



Župančičeva 3, 1000 Ljubljana

T: 01 369 53 42

F: 01 369 57 83

E: gp.mp@gov.si

Številka: 007-318/2017

Ljubljana, dne 13. 3. 2018

EVA 2017-2030-0039

GENERALNI SEKRETARIAT VLADE REPUBLIKE SLOVENIJE

Gp.gs@gov.si

**ZADEVA: Predlog Zakona o varstvu osebnih podatkov – predlog
za obravnavo – nujni postopek**

1. Predlog sklepov vlade:

Na podlagi drugega odstavka 2. člena Zakona o Vladi Republike Slovenije (Uradni list RS, št. 24/05 – uradno prečiščeno besedilo, 109/08, 38/10 – ZUKN, 8/12, 21/13, 47/13 – ZDU-1G in 65/14) je Vlada Republike Slovenije na ... seji dne... sprejela naslednji sklep:

Vlada Republike Slovenije je določila besedilo predloga Zakona o varstvu osebnih podatkov (EVA 2017-2030-0039) in ga predloži Državnemu zboru Republike Slovenije v obravnavo po nujnem postopku.

mag. Lilijana KOZLOVIČ
GENERALNA SEKRETARKA

Prejmejo:

- Državni zbor Republike Slovenije,
- Ministrstvo za pravosodje,
- Služba Vlade Republike Slovenije za zakonodajo.

2. Predlog za obravnavo predloga zakona po nujnem ali skrajšanem postopku v državnem zboru z obrazložitvijo razlogov:

Predlagana je obravnava predloga Zakona o varstvu osebnih podatkov (ZVOP-2) po nujnem zakonodajnem postopku, v skladu s prvim odstavkom 143. člena Poslovnika Državnega zbora, v delu, ki se nanaša na preprečitev težko popravljivih posledic za delovanje države. V primeru nesprejetja ZVOP-2 do 25. 5. 2018 za delovanju države, kolikor le-ta nastopa kot upravljavec ali obdelovalec osebnih podatkov ali pa jih čezmejno posreduje (npr. kazensko-pravosodnem in policijskem področju), ne bodo dovolj jasno zagotovljene pravne podlage za obdelavo osebnih podatkov, obdelave osebnih podatkov v druge (nove) namene ter dovolj pravno varno zagotovljeno izvajanje inšpekcijskih nadzorov s področja varstva osebnih podatkov ter povezano prekrškovno kaznovanje (po globah iz Splošne uredbe o varstvu podatkov Evropski unije, ki so izredno visoke) – kar pomeni kršitev pravne varnosti in zakonitosti, pa tudi kršitve s področja človekovih pravic. V zvezi z izvedbenimi zakoni držav članic EU po Splošni uredbi o varstvu osebnih podatkov Evropske unije iz leta 2016 ter povezani Direktive EU iz istega leta sicer v Evropski uniji obstaja splošna pravna nevarnost, saj so bili dosedaj sprejeti le trije izvedbeni zakoni (Avstrija, Nemčija, Slovaška), ostali se bodo pretežno in predvidoma sprejeli v marcu, aprilu, maju 2018, ko poteče rok za njuno uveljavitev.

3.a Osebe, odgovorne za strokovno pripravo in usklajenost gradiva:

- mag. Goran Klemenčič, minister za pravosodje,
- Darko Stare, državni sekretar,
- Tina Breclj, državna sekretarka,
- mag. Nina Koželj, v.d. generalne direktorice Direktorata za kaznovalno pravo in človekove pravice
- Peter Pavlin, višji sekretar, Direktorat za kaznovalno pravo in človekove pravice
- Igor Kolar, svetovalec, Direktorat za kaznovalno pravo in človekove pravice

3.b Zunanji strokovnjaki, ki so sodelovali pri pripravi dela ali celotnega gradiva:

Pri pripravi dela ali celotnega gradiva zunanji strokovnjaki niso sodelovali.

4. Predstavniki vlade, ki bodo sodelovali pri delu državnega zbora:

- mag. Goran Klemenčič, minister za pravosodje,
- Darko Stare, državni sekretar,
- Tina Breclj, državna sekretarka,
- mag. Nina Koželj, v.d. generalne direktorice Direktorata za kaznovalno pravo in človekove pravice
- Peter Pavlin, višji sekretar, Direktorat za kaznovalno pravo in človekove pravice
- Igor Kolar, svetovalec, Direktorat za kaznovalno pravo in človekove pravice

5. Kratek povzetek gradiva:

S predlaganim novim Zakonom o varstvu osebnih podatkov (ZVOP-2) se na sistemski ravni na novo urejajo pravice, obveznosti, postopki, nadzorne pristojnosti ter druga sistemska (pa tudi področna) vprašanja obdelave in varstva osebnih podatkov.

Pravne podlage za obdelavo osebnih podatkov so še vedno jasno razdelane, kot so bile v ZVOP-1, še vedno je pomemben koncept »zakona« - ni okrnjena urejevalna ali nadzorna pristojnost Državnega zbora RS. Prav tako Predlog ZVOP-2 še vedno izhaja iz spoštovanja človeka kot nosilca pravic s področja varstva osebnih podatkov.

Znatno je spremenjena definicija privolitve posameznika za obdelavo njegovih ali njenih osebnih podatkov, ki je bližja dosedanji definiciji posebne privolitve za obdelavo občutljivih osebnih podatkov.

Na novo so razdelane definicije in obdelave v zvezi s posebnimi vrstami osebnih podatkov (dosedaj: občutljivi osebni podatki), vključno s pravnimi podlagami za obdelavo. Od posebnih vrst osebnih podatkov so sedaj ločene pravne podlage glede obdelave osebnih podatkov o kazenskih obsodbah ter o kaznovanjih za prekrške, vendar se pravila varnosti osebnih podatkov (dosedanje zavarovanje osebnih podatkov) s področja posebnih vrst osebnih podatkov uporabljajo tudi za njih.

Pomembno je tudi, da je določena nova ureditev glede drugih (dosedaj: naknadnih) namenov obdelave osebnih podatkov, po predlagani ureditvi – v skladu s Splošno uredbo – so drugi (novi) nameni obdelave osebnih podatkov sedaj širši in je upoštevanje prvotnega namena zbiranja in obdelave osebnih podatkov nekoliko manj pomembno.

Za namene izkazovanja skladnosti obdelave osebnih podatkov je kot obveznost za upravljavce in obdelovalce določena izvedba ocene učinkov.

Določena je nova ureditev za osebe, ki znotraj upravljavcev ali obdelovalcev zagotavljajo varstvo osebnih podatkov, zlasti ko gre za tvegane ali množične obdelave osebnih podatkov, namreč vzpostavitev pooblaščenih oseb za varstvo osebnih podatkov (*»data protection officers«*). Ne uvaja se reguliran poklic, ampak določajo neodvisne osebe znotraj upravljavca ali obdelovalca, ki naj svetujejo glede skladnosti varstva osebnih podatkov. Glede pooblaščenih oseb za varstvo osebnih podatkov je predlagana ureditev dokaj »odprte narave«, tako z vidika dejanske usposobljenosti niso zahtevane delovne izkušnje samo s področja varstva osebnih podatkov, ampak tudi npr. s področja bančništva (zaupne informacije), omogočena lažjo izbiro javnemu sektorju (razen ministrstev), da jih pridobijo tudi iz zasebnega sektorja (najem fizične ali pravne osebe), omogočena je lažja izbira iz širšega kroga oseb občinam, sodelovanje preko medobčinskih uprav in najetje zunanjega izvajalca (zasebni sektor), prav tako je podana posebna centralizirana ureditev za sodišča in državna tožilstva, možno je pa tudi določiti namestnika pooblaščenih oseb. Določena je tudi možnost, da imajo lahko organi v sestavi lastno pooblaščenno osebo.

Prav tako je glede na predloge prakse v ZVOP-2 še vedno urejeno neposredno trženje, četudi je z vidika Splošne uredbe morda nekoliko sporno – stališče, da je bolje regulirati, kot prepustiti nejasni praksi, ki lahko področje čisto odpre ali pa pride do prepovedi.

Ni spremenjen položaj samostojnega in neodvisnega nadzornega organa za varstvo osebnih podatkov – Informacijski pooblaščenec – razen tega, da so določene izjeme v smeri, kjer je to glede na Splošno uredbo ali »naravo stvari« dopustno, npr. ne sme se posegati v neodvisnost sodstva, ne sme biti nadzorov tudi tam, kjer jih Državni zbor izjemoma ne izvaja (Komisija za nadzor obveščevalno-varnostnih služb) ipd..

Zelo so z vidika pravne jasnosti okrepljene obstoječe določbe ali določene nove določbe, kdaj Informacijski pooblaščenec ne ukrepa nadzorno – kadar bi šlo za neprimeren ali neustaven poseg v prostorsko ali komunikacijsko zasebnost ali svobodo izražanja z vidika varstva osebnih podatkov.

6. Presoja posledic za:		
a)	javnofinančna sredstva nad 40.000 EUR v tekočem in naslednjih treh letih	DA
b)	usklajenost slovenskega pravnega reda s pravnim redom Evropske unije	DA
c)	administrativne posledice	DA
č)	gospodarstvo, zlasti mala in srednja podjetja ter konkurenčnost podjetij	DA
d)	okolje, vključno s prostorskimi in varstvenimi vidiki	NE
e)	socialno področje	NE
f)	dokumente razvojnega načrtovanja: – nacionalne dokumente razvojnega načrtovanja – razvojne politike na ravni programov po strukturi razvojne klasifikacije programskega proračuna – razvojne dokumente Evropske unije in mednarodnih organizacij	NE
7.a Predstavitev ocene finančnih posledic nad 40.000 EUR: (Samo če izberete DA pod točko 6.a.)		

I. Ocena finančnih posledic, ki niso načrtovane v sprejetem proračunu				
	Tekoče leto (t)	t + 1	t + 2	t + 3
Predvideno povečanje (+) ali zmanjšanje (–) prihodkov državnega proračuna				
Predvideno povečanje (+) ali zmanjšanje (–) prihodkov občinskih proračunov				
Predvideno povečanje (+) ali zmanjšanje (–) odhodkov državnega proračuna				
Predvideno povečanje (+) ali zmanjšanje (–) odhodkov občinskih proračunov				
Predvideno povečanje (+) ali zmanjšanje (–) obveznosti za druga javnofinančna sredstva				
II. Finančne posledice za državni proračun				
II.a Pravice porabe za izvedbo predlaganih rešitev so zagotovljene:				
Ime proračunskega uporabnika	Šifra in naziv ukrepa, projekta	Šifra in naziv proračunske postavke	Znesek za tekoče leto (t)	Znesek za t + 1
Informacijski pooblaščenec (šifra: 12157)		1267 1273 1271	Skupno: 463,800,00 EUR	Skupno: 359.600,00 EUR
SKUPAJ			463,800,00 EUR	359.600,00 EUR
II.b Manjkajoče pravice porabe bodo zagotovljene s prerazporeditvijo:				
Ime proračunskega uporabnika	Šifra in naziv ukrepa, projekta	Šifra in naziv proračunske postavke	Znesek za tekoče leto (t)	Znesek za t + 1
SKUPAJ				
II.c Načrtovana nadomestitev zmanjšanih prihodkov in povečanih odhodkov proračuna:				

Novi prihodki	Znesek za tekoče leto (t)	Znesek za t + 1
SKUPAJ		

OBRAZLOŽITEV:

I. Ocena finančnih posledic, ki niso načrtovane v sprejetem proračunu

V zvezi s predlaganim vladnim gradivom se navedejo predvidene spremembe (povečanje, zmanjšanje):

- prihodkov državnega proračuna in občinskih proračunov,
- odhodkov državnega proračuna, ki niso načrtovani na ukrepih oziroma projektih sprejetih proračunov,
- obveznosti za druga javnofinančna sredstva (drugi viri), ki niso načrtovana na ukrepih oziroma projektih sprejetih proračunov.

II. Finančne posledice za državni proračun

Prikazane morajo biti finančne posledice za državni proračun, ki so na proračunskih postavkah načrtovane v dinamiki projektov oziroma ukrepov:

II.a Pravice porabe za izvedbo predlaganih rešitev so zagotovljene:

Navedejo se proračunski uporabnik, ki financira projekt oziroma ukrep; projekt oziroma ukrep, s katerim se bodo dosegli cilji vladnega gradiva, in proračunske postavke (kot proračunski vir financiranja), na katerih so v celoti ali delno zagotovljene pravice porabe (v tem primeru je nujna povezava s točko II.b). Pri uvrstitvi novega projekta oziroma ukrepa v načrt razvojnih programov se navedejo:

- proračunski uporabnik, ki bo financiral novi projekt oziroma ukrep,
- projekt oziroma ukrep, s katerim se bodo dosegli cilji vladnega gradiva, in
- proračunske postavke.

Za zagotovitev pravic porabe na proračunskih postavkah, s katerih se bo financiral novi projekt oziroma ukrep, je treba izpolniti tudi točko II.b, saj je za novi projekt oziroma ukrep mogoče zagotoviti pravice porabe le s prerazporeditvijo s proračunskih postavk, s katerih se financirajo že sprejeti oziroma veljavni projekti in ukrepi.

II.b Manjkajoče pravice porabe bodo zagotovljene s prerazporeditvijo:

Navedejo se proračunski uporabniki, sprejeti (veljavni) ukrepi oziroma projekti, ki jih proračunski uporabnik izvaja, in proračunske postavke tega proračunskega uporabnika, ki so v dinamiki teh projektov oziroma ukrepov ter s katerih se bodo s prerazporeditvijo zagotovile pravice porabe za dodatne aktivnosti pri obstoječih projektih oziroma ukrepih ali novih projektih oziroma ukrepih, navedenih v točki II.a.

II.c Načrtovana nadomestitev zmanjšanih prihodkov in povečanih odhodkov proračuna:

Če se povečani odhodki (pravice porabe) ne bodo zagotovili tako, kot je določeno v točkah II.a in II.b, je povečanje odhodkov in izdatkov proračuna mogoče na podlagi zakona, ki ureja izvrševanje

državnega proračuna (npr. priliv namenskih sredstev EU). Ukrepanje ob zmanjšanju prihodkov in prejemkov proračuna je določeno z zakonom, ki ureja javne finance, in zakonom, ki ureja izvrševanje državnega proračuna.

7.b Predstavitev ocene finančnih posledic pod 40.000 EUR:

8. Predstavitev sodelovanja z združenji občin:

Vsebina predloženega gradiva (predpisa) vpliva na:

- pristojnosti občin,
- delovanje občin,
- financiranje občin.

DA

Gradivo (predpis) je bilo poslano v mnenje:

- Skupnosti občin Slovenije SOS: **DA**
- Združenju občin Slovenije ZOS: **DA**
- Združenju mestnih občin Slovenije ZMOS: **NE**

(so se pa določene mestne občine seznanile z vsebino predloga ZVOP-2 in poslale pripombe)

9. Predstavitev sodelovanja javnosti:

Gradivo je bilo predhodno objavljeno na spletni strani predlagatelja:

DA

Datum objave:

– 3. 10. 2017 in 23. 1. 2018

Predlog osnutka zakona je bil za Javno razpravo dne 3. 10. 2017 z namenom posvetovanja s širšo (splošno) javnostjo in strokovno javnostjo objavljen na spletni strani Ministrstva za pravosodje – prvi krog Javne razprave. V drugi krog Javne razprave je bil predlog zakona posredovan dne 23. 1. 2018, z rokom za pripombe 2. 2. 2018.

Precejšnje število pripomb iz prakse (gospodarstva) je bilo upoštevanih, zlasti glede urejanja pooblaščenih oseb za varstvo osebnih podatkov, neposrednega trženja, hierarhije in jasnosti predlaganih norm (zlasti glede pravnih podlag za obdelavo osebnih podatkov). Enako velja za pripombe občin, ki se tičejo stroškov glede pooblaščenih oseb za varstvo osebnih podatkov – pogoji za izbiro, določitev in sodelovanje so sedaj znatno olajšani (prilagojeni na specifiko občin).

Predlog ZVOP-2 je bil nato posredovan v strokovno in medresorsko usklajevanje:

– 23. 1. 2018

Strokovno in medresorsko usklajevanje je trajalo od 23. 1. 2018 do 2. 2. 2018, dejansko pa vsaj do 9. 2. 2018, ko so bile prejete še zadnje pomembnejše pripombe.

Strokovno usklajevanje:

Bistvene pripombe Vrhovnega sodišča Republike Slovenije ter Vrhovnega državnega tožilstva Republike Slovenije so bile sprejete, dne 12. 3. 2018 smo pa prejeli še stališča Vrhovnega sodišča Republike Slovenije o novi področni ureditvi – »Pravosodni supervizor«, ki je v proučevanju in bo ustrezno vključeno v bodoče Novo gradivo št. 1. Določene bistvene pripombe Informacijskega pooblaščenca z dne 8. 3. 2018 so še v preučevanju, uskladitev ali opredelitev glede njih bo izvedena dokončno do 14. 3. 2018. Z Varuhom človekovih pravic je Predlog ZVOP-2 v tej fazi usklajen. S Službo Vlade RS za zakonodajo usklajevanja še potekajo (9.3.2018, 12.3.2018, 13.3.2018).

10. Pri pripravi gradiva so bile upoštevane zahteve iz Resolucije o normativni dejavnosti:

DA

11. Gradivo je uvrščeno v delovni program vlade:

DA

Mag. Goran Klemenčič
minister

Priloge:

- predlog Zakona o varstvu osebnih podatkov,
- obrazložitev členov.

PREDLOG ZAKONA O VARSTVU OSEBNIH PODATKOV (ZVOP-2)

I. UVOD

1. OCENA STANJA IN RAZLOGI ZA SPREJEM PREDLOGA ZAKONA

Predlog Zakona o varstvu osebnih podatkov (ZVOP-2) je pripravljen kot del novega razvoja zagotavljanja sistema in pravic s področja varstva osebnih podatkov v Republiki Sloveniji. Po letu 2004, ko je bil sprejet dosedaj že tretji slovenski Zakon o varstvu osebnih podatkov (ZVOP-1)¹, se je namreč nadaljeval tehnološki razvoj na področju varstva osebnih podatkov, osebni podatki pa so kot informacije preko sredstev elektronskih komunikacij postali vse bolj (in vse bolj) trajneje javno dostopni ali dostopni širšemu krogu državnih in drugih organov, zasebnemu sektorju, javnosti, posameznikom in posameznicam, izvajale so se vse bolj sistemske povezave med zbirkami osebnih podatkov, razvila se je tudi dodatna močnejša sodna praksa Sodišča Evropske unije in Evropskega sodišča za človekove pravice glede varstva osebnih podatkov.

Glede na navedene razvoje je leta 2012 Evropska komisija predlagala dva nova pravna akta Evropske unije kot del ti. »paketa reforme varstva osebnih podatkov«, namreč »Predlog Uredbe Evropskega parlamenta in Sveta o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem pretoku takih podatkov ter o razveljavitvi Direktive 95/46/ES (Splošna uredba o varstvu podatkov)«² ter »Predlog Direktive Evropskega parlamenta in Sveta 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«³.

1.1. Ocena stanja

1.1.1 Pregled normativnega urejanja v Republiki Sloveniji in na ravni Evropske unije

V času vložitve predlogov navedenih pravnih aktov je Republike Slovenije imela sistem varstva osebnih podatkov urejen v skladu z določbami 38. člena Ustave Republike Slovenije⁴, Direktive

¹ Prvi Zakon o varstvu osebnih podatkov Republike Slovenije je bil sprejet dne 7. 3. 1990 (Uradni list RS, št. 8/90, 19/91 in 59/99 - ZVOP), drugi Zakon o varstvu osebnih podatkov je bil sprejet dne 8. 7. 1999 (Uradni list RS, št. 59/99, 57/01, 59/01 – popr., 73/04 – ZUP-C in 86/04 – ZVOP-1), tretji Zakon o varstvu osebnih podatkov pa dne 15. 7. 2004 (Uradni list RS, št. 86/04, 113/05 – ZInfP, 51/07 – ZUstS-A, 67/07 in 94/07 – uradno prečiščeno besedilo 1).

² Št. 5853/12, 27.01.2012, Medinstitucionalna oznaka: 2012/0011(COD).

³ Št. 5833/12, 27.01.2012, Medinstitucionalna oznaka: 2012/0010(COD).

⁴ Takrat z vsebino, objavljeno v: Uradni list RS, št. 33/91-I, 42/97, 66/00, 24/03, 69/04 in 68/06.

95/46/ES⁵, Okvirnega sklepa 2008/977/PNZ⁶ in Konvencije o varstvu posameznikov glede na avtomatsko obdelavo osebnih podatkov⁷ (Sveta Evrope).

Republika Slovenija je iz načelnih sistemskih razlogov (pravna varnost, možnost znižanja dosežene visoke ravni varstva osebnih podatkov, pretirane obveznosti za upravljavce osebnih podatkov – tudi finančne, očitno pretirane globe za upravne kršitve, nato pretirana pooblastila Evropski komisiji glede izdaje izvedbenih in delegiranih aktov, izbira vrste pravnega akta v primeru predloga Splošne uredbe, ustreznost takratnega Okvirnega sklepa 2008/977/PNZ ipd.) navedenima predlogoma pretežno ali v celoti nasprotovala⁸, ob tem pa navedla tudi vrsto posebej obrazloženih pridržkov. Glede takratnega Predloga Splošne uredbe o varstvu podatkov je bil bistveni zaključek iz stališča Republike Slovenije, poleg želje za spremembo vrste pravnega akta iz uredbe v direktivo – da se mora Republika Slovenija v pogajanjih v okviru Sveta Evropske unije prizadevati, da »ne bi prišlo do neutemeljenega zniževanja standardov varstva osebnih podatkov, ki bi bili nižji glede na primerljivi kazalnik – »Direktivo 95/46/ES o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem pretoku takih podatkov««, glede predloga Direktive pa, da zadošča vsebina določb takrat veljavnega Okvirnega sklepa 2008/977/PNZ iz leta 2008 in da torej sprejetje predlagane Direktive ni potrebno.

