organu, da določi in objavi seznam vrst obdelave osebnih podatkov, za katere velja zahteva po oceni učinka v zvezi z varstvom osebnih podatkov ter nadalje tudi možnost, da nadzorni organ določi in objavi seznam vrst obdelave osebnih podatkov, za katere ne velja zahteva po oceni učinka v zvezi z varstvom osebnih podatkov. Določba 36. člena GDPR nadalje tudi določa, v katerih primerih je potrebno posvetovanje z nadzornim organom, glede ocene učinka v zvezi z varstvom osebnih podatkov. **Iz navedenega jasno izhaja, da izdelava ocene učinka in predhodni posvet z nadzornim organom ni potrebno izvesti v primeru kar vsake dejavnosti obdelave podatkov (kar skuša uvesti predlog ZVOP-2). Prav tako določbi 35. člena in 36. člena GDPR državam članicam ne dopuščata drugačne ureditve oziroma uvajanja novih obveznosti, kot jo določa GDPR.**

Drugi in tretji odstavek 23. člena (v nasprotju z določbo GDPR) določata, da je ocena učinka v zvezi z varstvom podatkov ter posvetovanje z nadzornim organom nujna vedno, kadar so izpolnjeni pogoji iz 1. odstavka 22. člena (kjer so ti pogoji taksativno navedeni za javni in za zasebni sektor). S tem se določajo povsem drugačni kriteriji za izdelavo ocene učinka v zvezi varstvom podatkov ter posvetovanje z nadzornim organom (tj. namesto kriterijev določenih v GDPR, se določajo drugi dodatni kriteriji, konkretno v zasebnem sektorju kriterij števila posameznikov, katerih osebnih podatki se obdelujejo, neodvisno od vrste, količine, obsega, namena ali načina obdelave osebnih podatkov). S tem se neupravičeno širi določba GDPR izven njenih meja urejanja oziroma v izrecnem nasprotju s GDPR. Neupravičena in nesmotrna je zahteva zakonodajalca, da bodo upravljavci v vsakem primeru, kadar bodo izpolnjeni pogoji iz 1. odstavka 22. člena ZVOP-2, izdelali oceno učinka v zvezi z varstvom osebnih podatkov in v zvezi s tem izvedli tudi posvet z nadzornim organom. To bi v praksi pomenilo, da bi upravljalec moral izvesti oceno učinka v zvezi z varstvom podatkov in izvesti posvet z nadzornim organom tako v primeru vpeljave novega sistema, preko katerega bi izvajal sistematično spremljanje posameznikov, z uporabno avtomatiziranega načina odločanja (kjer je ocena učinka potrebna že glede na zahteve GDPR), kot tudi v primeru kadar bi želel upravljalec pošiljati generični novičnik na elektronske naslove večjega številka svojih uporabnikov (kjer pa gre tipično za obdelavo kjer po GDPR ocena učinka ni obvezna).

Dalje ugotavljamo, da je **določba 2. odstavka hkrati kontradiktorna določbi 1. odstavka 23. člena**, ki sicer določa, da se ocena učinka in predhodno posvetovanje z nadzornim organom izvaja skladno z določbo 35. in 36. člena GDPR.

Skladno z določbo 1. odstavka 35. člena GDPR, je potrebno izdelati oceno učinka v zvezi z varstvom podatkov, **kadar bi ta povzročila veliko tveganje za pravice in svoboščine posameznikov.** Tudi na tem mestu ugotavljamo, da je predlagatelj zakona presegel namen GDPR, ki se nanaša na varstvo pravic in svoboščin **posameznika.**

Predlagatelj zakona torej v 2. odstavku 23. člena skuša uvesti povsem novo obveznost, s tem, ko določa, da je pri izdelavi ocene učinka v zvezi z varstvom podatkov potrebno upoštevati možne škodljive posledice za varnost države, vključno z njenimi političnimi ali gospodarskimi koristmi, če bi bili obdelovani podatki razkriti nepooblaščenim osebam ali subjektom. **Namen izdelave ocene učinka se skladno s GDPR nanaša na posameznike in nikakor ne na varnost države ali njene interese. Podredno ugotavljamo, da zasebni subjekt ni sposoben opredeliti, kaj so**

škodljive posledice, niti kaj je varnost države, ali kaj so politične ali gospodarske koristi države, ter katerim tretjim subjektom podatki ne bi smeli biti razkriti. Če bi morda takšno določilo še imelo smisel pri ocenah, ki bi jih izvedli organi javnega sektorja, pri zasebnih to prinaša takšno pravno negotovost, s katero se zasebni sektor izpostavlja toliko nepredvidenim tveganjem, da je že z vidika ustavno zavarovane svobodne gospodarske pobude jasno, da takšna ureditev ni primerna za urejanje v ZVOP-2.

GDPR natanko določa v katerih primerih je izdelava ocene učinka v zvezi z varstvom podatkov potrebna in Informacijski pooblaščenec je v zvezi s tem že izdal Smernice.

Predlog 2. in 3. odstavka 23. člena je primarno v nasprotju s 35. in 36. členom GDPR, saj določa povsem nove kriterije za izdelavo ocene učinka v zvezi z varstvom podatkov ter dodaja nove pogoje, ki jih je pri izdelavi ocene učinka potrebno upoštevati (škodljive posledice za varnost države, njene politične in gospodarske koristi, razkrivanje tretjim). Predlog 2. in 3. odstavka 23. člena je tudi pravno nedorečen, kot smo navedli v zgornji obrazložitvi, saj posamični pojmi, ki tvorijo tako resno tveganje, sploh niso nikjer preverljivi, niti niso objektivno določeni, kar pa bi pri takšnem posegu v ustavno zavarovano svobodno gospodarsko pobudo bilo treba predvideti vnaprej.

Nenazadnje ta predlog prinaša velike in nesorazmerna dodatne obveznosti na strani upravljavcev, iz predloga zakona pa ni razvidno, kakšne bi bile koristi teh dodatnih zahtev za posameznike, varovanju pravic in svoboščin katerih je izdelava učinka v zvezi z varstvom podatkov pravzaprav namenjena.

Če bi zakonodajalec vztrajal pri tej določbi 23. člena predlagamo, da se 2. odstavek 23. člena dopolni na način, da ta velja samo za osebe javnega sektorja.

K 40. členu (postopek posredovanja osebnih podatkov), 2. in nov 5. odstavek

Drugi odstavek se spremeni, tako da glasi:

(2) Upravljavec vlagatelju zahteve, proti plačilu stroškov posredovanja, če zakon ne določa drugačnega načina, zahtevane osebne podatke posreduje najpozneje v 30 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.

Doda se nov 5. odstavek:

(5) Ne glede na drugi 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 odstavki in sklici na določbe v tem členu se ustrezno preštevilčijo.

Obrazložitev:

Ugotavljamo, da predlog o podaljšanju roka za posredovanje osebnih podatkov, ki smo ga podali v okviru pripomb na predlog ZVOP-2 iz aprila 2021, ni bil ustrezno upoštevan. Možnost podaljšanja roka še ne pomeni, da bo podaljšanje vlagatelj zahteve odobril. Zaradi poenostavitve in enotnega vodenja postopkov in zahtev pozivamo na ponovni razmislek glede navedenega in korekcijo določbe, kot to izhaja iz zgornjega predloga. Glede na to, da 22. člen veljavnega ZVOP-1 (katerega vsebinsko nadomešča 40. člen ZVOP-2) določa, da se podatki posredujejo proti plačilu (če zakon ne določa drugače), predlagamo, da navedeno predvideva tudi 40. člen ZVOP-2.

K 42. členu (rok hrambe osebnih podatkov, določitev roka in vezanost na rok)

Primarno predlagamo, da se 42. člen v celoti briše.

Podredno, kolikor bi šteli, da je v GDPR pooblastilo državi članici, da na nacionalni ravni izven določb o načelu omejitve shranjevanja ureja obdelavo osebnih podatkov po izpolnitvi namena obdelave, predlagamo da se 3. odstavek 42. člena spremeni, tako da glasi:

(3) Po izpolnitvi namena obdelave se osebni podatki izbrišejo, uničijo, anonimizirajo oziroma se izvede drug postopek, ki ne omogoča identifikacije posameznika, na katerega se nanašajo osebni podatki, če zakon za posamezne vrste osebnih podatkov ne določa drugače, zlasti omejevanje dostopa do njih, njihovo blokiranje ali njihovo arhiviranje.

Obrazložitev:

Ugotavljamo, da je besedilo tega odstavka skoraj identično določbi sedanjega 21. člena ZVOP-1, s tem da je brisana le beseda »blokirajo«. **GDPR nikjer ne določa katerih postopkov se mora poslužiti upravljavec, da se šteje, da osebnih podatkov več ne hrani.** Točka (e) prvega odstavka 5. člena GDPR namreč določa le: »osebni podatki so hranjeni v obliki, ki dopušča identifikacijo posameznikov, na katere se nanašajo osebni podatki, le toliko časa, kolikor je potrebno za namene, za katere se obdelujejo…«. Citirana dikcija sicer ustreza določbi prvega odstavka 42. člena predloga ZVOP-2. Menimo, da je taksativno navajanje načinov, ki se jih mora poslužiti upravljavec, da zadosti določbi, ki opredeljuje način prenehanja hrambe, preveč restrikitiven ukrep, ki oži manevrski prostor, kot je določen z GDPR. Po poteku obdobja pravno-dopustne hrambe se je namreč možno poslužiti raznovrstnih postopkov, ki omogočajo, da so osebni podatki hranjeni v obliki, ki identifikacije posameznikov, na katere se nanašajo osebni podatki, ne omogočajo. Gre za primere, ko so s strani upravljavca osebni podatki psevdonimizirani, vendar je enolični identifikator izbrisan (in ne le shranjen ločeno), posledično pa z nobeno aktivnostjo (bodisi upravljavca, obdelovalca ali drugega uporabnika) ni mogoče povratno ugotoviti, na katerega posameznika se takšni psevdonimizirani podatki nanašajo (psevdonimizirani podatki dejansko postanejo anonimizirani, čeprav se anonimizacija ni izvedla s spremembo več enoličnih identifikatorjev, kot to praviloma velja za način izvedbe anonimizacije). Predlagamo torej, da se načini, ki se jih je zavezan poslužiti upravljavec po poteku roka hrambe napišejo na način, da bo upravljavec glede na vsak konkreten primer presodil, kakšno obliko t.i. »nehrambe« osebnih podatkov bo izbral. Nenazadnje je že s predhodno citirano določbo drugega odstavka 5. člena GDPR na samem upravljavcu odgovornost za skladnost obdelave s predpisi ter dokazno breme v zvezi s tem.