Glede vsebine Predloga Splošne uredbe so se pojavili ustavnopravni pomisleki tudi v Zvezni republiki Nemčiji, tako je leta 2012 nemški zvezni ustavni sodnik Johannes Masing objavil članek⁹, v katerem je z vidika nemškega Temeljnega zakona (Ustava) in obširne in ustaljene ustavnosodne presoje nemškega Zveznega Ustavnega sodišča izredno kritično nastopil proti Osnutku Splošne uredbe o varstvu podatkov. V članku je med drugim navedeno, da gre za neustaven in nesmiseln odvzem pristojnosti, da se ne upošteva, da je pravica do varstva osebnih podatkov individualna človekova pravica, ki izhaja iz nacionalnih Ustav, da se po njenem morebitnem sprejetju ne bo dalo več z nacionalnimi zakoni sploh (kaj več kot minimalno) regulirati osebnih podatkov... – ter da bo dosedanja ustaljena ustavnosodna presoja nemškega Zveznega Ustavnega sodišča torej šla kar v »razrez« (v »makulaturo«).

V nadaljnjih pogajanjih v okviru Sveta Evropske unije se je vsebina določb obeh predlogov pravnih aktov razdelovala in doseženi so bili tudi določeni kompromisi, ki so na koncu privedli do sprejetja obeh navedenih pravnih aktov dne 27. aprila 2016. Tako sta bili navedenega dne sprejeti »**Uredba (EU) 2016/679 Evropskega parlamenta in Sveta z dne 27. aprila 2016 o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem pretoku takih podatkov ter o razveljavitvi Direktive 95/46/ES (Splošna uredba o varstvu podatkov)**«¹⁰ – v nadaljnjem besedilu: Splošna uredba ter »**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**«¹¹ – v nadaljnjem besedilu: Direktiva.

⁵ Direktiva Evropskega parlamenta in Sveta 95/46/ES z dne 24. oktobra 1995 o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem pretoku takih podatkov, Uradni list EGS, L 281, 23. 11. 1995, str. 0031 – 0050 in Uradni list EU, L 284, 31. 10. 2003, str. 1–53 – Uredba (ES) št. 1882/2003.

⁶ Okvirni sklep Sveta 2008/977/PNZ z dne 27. novembra 2008 o varstvu osebnih podatkov, ki se obdelujejo v okviru policijskega in pravosodnega sodelovanja v kazenskih zadevah, Uradni list EU, L 350, 30. 12. 2008, str. 60–71.

⁷ Konvencija Sveta Evrope, h kateri lahko pristopijo tudi države izven Evrope. Oznaka Sveta Evrope za Konvencijo: ETS No. 108. Objava: Uradni list RS, št. 11/94 – Mednarodne pogodbe, št. 3/94 in 86/04 – ZVOP-1.

⁸ Stališči Državnega zbora Republike Slovenije z dne 23. 3. 2012, št. EPA 191-VI, EU U 393 in št. EPA 192-VI, EU U 394.

⁹ Masing, Johannes, Prof. dr., *Ein Abschied von den Grundrechten : Die Europäische Kommission plant per Verordnung eine ausnehmend problematische Neuordnung des Datenschutzes*, Suddeutsche Allgemeine Zeitung, 9. 1. 2012. Še podrobnejša kritika in analiza vsebinskega pristopa glede takratnega Predloga Splošne uredbe, zlasti z vidikov ustavnosti, je podana v: Masing, Johannes, Prof. dr., *Herausforderungen des Datenschutzes*, Neue Juristische Wochenschrift, 2012, str. 2305-2311.

¹⁰ Uradni list EU, L, št. 119/1 z dne 4. 5. 2016, str. 1–88.

¹¹ Uradni list EU, L, št. 119/89 z dne 4. 5. 2016, str. 89–131.

Z vidika končnega rezultata je možno oceniti, da določbe v Splošni uredbi o namenih obdelave osebnih podatkov (naknadna obdelava podatkov v druge namene, kot so bili prvotno zbrani) ter o pooblaščenih osebah morda pomenijo določeno stopnjo znižanja dosežene ravni varstva osebnih podatkov, da pa ima po drugi strani Splošna uredba v precejšnjem delu pomen ti. »direktivnega akta«¹², kot da bi bila direktiva Evropske unije. Kar pomeni, da je možno precej določb Splošne uredbe implementirati v slovenskih zakonih, z ozirom na konkretne okoliščine stanja ali razvoja varstva osebnih podatkov v Sloveniji. Delno podobno je glede sprejete Direktive, kar se tiče sistema določitve namenov obdelav osebnih podatkov (naknadna obdelava podatkov v druge namene, kot so bili prvotno zbrani) in tudi njene določbe je možno v zakonih Republike Slovenije izvesti glede na konkretne okoliščine stanja varstva osebnih podatkov v Sloveniji.

1.2 Razlogi za sprejem zakona

Glede na navedene ugotovitve je pripravljeno besedilo Predloga Zakona o varstvu osebnih podatkov (ZVOP-2), ki pa pri tem ustrezno upošteva tudi izkušnje in spoznanja glede uporabe dosedanjega ZVOP-1 iz leta 2004, določbe 38. člena Ustave Republike Slovenije o človekovi pravici do varstva osebnih podatkov¹³, obstoječo ustavnosodno presojo Ustavnega sodišča Republike Slovenije glede človekove pravice do varstva osebnih podatkov od leta 1992¹⁴ dalje ter tudi določbe še veljavne (še nespremenjene) Konvencije o varstvu posameznikov glede na avtomatsko obdelavo osebnih podatkov.

2. CILJI, NAČELA IN POGLAVITNE REŠITVE PREDLOGA ZAKONA

2.1 Cilji Predloga ZVOP-2

Cilji Predloga Zakona o varstvu osebnih podatkov (ZVOP-2) so:

- zagotoviti izvrševanje določb Splošne uredbe in Direktive v pravnem redu Republike Slovenije, tako da bi s sistemskega vidika bilo čim več vprašanj bilo urejeno ali rešeno v sistemskem zakonu s področja varstva osebnih podatkov in tako zagotovljeno uresničevanje osebne človekove pravice do varstva osebnih podatkov (38. člen Ustave Republike Slovenije).

Konkretnije: treba je zagotoviti spoštovanje pravne varnosti (tudi na način, da bi bilo čim več določb »na enem mestu« zaradi učinkovitega uresničevanja osebne človekove pravice do varstva osebnih podatkov), da bi bilo besedilo določb ZVOP-2 čimbolj v pomoč posameznikom, na katere se nanašajo osebni podatki. Izhodišče zakonodajnega urejanja je torej človek in njegove pravice (posameznik ali posameznica, na katerega ali katero se nanašajo osebni podatki),

- omogočiti ljudem (posameznice in posamezniki, na katere se nanašajo osebni podatki) ter javnopravnim organom in poslovnim subjektom (upravljavci in obdelovalci), da so sistemske norme

¹² Glejte tudi: Mnenje Državnega sveta Kraljevine Nizozemske, št. W03.17.0166/II, 10. 10. 2017 (str. 4), kjer je med drugim navedeno, da Splošna uredba ni prava uredba (pomeni: prava; običajna uredba Evropske unije), da ima uredba mešani značaj, da so določeni njeni deli uredbeni, določeni pa direktivni ter da je Splošna uredba (tudi v razmerju do veljavne zakonodaje Kraljevine Nizozemske) zelo zapletena in da glede nadaljnje razdelave v zakonodaji ter v praksi odpira in bo odpirala veliko neodgovorjenih vprašanj.

¹³ Uradni list RS, št. 33/91-I, 42/97, 66/00, 24/03, 69/04, 68/06, 47/13 in 75/16.

¹⁴ Začetna Odločba US, št. U-I-115/92, 24. 12. 1992; objava: OdlUS I, 105 in Uradni list RS, št. 3/93, iz vmesnega obdobja sta morda vodilni odločbi: Odločba US, št. U-I-252/00, 8. 10. 2003; objava: Uradni list RS, št. 105/03 in OdlUS XII, 80 ter Odločba US, št. U-I-298/04, 27. 10. 2005; objava: Uradni list RS, št. 100/05 in OdlUS XIV, 77; iz obdobja po letu 2010 pa sta npr. pomembni: Odločba US, št. U-I-98/11, 26. 9. 2012; objava: Uradni list RS, št. 79/12 in Odločba US, št. U-I-70/12, 21. 3. 2014; objava: Uradni list RS, št. 24/14 in OdlUS XX, 23.

varstva osebnih podatkov čimbolj povezane ali pojasnjevalno predpisane, tako da se omogoči čimbolj koherenten pristop k izvajanju uresničevanja in varstva pravic s področja varstva osebnih podatkov¹⁵.

2.2. Pravni pristop glede zakonske izvedbe obeh pravnih aktov Evropske unije s področja varstva osebnih podatkov

Pri slovenski zakonski izvedbi določb Splošne uredb in Direktive se z vidika pripravljene vsebine Predloga ZVOP-2 izhaja predvsem iz upoštevanja direktivnih določb Splošne uredbe (tako določb členov kot tudi uvodnih navedb), saj ima Splošna uredba tudi naslednje določbe o nacionalnih zakonskih izvedbah Splošne uredbe, namreč uvodna navedba št. 8 navaja, da »Kadar ta uredba določa natančnejše določitve ali omejitve svojih pravil s pravom držav članic, lahko države članice vključijo elemente te uredbe v svoje nacionalno pravo, kolikor je to potrebno zaradi skladnosti in razumljivosti nacionalnih določb za osebe, za katere se uporabljajo.«, nadalje v b) točki prvega odstavka člena 5 Splošne uredbe, da morajo biti osebni podatki »zbrani za določene, izrecne in zakonite namene...«, nadalje v c) in e) točki prvega odstavka člena 6 Splošne uredbe, po katerih je obdelava osebnih podatkov med drugim zakonita, kadar je obdelava potrebna za izpolnitev zakonske obveznosti, ki velja za upravljavca ter je potrebna za opravljanje naloge v javnem interesu ali pri izvajanju javne oblasti, dodeljene upravljavcu, ob tem pa drugi odstavek člena 6 Splošne uredbe med drugim povezano določa, da lahko države članice Evropske unije 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, tako da podrobneje opredelijo posebne zahteve v zvezi z obdelavo ter druge ukrepe za zagotovitev zakonite in poštene obdelave.

Direktiva, ki se načeloma nanaša na področje kaznovalnega delovanja države (kazensko pravosodje in policijsko delovanje) je urejena v posebnem delu (IX. del) Predloga ZVOP-2, pri tem pa splošne določbe iz Predloga ZVOP-2 veljajo tudi za navedena področja iz tega posebnega dela Predloga ZVOP-2 – ob področnih določbah zakonodaje (npr. policijske, državnotožilske, kazensko procesne ipd.).

Ključno glede zakonodajnih rešitev iz Predloga ZVOP-2 je tudi, da je treba upoštevati sistemske določbe Konvencije o varstvu posameznikov glede na avtomatsko obdelavo osebnih podatkov (Sveta Evrope), ki morajo tudi biti izvedene v tem zakonu.

Ključno je tudi, da za vprašanja, kjer ali Splošna uredba ali Direktiva določata izjeme, da določena vprašanja uresničevanja pravice do varstva osebnih podatkov niso zaobsežene v Splošni uredbi ali Direktivi in je to prepuščeno nacionalni zakonodaji (obdelava osebnih podatkov umrlih oseb, obdelava osebnih podatkov v okviru dejavnosti zunaj področja uporabe prava Evropske unije, obdelava osebnih podatkov, s strani Republike Slovenije, kadar deluje na področjih skupne varnostne in obrambne politike ter obveščevalno-varnostne dejavnosti. Ker ima Republika Slovenije že od leta 1990 celoviti (vseobsežni) pristop varstva osebnih podatkov na sistemskem področju (vsakokratni veljavni Zakon o varstvu osebnih podatkov) je treba tudi za ta področja, kolikor so v Sloveniji urejena, določiti uporabo ZVOP-2 (poleg področnih ureditev varstva osebnih podatkov) – zlasti določb o definicijah, pravnih podlagah za obdelavo osebnih podatkov, obdelav osebnih podatkov v druge namene, uporabe načel zakona ipd.

Delno primerljiv zakonodajni pristop, kot je predlagan v Predlogu ZVOP-2, so dosedaj sprejele tudi tri primerljive državi Evropske unije, namreč Zvezna republika Nemčija¹⁶, Republika Avstrija¹⁷ in Slovaška

¹⁵ Tovrsten pristop je tudi upravičen z vidika, da dosedaj sprejeta izvedbena zakonodaja (le) treh držav članic Evropske unije ter da tudi predlogi izvedbene zakonodaje drugih držav članic Evropske unije kažejo, da je vsaka država na svoje specifične izbrala način pravnega urejanja »v lastno smer«, torej se je dejansko zgodil ti. »pristop fragmentacije« (in ne unifikacije ali vsaj harmonizacije) – kot je to izkazano v prikazu primerjalnopravne ureditve.

¹⁶ Zakon o prilagoditvi zakonodaje o varstvu osebnih podatkov Uredbi (EU) 2016/679 in izvajanju Direktive (EU) 2016/680 (Zakon o prilagoditvi in izvajanju zakonodaje o varstvu osebnih podatkov EU; objava: Zakon z dne 30. junija 2017, Bundesgesetzblatt Teil I, 2097.

republika¹⁸ (države s primerljivim pravnim redom in ustavnopravnim oziroma ustavnosodnim razumevanjem pravice do varstva osebnih podatkov) v njihovih novih zakonih o varstvu osebnih podatkov iz leta 2017, namreč dokaj širšo implementacijo določb Splošne uredbe v nacionalni zakonodaji, razširitev določb Splošne uredbe na določena vprašanja, ki jih ureja sicer Direktiva (zaradi pravne varnosti in enakosti), natančnejše ureditve namenov obdelave osebnih podatkov, ureditev posebnih določb Direktive v posebnem delu zakona ipd. Bolj primerljiv slovenskim rešitvam iz Predloga ZVOP-2 je sicer bolj garantistični pristop Slovaške republike, ki je v njenem zakonu med drugim določila celo splošno uporabo (in istočasno neposredno uporabo) temeljnih definicij s področja varstva osebnih podatkov za vsa področja varstva osebnih podatkov iz njenega takratnega Predloga Zakona o varstvu osebnih podatkov in o spremembah in dopolnitvah določenih zakonov (št. UV-42294/2017, z dne 22. 9. 2017, sprejet dne 27. 11. 2017), natančno razdelala zakonska načela, ob tem da je dan poseben poudarek načelu zakonitosti, razdelala institut privolitve ter izgleda pravnosistemsko izhajala iz celovite uporabe pristopa klasičnega mednarodnega zasebnega prava in postopka.

Predlog ZVOP-2 sledi prenovljenemu izrazoslovju Splošne uredbe, npr. uporaba izrazov »zbirka« (dosedaj: zbirka osebnih podatkov), upravljavec (dosedaj: upravljavec zbirke osebnih podatkov), obdelovalec (dosedaj: pogodbeni obdelovalec), varnost osebnih podatkov (dosedaj: zavarovanje osebnih podatkov). Določene pojasnjevalne ali povezovalne spremembe glede teh izrazov so še možne v določenih delih Predloga ZVOP-2, odvisno od nadaljnjega proučevanja in razprav.

Prav tako utegne na dokončnejšo vsebino bodočega ZVOP-2 vplivati tudi dejstvo, da je predvidena objava popravkov uradne slovenske inačice besedil Splošne uredbe in Direktive šele v maju 2018, kar velja tudi za večino drugih jezikovnih inačic Splošne uredbe in Direktive. Vpliv na določbe Predloga ZVOP-2 utegne biti še nekoliko širši, saj utegnejo biti spremenjene tudi inačici besedil Splošne uredbe in Direktive v angleški jezikovni inačici, kar ni bilo pričakovano. Z vidika pravne varnosti bodo spremembe v slovenski (morda tudi angleški) inačici obeh besedil pravnih aktov Evropske unije lahko upoštevane le v zakonodajnem postopku v Državnem zboru RS, saj bodo objavljene v Uradnem listu Evropske unije predvidoma šele maja 2018.

Glede na posebno kombinacijo in vsebino pravnih aktov Evropske unije, ki zahtevajo spremembe na področju sistemske ureditve varstva osebnih podatkov, delno prilagojeno »filozofijo« varstva osebnih podatkov glede na te pravne akte, relevantno Konvencijo Sveta Evrope, pomen zlasti določb 38. in 87. člena Ustave Republike Slovenije ter povezane ustaljene ustavnosodne presoje Ustavnega sodišča Republike Slovenije in tradicijo zakonodajnega urejanja varstva osebnih podatkov v Republiki Sloveniji predlagatelj ocenjuje, da je bila edina možnost, da se pripravi nov Zakon o varstvu osebnih podatkov, ki bi omogočal povezan in čimbolj koherenten pristop glede vseh teh vsebin in njihovih zahtev. Teh vsebin in zahtev ne bi bilo možno doseči z novelo veljavnega ZVOP-1.

Predlog ZVOP-2 ima po predlagani vsebini dejansko in neizbežno skorajda pomen »zakonika« (za varstvo osebnih podatkov), saj kot je že navedeno, poskuša urediti čim več sistemske ozir splošne vsebine na enem mestu (razlog pravne varnosti), upošteva direktivni pristop iz določenih delov Splošne uredbe, uvaja nujne pojasnjevalne in povezovalne norme, izvaja določbe Direktive v istem zakonu, izvaja določbe Konvencije o varstvu posameznikov glede na avtomatsko obdelavo osebnih podatkov (Sveta Evrope), ureja varstvo osebnih podatkov za področja, ki jih Splošna uredba ne ureja (npr. varstvo osebnih podatkov umrlih oseb), določa, da velja za vse obdelave osebnih podatkov v Republiki Sloveniji (npr. področje varnosti države) ter tudi glede na absolutno dolžnost upoštevanja obveznosti zakonskega urejanja varstva osebnih podatkov glede na drugi odstavek 38. in 87. člen Ustave Republike Slovenije, ureja poleg sistemskih določb tudi določene področne ureditve (npr.

¹⁷ Zvezni zakon, s katerim se spreminja Zakon o varstvu osebnih podatkov iz leta 2000 (Zakon o prilagoditvi varstva osebnih podatkov 2018); objava: Bundesgesetzblatt I Nr. 120/2017, Teil I.

¹⁸ Zakon o varstvu osebnih podatkov in o spremembah in dopolnitvah določenih zakonov: objava: č. 704/2017 Z. z..

biometrija) ipd.. Zlasti z vidika spoštovanja načela pravne varnosti je tak pristop skupnega urejanja varstva osebnih podatkov na enem mestu (tradicionalen že od leta 1990¹⁹) – upravičen.

2. 3. O zakonodajni tehniki Predloga ZVOP-2

Zakonodajna tehnika Predloga ZVOP-2 je delno novota, glede na potrebo implementacije določb Splošne uredbe in Direktive, kombinacijo določb obeh pravnih aktov Evropske unije, dejstvo, da se precej določb Splošne uredbe uporablja neposredno in glede na primarno potrebo, da se zagotovi spoštovanje pravne varnosti zaradi učinkovitega uresničevanja osebne človekove pravice do varstva osebnih podatkov. V Predlogu ZVOP-2 je precej določb, ki urejajo določen del določb iz Splošne uredbe (konkretizacija zaradi pravne varnosti ali zaradi pravila podrobnega zakonskega urejanja – drugi odstavek 38. člena Ustave Republike Slovenije), vendar se v določenih delih tudi sklicujejo na neposredno (ali preostalo neposredno) uporabo določb Splošne uredbe.

Kot delna novota so v Predlogu ZVOP-2 tako uporabljene naslednje zakonodajne tehnike:

1. tehnika indikacije (sklica),
2. tehnika prepisa – npr. skupne definicije temeljnih pojmov za uredbo in direktivo,
3. tehnika povzetka,
4. tehnika združitve določb iz Splošne uredbe in Direktive, v smeri določb iz Splošne uredbe (npr. v IX. delu Predloga zakona).

2. 4. Načela Predloga ZVOP-2

Načelo spoštovanja osebnosti in pravic človeka

Prvo vodilno načelo novega Predloga ZVOP-2 je zakonodajno urejanje v smeri individualnega pristopa, po katerem je treba izhajati iz človeka kot upravičenca (nosilca; naslovnika; subjekta) pravice do varstva osebnih podatkov in torej njemu zagotoviti dejansko uresničevanje te pravice. Prosti pretok osebnih podatkov, prenos osebnih podatkov, čezmejne obdelave osebnih podatkov, posredovanja osebnih podatkov, obdelave osebnih podatkov v druge namene ipd. lahko delujejo le, če je navedeni individualni pristop spoštovan. Pri presoji zakonodajnih ali izvedbenih posegov v pravico do varstva osebnih podatkov je treba izhajati iz ocene vpliva posega varstvo osebnih podatkov na človeka kot subjekta ter opraviti oceno z vidika spoštovanja strogega načela sorazmernosti.

Načelo zakonitosti

Načelo zakonitosti v Predlogu ZVOP-2 izhaja iz drugega odstavka 38. člena Ustave Republike Slovenije (»Zbiranje, obdelovanje, namen uporabe, nadzor, in varstvo tajnosti osebnih podatkov določa zakon.«) ter iz 87. člena Ustave Republike Slovenije po katerem se pravice in obveznosti lahko urejajo le z zakonom. Navedeno načelo izhaja tudi iz temeljne navedbe št. 39 Splošne uredbe, (a) točke prvega odstavka člena 5 Splošne uredbe, prvega, drugega in tretjega odstavka člena 6 Splošne uredbe, (a) točke prvega odstavka člena 4 Direktive, člena 8 Direktive in a. točke 5. člena Konvencije. Ob tem je pomembno, da drugi stavek uvodne navedbe št. 45 Splošne uredbe navaja (ne pa prepoveduje) da »Ta uredba ne zahteva posebnega zakona za vsako posamezno obdelavo.« To pomeni da lahko države članice Evropske unije glede na svojo nacionalno (zlasti ustavno) ureditev vseeno določijo vsaj splošne pravne podlage za določene vrste obdelav konkretnih osebnih podatkov v sistemskem ali v področnih zakonih, ne pomeni pa za Republiko Slovenijo, da se lahko konkretne obdelave konkretnih osebnih podatkov določa v podzakonskih predpisih (kar je nedopustno po

¹⁹ Glejte: Zakon o varstvu osebnih podatkov iz leta 1990 (Uradni list RS, št. 8/90, 19/91 in 59/99 - ZVOP).

ustaljeni ustavnosodni presoji Ustavnega sodišča Republike Slovenije od leta 1992 dalje²⁰). Temu pristopu tako sledijo 10. točka tretjega odstavka 6. člena, nato a) točka prvega odstavka 7. člena, zlasti pa prvi odstavek 8. člena in delno prvi odstavek 9. člena ZVOP-2. Za delovanje (odločanje, poseganje v pravice določanje obveznosti) javnega sektorja (javne oblasti) velja strogo načelo zakonitosti, za zasebni sektor je načelo nekoliko omiljeno v smislu, da lahko splošne določbe Splošne uredbe ter ZVOP-2 določajo splošna pravila za posege v varstvo osebnih podatkov, ki se jih nato konkretno uporabi v praksi preko ocene učinkov na varstvo osebnih podatkov. Tako (delno) omiljeno spoštovanje načela zakonitosti za zasebni sektor (pogodbe, storitve) je zahteva iz točk (a), (b) (d) in (f) prvega odstavka člena 6 Splošne uredbe.

Načelo stroge sorazmernosti

Pri izvajanju posegov v pravico do varstva osebnih podatkov je treba izhajati iz načela sorazmernosti kot ga opredeljuje Predlog ZVOP-2, konkretnije, po ustavnosodni presoji z uporabo strogega testa sorazmernosti (predvsem odločba US, št. U-I-60/03, 4. 12. 2003²¹, zlasti 30. v zvezi s 17. točko odločbe).

Načelo namenske obdelave osebnih podatkov

Določbe Predloga ZVOP-2 o namenski obdelavi osebnih podatkov tudi izhajajo iz drugega odstavka 38. člena Ustave Republike Slovenije (»Zbiranje, obdelovanje, namen uporabe, nadzor, in varstvo tajnosti osebnih podatkov določa zakon.«), kar pomeni da kadar se po Ustavi, Splošni uredbi ali Direktivi obdelava osebnih podatkov določa z zakonom, mora biti namen njihove obdelave tudi izrecno določen v zakonu. Poleg tega je načelo namenske obdelave osebnih podatkov določeno tudi v drugem stavku prvega odstavka 38. člena Ustave Republike Slovenije (»Prepovedana je uporaba osebnih podatkov v nasprotju z namenom njihovega zbiranja.«). Navedeni del ustavne določbe (za razliko od določbe drugega odstavka 38. člena Ustave) je s Predlogom ZVOP-2 delno omejen (relativiziran) saj morajo glede na določbe četrtega odstavka člena 6 Splošne uredbe biti omogočene tudi obdelave osebnih podatkov v druge namene. Tovrstno omejitev omogočajo tudi določbe tretjega odstavka 15. člena Ustave Republike Slovenije o omejitvah človekovih pravic s pravicami drugih oseb.

Delno relevantno načelo »prepovedano vse, kar ni izrecno dovoljeno«-

Za represivne posege države človekove pravice ali temeljne svoboščine in interese še vedno velja načelo »prepovedano vse, kar ni izrecno dovoljeno«²². Za posege s strani zasebnega sektorja pa je navedeno načelo omejeno v skladu z določbami ZVOP-2 in točkami (a), (b) (d) in (f) prvega odstavka člena 6 Splošne uredbe.

2. 5. Poglavitne zakonodajne rešitve iz Predloga ZVOP-2

Poglavitne zakonodajne spremembe glede na dosednji Zakon o varstvu osebnih podatkov iz leta 2004 (ZVOP-1) se nanašajo tako na splošne, kot na posebne določbe, kot tudi na področne ureditve.

Tako so nekoliko drugače (sicer v skladu s Splošno uredbo) določena načela zakonitosti, poštenosti in sorazmernosti, ki veljajo za vse dele Predloga ZVOP-2 ter tudi za področne ureditve v drugih zakonih v Republiki Sloveniji, glede načela zakonitosti se sledi zavezujoči ustavni ureditvi iz drugega odstavka 38. in 87. člena Ustave Republike Slovenije, glede načela sorazmernosti pa 2. v zvezi s tretjim odstavkom 15. člena Ustave Republike Slovenije. Glede načela poštenosti (v zvezi z načelom preglednosti) pa dosedanjim dosežkom pravne ureditve (obligacijsko pravo, pravo dostopa do informacij javnega značaja), ustavnosodne presoje (sicer s področja prikritih preiskovalnih ukrepov po Zakonu o kazenskem postopku)

²⁰ Odločba US, št. U-I-115/92, 24. 12. 1992; objava: Uradni list RS, št. 3/93 in OdlUS I, 105.

²¹ Objava: Uradni list RS, št. 131/03 in OdlUS XII, 93.

²² Odločba US, št. U-I-25/95, 27. 11. 1997; objava: Uradni list RS, št. 5/98 in OdlUS VI, 158.

in sodne prakse (zlasti civilnopravne).

Znatno je spremenjena definicija privolitve posameznika za obdelavo njegovih ali njenih osebnih podatkov, ki se sedaj glasi: privolitev posameznika, na katerega se nanašajo osebni podatki, pomeni: vsako prostovoljno, konkretno, informirano in nedvoumno ravnanje v obliki izjave ali drugačnega jasnega aktivnega delovanja, iz katerega je mogoče sklepati na želje posameznika, na katerega se nanašajo osebni podatki, s katero izrazi strinjanje z obdelavo osebnih podatkov, ki se nanašajo nanj.

Na novo so razdelane definicije in obdelave v zvezi s posebnimi vrstami osebnih podatkov (dosedaj: občutljivi osebni podatki), vključno s pravnimi podlagami za obdelavo. Od posebnih vrst osebnih podatkov so sedaj ločene pravne podlage glede obdelave osebnih podatkov o kazenskih obsodbah ter o kaznovanjih za prekrške, vendar se pravila zavarovanja osebnih podatkov s področja posebnih vrst osebnih podatkov uporabljajo tudi za njih.

Določena je nova ureditev glede drugih (dosedaj: naknadnih) namenov obdelave osebnih podatkov, po predlagani ureditvi – v skladu s Splošno uredbo – so drugi (novi) nameni obdelave osebnih podatkov sedaj širši in je upoštevanje prvotnega namena zbiranja in obdelave osebnih podatkov nekoliko manj pomembno.

Za namene izkazovanja skladnosti obdelave osebnih podatkov sta kot obveznost za upravljavce in obdelovalce poleg izvedbo ocene učinkov določena tudi izvajanja ukrepa ti. notranje sledljivosti posredovanj osebnih podatkov ((f) točka drugega odstavka 34. člena ZVOP-2) ter ukrepa ti. zunanje sledljivosti obdelav osebnih podatkov (sedmi odstavek 40. člena ZVOP-2), precej podobno kot v dosedanjem tretjem odstavku 22. člena ZVOP-1.

Določena je nova ureditev za osebe, ki znotraj upravljavcev ali obdelovalcev zagotavljajo varstvo osebnih podatkov, zlasti ko gre za tvegane ali množične obdelave osebnih podatkov, namreč pooblaščen osebe za varstvo osebnih podatkov. Ne uvaja se reguliran poklic, ampak neodvisne osebe znotraj upravljavca ali obdelovalca, ki naj preprečijo tveganja ali kršitve varstva osebnih podatkov. Glede pooblaščenih oseb za varstvo osebnih podatkov je predlagana ureditev dokaj »odprte narave«, tako z vidika dejanske usposobljenosti niso več zahtevane delovne izkušnje samo s področja varstva osebnih podatkov, ampak tudi npr. s področja bančništva (zaupne informacije), omogoča lažjo izbiro javnemu sektorju (razen ministrstev) tudi v zasebnem sektorju (najem fizične ali pravne osebe), omogoča začasno lažjo izbiro iz širšega kroga oseb občinam, sodelovanje preko medobčinskih uprav in najetje zunanjega izvajalca (zasebni sektor), prav tako je podana posebna centralizirana ureditev za sodišča in državna tožilstva, vključno z namestnikom pooblaščen osebe. Določena je tudi možnost, da imajo lahko organi v sestavi lastno pooblaščen osebo.

Podrobno je v korist znanstvenega raziskovanja, zgodovinskega raziskovanja, statističnega raziskovanja in arhivskega delovanja razdelano razmerje napram varstvu osebnih podatkov, tudi z vidike ne-poseganja v veljavno arhivsko zakonodajo.

Posebej je v Predlogu ZVOP-2 poudarjen pomen svobode izražanja v razmerju do varstva osebnih podatkov, tako da je omogočeno zadržanje dosedanje ravni uresničevanja svobode izražanja v okviru pravnega reda Republike Slovenije²³.

²³ Gre za načelen in sistemski pristop Republike Slovenije, ki v obdobju zadnjih cca 6 let ni bil izražen samo pri sprejemanju Stališč Republike Slovenije glede predlogov Splošne uredbe in Direktive leta 2012, ampak tudi širše (mednarodno prepoznavno), npr. pisna in ustna intervencija Republike Slovenije leta 2014 v postopku v primeru *Maximilian Schrems* (ti. »Facebook primer«) - sodba SEU, C-362/14, 6. 10. 2015 ter v vzdržanosti pri glasovanju Republike Slovenije (kot ene od le štirih držav, ki so se vzdržale glasovanja iz načelnih razlogov) glede Ščita zasebnosti (»Privacy Shield«) dne 8. 7. 2016 (glejte npr.:

Nadzorni organ za varstvo osebnih podatkov Republike Slovenije po določbah ZVOP-2 ostaja Informacijski pooblaščenec, kot je bil dosedaj po določbah ZVOP-1 in po Zakonu o informacijskem pooblaščenču. Ostaja pristojen za inšpekcijski nadzor glede varstva osebnih podatkov glede vseh obdelav osebnih podatkov v Republiki Sloveniji, razen tistih, kjer to preprečujejo ustavne določbe ali določbe Splošne uredbe ali primerljivi položaji – npr. neodvisno odločanje sodstva. Delno podobno je urejeno tudi za področje (kriminalistične) policije, obveščevalno-varnostne dejavnosti – ni možno izvajati inšpekcijskih nadzorov s strani Informacijskega pooblaščenca, če bi se lahko razkrile identitete tajnih delavcev in tajnih sodelavcev, podobno tudi glede zaščiteneh prič po Zakonu o zaščiti prič.

Področje pravosodja in policije ter izvrševanja kazenskih sankcij in delno obrambe ter varnosti države je urejeno v posebnem delu ZVOP-2 (IX. del). Ustrezne specifične in izjeme, tako glede namenov obdelav osebnih podatkov, obveščanja posameznikov o njihovih osebnih podatkih, so urejene specifično, glede na določbe Direktive. V povezavi s tem delom zakona so urejene tudi specifične glede varnosti države in obrambe države, v okviru sistema in pravic ter njihovih omejitev po tem zakonu.

V področnih ureditvah obdelav osebnih podatkov (poseben del ZVOP-2) so npr. delno prenovljeno razdelane določbe o videonadzoru (npr. uvedba videonadzora na javnih površinah) ter o biometriji. Dodana je pomembna nova področna ureditev, namreč »Pravosodni supervizor, ki omogoča anonimizirano objavljane sodb sodišč Republike Slovenije, vključno sodbami prvostopenjskih sodišč. Predvidena informacijska rešitev bi omogočila avtomatizirano posredovanje novo izdanih sodb s strani Vrhovnega sodišča Republike Slovenije Ministrstvu za pravosodje (upravljavca), za njihovo strojno anonimizacijo ter nekatere dodatne popravke, za njihovo javno objavo, ter za upravljanje oziroma odločanje o morebitnih pritožbah in pripombah strank sodnih postopkov ali uporabnikov novonastalega spletnega portala sodne prakse.

Kazenske določbe določajo, da se upravne globe po določbah Splošne uredbe obravnavajo kot prekrški, da je prekrškovni organ Informacijski pooblaščenec ter da odloča tudi o prekrških v posebnem delu ZVOP-2 (npr. prekrški glede videonadzora, biometrije...), določen je tudi način ocenjevanja višine glob, ki naj se izrečejo za kršitve določb Splošne uredbe (glede na konkretne okoliščine, načelo sorazmernosti).

Morale so biti izvedene tudi znatne spremembe dosedanjega tradicionalnega izrazoslovja s področja varstva osebnih podatkov (ustaljeno od leta 1984²⁴) – ker je bilo treba to izvesti glede na drugačne definicije iz Splošne uredbe in Direktive.

Tako so sedanji novi temeljni izrazi zlasti:

1. zbirka (dosedaj zbirka osebnih podatkov),
2. varnost osebnih podatkov (dosedaj zavarovanje osebnih podatkov),
3. upravljavec (dosedaj upravljavec osebnih podatkov),
4. obdelovalec (dosedaj pogodbeni obdelovalec),
5. posebne vrste osebnih podatkov (dosedaj občutljivi osebni podatki),

<https://www.theguardian.com/technology/2016/jul/08/privacy-shield-data-transfer-us-european-union>) ter tudi glede vsebine določenih bilateralnih mednarodnih pogodb (npr. s področja policijskega in pravosodnega sodelovanja).

²⁴ Glejte: Prof. dr. Lovro Šturm: *Pravni vidiki zaščite podatkov v sodobnih informacijskih sistemih*, Zbornik znanstvenih razprav XLIV, 1984, str. 117-131.

6. prenos osebnih podatkov (doseđanji iznos osebnih podatkov v tretje države),
7. čezmejna obdelava osebnih podatkov (pomeni izmenjave in obdelave osebnih podatkom med državami članicami Evropske unije),
8. posredovanje osebnih podatkov pomeni izmenjavo osebnih podatkov med upravljavcem in uporabnikom ali upravljavcem in upravljavcem ali upravljalcem in obdelovalcem.

2. 6. Sprejetje zakona

Zakon mora biti sprejet in objavljen v Uradnem listu Republike Slovenije ter uveljavljen pred 25. majem 2018, v uporabi pa mora biti od 25. maja 2018.

3. OCENA FINANČNIH POSLEDIC PREDLOGA ZAKONA ZA DRŽAVNI PRORAČUN IN DRUGA JAVNA FINANČNA SREDSTVA – ocena finančnih sredstev za državni proračun:

Predlog zakona ne bo imel posledic za Proračun Republike Slovenije.

Uporabni postopki zavarovanja osebnih podatkov (sedaj: varnost osebnih podatkov) obstajajo pri subjektih javnega sektorja že od leta 1991 (od začetka veljavnosti Zakona o varstvu osebnih podatkov iz leta 1990). Kar pomeni, da mora javni sektor že sedaj posebno pozornost dajati varstvu osebnih podatkov. V okviru doseđanje organizacije dela bo sicer treba sistem prenoviti v še bolj »varovalno smer« - namreč vzpostaviti notranje ali zunanje (pogodbene) pooblašene osebe za varstvo osebnih podatkov (*»data protection officers«*). To tudi posledično pomeni, da je treba v okviru notranje organizacije v okviru javnega sektorja praviloma določiti pooblašene osebe za varstvo osebnih podatkov izmed že sedaj zaposlenih (ob upoštevanju kriterijev glede zagotavljanja samostojnosti ozir. nastanka konflikta interesov iz ZVOP-2) ali pa dodatno uporabiti (nameniti) že obstoječa finančna sredstva glede zunanjih storitev – npr. pravno svetovanje – za uvedbo zunanjih pooblaščenih oseb (relevantno npr. za občine) ali pa organizirati pooblašene osebe v okviru medobčinskega sodelovanja – skupne občinske uprave (kot npr. medobčinska redarstva ipd.).

Prav tako so relevantni dodatni ukrepi za okrepitev ozir. dodatno zagotovitev učinkovitega in neoviranega delovanja neodvisnega nadzornega mehanizma (Informacijski pooblaščenec), namreč glede dodatnih kadrov in prostorov, ki zagotavljajo učinkoviti nadzor glede spoštovanja določb Splošne uredbe o varstvu podatkov. Ti ukrepi so sicer že bili vnaprej zagotovljeni v letu 2017 za leti 2018 in 2019 (o tem v naslednji točki).

– ocena drugih javnih finančnih sredstev: Predlog zakona ne bo imel posledic za druga javna finančna sredstva.

– predvideno povečanje ali zmanjšanje prihodkov državnega proračuna: Zaradi predloga zakona ni predvideno povečanje ali zmanjšanje prihodkov državnega proračuna – sredstva so že zagotovljena (naslednja točka).

– predvideno povečanje ali zmanjšanje obveznosti za druga javna finančna sredstva: Zaradi predloga zakona ni predvideno povečanje ali zmanjšanje obveznosti za druga javna finančna sredstva.

– predvideni prihranki za državni proračun in druga javna finančna sredstva: Prihranki za državni proračun in druga javna finančna sredstva niso predvideni.

– sredstva bodo zagotovljena z zadolževanjem (poročstva): Zaradi predloga zakona ni potrebno zadolževanje.

– v naslednjem proračunskem obdobju bodo sredstva zagotovljena: V naslednjem proračunskem obdobju dodatnih sredstev zaradi predloga zakona ni treba zagotavljati izven že predhodno dodeljenih sredstev v naslednji točki.

4. NAVEDBA, DA SO SREDSTVA ZA IZVAJANJE ZAKONA V DRŽAVNEM PRORAČUNU ZAGOTOVLJENA, ČE PREDLOG ZAKONA PREDVIDEVA PORABO PRORAČUNSKIH SREDSTEV V OBDOBJU, ZA KATERO JE BIL DRŽAVNI PRORAČUN ŽE SPREJET

Predlog zakona ne predvideva porabe dodatnih proračunskih sredstev v obdobju, za katero je bil proračun že sprejet. Sredstva so že bila zagotovljena v letu 2017 za obdobje 2018 in 2019 – za delovanje neodvisnega nadzornega mehanizma (Informacijski pooblaščenec).

Podatki o sredstvih:

Leto 2018

Proračunska postavka 1267 plače, dodanih 10 državnih nadzornikov za varstvo osebnih podatkov (41. plačni razred in 10 let delovne dobe) - na letni ravni za enega 34.200,00 EUR, skupaj 342.000,00 EUR

Proračunska postavka 1273 investicije, osnovna sredstva za 10 novo zaposlenih, skupaj 10.000,00 EUR

Proračunska postavka 1271 materialni stroški, selitev, skupaj 20.000,00 EUR, najem poslovnih prostorov za 6 mesecev (15.300 EUR/mesec), skupaj 91.800,00 EUR

Vsi izdatki skupaj 463,800,00 EUR.

Leto 2019

Proračunska postavka 1267 plače, dodanih 5 državnih nadzornikov za varstvo osebnih podatkov (41. plačni razred in 10 let delovne dobe) - na letni ravni za enega 34.200,00 EUR, skupaj 171.000,00 EUR.

Proračunska postavka 1273 investicije, osnovna sredstva za 5 novo zaposlenih, skupaj 5.000,00 EUR, najem poslovnih prostorov za 12 mesecev (15.300 EUR/mesec), skupaj 183.600,00 EUR.

Vsi izdatki skupaj 359.600,00 EUR.

5. Prikaz ureditve v drugih pravnih sistemih in prilagojenosti predlagane ureditve v pravu Evropske unije

5. 1. Uvodno o primerjalnopravni ureditvi

V letu 2017 so bili sprejeti le trije izvedbeni zakoni držav članic Evropske unije – v Zvezni republiki Nemčiji, v Republiki Avstriji in v Slovaški republiki. Večina preostalih držav članic Evropske unije ima pripravljene predloge ali osnutke izvedbenih zakonov ali pa jih še pripravlja²⁵. »Modeli« oziroma »smeri« zakonodajnega urejanja iz navedenih zakonov ali predlogov ali osnutkov so si precej različne (načeloma je vsaka država dokaj razvila zakonsko izvedbeno ureditev v njej lastno smer)²⁶, nekateri zakoni so tudi minimalistični (predlog Finske republike z dne 21. 6. 2017), nekateri zakoni so tudi vsebinsko nepopolni.

Kot možen primer - Francoska republika je sprejela delni izvedbeni zakon leta 2016²⁷ ter naknadno glede njega ocenila, da bo treba zaradi vsebinske nepopolnosti ozir. vsebinskih problemov že sprejeti zakon razveljaviti (v delu, ki se nanaša na varstvo osebnih podatkov) ter pripraviti popolnoma nov Zakon o varstvu osebnih podatkov, ki je sedaj v letu 2018 v začetni pripravi. V zakonu iz leta 2016 je tako med drugim uredila vprašanje izrekanja visokih glob po Splošni uredbi, varstvo osebnih podatkov umrlih oseb, pravico do pozabe ipd..