II. DEL
PODROČNE UREDITVE OBDELAVE OSEBNIH PODATKOV

1. poglavje

Posebna pravila glede obdelave osebnih podatkov za znanstvenoraziskovalne, zgodovinskoraziskovalne, statistične in arhivske namene

67. člen

Na koncu 1. odstavka se namesto pike doda vejica, za vejico pa besedilo:

...in so vpisani v Evidence izvajalcev raziskovalne in razvojne dejavnosti pri Javni agenciji za raziskovalno dejavnost Republike Slovenije.

Obrazložitev:

Ugotavljamo, da je opredelitev organizacij in posameznikov, ki bodo osebne podatke lahko obdelovali za znanstvenoraziskovalne, zgodovinskoraziskovalne in statistične namene zelo splošna. V primeru, da navedenega pogoja določba ne bi vsebovala, bo upravljavec težko preverjal, ali je zaprosilo vložil upravičen subjekt. Posledično bi bili podatki tako lahko posredovani subjektu, ki se z njimi sploh ne bi smel seznaniti.

V kolikor predlogu spremembe 1. odstavka 67. člena, kot izhaja zgoraj, ne bo ugodeno, podajamo podredni predlog amandmaja, in sicer k 2. odstavku 68. člena. Iz navedenega podrednega predloga izhaja, da se v 2. odstavku 68. člena za 7. točko doda nova 8. točka, ki od raziskovalne organizacije ter raziskovalca zahteva, da opisu raziskave priloži tudi izjavo, da uporablja etična pravila in metodologijo s sklicem na konkretna pravila etike in metodologijo, ki ji sledi pri raziskavi. Menimo sicer, da je korekcija 1. odstavka 67. člena boljša rešitev, saj bi v praksi onemogočala zlorabe, vezane na posredovanje osebnih podatkov za namen raziskav. S podrednim predlogom, torej spremembo 2. odstavka 68. člena, pa se zlorabe ne bi onemogočile. Podatke bi upravljavec namreč v tem primeru še vedno lahko posredoval subjektu, ki bo te podatke zahteval, četudi ta subjekt do teh podatkov ne bi bil upravičen, ker bo npr. ta subjekt podal lažno izjavo. V primeru zahteve, da subjekt, ki zaproša podatke, poda tudi izjavo, da uporablja etična pravila in metodologijo, bi se tako odpravila odgovornost upravljavcev, ki bi podatke raziskovalni organizaciji oziroma raziskovalcu, ki to ni, posredovali.

68. člen (pogoji obdelave osebnih podatkov v raziskovalne namene), 1. , 2. in 4. odstavek

Z namenom opustitve dodajanja pogojev za združljivost obdelave osebnih podatkov, predlagamo spremembo 1. odstavka, ki pomeni zgolj uskladitev z GDPR. Odstavek bi se lahko tudi izpustil (še posebej upoštevaje okoliščino, da je primerljiva vsebina že vsebovana v drugem odstavku 7. člena predloga ZVOP-2).

1. odstavek naj se spremeni, tako da glasi:

Ne glede na prvotni namen obdelave lahko upravljavec osebne podatke, vključno s posebnimi vrstami osebnih podatkov, nadalje obdeluje za namen raziskovanja, pri čemer je dolžan zagotoviti zaščitne ukrepe v skladu z 89/I členom Splošne uredbe.

V 4. odstavku se za 5. točko doda nova 6. točka, ki se glasi:

6. če posredovanje zahtevanih osebnih podatkov z organizacijskega ali tehničnega vidika posega v njegovo redno poslovanje oziroma prosilec odkloni sklenitev dogovora o plačilu stroškov posredovanja podatkov.

Podredni predlog korekcije 2. odstavka (slednji naj se upošteva, če predlogu amandmaja k 1. odstavku 67. člena predloga ZVOP-2 ne bo ugodeno)

Podredni predlog se glasi:
V 2. odstavku se za 7. točko doda nova 8. točka, ki se glasi:

8. izjavo raziskovalca oziroma raziskovalne organizacije, da pri svojem delovanju uporablja etična pravila in metodologijo s sklicem na konkretna pravila etike in metodologijo, ki ji sledi pri predmetni raziskavi.

Obrazložitev k predlogu korekcije 1. odstavka 68. člena:

Državam članicam ni dano pooblastilo, da drugače, izven določb 6. člena GDPR urejajo pravne podlage za obdelavo osebnih podatkov v znanstveno-raziskovalne namene. GDPR tudi ne pozna domnevanega soglasja (opt-out princip) kot podlage za obdelavo osebnih podatkov, kot to predvideva 1. točka 1. odstavka 68. člena predloga ZVOP-2. Nadaljnja obdelava osebnih podatkov v znanstveno ali zgodovinsko-raziskovalne namene je vselej združljiva z nameni, za katere so bili osebni podatki prvotno zbrani, posledično pa je takšna nadaljnja obdelava osebnih podatkov dopustna. Navedeno izhaja iz recitala št. 50 GDPR ter točke b) prvega odstavka 5. člena GDPR. Z določanjem dodatnih pogojev za združljivost znanstveno-raziskovalnih namenov s prvotnimi predlogi ZVOP-2 presega okvir pooblastil, ki so državam članicam dane v GDPR.