Dokaj možna potencialna posledica navedenih precejšnjih razlik glede »modelov« ozir. »smeri« zakonodajnega urejanja s strani držav članic Evropske unije je tudi (možna) bodoča situacija, da bo treba v letih 2018 in 2019 po proučitvi vseh sprejetih zakonskih rešitev večino izvedbenih zakonov držav članic Evropske unije dopolnjevati (kar velja tudi za ZVOP-2). Vse države članice pri teh zakonodajnih pristopih štejejo, da ustrezno izvajajo določbe Splošne uredbe in Direktive.

V nadaljevanju so tako predstavljeni že sprejeti nemški, avstrijski in slovaški zakon (torej le **trije že sprejeti zakoni držav članic Evropske unije**).

5.2. Zvezna republika Nemčija

Zvezna republika Nemčija je 27. aprila 2017 sprejela Zakon o prilagoditvi zakonodaje o varstvu osebnih podatkov Uredbi (EU) 2016/679 in izvajanju Direktive (EU) 2016/680 (Zakon o prilagoditvi in izvajanju zakonodaje o varstvu osebnih podatkov EU)²⁸. Sistemski pristop zakona je, da precej upošteva obstoječo nacionalno pravno ureditev (ustavnopravno), ustaljene rešitve iz področnih zakonov Nemčije ter tradicionalno prakso varstva osebnih podatkov v Nemčiji.

I. Del zakona velja za vsa področja obdelave osebnih podatkov, tako tudi za področje nacionalne varnosti, obrambe in pomeni tudi izvedbo določb Direktive (EU) 2016/680. Enako velja za pristojnosti Zveznega pooblaščenca za varstvo osebnih podatkov (nadzorni organ za varstvo osebnih podatkov).

V 2. členu so podane definicije subjektov javnega in zasebnega sektorja. 3. člen določa (na posreden način) uporabo strogega načela zakonitosti za javni sektor (javno oblast) – stroga uporaba (in interpretacija) (e) točke prvega odstavka člena 6 Splošne uredbe.

²⁵ Osutek zakona Kraljevine Belgije bi moral biti znan konec meseca januarja 2018.

²⁶ Glede na to, da je vsaj Splošna uredba namenjena določeni zelo močni stopnji unifikacije varstva osebnih podatkov v Evropski uniji, hitra primerjava pokaže, da so si bili dosedanja zakoni o varstvu osebnih podatkov držav članic Evropske unije, ki so bili izvedbeni zakoni po Direktivi 95/46/ES (harmonizacija!) iz leta 1995 (zakoni so bili sprejeti v obdobju 1998-2004) vsebinsko in tudi oblikovno med seboj veliko bolj podobni. Rezultat sedanjega izredno različnega zakonodajnega pristopa držav članic Evropske unije glede Splošne uredbe je z vidika skupne evropske pravne varnosti in celo varstva pravice do osebnih podatkov kot človekove pravice sporen, ni pa bil nepričakovan.

²⁷ Zakon št. 2016-1321 z dne 7. oktobra 2016 za digitalno republiko.

²⁸ Zakon z dne 30. junija 2017, Bundesgesetzblatt Teil I, 2097.

4. člen določa dokaj široko uporabo videonadzora glede javnih površin, pri čemer se upoštevajo tudi legitimni interesi upravljavca (3. točka prvega odstavka – izvedba (f) točke prvega odstavka člena 6 Splošne uredbe). V 22. členu so določena pravila (pravne podlage) glede obdelave posebnih vrst osebnih podatkov - podano je pooblastilo upravljavcem (sicer po predpisanih strogih pravilih) kako naj tehtajo možnost obdelave posebnih vrst osebnih podatkov v konkretnih primerih, kar pa lahko določi tudi področna zakonodaja (izjemoma) Na ta način je nekoliko nadgrajen sistem iz člena 9 Splošne uredbe. Ko gre za obdelavo teh podatkov v druge namene se po uvodnem delu drugega odstavka upošteva tudi področna zakonodaja. 24. člen določa dokaj stroga pravila glede obdelave osebnih podatkov v druge namene - le za potrebe preprečevanja nevarnosti za državno ali javno varnost ali za kazenski pregon²⁹ ali če je to potrebno za uveljavljanje, izvajanje ali obrambo civilnopravnih zahtevkov, če ne prevladujejo interesi posameznika, na katerega se nanašajo osebni podatki, za izključitev obdelave osebnih podatkov. V 35. členu so določene omejitve pravice do izbrisa osebnih podatkov – če bi bil poseg nesorazmeren ali pa gre le za minimalno korist za posameznika.

III. Del zakona določa izvedbo določb Direktive (EU) 2016/680. Določbe v njem, ki so enake ali podobne istim, ki so v Splošni uredbi ali v predhodnih delih zakona izhajajo iz pristopa (kot je določen že v I. delu zakona), po katerem je nacionalnemu zakonodajalcu prepuščeno, kako bo izvedel določbe navedene Direktive in lahko tako tudi uporabi (z vidika pravne varnosti) splošni sistem urejanja varstva osebnih podatkov iz Splošne uredbe.

To predstavitev nemške pravne ureditve glede novega sistema varstva osebnih podatkov še ni možno šteti za popolno predstavitev, saj še niso sprejeti (pretežno tudi še ne pripravljene) zakoni zveznih dežel Zvezne republike Nemčije, ki so pristojne za obdelavo osebnih podatkov v zasebnem sektorju ter deželne nadzorne organe za varstvo osebnih podatkov.

Znano je da je sprejeti Zakon o prilagoditvi in izvajanju zakonodaje o varstvu osebnih podatkov EU deležen (sicer neupoštevanih) kritik iz dela zasebnega sektorja in dela javnosti³⁰, češ da ni dovolj v skladu z določbami Splošne uredbe - da naj bi bile občasno njegove določbe prestroge ali preširoke. Možno je, da bo Nemčija v primeru kritik z vidika domnevne neskladnosti določb Zakona o prilagoditvi in izvajanju zakonodaje o varstvu osebnih podatkov EU v razmerju do določb Splošne uredbe uporabila podlago (ugovor) varstva temeljnih pravic po Temeljnem zakonu (Ustavi) Zvezne republike Nemčije ter ustaljene ustavnosodne presoje Zveznega Ustavnega sodišča Zvezne republike Nemčije.

5.3. Republika Avstrija

Republika Avstrija je v letu 2017 sprejela Zvezni zakon, s katerim se spreminja Zakon o varstvu osebnih podatkov iz leta 2000 (Zakon o prilagoditvi varstva osebnih podatkov 2018)³¹.

Sprejeti zakonski okvir precej sledi dosedanji ureditvi varstva osebnih podatkov v Republiki Avstriji, Avstrija je namreč izbrala način novelacije (spremembe in dopolnitve) veljavnega zakona. 1. člen veljavnega zakona, ki ureja varstvo osebnih podatkov kot osebno človekovo pravico in ima uradno pomen ustavne norme, ni bil spremenjen zaradi neobstoja zahtevane dvotretjinske večine vseh poslancev in poslank za ustavno revizijo, kar pomeni, da je Avstrija zadržala dosedanjo širšo opredelitev varstva osebnih podatkov kot temeljne pravice – kot nadrejeno glede vseh obdelav osebnih podatkov (tudi obdelav v druge namene). Prav tako je Avstrija zadržala dosedanjo

²⁹ Zasebni sektor npr. uporablja videonadzor in bi hotel vložiti kazensko ovadbo, saj je ocenil, da obstaja sum storitve kaznivega dejanja.

³⁰ Glejte: *Interview with Jan Albrecht, Dr. Stefan Brink and Tim Wybitul on the New German Data Protection Bill*, 6. 2. 2017, dostopno na: <https://www.hldataprotection.com/2017/02/articles/international-eu-privacy/interview-with-jan-albrecht-dr-stefan-brink-and-tim-wybitul-on-the-new-german-data-protection-bill/>

³¹ Bundesgesetzblatt I Nr. 120/2017, Teil I.

tradicionalno ureditev (po sodni praksi od leta 1951 dalje) tudi (dela) podatkov pravnih oseb, ki se obravnavajo in varujejo kot (da so) osebni podatki. Za obdelavo osebnih podatkov otrok v zvezi storitvami informacijske družbe je določena mejna starost 14 let (v predlogu je bilo 16 let). Glede osebnih podatkov v zvezi s kazenskimi obsodbami je določeno (nekoliko drugače kot v členu 10 Splošne uredbe), da se lahko ti podatki obdelujejo tudi s strani upravitelja, če ima za to legitimen interes. Avstrija ni sprejela rešitve glede kritiziranih (spornih) visokih glob po Splošni uredbi, glede katerih se zatrjuje kršitev človekovih pravic ozir. neustavnost (tudi z vidika, da tako visokih glob ne bi smel izreka nadzorni organ – ker ni sodišče), ampak bo počakala na odločitev Ustavnega sodišča Republike Avstrije v primerljivem primeru – presoja ustavnosti previsokih glob, katere lahko izreka avstrijski Urad za finančni trg. Glede razmerja varstvo osebnih podatkov – znanstveno raziskovanje je Avstrija določila le splošne določbe, obdelave pa bodo potekale po obstoječih področnih zakonih. Ni podana jasna rešitev glede dosedanjih pridobljenih privolitvev za obdelavo osebnih podatkov, če namreč ostanejo veljavne (nespremenjene) po novi ureditvi po Splošni uredbi – le v obrazložitvi prehodnih določb je v zvezi z omembo uvodne navedbe št. 171 Splošne uredbe nekoliko nejasno navedeno, da dosedanje privolitve za obdelavo osebnih podatkov ostanejo v veljavi, če ustrezajo pogojem iz Splošne uredbe.

3. del zakona določa varstvo in obdelavo osebnih podatkov kot del izvedbe določb Direktive (EU) 2016/680.

V prihodnosti se bo kot dosedaj dajalo močan poudarek področni zakonodaji, kjer se bodo urejale vrste osebnih podatkov, nameni obdelave, roki hrambe, omejitve pravic ipd.

Pristop avstrijskega zakonodajalca je v razmerju do začetnih zakonodajnih ambicij (besedilo predloga zakona) morda pokazal, da ne gre ne za unificiran pristop, niti ne za (dovolj) harmoniziran pristop, ampak ob upoštevanju nespremenjenih določenih sistemskih rešitev ter novih rešitev in rešitev iz področne zakonodaje – da gre morda dejansko za nastanek pristopa ti. fragmentacije.

5. 4. Slovaška republika

Vlada Slovaške republike je dne 20. 9. 2017 (vloženo v zakonodajni postopek dne 22. 9. 2017) sprejela besedilo Predloga Zakona o varstvu osebnih podatkov in o spremembah in dopolnitvah določenih zakonov, njen Ljudski svet (Parlament) pa ga je sprejel dne 27. 11. 2017³². Njegove bistvene nacionalne (sistemske) rešitve zlasti glede Splošne uredbe so predstavljene v nadaljevanju.

Tako je zelo bistvena sistemska rešitev v zakonu določitev splošne uporabe (in istočasno neposredne uporabe) temeljnih definicij s področja varstva osebnih podatkov za vsa področja (5. člen), kot so to npr. obdelava osebnih podatkov, privolitvev ipd.. Povezano s tem je v posebnem 2. členu iz 1. točke člena 4 Splošne uredbe prenesena tudi definicija pojma osebni podatek. V 6. členu je vzpostavljeno strogo načelo zakonitosti, po katerem se lahko osebne podatke obdeluje le v skladu z zakonom in tako da niso prekršene temeljne pravice posameznikov, na katere se nanašajo osebni podatki. V tem členu Slovaška republika tudi primarno izhaja iz pristopa, da je varstvo osebnih podatkov osebna človekova pravica. V 7. členu je določena dokaj stroga namenska obdelava osebnih podatkov, po kateri se sme osebne podatke pridobiti le za specifično določene, izrecne in legitime namene in se jih ne sme nadalje obdelovati na način, ki bi bil v neskladju s temi nameni, obdelavo v druge namene pa je dopuščena le glede arhivskih, statističnih, znanstvenih, zgodovinsko raziskovalnih namenov. V 17. členu je določeno, da je obdelava osebnih podatkov o kazenskih obsodbah možna le v primeru podlage v zakonitem predpisu ali na podlagi obvezujoče mednarodne pogodbe, te podatke pa lahko upravlja le državni organ. V 26. členu je npr. urejena pravica do

³² Zakon o varstvu osebnih podatkov in o spremembah in dopolnitvah določenih zakonov: objava: č. 704/2017 Z. Z..

prenosljivosti osebnih podatkov, s tem da je določeno, da ta pravica ne sme imeti škodljivega učinka na pravice drugih oseb. 28. člen ureja avtomatizirano obdelavo osebnih podatkov, vključno s profiliranjem in določa, da se ne sme izvajati avtomatizirana obdelava glede posebnih vrst osebnih podatkov. III. Poglavje II. Dela, III. Del in IV. Del zakona pa določajo zakonsko izvedbo določb Direktive (EU) 2016/680.

6. DRUGE POSLEDICE, KI JIH BO IMELO SPREJETJE ZAKONA

6.1 Administrativne in druge posledice

a) V postopkih oziroma poslovanju javne uprave ali pravosodnih organov:

Vzpostavitev pooblaščenih oseb za varstvo osebnih podatkov, z zakonsko določenimi izjemami.

b) Pri obveznostih strank do javne uprave ali pravosodnih organov:

Predlog zakona nima tovrstnih posledic.

6.2 Presoja posledic za okolje, ki vključuje tudi prostorske in varstvene vidike

Predlog zakona ne bo imel tovrstnih posledic.

6.3 Presoja posledic za gospodarstvo

Predlog zakona nima tovrstnih posledic.

6.4 Presoja posledic za socialnem področju

Predlog zakona nima tovrstnih posledic.

6.5 Presoja posledic za dokumente razvojnega načrtovanja

Predlog zakona nima tovrstnih posledic.

6.6 Presoja posledic za druga področja

Predlog zakona nima tovrstnih posledic.

6.7. Izvajanje sprejetega predpisa

Vlada oziroma resorno ministrstvo bo predstavilo zakon širši javnosti z objavo na spletu, ožji javnosti pa na predavanjih, srečanjih, posvetih v okviru izobraževalnih dejavnosti ipd.

6.8 Druge pomembne okoliščine v zvezi z vprašanji, ki jih ureja predlog zakona:

Druge tovrstne okoliščine niso podane.

7. PRIKAZ SODELOVANJA JAVNOSTI PRI PRIPRAVI PREDLOGA ZAKONA:

Javna razprava (prvi krog) med 3. 10. 2017 do 13. 11. 2017 ter od 23. 1. 2018 do 2. 2. 2018. Precej pripomb je bilo upoštevanih, zlasti glede neposrednega trženja, pooblaščenih oseb, privolitve, obdelave v druge namene.

8. PODATEK O ZUNANJEM STROKOVNJAKU OZIROMA PRAVNI OSEBI, KI JE SODELOVALA PRI PRIPRAVI PREDLOGA ZAKONA, IN ZNESKU PLAČILA ZA TA NAMEN:

Zunanji strokovnjaki niso sodelovali pri pripravi predloga zakona.

9. NAVEDBA, KATERI PREDSTAVNIKI PREDLAGATELJA BODO SODELOVALI PRI DELU DRŽAVNEGA ZBORA IN DELOVNIH TELES

- mag. Goran Klemenčič, minister za pravosodje,
- Darko Stare, državni sekretar na Ministrstvu za pravosodje,
- Tina Breclj, državna sekretarka na Ministrstvu za pravosodje,
- mag. Nina Koželj, generalna direktorica Direktorata za kaznovalno pravo in človekove pravice
- Peter Pavlin, višji sekretar, Direktorat za kaznovalno pravo in človekove pravice
- Igor Kolar, svetovalec, Direktorat za kaznovalno pravo in človekove pravice

II. BESEDILO ČLENOV

ZAKON O VARSTVU OSEBNIH PODATKOV

I. DEL – TEMELJNE DOLOČBE

1. člen

(vseбина)

(1) S tem zakonom se določajo pravice, obveznosti, upravičenja, načela, postopki in ukrepi, s katerimi se preprečujejo neustavni, nezakoniti ali neupravičeni posegi v zasebnost, dostojanstvo oziroma druge temeljne pravice posameznika pri obdelavi osebnih podatkov.

(2) S tem zakonom se v pravni red Republike Slovenije prenašajo določbe Direktive (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 (Uradni list EU, L, št. 119/89 z dne 4. 5. 2016, str. 89–131; v nadaljnjem besedilu: Direktiva) ter zagotavlja izvajanje določb Uredbe (EU) 2016/679 Evropskega parlamenta in Sveta z dne 27. aprila 2016 o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem pretoku takih podatkov ter o razveljavitvi Direktive 95/46/ES (Splošna uredba o varstvu podatkov) (Uradni list EU, L, št. 119/1 z dne 4. 5. 2016, str. 1–88; v nadaljnjem besedilu: Splošna uredba).

2. člen

(pravica do varstva osebnih podatkov)

Vsaka posameznica in posameznik (v nadaljnjem besedilu: posameznik) ima osebno človekovo pravico do varstva njegovih osebnih podatkov, tako da se mu zagotavlja zasebnost in dostojanstvo ob upoštevanju njegove podatkovne samoodločbe. Ta pravica vsebuje tudi upravičenje, da se z zakonom ter pošteno in na pregleden način ureja in zagotavlja obdelava njegovih osebnih podatkov, do tajnosti njegovih osebnih podatkov ter druga upravičenja, določena z zakonom, v zvezi z obdelavo njegovih osebnih podatkov in uresničevanja teh njegovih pravic.

3. člen

(prepoved diskriminacije glede varstva osebnih podatkov)

Varstvo osebnih podatkov je zagotovljeno vsaki posameznici ali posamezniku (v nadaljnjem besedilu: posameznik) 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, zdravstvenega stanja ali genske predispozicije ali katerokoli drugo osebno okoliščino.

4. člen

(področje uporabe)

(1) Določbe tega zakona veljajo za popolnoma ali delno avtomatizirano obdelavo osebnih podatkov ter za drugačne obdelave osebnih podatkov, ki so vključeni ali so namenjeni vključitvi v zbirko.

(2) Določbe tega zakona ne veljajo za obdelave osebnih podatkov, ki jih izvajajo posamezniki popolnoma za osebno uporabo ali za druge domače potrebe, kar vključuje tudi družinsko življenje.

(3) Če V. in IX. del tega zakona ne določata drugače, določbe tega zakona veljajo tudi za obdelave osebnih podatkov s strani pristojnih državnih organov ali organov samoupravnih lokalnih skupnosti ali nosilcev javnih pooblastil za namene preprečevanja, preiskovanja, odkrivanja ali pregona kaznivih dejanj, izvrševanja nalog in pooblastil policije, varnosti države, obrambe države ter izvrševanja kazenskih sankcij.

5. člen

(ozemeljska veljavnost zakona)

(1) Ta zakon velja za obdelavo osebnih podatkov, ki se izvaja v okviru javnega sektorja Republike Slovenije, ter za obdelavo osebnih podatkov, ki poteka v okviru dejavnosti sedeža, podružnice ali drugačne poslovne enote upravljavca ali obdelovalca, ustanovljene ali registrirane v Republiki Sloveniji.

(2) Ta zakon velja tudi za obdelavo osebnih podatkov, ki se izvaja v okviru dejavnosti sedeža, podružnice ali drugačne poslovne enote upravljavca ali obdelovalca, ki je ustanovljena ali registrirana zunaj Evropske unije, če so dejavnosti obdelave povezane z nudenjem blaga ali storitev prebivalcem s stalnim prebivališčem Republike Slovenije, ne glede na to, ali je zanje potrebno plačilo, oziroma če so povezane s spremljanjem njihovega delovanja ali vedenja, kolikor to poteka v Republiki Sloveniji.

(3) Določbe tega zakona o privolitvi otrok za uporabo storitev informacijske družbe, obdelavi posebnih vrst osebnih podatkov ter razmerju med pravico do varstva osebnih podatkov in pravicama do svobode izražanja ali dostopa do informacij javnega značaja veljajo tudi za obdelavo osebnih podatkov prebivalcev Republike Slovenije, ki poteka v okviru dejavnosti sedeža, podružnice ali drugačne poslovne enote upravljavca ali obdelovalca, ki je ustanovljen ali registriran v drugi državi članici.