Obrazložitev k predlogu korekcije 4. odstavka 68. člena:

Posredovanje osebnih podatkov za raziskovalni namen lahko za upravljavce predstavlja velik kadrovski, časovni in finančni angažma. Dodatno breme za upravljavca predstavlja že zahteva zakona, da subjekt, ki prejme zahtevo za posredovanje osebnih podatkov za raziskovalni namen, sam presodi, ali so izpolnjeni pogoji za posredovanje oziroma poda oceno o okoliščinah posredovanja podatkov, kot vse to izhaja iz četrtega odstavka 68. člena predloga ZVOP-2. Za presojo okoliščin iz četrtega odstavka obstoječega predloga določbe 68. člena bi subjekt, ki prejme zahtevo za posredovanje, potreboval ustrezno usposobljen kader. Potrebno je upoštevati dejstvo, da delodajalci praviloma zaposlujejo le toliko kadra določene strokovne usposobljenosti, kot je to potrebno za izvajanje njihove registrirane dejavnosti. Zaradi zahteve po presoji okoliščin, ki jo

predlog zakona dodatno nalaga samemu upravljavcu v četrtem odstavku, bi bil marsikateri subjekt, ki bi prejel zahtevo za posredovanje podatkov za raziskovalni namen, primoran zaposliti dodaten kader. Ni utemeljeno pričakovanje, da bi gospodarski subjekt, zaradi izvajanja naloge, ki je postranskega pomena (glede na registrirano dejavnost upravljavca) in se opravlja v imenu in za račun drugega subjekta, v vsakem primeru pristal na posredovanje osebnih podatkov, in sicer tudi v primerih, ko bi to od njega zahtevalo nesorazmerne stroške (ki ne bi bili povrnjeni) oziroma napor ali celo ogrozitev njegovega poslovanja.

Pravilno bi bilo tudi, da bi zakon predvidel možnost, da upravljavci, ki so subjekti zasebnega sektorja, posredovanje opravijo proti plačilu. Primerno je, da se o višini plačila izvajalec raziskave in upravljavec dogovorita predhodno, in sicer v vsakem posamičnem primeru. Obseg podatkov, ki jih bodo izvajalci raziskave potrebovali za izvedbo raziskave, bo namreč variiral. Realizacija zahteve za posredovanje osebnih podatkov, ki bi terjala posredovanje velikega obsega osebnih podatkov, bo za upravljavca nedvomno predstavljala časovno in kadrovsko ter s tem stroškovno obremenitev. V primeru, da upravljavec tako nastalih stroškov (vsaj delno) ne bi dobil povrnjenih, bi to zagotovo vplivalo na uspešnost njegovega poslovanja. Hipotetično je možen tudi skrajni primer, ki bi se zgodil, če bi upravljavec prejel takšno število zahtev za posredovanje osebnih podatkov, da bi moral angažirati ves ali večino svojega razpoložljivega kadra. Izvedba nalog posredovanja podatkov izvajalcu raziskave bi tako lahko ogrozila opravljanje njegove registrirane dejavnosti, s tem pa bi bil ogrožen obstoj upravljavca kot akterja na gospodarskem trgu.

V primeru, da raziskovalna organizacija oziroma raziskovalec odkloni sklenitev dogovora o plačilu posredovanja z upravljavcem ali ko bi posredovanje osebnih podatkov za namen raziskovanja negativno posegalo v poslovanje upravljavca na način, ki ga tudi proti plačilu stroškov posredovanja ne bi bilo možno sanirati, je primerno, da se upravljavcu podeli pravica, da posredovanje osebnih podatkov za namen raziskovanja zavrne.

Obrazložitev k podrednemu predlogu korekcije 2. odstavka 68. člena:

V obrazložitvi k predlogu spremembe 1. odstavka 67. člena predloga ZVOP-2 smo že navedli, naj se slednji podredni predlog korekcije upošteva le v primeru, če predlogu amandmaja k 1. odstavku 67. člena predloga ZVOP-2 ne bo ugodeno. Upravljavec namreč ne bi smel nositi odgovornosti, če bi se nanj obrnil subjekt, ki bi zaprosil za posredovanje osebnih podatkov za namen raziskovanja, pa ta subjekt za podajo tega zahtevka ne bi bil upravičen. Upravljavec v primeru neupoštevanja korekcije 1. odstavka 67. člena ZVOP-2, kot smo ga predlagali, ne bo mogel preveriti, ali raziskovalna organizacija oziroma raziskovalec, ki podatke zaproša, izpolnjuje pogoje za upravičenega prosilca. V primeru neupoštevanja 1. odstavka 67. člena ZVOP-2 je tako potrebno, da se določba 2. odstavka 68. člena korigira na način, da odpade odgovornost upravljavca, če bo posredoval osebne podatke, subjektu, ki bo podal lažno izjavo o uporabi etičnih pravil in metodologije, upravljavec pa v resničnost te izjave ne bo dvomil.

69. člen (kontaktiranje posameznikov)

Primarni predlog:

Predlagamo, da se 69. člen v celoti briše.