6. člen

(pomen izrazov)

(1) Izrazi, uporabljeni v tem zakonu, pomenijo:

1. osebni podatki pomeni: katero koli informacijo v zvezi z določenim ali določljivim posameznikom (v nadaljnjem besedilu: posameznik, na katerega se nanašajo osebni podatki); določljiv posameznik je tisti, ki ga je mogoče neposredno ali posredno določiti, zlasti z navedbo identifikatorja, kot je ime, identifikacijska številka, podatki o lokaciji, spletni identifikator, ali z navedbo enega ali več dejavnikov, ki so značilni za fizično, fiziološko, gensko, duševno, gospodarsko, kulturno ali družbeno identiteto tega posameznika;

2. obdelava pomeni: vsako dejanje ali niz dejanj, ki se izvaja v zvezi z osebnimi podatki ali nizi osebnih podatkov z avtomatiziranimi sredstvi ali brez njih, kot je zbiranje, beleženje, urejanje, strukturiranje, shranjevanje, prilagajanje ali spreminjanje, priklic, vpogled, uporaba, razkritje s posredovanjem, razširjanje ali drugačno omogočanje dostopa, prilagajanje ali kombiniranje, omejevanje, izbris ali uničenje;

3. omejitev obdelave pomeni: označevanje shranjenih osebnih podatkov zaradi omejevanja njihove obdelave v prihodnosti;
4. oblikovanje profilov pomeni: vsako obliko avtomatizirane obdelave osebnih podatkov, ki vključuje uporabo osebnih podatkov za ocenjevanje nekaterih osebnih vidikov v zvezi s posameznikom, zlasti za analizo ali predvidevanje uspešnosti pri delu, ekonomskega položaja, zdravja, osebnega okusa, interesov, zanesljivosti, vedenja, lokacije ali gibanja tega posameznika;
5. psevdonimizacija pomeni: obdelavo osebnih podatkov na tak način, da osebnih podatkov brez dodatnih informacij ni več mogoče pripisati specifičnemu posamezniku, na katerega se nanašajo osebni podatki, če se take dodatne informacije hranijo ločeno ter zanje veljajo tehnični in organizacijski ukrepi za zagotavljanje, da se osebni podatki ne pripišejo določenemu ali določljivemu posamezniku;
6. zbirka pomeni: vsak strukturiran niz osebnih podatkov, ki so dostopni v skladu s posebnimi merili, niz pa je lahko centraliziran, decentraliziran ali razpršen na funkcionalni ali geografski podlagi;
7. upravljavec pomeni: fizično ali pravno osebo, javni organ, agencijo ali drugo telo, ki samo ali skupaj z drugimi določa namene in sredstva obdelave; kadar namene in sredstva obdelave določa pravo Unije ali pravo države članice, se lahko upravljavec ali posebna merila za njegovo imenovanje določijo s pravom Unije ali pravom države članice;
8. obdelovalec pomeni: fizično ali pravno osebo, javni organ, agencijo ali drugo telo, ki obdeluje osebne podatke v imenu upravljavca;
9. uporabnik pomeni: fizično ali pravno osebo, javni organ, agencijo ali drugo telo, ki so mu bili osebni podatki razkriti, ne glede na to, ali je tretja oseba ali ne. Vendar pa se javni organi, ki lahko prejmejo osebne podatke v okviru posamezne poizvedbe v skladu s pravom Unije ali pravom države članice, ne štejejo za uporabnike; obdelava teh podatkov s strani teh javnih organov poteka v skladu z veljavnimi pravili o varstvu podatkov glede na namene obdelave;
10. tretja oseba pomeni: fizično ali pravno osebo, javni organ, agencijo ali telo, ki ni posameznik, na katerega se nanašajo osebni podatki, upravljavec, obdelovalec in osebe, ki so pooblaščenice za obdelavo osebnih podatkov pod neposrednim vodstvom upravljavca ali obdelovalca;
11. privolitev posameznika, na katerega se nanašajo osebni podatki, pomeni: vsako prostovoljno, konkretno, informirano in nedvoumno ravnanje v obliki izjave ali drugačnega jasnega aktivnega delovanja, iz katerega je mogoče sklepati na želje posameznika, na katerega se nanašajo osebni podatki, s katero izrazi strinjanje z obdelavo osebnih podatkov, ki se nanašajo nanj;
12. kršitev varnosti osebnih podatkov pomeni: kršitev varnosti, ki povzroči nenamerno ali nezakonito uničenje, izgubo, spremembo, nepooblaščen razkritje ali dostop do osebnih podatkov, ki so poslani, shranjeni ali kako drugače obdelani;
13. genski podatki pomeni: osebne podatke v zvezi s podedovanimi ali pridobljenimi genskimi značilnostmi posameznika, ki dajejo edinstvene informacije o fiziologiji ali zdravju tega posameznika in so zlasti rezultat analize biološkega vzorca zadevnega posameznika;
14. biometrični podatki pomeni: osebne podatke, ki so rezultat posebne tehnične obdelave v zvezi s fizičnimi, fiziološkimi ali vedenjskimi značilnostmi posameznika, ki omogočajo ali potrjujejo edinstveno identifikacijo tega posameznika, kot so podobe obraza ali daktiloskopski podatki;
15. podatki o zdravstvenem stanju pomeni: osebne podatke, ki se nanašajo na telesno ali duševno zdravje posameznika, vključno z zagotavljanjem zdravstvenih storitev, in razkrivajo informacije o njegovem zdravstvenem stanju;
16. glavni sedež pomeni:
- a) v zvezi z upravljavcem, ki ima sedeže v več kot eni državi članici, kraj njegove osrednje uprave v Uniji ali, kadar se odločitve o namenih in sredstvih obdelave osebnih podatkov sprejemajo na drugem

sedežu upravljalca v Uniji in ima ta sedež pooblastila za izvajanje takih odločitev, sedež, ki sprejema take odločitve;

b) v zvezi z obdelovalcem, ki ima sedeže v več kot eni državi članici, kraj njegove osrednje uprave v Uniji ali, če obdelovalec nima osrednje uprave v Uniji, sedež obdelovalca v Uniji, kjer se izvajajo glavne dejavnosti obdelave v okviru dejavnosti sedeža obdelovalca, kolikor za obdelovalca veljajo posebne obveznosti iz te uredbe;

17. predstavnik pomeni: fizično ali pravno osebo s sedežem v Uniji, ki jo pisno imenuje upravljavec ali obdelovalec v skladu s členom 27 Splošne uredbe in ki predstavlja upravljalca ali obdelovalca v zvezi z njegovimi obveznostmi iz te uredbe;

18. podjetje pomeni: fizično ali pravno osebo, ki opravlja gospodarsko dejavnost, ne glede na njeno pravno obliko, vključno s partnerstvi ali združenji, ki redno opravljajo gospodarsko dejavnost;

19. povezana družba pomeni: obvladujočo družbo in njene odvisne družbe;

20. zavezujoča poslovna pravila pomeni: politike na področju varstva osebnih podatkov, ki jih upravljavec ali obdelovalec s sedežem na ozemlju Republike Slovenije spoštuje pri prenosih ali nizih prenosov osebnih podatkov upravljavcu ali obdelovalcu povezane družbe ali skupine podjetij, ki opravljajo skupno gospodarsko dejavnost, v eni ali več tretjih državah;

21. nadzorni organ pomeni: Informacijskega pooblaščenca, določenega z zakonom, ki ureja informacijskega pooblaščenca;

22. zadevni nadzorni organ pomeni: nadzorni organ, ki ga obdelava osebnih podatkov zadeva, ker:

a) ima upravljavec ali obdelovalec sedež na ozemlju države članice tega nadzornega organa;

b) obdelava znatno vpliva ali bi lahko znatno vplivala na posameznike, na katere se nanašajo osebni podatki, s prebivališčem v državi članici tega nadzornega organa, ali

c) je bila vložena pritožba pri tem nadzornem organu;

23. čezmejna obdelava osebnih podatkov pomeni bodisi:

a) obdelavo osebnih podatkov, ki poteka v Uniji v okviru dejavnosti sedežev upravljalca ali obdelovalca v več kot eni državi članici, kadar ima upravljavec ali obdelovalec sedež v več kot eni državi članici, bodisi

b) obdelavo osebnih podatkov, ki poteka v Uniji v okviru dejavnosti edinega sedeža upravljalca ali obdelovalca, vendar obdelava znatno vpliva ali bi lahko znatno vplivala na posameznike, na katere se nanašajo osebni podatki, v več kot eni državi članici;

24. ustrezen in utemeljen ugovor pomeni: ugovor osnutku odločitve glede tega, ali je bila uredba kršena, oziroma glede tega, ali je predvideno ukrepanje v zvezi z upravljavcem ali obdelovalcem v skladu s to uredbo, kar jasno navede pomen tveganja, ki ga predstavlja osnutek odločitve, kar zadeva temeljne pravice in svoboščine posameznikov, na katere se nanašajo osebni podatki, in – kjer je to ustrezno – prosti pretok osebnih podatkov v Uniji;

25. storitev informacijske družbe pomeni: storitev, kakor je opredeljena v točki (b) člena 1(1) Direktive (EU) 2015/1535 Evropskega parlamenta in Sveta (Uradni list EU, L 241, 17. 9. 2015, str. 1);

26. mednarodna organizacija pomeni: organizacijo in njena podrejena telesa, ki jih ureja mednarodno javno pravo ali kateri koli drugo telo, ustanovljeno s sporazumom med dvema ali več državami ali na podlagi takega sporazuma ali za sodelovanje na področju mednarodnega javnega prava tudi organizacija in njena podrejena telesa, ki jih ureja mednarodno javno pravo, ali katera koli druga telesa, ustanovljene z mednarodno pogodbo med Republiko Slovenijo in drugo državo ali med Republiko Slovenijo in več državami ali na podlagi take mednarodne pogodbe

(2) Pristojni organ za izvajanje IX. dela tega zakona pomeni:

a) kateri koli organ ali subjekt javnega prava Republike Slovenije, ki je pristojen za preprečevanje, preiskovanje, odkrivanje ali pregon kaznivih dejanj ali sojenje o njih ali izvrševanje kazenskih sankcij, varnosti države in obrambe države vključno z varovanjem pred grožnjami javni varnosti in njihovim preprečevanjem, ali

b) kateri koli drug organ ali subjekt, ki v skladu z zakonom Republike Slovenije lahko opravlja javne funkcije ali izvaja javna pooblastila za preprečevanje, preiskovanje, odkrivanje ali pregon kaznivih dejanj ali izvrševanje kazenskih sankcij, vključno z varovanjem pred grožnjami javni varnosti in njihovim preprečevanjem.

(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;

2. državni organ pomeni organ kot je določen v 6. členu zakona, ki ureja plače v javnem sektorju;

3. zasebni sektor pomeni pravne in fizične osebe, ki opravljajo dejavnost po zakonu, 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, samoupravne lokalne skupnosti ali samoupravne narodne skupnosti ter izvajalci gospodarskih javnih služb, ki so tudi nosilci javnega pooblastila;

4. povezovalni znaki – so osebna identifikacijska številka in druge z zakonom opredeljene enolične identifikacijske številke posameznika, z uporabo katerih je mogoče zbrati oziroma priklicati osebne podatke iz zbirk osebnih podatkov, v katerih so enolične identifikacijske številke obdelovane ter drugi podobni znaki, ki se redno ali sistematično uporabljajo za povezovanje zbirk med različnimi upravljavci ali dveh ali več zbirk znotraj enega upravljavca;

5. izbris pomeni trajno odstranitev ali uničenje osebnega podatka, tako da ga več ni mogoče obnoviti; pri tem je zaradi zagotavljanja sledljivosti obdelave osebnih podatkov po sedmem odstavku 40. člena tega zakona dopustno tudi zabeležiti zaznamek, da je bil v zvezi osebnimi podatki določenega posameznika izveden izbris, pri čemer pa zaznamek ne sme vsebovati podatkov, ki bi omogočali obnovo izbrisane osebnega podatka;

6. anonimizacija pomeni takšno obdelavo osebnih podatkov, da je omogočena nepovratnost identifikacije posameznika, na katerega se nanašajo osebni podatki, tako da ni več določen ali določljiv, zlasti če ni možno, da bi se posameznika lahko identificiralo z uporabo drugih razpoložljivih osebnih podatkov;

7. skupni upravljavci pomenijo položaj, kadar dva ali več upravljavcev skupaj določijo namene in sredstva obdelave;

8. Odbor pomeni Evropski odbor za varstvo podatkov po členu 68 Splošne uredbe;

9. zakon pomeni glede na člen 6 Splošne uredbe ter člen 4 Direktive ta zakon, druge zakone Republike Slovenije, obvezujoče mednarodne pogodbe, ki zavezujejo Republiko Slovenijo ter pravne akte ali odločitve Evropske unije, katerih določbe so enakovredne zakonom in neposredno uporabljive ali neposredno učinkovite;

10. varnost države pomeni izvajanje nalog ali pooblastil v skladu z zakoni, ki urejajo izvajanje obveščevalnih in protiobveščevalnih dejavnosti države.

7. člen

(temeljna načela varstva osebnih podatkov)

(1) Osebni podatki se:

a) obdelujejo zakonito, tako da so izkazane pravne podlage iz člena 6 ali 9 Splošne uredbe, kar vključuje tudi, da so določene zakonske podlage za njihovo konkretno obdelavo, da so v skladu s tem zakonom določeni nameni obdelave osebnih podatkov, vrste osebnih podatkov, ki naj bi se obdelovale in rok hrambe ali izbriša osebnih podatkov ter da se obdelujejo pošteno in na pregleden način za posameznika, tako da se ne obdelujejo za prikrite ali drugače nepošteno namene, zato da posamezniki lahko ocenijo, ali lahko prostovoljno sodelujejo pri obdelavi njihovih osebnih podatkov ali da lahko temu zakonito in učinkovito ugovarjajo (»zakonitost, poštenost in preglednost«);

b) zbirajo za določene, izrecne in zakonite namene ter se ne smejo nadalje obdelovati na način, ki ni zdruhljiv s temi nameni (»omejitev namena«);

c) ustrezni, relevantni in omejeni na to, kar je potrebno za namene, za katere se obdelujejo („najmanjši obseg podatkov“);

č) točni in, kadar je to potrebno, posodobljeni; sprejeti je treba vse razumne ukrepe za zagotovitev, da se netočni osebni podatki brez odlašanja izbrišejo ali popravijo ob upoštevanju namenov, za katere se obdelujejo (»točnost in posodobljenost«);

d) hranijo v obliki, ki dopušča identifikacijo posameznikov, na katere se nanašajo osebni podatki, le toliko časa, kolikor je potrebno za namene, za katere se osebni podatki obdelujejo, razen če je z zakonom določen drug rok hrambe (»omejitev roka hrambe«);

e) obdelujejo na način, ki zagotavlja ustrezno varnost osebnih podatkov, vključno z zaščito pred nedovoljeno ali nezakonito obdelavo, pred nenamerno izgubo, uničenjem, poškodbo ali izgubo razpoložljivosti, z ustreznimi tehničnimi ali organizacijskimi ukrepi (»celovitost, zaupnost in razpoložljivost«).

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

(3) Načelo sorazmernosti obdelave osebnih podatkov iz c) točke v zvezi z b) in d) točko prvega odstavka tega člena velja za vse obdelave osebnih podatkov v Republiki Sloveniji.

8. člen

(pravna podlage za obdelavo osebnih podatkov v javnem sektorju

ter obdelava za drug namen)

(1) Osebni podatki v javnem sektorju se lahko obdelujejo, če zakon določa obdelavo osebnih podatkov, namen obdelave in vrste osebnih podatkov, ki se obdelujejo, kategorije posameznikov, na katere se nanašajo osebni podatki in po možnosti tudi rok hrambe. Zakon lahko določi tudi druge ukrepe za zagotovitev zakonite, poštene in pregledne obdelave, omejitve namena in uporabnike in druge upravljavce osebnih podatkov, ki se jim osebni podatki lahko razkrijejo. Z zakonom se lahko določi, da se določeni osebni podatki za enega ali več določenih namenov obdelujejo le na podlagi privolitve posameznika.

(2) Ne glede na prejšnji odstavek se lahko v javnem sektorju obdelujejo osebni podatki na podlagi samostojne odločitve posameznika, da jih razkrije javnemu sektorju, osebni podatki iz javnega vira ter osebni podatki, pridobljeni na drug zakonit ali običajen način, če ne gre za izvrševanje oblastvenih nalog ali pristojnosti javnega sektorja glede odločanja o človekovih pravicah, temeljnih svoboščinah ali obveznostih posameznikov, izjemoma pa tudi kadar je to nujno za izvrševanje drugih nalog javnega sektorja in se z obdelavo ne poseže v upravičen interes posameznika, na katerega se osebni podatki

nanašajo, če interes izvrševanja prevlada nad človekovimi pravicami, temeljnimi svoboščinami ali obveznostmi posameznikov. Zbirke, ki nastanejo na tej podlagi, morajo biti ločene od zbirk, ki nastanejo pri izvrševanju zakonskih nalog ali pristojnosti javnega sektorja.

(3) Ne glede na prvi odstavek tega člena se lahko v javnem sektorju obdelujejo osebni podatki posameznika, ki je z osebo javnega sektorja sklenil pogodbo, ali pa je na podlagi zahteve tega posameznika v fazi pogajanj za sklenitev pogodbe z njim, če je obdelava osebnih podatkov potrebna in primerna za izvajanje ukrepov pred sklenitvijo pogodbe ali za izvajanje pogodbe.

(4) Ne glede na prvi odstavek tega člena se lahko v javnem sektorju izjemoma obdelujejo tisti osebni podatki, ki so potrebni za zaščito življenjskih interesov posameznika, na katerega se nanašajo osebni podatki, ali druge fizične osebe.

(5) 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 izvrševanja ciljev iz prvega odstavka člena 23 Splošne uredbe in pod pogoji iz prvega odstavka tega člena določa drug zakon.

(6) Obdelava osebnih podatkov v javnem sektorju za drug namen kot za tistega, za katerega so bili zbrani, ni dopustna na podlagi prvotne privolitve, če je bila ta privolitev podana za določen namen, ki lahko vsebuje eno ali več dejanj obdelave v skladu z določenim namenom. Če je načrtovana obdelava za drug namen na podlagi privolitve, se lahko izvede le na podlagi nove privolitve posameznika, na katerega se nanašajo osebni podatki, če druga zakonska podlaga izrecno ne določa drugače.

9. člen

(pravne podlage za obdelavo osebnih podatkov v zasebnem sektorju ter obdelava za drug namen)

(1) Osebni 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 in vrste osebnih podatkov, ki se obdelujejo, kategorije posameznikov, na katere se nanašajo osebni podatki in po možnosti tudi rok hrambe. Zakon lahko, če je to potrebno, določi tudi morebitne druge ukrepe za zagotovitev zakonite, poštene in pregledne obdelave, omejitve namena in uporabnike in druge upravljavce osebnih podatkov, ki se jim osebni podatki lahko razkrijejo. Z zakonom se lahko določi, da se določeni osebni podatki za enega ali več določenih namenov obdelujejo le na podlagi privolitve posameznika.

(2) Ne glede na prejšnji odstavek se lahko v zasebnem sektorju obdelujejo osebni podatki posameznika, ki je z zasebnim sektorjem sklenil pogodbo, ali pa je na podlagi zahteve tega posameznika v fazi pogajanj za sklenitev pogodbe z njim, če je obdelava osebnih podatkov potrebna in primerna za izvajanje ukrepov pred sklenitvijo pogodbe ali za izvajanje pogodbe.

(3) Ne glede na prvi odstavek tega člena se lahko v zasebnem sektorju obdelujejo tisti osebni podatki, ki so potrebni za zaščito življenjskih interesov posameznika, na katerega se nanašajo osebni podatki, ali druge fizične osebe.

(4) Ne glede na prvi odstavek tega člena se lahko v zasebnem sektorju obdelujejo osebni podatki, če je obdelava potrebna zaradi uresničevanja upravičenih interesov, 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.

(5) Obdelava osebnih podatkov za druge namene kot tiste, za katere so bili osebni podatki prvotno zbrani, je v zasebnem sektorju dovoljena le, kadar ni nezdržljiva z nameni, za katere so bili osebni podatki prvotno zbrani ali kadar to določa ta zakon. Za ugotovitev, ali je namen nadaljnje obdelave

združljiv z namenom, za katerega so bili osebni podatki prvotno zbrani, mora upravljavec, potem ko je izpolnil vse zahteve glede zakonitosti prvotne obdelave, opraviti presojo v skladu s četrtnim odstavkom člena 6 Splošne uredbe. Presoja mora biti opravljena pred začetkom obdelave za druge namene, v pisni obliki, in je sestavni del dokumentacije po drugem odstavku člena 5 Splošne uredbe.

(6) Obdelava osebnih podatkov v zasebnem sektorju za drug namen kot za tistega, za katerega so bili zbrani, ni dopustna na podlagi prvotne privolitve, če je bila ta privolitev podana za določen namen, ki lahko vsebuje eno ali več dejanj obdelave v skladu z določenim namenom. Če je načrtovana obdelava za drug namen na podlagi privolitve, se lahko izvede le na podlagi nove privolitve posameznika, na katerega se nanašajo osebni podatki, ali na podlagi druge ustrezne pravne podlage iz tega člena.

10. člen

(posebno varstvo osebnih podatkov umrlih posameznikov)

(1) Osebni podatki umrlih posameznikov se varujejo po tem zakonu in drugih zakonih.

(2) Upravljavec podatke o umrlem posamezniku posreduje le tistim uporabnikom, ki so za obdelavo osebnih podatkov pooblaščen z zakonom in tistim, ki izkažejo pravni interes za uveljavljanje pravic pred osebami javnega sektorja.

(3) Ne glede na določbe prejšnjega odstavka upravljavec osebne podatke o umrlem posamezniku posreduje zakoncu, zunajzakonskemu partnerju, otrokom ali staršem, dedičem ali drugim osebam, če izkažejo pravni interes.

(4) Če zakon ne določa drugače, lahko upravljavec podatke o umrlem posamezniku posreduje tudi drugi osebi, ki namerava te podatke uporabljati za zgodovinske raziskovalne, znanstvene raziskovalne, statistične ali arhivske namene pod pogoji iz VII. dela tega zakona.

(5) V zgodovinskih in drugih izobraževalnih publikacijah v fizični ali elektronski obliki se lahko objavljajo zakonito pridobljeni osebni podatki umrlih posameznikov, če znanstveni ali izobraževalni namen objave prevladata nad upravičenimi interesi varstva zasebnosti umrlega posameznika, njegovega zakonca ali zunajzakonskega partnerja, otrok ali staršev ali če tako določa drug zakon.

11. člen

(pogoji za privolitev mladoletne osebe za uporabo storitev informacijske družbe)

(1) Privolitev mladoletne osebe za uporabo storitev informacijske družbe, ki se jih ponuja neposredno mladoletnim osebam oziroma za katere se lahko verjetno domneva, da jih bodo uporabljale mladoletne osebe, je veljavna le, če jo je podala mladoletna oseba, stara 15 let ali več. Če je mladoletna oseba mlajša od 15 let, je privolitev veljavna le, če jo poda ali odobri eden od staršev mladoletne osebe ali njen rejnik ali skrbnik.

(2) Upravljavec je dolžan ves čas nudenja storitve ob upoštevanju razpoložljive tehnologije v primerih iz drugega stavka prejšnjega odstavka izvajati razumna prizadevanja, zlasti s kontaktiranjem staršev, rejnikov ali skrbnikov, s katerimi preveri, ali je starš, rejnik ali skrbnik za mladoletno osebo podal ali odobril privolitev ter ali je privolitev še veljavna.

(3) Privolitev mladoletne osebe iz prvega odstavka tega člena ne sme biti pogojevana s pretiranimi pogoji s strani upravljavca, zlasti da bi bila omogočena udeležba mladoletnih oseb v igri, ponujanje nagrade, vključitve v družbeno omrežje ali druge podobne dejavnosti, tako da bi mladoletna oseba morala posredovati več osebnih podatkov, kot je potrebno za namen opravljanje takšne dejavnosti. Prepoved iz prejšnjega stavka velja tudi v primerih iz drugega stavka prvega odstavka.

12. člen

(obdelava posebnih vrst osebnih podatkov)

(1) Obdelava osebnih podatkov, ki razkrivajo rasno ali etnično poreklo, politično mnenje, versko ali filozofsko prepričanje ali članstvo v sindikatu, in obdelava genskih podatkov, biometričnih podatkov za namene edinstvene identifikacije posameznika, podatkov v zvezi z zdravjem ali podatkov v zvezi s posameznikovim spolnim življenjem ali spolno usmerjenostjo, je prepovedana.

(2) Ne glede na določbe prejšnjega odstavka je obdelava posebnih vrst osebnih podatkov dovoljena v javnem in zasebnem sektorju, če:

a) je posameznik za to podal izrecno privolitev, ki je praviloma pisna, je bila privolitev podana za enega ali več določenih namenov, v javnem sektorju pa je privolitev tudi določena z zakonom,

b) je potrebna zaradi izpolnjevanja obveznosti in posebnih pravic upravljavca na področju zaposlovanja ali je potrebna za izvajanje pravic, ki izhajajo iz zakonov s področja socialno varstvene dejavnosti, ter za izpolnjevanje obveznosti v zvezi s tem, v skladu z zakonom, ki določa tudi ustrezna jamstva pravic posameznika,

c) je nujno potrebna za varovanje življenja ali telesa ali zdravja posameznika, na katerega se osebni podatki nanašajo, ali druge osebe, kadar posameznik, na katerega se osebni podatki nanašajo, fizično ali poslovno ni sposoben dati svoje privolitve iz a) točke tega člena,

č) jih za namene zakonitih dejavnosti obdelujejo ustanove, društva, verske skupnosti, sindikati, politične stranke ali druge nepridobitne organizacije s političnim, filozofskim, verskim ali sindikalnim ciljem, vendar le, če se obdelava nanaša na njihove člane ali na posameznike, ki so v zvezi s temi cilji z njimi v rednem stiku, ter če se ti podatki ne posredujejo drugim posameznikom ali osebam javnega ali zasebnega sektorja brez pisne privolitve posameznika, na katerega se nanašajo,

d) je posameznik, na katerega se nanašajo občutljivi osebni podatki, te javno objavil, brez očitnega ali izrecnega namena, da omeji namen njihove obdelave,

e) jih za namene zdravstvenega varstva prebivalstva in posameznikov ter vodenja ali opravljanja zdravstvenih služb obdelujejo zdravstveni delavci in zdravstveni sodelavci v skladu z zakonom,

f) jih za namene izvajanja socialnega varstva prebivalstva in posameznikov ter vodenja ali opravljanja socialnih varstvenih služb obdelujejo delavci s področja socialnega varstva v skladu z zakonom,

g) tako določa zakon ali je posameznik za to podal izrecno privolitev in je obdelava potrebna iz razlogov javnega interesa na področju javnega zdravja, kot je zaščita pred velikimi nevarnostmi za zdravje ljudi s področja nalezljivih bolezni, zlasti epidemij, ki so lahko tudi čezmejne narave ali za zagotavljanje visokih standardov kakovosti in varnosti pri zdravstvenem varstvu ter zdravilnih in medicinskih izdelkih in te podatke obdelujejo zdravstveno osebje ali druge osebe, ki je zavezano k ustreznemu varovanju tajnosti in se ti podatki obdelujejo v okviru njihovih nalog,

h) je to potrebno zaradi uveljavljanja ali izvajanja pravnih zahtevkov ali obrambo pred njimi v okviru zakonsko določenih uradnih postopkov,

i) tako določa drug zakon zaradi izvrševanja bistvenega javnega interesa, kar mora biti sorazmerno z zastavljenim ciljem, spoštovati bistvo pravice do varstva podatkov ter zagotavljati ustrezne in posebne ukrepe za varstvo človekovih pravic in temeljnih svoboščin ali interesov posameznika, na katerega se nanašajo osebni podatki

j) tako določajo zakoni, ki urejajo izvajanje obveščevalnih in protiobveščevalnih dejavnosti države.

(3) V primerih obdelav posebnih vrst osebnih podatkov iz drugega odstavka je treba poleg ukrepov iz 34. člena določiti in vzpostaviti in pisno opredeliti še primerne in posebne zaščitne ukrepe za varstvo pravic, svoboščin ali interesov posameznika, na katerega se nanašajo osebni podatki. Ob upoštevanju

tehnološkega razvoja, stroškov izvajanja ter vrste, obsega, okoliščin in namenov obdelave ter različnih stopenj verjetnosti pojava tveganj, povezanih z obdelavo, za človekove pravice in temeljne svoboščine in interese posameznikov ter njihove resnosti, so ti zaščitni ukrepi najmanj naslednji:

- a) politike, postopki in ukrepi za varnost osebnih podatkov, ki zagotavljajo, da obdelava poteka skladno z zahtevami iz 29. člena tega zakona,
- b) ozaveščanje oseb, udeleženih v postopkih obdelave, o varnostnih politikah, postopkih in ukrepih za zagotavljanje varnosti osebnih podatkov,
- c) pri zagotavljanju elektronskih storitev javnega sektorja, ki vključujejo obdelavo posebnih vrst osebnih podatkov, je za dostop do teh storitev potrebno zagotoviti takšna sredstva elektronske identifikacije, kjer se ob njihovi izvedbi zahteva osebno navzočnost posameznika in njegovo identiteto preveri z vpogledom v uradni osebni dokument posameznika,
- č) pri prenosu posebnih vrst osebnih podatkov preko elektronske pošte morajo biti ti podatki šifrirani tako, da je zagotovljena njihova neprepoznavnost med prenosom in da so kontaktni podatki naslovnika predhodno preverjeni s potrditvenim sporočilom, s katerim naslovnik potrdi pravilnost podatkov za dostavo,
- d) ustrezno upravljanje uporabniških pooblastil pri upravljavcih in obdelovalcih, in
- e) kjer ustrezno, tudi psevdonimizacija oziroma šifriranje osebnih podatkov.

13. člen

(barstvo in obdelava osebnih podatkov o kazenskih obsodbah ter o odločitvah o kaznovanju za prekrške)

(1) Za podatke o vpisu ali izbrisu v ali iz kazenske evidence ali evidenc, ki se upravljajo na podlagi zakona, ki ureja prekrške (v nadaljnjem besedilu: prekrškovne evidence) ter za prenose teh podatkov velja, da gre za osebne podatke, ki morajo biti obravnavani kot posebne vrste osebnih podatkov po prvem in tretjem odstavku prejšnjega člena tega zakona.

(2) Za obdelave določenih osebnih podatkov iz kazenskih evidenc ali prekrškovnih evidenc ter v zvezi z njimi zakonsko določene namene obdelave, roke hrambe ter posredovanje osebnih podatkov javnemu ali zasebnemu sektorju iz teh evidenc veljajo pravila iz zakona, ki ureja izvrševanje kazenskih sankcij, zakona, ki ureja kazenski postopek, kazenskega zakonika, zakona, ki ureja prekrške ter mednarodnih pogodb, ki obvezujejo Republiko Slovenijo. Za posredovanje osebnih podatkov javnemu ali zasebnemu sektorju ali prenose ali čezmejne obdelave organom drugih držav ali mednarodnim organizacijam iz teh evidenc za zakonsko določene namene veljajo tudi pravila po drugih zakonskih podlagah.

(3) Kazenske evidence in prekrškovne evidence se lahko povezujejo s Centralnim registrom prebivalstva tako, da se zagotovi točnost in posodobljenost podatkov v kazenskih ali prekrškovnih evidencah.

(4) Povezovanje iz prejšnjega odstavka se izvede tako, da je možno avtomatično posodabljanje podatkov v evidencah oziroma na način, da povezovanje omogoča vsaj, da se v evidencah pri osebnih podatkih določenega ali določljivega posameznika pojavi samodejno opozorilo, da je pri njegovih podatkih v drugi zbirki osebnih podatkov prišlo do spremembe.

(5) Za povezovanje iz tretjega odstavka tega člena se za državljane Republike Slovenije ali osebe s prebivališčem v Republiki Sloveniji kot identifikacijska znaka uporabita osebno ime in njihova enotna matična številka, za tujca pa njegovo osebno ime in njegova enotna matična številka ali drug ustrezen identifikacijski znak iz kazenske evidence ali prekrškovne evidence.

II. DEL

PRAVICE POSAMEZNIKA, NA KATEREGA SE NANAŠAJO OSEBNI PODATKI

14. člen

(odgovornost upravljavca)

(1) Upravljavec sprejme ustrezne ukrepe, s katerimi zagotovi posamezniku, na katerega se nanašajo osebni podatki, vse informacije iz členov 13 in 14 ter vsa sporočila iz členov 15 do 22 in 34 v jedrnatih, preglednih, razumljivih in lahko dostopnih oblikah ter jasnem in preprostem jeziku.

(2) Upravljavec mora posamezniku, na katerega se nanašajo osebni podatki, olajšati pridobitev informacij oziroma sporočil iz prejšnjega odstavka tega člena. Če je mogoče, upravljavec na svoji spletni strani v ta namen objavi navodila ter obrazce za uveljavljanje posameznih pravic.

15. člen

(vložitev zahteve)

(1) Zahteva za uveljavljanje pravic po členih 15 do 22 Splošne uredbe se vloži pisno ali ustno na zapisnik pri upravljavcu osebnih podatkov.

(2) Upravljavec posamezniku ob prejemu zahteve pisno potrdi njen prijem, če pa to zaradi načina vložitve zahteve ni mogoče, pa mu potrditev v pisni obliki pošlje v treh delovnih dneh od prejema zahteve.

(3) Za obravnavo zahtev v zvezi z osebnimi podatki, ki jih obdelujejo upravljavci iz javnega sektorja, ter osebni podatki, ki jih zaradi izvrševanja javnih nalog ali javne oblasti izvršujejo na podlagi zakona izvršujejo upravljavci iz zasebnega sektorja, se glede vprašanj, ki niso urejena v tem delu zakona, smiselno uporablja zakon, ki ureja splošni upravni postopek.

16. člen

(ravnanje z nepopolno ali nerazumljivo zahtevo)

(1) Zahteva mora biti razumljiva in mora obsegati vse, kar je treba, da se lahko obravnava. Predvsem mora obsegati: osebno ime posameznika in druge njegove podatke, ki so potrebni za določitev osebnih podatkov, na katere se zahteva nanaša oziroma za rešitev zahteve, morebitne podatke o pooblaščenca ali zastopnika posameznika, opredelitev oblike, v kateri želi prejeti odgovor, ter opredelitev zahteve.

(2) Če je zahteva nepopolna ali nerazumljiva, mora upravljavec v roku 5 delovnih dni zahtevati, da se pomanjkljivosti odpravijo, in določiti vložniku rok, v katerem jo mora popraviti. Zahtevo za odpravo pomanjkljivosti se v obliki pisnega sporočila pošlje posamezniku na naslov, ki ga je navedel v zahtevi oziroma s katerega je poslal zahtevo, ali se mu jo izroči, če je podal zahtevo neposredno pri upravljavcu. Če posameznik v tem roku pomanjkljivosti ne odpravi, upravljavec s pisnim sporočilom zavrže njegovo zahtevo.

(3) Upravljavec lahko zaradi potrditve identitete posameznika zahteva dodatne potrebne informacije. Ugotavljanje identitete posameznika pri zahtevah, vloženih po elektronski pošti se lahko izvaja tudi:

- z varnim elektronskim podpisom s kvalificiranim potrdilom,

- s potrditvijo vloge v papirni obliki ali osebno ali
- na način osebne vročitve upravljavčeve odločitve o zahtevi na uradni naslov posameznika ali naslov, ki izhaja iz lastnih zbirk upravljavca.

17. člen

(omejitve vlaganja zahtev)

- (1) Zahteva se lahko vloži enkrat na tri mesece, glede posebnih vrst osebnih podatkov, osebnih podatkov v zvezi s kazenskimi obsodbami in kaznovanji za prekrške ali osebnih podatkov iz sistemov videonadzora pa enkrat na mesec.
- (2) Kadar je to potrebno za zagotavljanje poštene, zakonite ali sorazmerne obdelave osebnih podatkov, zlasti kadar se osebni podatki posameznika v zbirki osebnih podatkov pogosto ažurirajo ali posredujejo ali bi se lahko pogosto ažurirali ali posredovali uporabnikom osebnih podatkov, mora upravljavec osebnih podatkov posamezniku omogočiti, da vloži zahtevo tudi v krajšem ustreznem roku, ki ni krajši od petih dni od dneva odločitve o prejšnji zahtevi oziroma od poteka roka za odločitev o tej zahtevi.
- (3) Če posameznik zahtevo vloži v nasprotju s pravili iz prejšnjih dveh odstavkov, jo lahko upravljavec s pisnim sporočilom zavrže.
- (4) Pravica dostopa posameznika do lastnih osebnih podatkov po členu 15 Splošne uredbe ne vpliva na pravico do seznanitve z lastno zdravstveno dokumentacijo in z njo povezane pravice po zakonu, ki ureja pacientove pravice. Glede pravice do seznanitve z lastno zdravstveno dokumentacijo in pravice do seznanitve z zdravstveno dokumentacijo umrlih pacientov se za odločanje na prvi stopnji uporabljajo določbe zakona, ki ureja pacientove pravice in tretji odstavek tega člena in 24. člen tega zakona (omejitev pravic zakonitega zastopnika), ter na drugi stopnji določbe 21. do 25. člena tega zakona.

18. člen

(odločitev o zahtevi)

- (1) Upravljavec mora o zahtevi posameznika odločiti brez nepotrebnega odlašanja in v vsakem primeru v enem mesecu po prejemu zahteve. Ta rok se lahko po potrebi podaljša za največ dva dodatna meseca ob upoštevanju zapletenosti in števila zahtev. Upravljavec obvesti posameznika, na katerega se nanašajo osebni podatki, o vsakem takem podaljšanju v enem mesecu po prejemu zahteve skupaj z razlogi za zamudo in informacijo o možnosti pritožbe po tem ali drugem zakonu.
- (2) Če upravljavec o zahtevi ne ravna skladu s prejšnjim odstavkom tega člena, se šteje, da je zahtevo zavrnil.

19. člen

(oblika odgovora)

- (1) Upravljavec lahko o posameznikovi zahtevi odloči v obliki pisnega obvestila, ki mora vsebovati obrazložitev razlogov za odločitev in informacijo o možnosti pritožbe po tem zakonu.

20. člen

(ugovor v primeru nepopolne odločitve upravljavca)

Če posameznik po prejeti odločitvi upravljavca meni, da osebni podatki, ki jih je prejel, niso osebni podatki, ki jih je zahteval, ali da ni prejel vseh zahtevanih osebnih podatkov, lahko pred vložitvijo pritožbe pri upravljavcu vloži obrazložen ugovor v roku 15 dni. Upravljavec mora o ugovoru odločiti kot o novi zahtevi v 5 delovnih dneh.

21. člen

(pritožba)

(1) Če upravljavec ne odloči o zahtevi posameznika v roku iz petega odstavka 19. člena tega zakona, lahko posameznik pri Informacijskem pooblaščenca vloži pritožbo zaradi molka upravljavca. Če upravljavec zahtevo zavrne, lahko posameznik pri upravljavcu, če gre za javni sektor oziroma pri Informacijskem pooblaščenca, če gre za zasebni sektor vloži obrazloženo pritožbo v roku 15 dni od prejema obvestila ali odločbe upravljavca.

(2) Pravica strank do pregledovanja dokumentov v zadevah odločanja o posameznikovi pritožbi po določbah zakona, ki ureja splošni upravni postopek, do pravnomočnosti odločbe Informacijskega pooblaščenca ne vključuje pregledovanja upravne zadeve v delu, ki se nanaša na dokumente, ki so predmet zahteve in drugih dokumentov zadeve, iz katerih bi se dalo razbrati ali sklepati na vsebino zahtevanih osebnih podatkov. Smiselno enaka omejitev glede omejitev pravic do pregledovanja upravne zadeve velja tudi pri odločanju o zahtevi pri upravljavcu.

(3) Po pravnomočnosti odločbe Informacijskega pooblaščenca ali odločitve upravljavca pravica stranke iz drugega odstavka tega člena vključuje pregled zadeve zgolj s strani posameznika, na katerega se nanašajo osebni podatki, v obsegu, dovoljenem s pravnomočno odločbo Informacijskega pooblaščenca ali pravnomočno odločitvijo upravljavca.

(4) Upravljavec od prejema posameznikove zahteve do ugoditve ali v primeru zavrnitve, do pravnomočnega zaključka postopka ne sme uničiti, spremeniti ali odsvojiti zahtevanih osebnih podatkov, ne glede na potek predpisanih ali interno določenih rokov hrambe.

22. člen

(postopek obravnave pritožbe)

(1) V postopku pritožbe zoper odločitev upravljavca po tem delu zakona odloča Informacijski pooblaščenec po pravilih splošnega upravnega postopka, razen če je v tem delu zakona določeno drugače.

(2) Posameznik se lahko pritoži tudi zoper:

1. višino zaračunane razumne pristojbine iz petega odstavka člena 12 in tretjega odstavka člena 15 Splošne uredbe ter pravil iz 26. člena tega zakona in

2. odločitev upravljavca o podaljšanju roka za obravnavo zahtevkov posameznika iz petega odstavka 19. člena tega zakona.

(3) Pritožba ne vpliva na potek podaljšanega roka za odločitev.

23. člen

(pooblastila Informacijskega pooblaščenca v pritožbenem postopku)

(1) V postopku iz prejšnjega člena tega zakona ima pooblaščenca uradna oseba Informacijskega pooblaščenca, ki mora izpolnjevati pogoje za nadzornika, poleg preiskovalnih in popravilnih pooblastil iz drugega odstavka člena 58 Splošne uredbe, 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 tudi pooblaščen uradna oseba, ki ne izpolnjuje pogojev za nadzornika.

(2) V postopkih iz prejšnjega člena tega zakona lahko pooblaščen uradna oseba Informacijskega pooblaščenca opravlja ogled prostorov, osebnih podatkov in dokumentarnega gradiva ter zaslišuje osebe pri upravljavcu in priče brez prisotnosti strank postopka. 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 pooblaščen 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.

(3) V postopku iz prejšnjega člena tega zakona lahko pooblaščen uradna oseba Informacijskega pooblaščenca namesto izdaje upravne odločbe upravljavcu z ureditvenim predlogom predlaga prostovoljno rešitev posameznikove pritožbe v postavljenem roku, ki ne more biti daljši od enega meseca, če se z ureditvenim predlogom predhodno strinja posameznik in je to smiselno zaradi učinkovitega uresničevanja pravic posameznika. Po izpolnitvi ureditvenega predloga Informacijski pooblaščenec pritožbeni postopek zaključi s sklepom o ustavitvi postopka. Zoper sklep ni dovoljena pritožba, je pa dopusten upravni spor.

(4) Informacijski pooblaščenec v primerih, ki jih ni možno rešiti drugače, o pritožbi odloči z odločbo. Zoper odločbo ni dovoljena pritožba, je pa dopusten upravni spor.

(5) Informacijski pooblaščenec ima za potrebe opravljanja dejanj v pritožbenem postopku upravičenje tudi do brezplačnega in neposrednega elektronskega dostopa do osebnih podatkov v uradnih evidencah ali javnih knjigah.

(6) Če tako narekuje učinkovitost postopka, lahko Informacijski pooblaščenec o pritožbi odloči z odločbo s skrajšano obrazložitvijo, v kateri poleg izreka navede le pravno podlago in temeljni razlog odločitve ter pravni pouk. Če po prejemu odločbe s skrajšano obrazložitvijo prosilec, upravljavec ali stranski udeleženec najkasneje v 8 dneh neobvezujoče napove upravni spor zoper odločitev Informacijskega pooblaščenca, ta izda odločbo s polno obrazložitvijo v 15 dneh, s katero tudi razveljavi odločbo s skrajšano obrazložitvijo.

24. člen

(izjema glede uveljavljanja pravic posameznika preko zakonitega zastopnika)

Upravljavec lahko izjemoma zavrne zahtevo posameznika iz tega dela zakona ali dostop do lastne zdravstvene dokumentacije, ki je vložena prek zakonitega zastopnika, če so podane konkretne in objektivne okoliščine, zaradi katerih bi bilo utemeljeno sklepati, da bi bile zaradi seznanitve z določenimi osebnimi podatki neposredno ali posredno prizadete koristi, pravice ali upravičeni interesi mladoletnih oseb ali oseb z omejeno ali odvzeto poslovno sposobnostjo ali drugih oseb, za katere tako določa zakon, pri čemer te pravice in interesi pretehtajo nad interesi zakonitega zastopnika za seznanitev.