Podredni predlog – 2. odstavek naj se glasi:

(2) Upravljavec odkloni kontaktiranje posameznikov po prvem odstavku tega člena, če z organizacijskega ali tehničnega vidika takšna obdelava osebnih podatkov posega v njegovo redno poslovanje oziroma prosilec odkloni sklenitev dogovora o plačilu storitve kontaktiranja posameznikov.

Obrazložitev:

Glede na to, da je skladno z GDPR obdelava osebnih podatkov v znanstveno raziskovalne namene vedno združljiva s prvotnim namenom obdelave (kot smo to že navajali v obrazložitvi k predlogu sprememb 68. člena) ni potrebe po dodatni podlagi za nadaljnjo obdelavo osebnih podatkov za raziskovalni namen, torej ni potrebe po soglasju posameznika za nadaljnjo obdelavo osebnih podatkov za raziskovalni namen. Naveden člen tako ni smiseln in naj se briše. V primeru neupoštevanja našega primarnega predloga korekcije tega člena (brisanje določbe) pa predlagamo, da se drugi odstavek napiše na način, da bo bolj jasno, da kontaktiranje posameznikov za namen pridobivanja privolitev ni dolžnost upravljavca ampak zgolj možnost, ki jo slednji lahko odkloni, če bi kontaktiranje posameznikov posegalo v njegovo redno poslovanje oziroma če prosilec odkloni sklenitev dogovora o plačilu storitve kontaktiranja posameznikov.

3. poglavje
Videonadzor

Določbe poglavja o videonadzoru so v veliki meri prenesene iz obstoječega ZVOP-1, ki pa je bil pripravljen in sprejet v posvsem drugačnih okoliščinah. Z GDPR je bil postavljen nov okvir pri obdelavi osebnih podatkov, ki na eni strani zagotavlja robustne pravice posameznikov in na drugi strani upravljavcem znan okvir za odločanje glede obdelave osebnih podatkov. Pri tem skozi splošna pravila in zahteve glede obdelave osebnih podatkov – ki veljajo tudi za obdelavo osebnih podatkov pri videonadzoru – omogoča, da so le ta tehnološko nevtralna in prilagodljiva oziroma uporabna tudi pri razvoju novih tehnologij.

Določbe obstoječega ZVOP-1, ki jim določbe v predlogu zakona sledijo, so bile oblikovane pred sprejetjem splošnih načel in pravil, ki jih določa GDPOR. Določbe tako pri tem kot eno od ključnih orodij uporabijo omejitve namenov za katere je obdelava osebnih podatkov z videonadzorom sploh dopustna: Pri tem dopuščajo predvsem obdelavo za t.i. »varnost ljudi ali premoženja« ter tudi za posamezne druge specifične namene. Navedeno ni skladno z GDPR - po GDPR videonadzor ne sodi med posebne vrste obdelave osebnih podatkov, temveč zanjo veljajo splošna pravila obdelave osebnih podatkov, ki ne omejujejo namenov obdelave, prav tako pa v tem delu GDPR ne predvideva pravice držav članic za specifično urejanje tega področja obdelave osebnih podatkov. Pri uporabi določb GDPR za izvajanje videonadzora lahko pri določenih namenih obdelave, predvsem teh urejenih v členih 76-78, pridemo do smiselno podobnih omejitev, kot jih vsebuje predlog zakona. Bistvena razlika je v tem, da so po predlogu zakona omejitve določene skozi specifične in konkretne zakonske določbe, ki brez spremembe zakona ne omogočajo prilagodljivosti različnim okoliščinam, pri uporabi določb GDPR pa se uporabijo splošne določbe GDPR in se za vsak posamezen primer presodi in obravnava s strani upravljavca, ki lahko oceni ali so podane ustrezne podlage in upravičeni in sorazmerni razlogi za izvajanje videonadzora (ter je pri tem tudi podvržen nadzoru).

<u>75. člen (splošne določbe o videonadzoru in varstvu osebnih podatkov)</u>

1. odstavek

Predlagamo, da se doda nov drugi stavek, ki glasi:

Ne gre za video-nadzor po določbah tega poglavja, če je video-nadzorni sistem namenjen le inteligentni video-analitiki, ki neposredno po zajemu posnetka ciljne podatke nepovratno razosebi.

Obrazložitev:

Izvajanje videonadzora za namene, dopustne v predlogu – npr. za zagotavljanje varnosti - lahko predstavlja večji poseg v zasebnost kot npr. izvajanje videonadzora za potrebe videoanalitke – štetja obiskovalcev. Takšno omejevanje namenov tako ni učinkovito pri zasledovanju svojega osnovnega cilja – zagotavljanju pravic posameznikov – saj dopušča prav obdelave, ki predstavljajo največje tveganje za pravice posameznikov. S tem se onemogoča razvoj tehnologij in novih rešitev in storitev, ki ne spadajo med izjeme. S tem povezane omejitve pridejo še posebej do izraza pri izvajanju anonimne inteligentne videoanalitike, npr. pri različnih storitvah pametnih mest (npr. zasedenost parkirnih mest, …), ki ni usmerjena v obdelavo podatkov o posameznikih, vendar pa je njeno izvajanje neločljivo povezano z obdelavo video podatkov. Nov drugi odstavek predlagamo zaradi razmejitve med enostavno video-analitiko in video-nadzorom, tako da se določi, kdaj se za enostavno video-analitiko ne uporabljajo določbe o video-nadzoru.