25. člen

(upravna izvršba)

(1) Za izvedbo upravne izvršbe v zvezi z odločbami, izdanimi v postopku v pritožbenem postopku je pristojen Informacijski pooblaščenec.

(2) Upravna izvršba se opravi na predlog posameznika na podlagi izvršljive odločbe in sklepa o dovolitvi izvršbe, in sicer s prisilnitvijo zoper upravljavca.

(3) Zoper sklep o dovolitvi izvršbe ni pritožbe, dovoljen pa je upravni spor.

26. člen

(zaračunavanje stroškov)

(1) Informacije in sporočila ter ukrepi iz tega dela zakona se zagotavljajo brezplačno.

(2) Kadar so zahteve posameznika, na katerega se nanašajo osebni podatki, očitno neutemeljene ali pretirane, zlasti ker se zahteve pogosto ponavljajo, zlasti če so glede istih osebnih podatkov ponovljene trikrat v enem letu, lahko upravljavec s posebno obrazloženo odločitvijo:

a) zavrne ukrepanje v zvezi z zahtevo, pri čemer mora obrazložitev iz prejšnjega stavka vsebovati tudi razloge glede očitne neutemeljenosti ali pretiranosti zahteve in nosi dokazno breme glede tega upravljavec; ali

b) zahtevi ugotovi, če so za to izpolnjeni pogoji in posamezniku zaračuna razumno pristojbino, pri čemer upošteva administrativne stroške posredovanja informacij ali sporočila oziroma izvajanja zahtevanega ukrepa po tem delu zakona.

(3) Višino pristojbine iz prejšnjega odstavka ter iz tretjega odstavka člena 15 Splošne uredbe glede dodatnih kopij osebnih podatkov in pravila o zaračunavanju predpiše Informacijski pooblaščenec, po predhodnem soglasju ministra, pristojnega za pravosodje, v predpisu se določi tudi višina stroškov na področju seznanitve z lastno zdravstveno dokumentacijo in dokumentacijo umrlih pacientov ter pravila o zaračunavanju, na kar poda predhodno soglasje minister, pristojen za zdravje.

(4) Stroške izvajanja delnega dostopa in stroške dokazovanja tehnične izvedljivosti prenosljivosti osebnih podatkov nosi upravljavec.

27. člen

(omejitve pravic posameznikov)

(1) Pravice posameznika iz tega dela zakona je mogoče z zakonom izjemoma omejiti iz razlogov in pod pogoji navedenimi v členu 23 Splošne uredbe.

(2) Omejitve iz prejšnjega odstavka se lahko določijo v skladu s prvim odstavkom 7. člena tega zakona.

(3) Ne glede na določbe prvega odstavka in še zlasti v primerih obdelave osebnih podatkov v okviru strokovnih mnenj, izdelanih v skladu z določbami zakonov, ki urejajo uradne postopke, je treba v primeru, kadar posameznik, na katerega se nanašajo osebni podatki, navaja netočnost in neposodobljenost svojih osebnih podatkov, posamezniku dati na razpolago možnost za nasprotni prikaz dejstev. Upravljavec mora nasprotni prikaz dejstev priložiti dokumentom ali ustrezno označiti na njih, kje se ta prikaz nahaja.

28. člen

(sodno varstvo pravic posameznika)

(1) Posameznik, ki ugotovi, da so kršene njegove pravice, določene s tem zakonom, lahko zahteva sodno varstvo ves čas, dokler kršitev traja.

(2) Če je kršitev iz prejšnjega odstavka prenehala, lahko posameznik vloži tožbo za ugotovitev, da je kršitev obstajala, če mu v zvezi s kršitvijo ni zagotovljeno drugo sodno varstvo.

(3) V postopku odloča pristojno sodišče po določbah zakona, ki ureja upravni spor, kolikor drug zakon ne določa drugače.

(4) V postopku je javnost izključena, če sodišče na predlog posameznika, na katerega se nanašajo osebni podatki, iz utemeljenih razlogov ne odloči drugače.

(5) V skladu s prvim odstavkom člena 80 Splošne uredbe lahko posameznik, na katerega se nanašajo osebni podatki, pisno pooblasti nevladno organizacijo s področja varstva osebnih podatkov ali zasebnosti, ki ima status nevladne organizacije v javnem interesu, da v njegovem imenu uveljavlja sodno varstvo po določbah tega člena.

(6) Postopek po določbah tega člena je prednosten.

III. DEL

UPRAVLJAVEC IN OBDELOVALEC

1. poglavje Splošne obveznosti

29. člen

(odgovornost za skladnost obdelav osebnih podatkov)

(1) Upravljavec mora izvajati ustrezne tehnične in organizacijske ukrepe za zagotovitev skladnosti obdelave z določbami Splošne uredbe, tega zakona in drugih predpisov, ki urejajo varstvo osebnih podatkov. Ukrepi morajo biti primerni glede na naravo, obseg, okoliščine in namene obdelave ter tveganja za poseg v človekove pravice in temeljne svoboščine posameznikov, ki nastajajo pri obdelavi. Ukrepe je treba tudi pregledovati in dopolnjevati, kadar je to potrebno.

(2) Upravljavec, ki obdeluje obsežno obdelavo posebnih vrst osebnih podatkov ali osebnih podatkov v zvezi s kazenskimi obsodbami in 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, mora poleg ukrepov po prejšnjem odstavku vzpostaviti in izvajati še splošno politiko varstva osebnih podatkov.

(3) Upravljavec mora biti sposoben dokazati, da obdelava poteka v skladu z določbami Splošne uredbe, tega zakona oziroma drugih predpisov, ki urejajo varstvo osebnih podatkov. To dokazuje še zlasti z vodenjem ustrezne dokumentacije glede izvajanja obveznosti po tem poglavju.

(4) Informacijski pooblaščenec izda smernice za izvajanje obveznosti po tem členu, pri čemer upošteva tudi izdane smernice Odbora glede tega vprašanja.

30. člen

(vgrajeno in privzeto varstvo osebnih podatkov)

Upravljavec mora že tekom načrtovanja nove obdelave predvideti ustrezne tehnične in organizacijske ukrepe ter varovalke za zagotovitev, da bo obdelava spoštovala temeljna načela varstva podatkov iz 7. člena tega zakona, še zlasti pa načeli sorazmernosti ter omejitve roka hrambe. Ukrepi morajo biti primerni glede na stanje najnovejšega tehnološkega razvoja na tem področju, na naravo, obseg,

okolščine 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 je treba pod pogoji iz prejšnjega člena nadaljevati tudi po začetku obdelave.

31. člen

(pogodbena obdelava)

(1) Upravljavec lahko posamezna opravila v zvezi z obdelavo osebnih podatkov s pogodbo ali dogovorom zaupa obdelovalcu.

(2) Upravljavec sme sodelovati samo s tistimi obdelovalci, ki zagotovijo zadostna jamstva o tem, da bodo izvajali ustrezne tehnične in organizacijske ukrepe za zagotavljanje skladnosti prevzetih opravil obdelave s Splošno uredbo, tem zakonom oziroma drugimi predpisi, ki urejajo varstvo osebnih podatkov.

(3) Obdelovalec brez predhodnega posebnega ali splošnega pisnega dovoljenja upravljavca v obdelavo ne sme vključiti drugih obdelovalcev, pri čemer mora upravljavec posebej presoditi ali vključitev dodatnega obdelovalca lahko vpliva na tveganost obdelave osebnih podatkov.

(4) Pogodbena obdelava pri obdelovalcu mora potekati na podlagi pogodbe ali drugega dogovora ali na podlagi izrecnega zakonskega pooblastila, ki obdelovalca zavezuje napram upravljavcu ter določa predmet, trajanje, vrsto in namen obdelave, vrsto osebnih podatkov, kategorije posameznikov, na katere se nanašajo osebni podatki ter pravice in obveznosti upravljavca ter obdelovalca. Pogodba ali dogovor mora zlasti določiti, da obdelovalec:

1. osebne podatke obdeluje samo po izkazanih navodilih upravljavca, kar vključuje tudi prenos osebnih podatkov tretji državi ali mednarodni organizaciji, če ni drugačne zakonske obveznosti, ki velja tudi za obdelovalca, vendar mora v takšnem primeru obdelovalec upravljavcu sporočiti obstoj teh pravnih podlag še pred začetkom izvajanja pogodbene obdelave, razen, če zakon ureja drugače zaradi bistvenega javnega interesa;

2. zagotovi, da so osebe, pooblaščenice za obdelavo osebnih podatkov, zavezane k varovanju zaupnosti ali da za njih velja ustrezna zakonska dolžnost varovanja tajnosti;

3. izvede vse potrebne ukrepe za zagotovitev varnosti osebnih podatkov;

4. upošteva pogoje za uporabo storitev drugega obdelovalca, kot so določene v tem členu;

5. glede na vrsto obdelave pri tej po možnosti podpira upravljavca s primernimi tehničnimi in organizacijskimi ukrepi, da izpolni svojo obveznost odgovorov na zahteve po upoštevanju v tem zakonu navedenih pravic posameznikov, na katere se nanašajo podatki;

6. ob upoštevanju vrste obdelave in razpoložljivih informacij upravljavcu pomaga pri izpolnjevanju obveznosti, navedenih v členih 32 – 36 Splošne uredbe ter po dogovoru iz pogodbe lahko tudi nudi pomoč pri izpolnjevanju drugih obveznosti po tem zakonu ali po Splošni uredbi;

7. po koncu zagotavljanja storitev pogodbene obdelave vse podatke po navodilu upravljavca vrne ali izbriše, če ne obstaja pravna obveznost glede hrambe osebnih podatkov;

8. upravljavcu zagotovi vse potrebne informacije, ki dokazujejo izpolnjevanje vseh njegovih obveznosti ter omogoči preverjanja, vključno s kontrolami, ki jih izvede upravljavec ali z njegove strani pooblaščenica oseba ter sodeluje pri njihovi izvedbi;

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

(5) Če obdelovalec uporablja tudi storitve drugega obdelovalca, da v imenu upravljavca izvede določena delovanja obdelave, se temu drugemu obdelovalcu s pogodbo ali dogovorom ali na podlagi izrecnega zakonskega pooblastila naložijo enake dolžnosti varstva osebnih podatkov, kot so navedene kot pravna obveznost za prvega obdelovalca. Če drugi obdelovalec ne izpolnjuje svojih obveznosti glede varstva osebnih podatkov, za izpolnjevanje obveznosti drugega obdelovalca v odnosu do upravljavca odgovarja prvi obdelovalec.

(6) Pogodba ali drug dogovor po določbah tretjega in četrtega odstavka tega člena mora biti sestavljena pisno ali v enakovredni elektronski obliki.

(7) Obdelovalec in vsaka oseba, podrejena upravljavcu ali obdelovalcu, ki ima dostop do osebnih podatkov, sme te podatke obdelovati le v skladu z navodili upravljavca, razen če od njiju pravo Unije ali zakonska podlaga zahtevata drugačno ravnanje.

(8) Osebnih podatkov javnih uslužbencev s področij obveščevalne in protibveščevalne dejavnosti države ni dovoljeno pogodbeno obdelovati, razen če to dovolijo predstojniki organizacij s tega področja.

(9) Obdelovalec, ki bi samostojno določil namene in sredstva obdelave, velja za upravljavca v zvezi s tako obdelavo in je odgovoren kot upravljavec.

32. člen

(evidenca dejavnosti obdelav)

(1) Upravljavec in obdelovalec upravljata evidenco dejavnosti obdelav v skladu s členom 30 Splošne uredbe in skrbita za točnost in posodobljenost te evidence.

(2) Obveznost iz prejšnjega odstavka se ne uporablja za upravljavce in obdelovalce, ki so fizične osebe ali ki so pravne osebe z manj kot 250 zaposlenimi. Izjema iz prejšnjega stavka ne velja za:

- tiste njihove obdelave, za katere je verjetno, da predstavljajo tveganje za človekove pravice ali temeljne svoboščine posameznikov, na katere se nanašajo osebni podatki,

- obdelave, ki niso le občasne obdelave osebnih podatkov, ali

- obdelave osebnih podatkov, ki vključujejo posebne vrste podatkov ali osebne podatke v zvezi s kazenskimi obsodbami ali prekrški.

(3) Izjema iz prejšnjega odstavka 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.

33. člen

(skupni upravljavci)

(1) Če dva ali več upravljavcev skupaj določijo namene in sredstva obdelave, ti upravljavci veljajo za skupne upravljavce. V dogovoru morajo določiti ali razdeliti svoje naloge v skladu s tem zakonom, zlasti v zvezi z uveljavljanjem pravic posameznikov, na katere se nanašajo osebni podatki, in s tem, kdo izpolnjuje katere od dolžnosti zagotavljanja informacij po členih 13 in 14 Splošne uredbe oziroma v primerih iz IX dela tega zakona, po 92. členu tega zakona.

(2) V dogovoru se mora navesti tudi kontaktno mesto ali kontaktna mesta za posameznike, na katere se nanašajo osebni podatki.

2. poglavje

Varnost osebnih podatkov

34. člen

(varnost osebnih podatkov)

(1) Upravljavec in obdelovalec morata zagotoviti ustrezne tehnične in organizacijske ukrepe, s katerimi se varujejo osebni podatki ter preprečuje njihovo slučajno, namerno ali drugače nezakonito uničenje, spremembo, izgubo, nepooblaščenno razkritje, dostop ali drugo nepooblaščenno obdelavo.

(2) Ukrepi po prejšnjem členu morajo biti primerni glede na stanje najnovejšega tehnološkega razvoja na tem področju, na naravo, obseg, okoliščine in namene obdelave ter resnost in verjetnost tveganj za človekove pravice in temeljne svoboščine posameznikov, ki nastajajo pri obdelavi, lahko pa se upošteva tudi stroške njihovega izvajanja. Upošteva se te okoliščine, to zlasti vključuje:

(a) psevdonimizacijo in šifriranje osebnih podatkov;

(b) ukrepe za zagotovitev stalne tajnosti, celovitosti, dostopnosti in odpornosti sistemov in storitev za obdelavo;

(c) ukrepe za zmožnost pravočasne povrnitve razpoložljivosti osebnih podatkov v primeru varnostnega incidenta;

(d) postopke rednega testiranja, ocenjevanja in vrednotenja učinkovitosti tehničnih in organizacijskih ukrepov teh ukrepov;

(e) v primeru dosegljivosti osebnih podatkov preko elektronskega komunikacijskega sredstva ali omrežja, morajo strojna, sistemska in aplikativno programska oprema zagotavljati, da je obdelava osebnih podatkov v zbirkah osebnih podatkov v mejah pooblastil uporabnika takšnega sredstva oziroma omrežja;

(f) ukrepe, ki omogočajo poznejše ugotavljanje, kdaj so bili posamezni osebni podatki vneseni v zbirko osebnih podatkov, uporabljeni ali drugače obdelani in kdo je to storil, in sicer za obdobje 5 let od zaključka leta, v katerem je potekala obdelava, razen če za obdelave posameznih vrst osebnih podatkov drug zakon ne določa drugače.

(3) Upravljavec in obdelovalec zagotovita, da katera koli fizična oseba, ki ukrepa pod vodstvom upravljavca ali obdelovalca, ki ima dostop do osebnih podatkov, slednjih ne sme obdelati brez navodil upravljavca, razen če to od nje zahteva zakon ali zakonu enakovreden predpis.

(4) Upravljavec in obdelovalec v svojih notranjih aktih predpišeta ukrepe iz prejšnjih odstavkov ter določita osebe, ki so odgovorne za določene zbirke osebnih podatkov, in osebe, ki lahko zaradi narave njihovega dela obdelujejo osebne podatke iz posamezne zbirke osebnih podatkov.

(5) Informacijski pooblaščenec izda smernice za izvajanje obveznosti po tem členu, pri čemer upošteva tudi smernice Odbora na to temo.

35. člen

(obveščanja Informacijskega pooblaščenca o kršitvah varstva osebnih podatkov)

(1) Upravljavec oziroma obdelovalec morata v skladu s členom 33 Splošne uredbe brez nepotrebnega odlašanja, najpozneje pa v roku 72 ur po seznanitvi s kršitvijo, obvestiti Informacijskega pooblaščenca o vsaki kršitvi varstva osebnih podatkov, ki jo zaznata, če je verjetno, da bo povzročila tveganje za posege v človekove pravice in temeljne svoboščine ter interese posameznikov, na katere se nanašajo osebni podatki.

(2) Upravljavec oziroma obdelovalec mora takoj po zaznavi kršitve zavarovati dnevniške zapise in druge podatke, na podlagi katerih bi se dalo ugotoviti dejstva v zvezi s kršitvijo, ter jih na poziv predložiti Informacijskemu pooblaščenцу. Navedena obveznost ne posega v obveznosti upravljavca oziroma obdelovalca do dokumentiranja kršitve po petem odstavku člena 33 Splošne uredbe.

(3) Če Informacijski pooblaščenec presodi, da je to potrebno, upravljavcu oziroma obdelovalcu v okviru inšpekcijskega postopka naloži ustrezne ukrepe, ki bi lahko prispevali k učinkovitemu obvladovanju kršitve.

(4) Če sta upravljavec oziroma obdelovalec osebne podatke prejela oziroma posredovala upravljavcu ali obdelovalcu v drugi državi članici, pa je verjetno, da zaradi kršitve lahko nastala tveganja tudi za varnost osebnih podatkov pri tem upravljavcu oziroma obdelovalcu, morata upravljavec oziroma obdelovalec o kršitvi obvestiti tudi upravljavca oziroma obdelovalca iz druge države članice.

36. člen

(obveščanje posameznikov o kršitvah varstva osebnih podatkov)

(1) Upravljavec oziroma obdelovalec morata v skladu s členom 34 Splošne uredbe brez nepotrebnega odlašanja obvestiti posameznike, katerih osebni podatki so bili kršeni ali je verjetno da so bili kršeni, o kršitvi varstva osebnih podatkov, ki jo zaznata, če je verjetno, da bo povzročila velika tveganja za pravice in svoboščine posameznikov.

(2) Obveščanje iz prejšnjega odstavka se lahko po pogoji iz tretjega odstavka člena 34 Splošne uredbe začasno odloži, omeji ali izjemoma opusti. Obveščanje je obvezno, če ga v skladu s četrtrim odstavkom člena 34 Splošne uredbe naloži Informacijski pooblaščenec.

(3) Ne glede na določbe prejšnjega odstavka lahko upravljavec v primerih, ko bi posamično obveščanje posameznikov, na katere se nanašajo osebni podatki, vključevalo nesorazmeren napor upravljavca, kar vključuje tudi neučinkovitost obveščanja in vpliv na spoštovanja pravne varnosti ali bistvenih človekovih pravic ali temeljnih svoboščin, opravi tudi obveščanje preko medijev.

3. poglavje

Ocena učinka in predhodno posvetovanje

37. člen

(Ocena učinka v zvezi z varstvom osebnih podatkov)

(1) Kadar je možno, da bi lahko obdelava, zlasti z uporabo novih tehnologij in upoštevanje naravo, obseg, okoliščine in namen te obdelave, povzročila veliko tveganje za človekove pravice in temeljne svoboščine posameznikov, mora upravljavec pred začetkom obdelave opraviti oceno učinka predvidenih dejanj obdelave na varstvo osebnih podatkov v skladu s členom 35 Splošne uredbe.

(2) Oceno učinkov je vedno treba opraviti glede:

1. obdelav, ki vključujejo sistematično in obsežno vrednotenje podatkov o posameznikih s sredstvi avtomatizirane obdelave, vključno z oblikovanjem profilov, ki potem služi kot osnova za odločitve, ki imajo za posameznika pravne posledice ali nanj na podoben način znatno vplivajo,
2. obdelave posebnih vrst podatkov ali osebnih podatkov v zvezi s kazenskimi obsodbami in prekrški v velikem obsegu,
3. sistematičen nadzor javno dostopnega območja v velikem obsegu, oziroma

4. obdelav s seznama, ki ga v skladu s pogoji iz četrtega in šestega odstavka člena 35 Splošne odredbe določi in objavi Informacijski pooblaščenec.

(3) Ocene učinkov ni treba opraviti glede:

1. obdelav s seznama, ki ga v skladu s pogoji iz petega in šestega odstavka člena 35 Splošne odredbe določi in objavi Informacijskih pooblaščenec,

2. obdelav, ki jih izvajajo upravljavci iz javnega sektorja in imajo pravno podlago v zakonu, pa je bila ocena učinkov izvedena že med sprejemanjem te zakonske podlage, vendar le, če se narava, obseg, okoliščine ali namen obdelave niso v ničemer bistvenem spremenile po izdelavi ocene.

(3) Upošteva pogoje iz prvega odstavka tega člena mora upravljavec redno pregledovati, ali obdelava poteka v skladu s priporočili iz ocene učinkov. Pregled mora vedno izvesti v primeru, da se spremeni tveganje, ki ga povzroča zadevna obdelava.

(4) Če upravljavec obdelavo, za katero je treba opraviti oceno učinkov, zaupa obdelovalcu, brez da bi prej opravil takšno oceno in ugotovljene ukrepe vključil v navodila obdelovalcu, mora obdelovalec bodisi sam izvesti oceno in jo potrditi pri upravljavcu, bodisi zavrniti izvedbo obdelave.