<u>79. člen (videonadzor na javnih površinah)</u>

Primarni predlog korekcije:

Predlagamo, da se 79. člen v celoti briše.

Podredni predlog korekcije 1. in 10. odstavka:

Podredni predlog korekcije – 1. odstavek:

V prvem stavku 1. odstavka se za besedno zvezo »*ki ureja urejanje prostora*«, doda vejica in besedilo:

‚z izjemo videonadzora v atrijih, v športnih dvoranah in na parkiriščih.

Na koncu 1. odstavka se doda nov zadnji stavek:

Videonadzor v atrijih, v športnih dvoranah in na parkiriščih je dovoljen v skladu s splošnimi pravili iz 75. člena tega zakona, na eni od pravnih podlag iz Splošne uredbe o varstvu podatkov.

Podredni predlog korekcije - 10. odstavku:

Deseti odstavek 79. člena se v celoti briše.

Alternativni predlog podrednega amandmaja k 10. odstavku– besedilo se spremeni tako da se glasi:

(10) Na javnih površinah, ki so predmet posebne ureditve v tem členu, je prepovedana uporaba sistemov za avtomatsko prepoznavo registrskih tablic in sistemov, s katerimi se obdelujejo biometrični osebni podatki, razen če zakon določa drugače.

Predlog podpodrednega amandmaja k 10. odstavku – besedilo se spremeni tako da se glasi:

(10) Na javnih površinah, je prepovedana uporaba sistemov s katerimi se obdelujejo biometrični osebni podatki, razen če zakon določa drugače.

Obrazložitev:

Obdelava osebnih podatkov v sklopu videonadzora po GDPR ne sodi med posebne vrste obdelave osebnih podatkov, temveč zanjo veljajo splošna pravila obdelave osebnih podatkov. Tako zakon ni edina možna in dopustna podlaga za obdelavo osebnih podatkov sklopu videonadzora, temveč se podatki lahko obdelujejo v skladu s pravnimi podlagami kot jih določa 6. člen GDPR. V skladu s tem je tudi Evropski odbor za varstvo podatkov sprejel smernice za obdelavo osebnih podatkov preko video naprav (Guidelines 3/2019 on processing of personal data through video devices), kjer kot pravno podlago za izvajanje video nadzora izrecno obravnava tudi zakoniti interes v skladu s točko (f) 1. odstavka 6. člena GDPR.

Tako ta člen ni potreben za določitev pravne podlage za obdelavo osebnih podatkov v sklopu videonadzora. Tudi sicer je izvajanje videonadzora ustrezno urejeno preko splošnih določb v 75. členu predloga zakona in za posebne primere preko omejitev v 76., 77. in 78. členu predloga zakona.

Omejitev namenov obdelave na namene, določene v predlaganem besedilu zakona, je tako v nasprotju s GDPR. Prav tako pa so obdelave, ki jih dopušča, prav obdelave, kjer lahko pride do največjih posegov v zasebnost posameznikov, omejuje pa uporabo videonadzora za morebitne druge namene, ki (ob pravilni izvedbi – vendar to velja za vse obdelave, še toliko bolj za te, ki jih predlog dopušča), ki so lahko tudi v interesu posameznikov.

Obenem izrecna prepoved uporabe sistemov za avtomatsko prepoznavo registrskih tablic in biometrije na javnih površinah onemogoča razvoj naprednih storitev za nadzor, umirjanje in upravljanje prometa, storitev pametnih mest in verjetno tudi morebitnih storitev napredne videoanalitike (tako npr. prepoved avtomatske prepoznave registrskih tablic v povezavi s predlagano določbo 2. odstavka 6. člena pomeni, da sekcijske meritve hitrosti prometa ne bodo dopustne do morebitne spremembe Zakona o pravilih cestnega prometa, prepoved biometrije npr. postavlja pod vprašaj napredno videoanalitiko, ki bi ugotavljala koliko obiskovalcev parka je moških, žensk in otrok). Prav tako bi to pomenilo prepoved avtomatske prepoznave registrskih tablic npr. pri pametnih parkiriščih, ki se v skladu z GDPR že uporablja, predvsem pri večjih parkiriščih v trgovskih centrih.

Podredno, v kolikor so morebitne omejitve videonadzora na javnih površinah res potrebne pa je

naj se le oblikujejo tako, da ne bodo onemogočile razvoja sodobne družbe (npr. storitve pametnih mest) in novih modernih storitev. Omejitev dopustnih namenov obdelave izključno na namene, določene z zakonom, v praksi onemogoči razvoj novih storitev dokler le-te niso določene in urejene v zakonodaji. Tako je jasno, da taka zaprta ureditev področja onemogoča praktično kakršenkoli razvoj oziroma vsaj kakršen koli hiter razvoj storitev. Ena izmed bistvenih pridobitev GDPR so ravno odprte definicije, ki vnaprej ne onemogočajo razvoja novih storitev, temveč skrbijo za ustrezno obravnavo tveganj (npr. preko obveznih ocen učinkov), ki jih nove predvidene obdelave osebnih podatkov prinašajo.

4. poglavje
Obdelava osebnih podatkov z uporabo biometrije

80. člen (omejitev biometrije)

Predlagamo, da se besedilo 2. odstavka spremeni, tako da glasi:

(2) Obdelava biometričnih osebnih podatkov je dopustna, če je skladna s tem ali drugim zakonom, s pogoji iz drugega odstavka 9. člena Splošne uredbe za obdelavo posebnih vrst osebnih podatkov in dodatnimi omejitvami, določenimi s tem zakonom.

Obrazložitev:

9. člen GDPR že določa primere in namene, za katere je dopustna obdelava posebnih vrst osebnih podatkov. Predlagamo, da se z ustreznim sklicem med namene uvrsti tudi njih.

82. člen (biometrični ukrepi v zasebnem sektorju)

Predlagamo, da se 1. odstavek spremeni, tako da glasi:

(1) Obdelava biometričnih osebnih podatkov v zasebnem sektorju je dopustna pod pogoji tega člena, če je enolična identifikacija posameznika z biometričnimi podatki nujna za varnost ljudi ali premoženja, varovanje tajnih podatkov, varovanje poslovnih skrivnosti oziroma za sklenitev pravnega posla na daljavo.

Predlagamo, da se 2. odstavek spremeni, tako da glasi:

(2) V zasebnem sektorju se lahko obdelujejo biometrični osebni podatki zaposlenih, pogodbenih sodelavcev, zaposlenih pri pogodbenih sodelavcih, strank in posameznikov, katerih istovetnost je nujno ugotoviti z biometričnimi osebnimi podatki že ob njihovi pobudi za sklenitev pravnega posla na daljavo. Pravni temelj je lahko določen z zakonom, pogodbo ali izrecno privolitvijo posameznika. Kadar se biometrični osebni podatki obdelujejo na podlagi pogodbe s posameznikom, ki je potrošnik, mora upravljavec posamezniku, na katerega se nanašajo osebni podatki, omogočiti tudi identifikacijo brez obdelave biometričnih osebnih podatkov.

Predlagamo, da se 3. odstavek spremeni, tako da glasi:

(3) Poleg primerov iz prejšnjih odstavkov se lahko v zasebnem sektorju biometrični osebni podatki obdelujejo tudi v primeru, da se dejanja obdelave izvajajo na način, ki zagotavlja obdelavo in uporabo teh podatkov posameznika pod njegovih izključnim nadzorom ali njegovo izključno oblastjo ter mu omogoča, da vsakokrat izrecno privoli v obdelavo teh podatkov za svojo enolično identifikacijo.

Obrazložitev:

Če bo obdelavo biometričnih podatkov določil drug zakon, bo le-ta določil tudi namene. Vnaprejšnje omejevanje le-teh lahko privede do pravnih nejasnosti v primeru nasprotujočih si določb v predpisih. Obenem pa pretirano omejevanje uporabe biometričnih podatkov ni primerno, niti potrebno v primerih, ko ima posameznik nadzor nad temi podatki – in se le ti praviloma uporabljajo za zagotovitev večje varnosti posameznika ali boljše uporabniške izkušnje (npr. zaklepanje telefonov s prstnim odtisom).

9. poglavje
Obdelava kontaktnih podatkov in osebnih dokumentov

92. člen (obdelava osebnih podatkov za izvajanje določenih dejavnosti osebe javnega ali zasebnega sektorja)

Primarno predlagamo, da se 92. člen v celoti briše.

Podredno predlagamo, da se iz naslova 92. člena za besedo »javnega« nadaljnje besedilo ”ali zasebnega” briše. Prav tako podredno predlagamo, da se v prvem odstavku 92. člena v prvem stavku za besedo »javnega« izpusti besedilo »ali zasebnega«.

Obrazložitev k primarnemu predlogu korekcije:

Pravne podlage za obdelavo osebnih podatkov so že določene v prvem odstavku 6. člena GDPR. Državam članicam ni dano pooblastilo, da navedene pravne podlage širijo.

Obrazložitev k podrednemu predlogu korekcije:

Kot izhaja iz III. Obrazložitve Predloga zakona o varstvu osebnih podatkov (ZVOP-2), vezanega na 92. člen, je sporno določilo 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 ipd.). Tako predlagana določba tudi vsebinsko ureja ustrezno pravno podlago za obdelavo podatkov za predvidene namene za javni sektor.

Zasebni sektor lahko izvaja obdelave podatkov predvidene v tem členu na podlagi pravnih podlag določenih v 6. členu GDPR. Omejitve, določene v predlagani določbi, so za zasebni sektor neutemeljene. Niti iz obrazložitve ni nikjer razvidno, zakaj bi bilo takšno omejevanje pravic, kot jih ima zasebni sektor v skladu s GDPR, primerno in nujno.

Sporna določba je tudi v nasprotju z 158/VI členom ZEKom-1, po katerem je dovoljena uporaba

elektronskih naslovov, ki jih pravne osebe javno objavijo kot svoj kontaktni naslov, tudi v primeru, ko je ta elektronski naslov, naslov fizične osebe (in posledično osebni podatek).

Obenem je sporna določba napisana tako splošno, da je v primeru veljavnosti tudi za zasebni sektor, lahko tudi v nasprotju z 158/II členom ZEKom-1, po katerem je dovoljena uporaba elektronskih naslovov kupcev za neposredno trženje svojih podobnih izdelkov ali storitev pod pogojem, da je kupcu ponujena jasna in izrecna možnost, da brezplačno in enostavno zavrne takšno uporabo svojega elektronskega naslova.

93. člen (obdelava osebnih podatkov iz uradnega identifikacijskega dokumenta)

Prvi odstavek se spremeni, tako da glasi:

(1) Upravljavec osebnih podatkov lahko pred vnosom v zbirko osebnih podatkov preveri točnost osebnih podatkov z vpogledom v uradni identifikacijski dokument posameznika, na katerega se nanašajo.

Drugi odstavek se v celoti briše.

Tretji odstavek postane drugi odstavek.

Obrazložitev:

Zaradi zagotavljanja točnosti osebnih podatkov, ki je eno od temeljnih načel GDPR (točka (d) prvega odstavka 5. člena GDPR), naj bo možnost preverbe identitete posameznika zagotovljena vsem subjektom, ki bodo osebne podatke obdelovali (in ne le tistim, ki izvajajo z zakonom predpisano nalogo). Omejitev možnosti glede prepisovanja, kopiranja ali drugega načina obdelave zgolj na upravljavca, ki izvaja z zakonom predpisano nalogo, kot to izhaja iz drugega odstavka predloga 93. člena ZVOP-2, je v nasprotju z veljavno zakonodajo. Slednja namreč omogoča takšno obdelavo, če posameznik s takšno obdelavo soglaša (možna podlaga torej ni le zakon).

Predlagana sprememba določbe, na način, da je le-ta enaka določbi drugega odstavka 18. člena ZVOP-1, je edina smotrna, saj bo zgolj na ta način upravljavcu v vseh primerih, ne zgolj omejeno na izvajanje zakonskih pooblastil, omogočeno preverjanje točnosti podatkov. V nasprotnem primeru obstoji velika možnost, da posredovani podatki ne bodo točni in bo lahko prihajalo do zlorab.

III. DEL
KAZENSKE DOLOČBE

Splošna pripomba glede členov od 97. do 112. člena:

Določanje spodnje meje globe ni skladno z določbami GDPR, ki jih država članica ne sme uporabiti drugače, kot so urejene v navedenem predpisu. Zato predlagamo, da se najnižja globa za kršitve določb 97. do 112. člena ne določi, ampak da se določi zgolj zgornja višina globe. Le na tak način bo ureditev iz zakona sledila rešitvi iz GDPR. Pri tem se sklicujemo na prvi odstavek

94. člena, ki pravi, da se sankcije za kršitve, ki jih predpisuje GDPR, izrekajo pravnim osebam, samostojnim podjetnikom posameznikom in posameznikom, ki opravljajo dejavnost kot globe za prekrške, v višini in razponih, kot jih določa GDPR. Spodnje meje razpona glob za storilca prekrškov pravno osebo, samostojnega podjetnika posameznika ali posameznika, ki samostojno opravlja dejavnost, sistemsko določata druga in tretja alineja drugega odstavka 17. člena Zakona o prekrških (Uradni list RS, št. 29/11, s spremembami in dopolnitvami, ZP-1), in sicer v višini 200 eurov za vse tri kategorije storilcev prekrškov. Zaradi navedenega menimo, da ni utemeljeno, da se spodnja meja glob določa z ZVOP-2 (niti za pravne osebe, niti za odgovorne osebe in posameznike). Izpostavljamo tudi uvodni recital 149 GDPR, ki določa, da »*bi morale države članice imeti možnost, da določijo pravila o kazenskih sankcijah za kršitve te uredbe, tudi za kršitve nacionalnih pravil, sprejetih v skladu s to uredbo in v mejah te uredbe*«. Menimo torej, da ne obstaja utemeljen razlog za določitev najnižje globe v primeru kršitve nacionalnih določb (tj. od člena 97 do 112). Poudarjamo tudi, da so najnižje globe za primere kršitev nacionalnih določb določene višje (pri večini primerov celo nesorazmerno višje) glede na najnižjo globo, ki bi se lahko po Zakonu o prekrških izrekla za kršitev določb GDPR. Zaradi navedenega torej predlagamo, da se uporabi enak način določitve glob skozi celoten III. del zakona, in sicer s sklicevanjem na ZP-1. ZVOP-2 naj torej predvidi globe na način, da bo nadzorni organ pri odmeri globe lahko v vseh primerih uporabil tudi najnižje globe, kot so le-te določene v drugem odstavku 17. člena Zakona o prekrških[5].

S spoštovanjem,

Nenad Šutanovac
Direktor Združenja za informatiko in telekomunikacije

Poslano naslovniku na e-naslov: gp@dz-rs.si

Poslano na elektronske naslove poslanskih skupin.

Priloga: - kot navedeno v dopisu

[5] Z zakonom ali z uredbo Vlade Republike Slovenije se lahko predpiše globa v razponu:
- za posameznika od 40 do 5.000 eurov;
- za samostojnega podjetnika posameznika in posameznika, ki samostojno opravlja dejavnost, od 200 do 150.000 eurov;
- za pravno osebo od 200 do 250.000 eurov, če se pravna oseba po zakonu, ki ureja gospodarske družbe, šteje za srednjo ali veliko gospodarsko družbo, pa od 400 do 500.000 eurov;
- za odgovorno osebo pravne osebe ali odgovorno osebo samostojnega podjetnika posameznika oziroma posameznika, ki samostojno opravlja dejavnost in za odgovorno osebo v državnem organu ali v samoupravni lokalni skupnosti od 40 do 10.000 eurov.