4. poglavje **Posebne določbe**

38. člen

(posredovanje podatkov, ki ga izvajajo organi javnega sektorja)

(1) Posredovanje osebnih podatkov, ki ga izvedejo osebe javnega sektorja, v druge osebe javnega sektorja, je dovoljeno, če je potrebno za izvajanje nalog v pristojnosti osebe javnega sektorja, ki posreduje podatke, ali tretje osebe, ki se ji podatki prenašajo, ali so izpolnjeni pogoji, ki bi dopuščali obdelavo po četrtem odstavku 8. člena in tretjem odstavku 9. člena tega zakona. Oseba javnega sektorja ali tretja oseba, ki se ji podatki posredujejo, sme osebne podatke obdelovati samo v namen, za uresničevanje katerega se ji posredujejo. Obdelava v druge namene je dovoljena le pod pogoji iz petega odstavka 8. člena tega zakona.

(2) Prenos osebnih podatkov, ki ga izvedejo organi javnega sektorja, pravnim ali fizičnim osebam zasebnega sektorja je dovoljen, če:

1. je potreben za izvajanje nalog v pristojnosti organa, ki prenaša podatke, in so izpolnjeni pogoji, ki bi dopuščali obdelavo 8. členu tega zakona;

2. tretja oseba, ki se ji podatki prenašajo, prepričljivo pojasni zakoniti interes za seznanjenost s podatki, ki naj bi se posredovali, in posameznik, na katerega se nanašajo osebni podatki, nima upravičenega interesa za izključitev posredovanja, ki bi ga bilo treba zaščititi, ali

3. je potreben za uveljavljanje, izvajanje ali obrambo pravnih zahtevkov in se je tretja oseba do organa javnega sektorja, ki prenaša podatke, obvezala, da bo podatke obdelovala samo za namen, za uresničevanje katerega se ji prenašajo.

(3) Prenos posebnih vrst osebnih podatkov po prvem odstavku člena 9 Splošne uredbe je dovoljen, če so izpolnjeni pogoji iz prvega ali drugega odstavka tega člena in gre za dejansko stanje, ki je izjema po drugem odstavku člena 9 Splošne uredbe ali po drugem odstavku 12. členu tega zakona.

(4) Upravljavec centralnega registra prebivalstva ali evidenc stalno in začasno prijavljenih prebivalcev mora na način, ki je določen za izdajo potrdila, posredovati upravičencu, ki izkaže pravni interes za

uveljavljanje pravic pred osebami javnega sektorja, osebno ime in naslov stalnega ali začasnega prebivališča ter datum smrti posameznika, zoper katerega ali v zvezi s katerim uveljavlja svoje pravice.

(5) Posredovanje osebnih podatkov na področjih varnosti države se uredi v zakonih, ki urejajo izvajanje obveščevalnih in protiobveščevalnih nalog.

39. člen

(posredovanje podatkov, ki ga izvajajo upravljavci iz zasebnega sektorja)

Upravljavec iz zasebnega sektorja posreduje osebne podatke drugim fizičnim ali pravnim osebam ali subjektom javnega sektorja zgolj na podlagi utemeljene zahteve iz drugega odstavka 40. člena, iz katere izhaja veljavna pravna podlaga za pridobitev podatkov ter utemeljenost zahteve.

40. člen

(postopek posredovanja osebnih podatkov)

(1) Upravljavec osebnih podatkov mora proti plačilu stroškov posredovanja, če zakon ne določa drugače, posredovati osebne podatke drugim fizičnim ali pravnim osebam ali subjektom javnega sektorja, ki izkažejo pravno podlago za pridobivanje zahtevanih osebnih podatkov.

(2) Zahteva za posredovanje mora vsebovati:

1. podatke o uporabniku ali upravljavcu (za fizično osebo: osebno ime, naslov opravljanja dejavnosti ali naslov stalnega ali začasnega prebivališča; za samostojnega podjetnika ter za pravno osebo: naziv oziroma firmo in naslov oziroma sedež in matično številko) ter podpis pooblaščenice osebe;
2. pravno podlago za pridobitev zahtevanih osebnih podatkov;
3. namen obdelave osebnih podatkov oziroma razloge, ki izkazujejo potrebnost in primernost osebnih podatkov za doseg namena pridobitve;
4. predmet in številko ali drugo identifikacijo zadeve, v zvezi s katero so osebni podatki potrebni;
5. vrste osebnih podatkov, ki naj se mu posredujejo; in
6. obliko in način pridobitve zahtevanih osebnih podatkov.

(3) Upravljavec osebnih podatkov mora vlagatelju zahteve, če zakon ne določa drugače, zahtevane osebne podatke posredovati najpozneje v 15 dneh od dne prejema popolne zahteve, ali pa ga v tem roku pisno obvestiti o razlogih, zaradi katerih mu zahtevanih osebnih podatkov ne bo posredoval.

(4) Če upravljavec osebnih podatkov ne ravna v skladu s prejšnjim odstavkom, se šteje, da je zahteva zavrnjena.

(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 po določbah zakona, 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 po določbah zakona, ki ureja nepravdni postopek.

(6) Določbe tega člena se ne uporabljajo, če fizična ali pravna oseba ali subjekt javnega sektorja uveljavlja pravico do pregledovanja in pridobivanja podatkov iz sodnih, upravnih ali drugih spisov po drugem zakonu.

(7) Upravljavec mora za vsako posredovanje osebnih podatkov zagotoviti, da je mogoče pozneje ugotoviti, kateri osebni podatki so bili posredovani, komu, kdaj in po kateri pravni podlagi, za kateri namen oziroma iz katerih razlogov oziroma za potrebe katerega postopka, razen če drug zakon za posredovanje posameznih vrst podatkov ne določa drugače.

(8) Revizijsko sled iz prejšnjega odstavka mora upravljavec hraniti za obdobje pet let, razen če drug zakon za posredovanje posameznih vrst podatkov ne določa drugačnega roka.

(9) Določbe sedmega in osmega odstavka veljajo tudi za obdelovalce, če so z zakonom ali pogodbo zavezani posredovati določene osebne podatke.

41. člen

(pravica do vpogleda v osebni dokument)

Upravljavec osebnih podatkov lahko pred vnosom osebnih podatkov v zbirko ali njihovo spremembo ali dopolnitvijo v zbirki preveri točnost osebnih podatkov z vpogledom v osebno izkaznico, potni list, vozniško dovoljenje ali drug osebni dokument ali drugo ustrezno javno listino posameznika, na katerega se nanašajo, ki vsebuje tudi fotografijo posameznika. Določbe prejšnjega stavka ne posegajo v določbe drugih zakonov, ki urejajo posamezne osebne dokumente glede dopustnosti kopiranja osebnega dokumenta.

42. člen

(obdelava povezovalnih znakov)

(1) Pri pridobivanju osebnih podatkov iz zbirk osebnih podatkov s področja zdravstva, policije, obrambe države, sodstva in državnega tožilstva ter kazenske evidence in prekrškovnih evidenc ni dovoljena uporaba povezovalnega znaka, določenega z zakonom, na način, da bi se za pridobitev osebnega podatka uporabil izključno ta znak.

(2) Ne glede na prejšnji odstavek se lahko izjemoma uporabi povezovalni znak za pridobivanje osebnih podatkov, če je to podatek v konkretni zadevi, ki lahko omogoči, da se odkrije ali preganja kaznivo dejanje po uradni dolžnosti, da se zavaruje življenje ali telo posameznika. O tem je potrebno brez odlašanja napraviti uradni zaznamek ali drug ustrezni zapis, ki omogoča naknadno preverjanje nujnosti uporabe povezovalnega znaka.

(3) Na področjih varnosti države se povezovalni znak lahko uporablja na način, da se za pridobitev določenega osebnega podatka uporabi izključno ta znak, v skladu z aktom o varnosti osebnih podatkov ter ob upoštevanju sledljivosti obdelav osebnih podatkov iz sedmega odstavka 40. člena tega zakona.

(4) Prvi odstavek tega člena se ne uporablja za zemljiško knjigo, sodni register in poslovni register, če tako določa drug zakon.

43. člen

(rok hrambe osebnih podatkov, določitev roka in vezanost na rok)

(1) Rok hrambe osebnih podatkov mora biti zaradi spoštovanja določenega namena obdelave osebnih podatkov omejen na najkrajše možno obdobje, in le dokler je to potrebno za doseg namena obdelave, zaradi katerega so se osebni podatki zbirali in nadalje obdelovali, razen če zakon za posamezne obdelave določa poseben rok hrambe.

(2) Upravljavec mora, upoštevaje naravo obdelovanih podatkov in tveganja, redno in na dokumentiran način preverjati, ali so roki hrambe skladni s prejšnjim odstavkom .

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

IV. DEL

POOBLAŠČENE OSEBE ZA VARSTVO OSEBNIH PODATKOV, KODEKSI RAVNANJA IN CERTIFICIRANJE

1. poglavje

Pooblaščen osebe za varstvo podatkov

44. člen

(opredelitev pooblaščen osebe za varstvo osebnih podatkov)

Pooblaščen oseba za varstvo osebnih podatkov (v nadaljevanju: pooblaščen oseba) je oseba z ustreznimi poklicnimi odlikami in zlasti strokovnim znanjem ter dejanskimi izkušnjami o zakonodaji in praksi na področju varstva osebnih podatkov ali na primerljivem področju, ki upravljavcu ali obdelovalcu na neodvisen način pomaga pri zagotavljanju skladnosti obdelave osebnih podatkov s pravili Splošne uredbe ter določbami tega zakona in drugih zakonov, ki urejajo obdelavo in varstvo osebnih podatkov.

45. člen

(obveznost določitve pooblaščen osebe)

(1) Pooblaščen osebo morajo določiti:

1. vsi upravljavci in obdelovalci v javnem sektorju;

2. tisti upravljavci ali obdelovalci v zasebnem sektorju, katerih temeljne dejavnosti zajemajo takšne obdelave osebnih podatkov, ki zaradi svoje narave, obsega oziroma namenov vključujejo redno, in sistematično obsežno spremljanje posameznikov, na katere se nanašajo osebni podatki,

3. tisti upravljavci ali obdelovalci, katerih temeljne dejavnosti zajemajo obsežne obdelave posebnih vrst osebnih podatkov ali osebnih podatkov v zvezi s kazenskimi obsodbami in prekrški.

(2) Drugi upravljavci ali obdelovalci lahko prostovoljno določijo pooblaščen osebo.

(3) Vsak upravljavec ali obdelovalec, ki je določil pooblaščen osebo, lahko imenuje njenega namestnika za čas njene zadržanosti ali odsotnosti. Namestnik opravlja njene naloge in ima vsa pooblastila in upravičenja po določbah tega zakona za čas zadržanosti ali odsotnosti pooblaščen osebe.

(4) Upravljavac ali obdelovalec, ki je določil pooblaščen osebo, mora v roku osmih dni od imenovanja vpisati njene kontaktne podatke po členu 30 Splošne uredbe v svoji evidenci dejanj obdelave po 32. členu tega zakona, jih javno objaviti na primeren način, zlasti na spletni strani ter jih sporočiti

Informacijskemu pooblaščenцу, ki teh podatkov ne objavi javno. Prav tako s temi kontaktnimi podatki, zlasti preko objave na spletni strani, seznanijo posameznike, na katere se nanašajo osebni podatki, ki jih obdeluje.

46. člen

(pogoji za imenovanje pooblaščenih oseb)

(1) Za pooblaščen osebno je lahko določen posameznik ali posameznica, ki izpolnjuje pogoje iz petega odstavka člena 37 v zvezi s členom 39 Splošne uredbe ter drugega odstavka tega člena.

(2) Za pooblaščen osebno upravljalca ali obdelovalca v javnem sektorju je lahko določen posameznik, ki poleg pogojev iz prejšnjega odstavka izpolnjuje še naslednje pogoje:

1. je državljan Republike Slovenije ali države članice Evropske unije ali države članice Evropskega gospodarskega prostora in aktivno obvlada slovenski jezik,

2. je poslovno sposoben,

3. ima najmanj izobrazbo, pridobljeno po študijskem programu druge stopnje, oziroma izobrazbo, ki ustreza ravni izobrazbe, pridobljene po študijskem programu druge stopnje, in je v skladu z zakonom, ki ureja slovensko ogrodje kvalifikacij, uvrščena na 8. raven ali ima najmanj izobrazbo, pridobljeno po študijskem programu druge stopnje, oziroma izobrazbo, ki ustreza ravni izobrazbe, pridobljene po študijskem programu druge stopnje, in je v skladu z zakonom, ki ureja slovensko ogrodje kvalifikacij, uvrščena na 9. raven,

4. ima vsaj tri leta delovnih izkušenj s področja varstva osebnih podatkov ali področja informacijske varnosti ali na primerljivih področjih varstva poslovne skrivnosti po zakonu, ki ureja gospodarske družbe ali varstva zaupnih podatkov po zakonu, ki ureja bančništvo,

5. je zaposlen v javnem sektorju,

6. ni bil pravnomočno obsojen na kazen najmanj šestih mesecev zapora, oziroma ni bil pravnomočno obsojen za kaznivo dejanje glede zlorabe osebnih podatkov ali kraje identitete.

(3) Če je za pooblaščen osebno upravljalca ali obdelovalca na področju vzgoje in izobraževanja določena oseba, ki izpolnjuje pogoje za strokovnega delavca, se šteje da izpolnjuje pogoj iz 4. točke prejšnjega odstavka.

(4) Osebe javnega sektorja, razen državnih organov, lahko za pooblaščen osebno izjemoma s pogodbo v pisni obliki določi tudi posameznika ali posameznico iz zasebnega sektorja ali pravno osebo zasebnega sektorja.

(5) Zasebni sektor lahko za pooblaščen osebno upravljalca ali obdelovalca s pogodbo v pisni obliki določi tudi posameznika ali posameznico, ki ni zaposlena pri upravljavcu ali obdelovalcu, ali pravno osebo. Pooblaščen oseba, ki je lahko le posameznik ali vodilna oseba v pravni osebi po določbi naslednjega odstavka, mora izpolnjevati vsaj pogoje iz 2., 3., 4. in 6. točke drugega odstavka tega člena.

(6) Če se v skladu s tretjim ali četrtem odstavkom tega člena določi za pooblaščen osebno pravno osebo, mora tisti njen zaposleni, ki bo opravljal naloge pooblaščenih oseb, izpolnjevati vse pogoje za določitev pooblaščenih oseb, enako velja za sodelavce iz pravne osebe, ki mu bodo pomagali. Prav tako mora biti v pogodbi z njo določen vodilni član, ki odgovarja za delo pravne osebe kot pooblaščen oseba in katerega kontaktni podatki bodo objavljeni v skladu določbami tretjega odstavka prejšnjega člena tega zakona.

(7) Če izvajajo pomoč pri opravljanju nalog pooblaščenih oseb tudi druge osebe, so te osebe vezane na navodila pooblaščenih oseb.

(8) Za pooblaščen osebo in osebe, ki ji pomagajo pri opravljanju njenih nalog ne sme biti imenovana oseba, ki ima konflikt interesov z upravljavcem ali obdelovalcem ali med njegovimi nalogami in položajem pri upravljavcu ali obdelovalcu.

(9) V javnem sektorju se šteje, da ima določena oseba konflikt interesov, če ima položaj predstojnika osebi javnega sektorja, če je član organov upravljanja ali nadzora pri upravljavcu ali obdelovalcu, če njene druge naloge vključujejo sistemsko odločanje o obdelavi osebnih podatkov pri upravljavcu ali obdelovalcu, ali če zastopa upravljavca oziroma obdelovalca v sodnih ali arbitražnih postopkih v zvezi z vprašanji varstva osebnih podatkov. V primeru, da pooblaščen oseba izve za situacijo, ki predstavlja ali bi lahko predstavljala konflikt interesov, mora o tem takoj pisno obvestiti upravljavca oziroma obdelovalca. Upravljavec oziroma obdelovalec mora v tem primeru bodisi odpraviti konflikt bodisi pooblaščen osebo razrešiti ob upoštevanju določb tretjega in četrtega odstavka 50. člena tega zakona. Enako ravna v primeru, če se na drug način seznanijo z obstojem ali verjetnostjo obstoja konflikta interesov. Vse navedeno velja tudi za osebe, ki pooblaščen osebi pomagajo pri opravljanju njenih nalog.

(10) Določbe prejšnjega odstavka se smiselno uporabljajo za zasebni sektor.

47. člen

(skupna določitev pooblaščen osebe)

(1) Več upravljavcev oziroma obdelovalcev iz javnega ali več upravljavcev iz zasebnega sektorju lahko, upošteva njihovo delovno področje, organizacijsko strukturo in velikost, ter pod pogoji iz tretjega in četrtega odstavka 46. člena, določi skupno pooblaščen osebo. Pri tem morajo zagotoviti, da je pooblaščen oseba, še vedno sposobna opravljati svoje naloge v zvezi z vsemi upravljavci ali obdelovalci, za katere je imenovana.

(2) Občine lahko določijo skupno pooblaščen osebo tudi za javne zavode, katerih ustanovitelj je, tudi v okviru skupne občinske uprave ali v okviru drugih oseb javnega sektorja, razen ministrstva. Medsebojne pravice in obveznosti se uredijo s pisno pogodbo, ki opredeli dogovor o brezplačnem sodelovanju. (3) Odvetniki lahko samostojno določijo skupno pooblaščen osebo pri Odvetniški zbornici Slovenije.

(4) Notarji lahko samostojno določijo skupno pooblaščen osebo pri Notarski zbornici Slovenije.

48. člen

(naloge pooblaščen osebe)

(1) Pooblaščen oseba opravlja naloge iz člena 39 Splošne uredbe.

(2) Pooblaščen oseba opravlja navedene naloge v zvezi z vsemi obdelavami osebnih podatkov, ki jih izvaja upravljavec oziroma obdelovalec, pri katerem je imenovana.

(3) Pooblaščen oseba sodišča ali državnega tožilstva ne sme opravljati navedenih nalog v zvezi z obdelavami osebnih podatkov, izvršenih v okviru izvajanja neodvisnega sodniškega odločanja ali odločanja strokovnih sodelavcev ali sodniških pomočnikov po odredbi sodnika ali samostojnega opravljanja državnotožilske funkcije odločanja o kazenski obtožbi ali drugi podobni odločitvi, kot ju opredeljujeta zakon, ki ureja sodišča in zakon, ki ureja državna tožilstva. Pooblaščen oseba sme opravljati te naloge samo glede zadev sodne uprave in državnotožilske uprave, kar vključuje tudi zagotavljanje varnosti osebnih podatkov.

(4) Pooblaščen oseba Ustavnega sodišča Republike Slovenije ne sme opravljati navedenih nalog v zvezi z obdelavami osebnih podatkov, izvršenih v okviru odločanja Ustavnega sodišča Republike Slovenije, kot jih opredeljuje zakon, ki ureja ustavno sodišče ali drugi zakoni. Pooblaščen oseba sme

opravljati te naloge samo glede zadev uprave Ustavnega sodišča ter glede izvajanja varnosti osebnih podatkov.

(5) Pooblaščen oseb Varuha oziroma Varuhinje človekovih pravic (v nadaljnjem besedilu: Varuh človekovih pravic) ne sme opravljati navedenih nalog v zvezi z obdelavami osebnih podatkov, izvršenih v okviru delovanja Varuha človekovih pravic, kot jih opredeljujejo zakoni, ki določajo njegove pristojnosti ali pooblastila. Pooblaščen oseb sme opravljati te naloge samo glede zadev obdelav osebnih podatkov s področja zagovornišva otrok ter glede izvajanja varnosti osebnih podatkov.

49. člen

(določitev pooblaščenih oseb in njihove naloge v določenih državnih organih)

(1) Na Ustavnem sodišču Republike Slovenije Ustavno sodišče določi eno pooblaščen oseb, ki opravlja naloge v skladu s četrtem odstavkom prejšnjega člena tega zakona.

(2) Vrhovno sodišče Republike Slovenije določi eno pooblaščen oseb, ki opravlja naloge v skladu s tretjim odstavkom prejšnjega člena tega zakona za vsa sodišča s splošno pristojnostjo in specializirana sodišča v Republiki Sloveniji.

(3) Vrhovno državno tožilstvo Republike Slovenije določi eno pooblaščen oseb, ki opravlja naloge v skladu s tretjim odstavkom prejšnjega člena tega zakona za vsa državna tožilstva v Republiki Sloveniji.

(4) Varuh človekovih pravic določi eno pooblaščen oseb, ki opravlja naloge v skladu s petim odstavkom prejšnjega člena tega zakona.

(5) Državni organi iz prvega do četrtega odstavka tega člena lahko določijo namestnike pooblaščen osebe, ki opravlja naloge pooblaščen osebe le za čas njene odsotnosti ali zadržanosti, kateri mora izpolnjevati pogoje iz drugega odstavka 46. člena tega zakona, razen pogoja iz 4. točke, kjer velja pogoj dveh let delovnih izkušenj.

(6) Vsak minister ali ministrica mora določiti svojo pooblaščen oseb, ki je zaposlena na tem ministrstvu. Če je v okviru ministrstva ustanovljen organ v sestavi, lahko minister ali ministrica kot pooblaščen oseb organa v sestavi določi javnega uslužbenca, ki je zaposlen v organu v sestavi.

(7) Na področjih izvajanja obveščevalnih in protiobveščevalnih nalog države predstojnik organizacije s tega področja določi eno pooblaščen oseb in njenega namestnika znotraj organizacije s tega področja, ki opravlja tiste naloge iz člena 39 Splošne uredbe, za katere tako določi predstojnik, med njih pa so obvezno vključene naloge glede izvajanja varnosti osebnih podatkov ter posredovanja osebnih podatkov Vladi Republike Slovenije, Predsedniku Republike Slovenije, policiji, državnim tožilstvom ali sodiščem ali pristojnemu delovnem telesu Državnega zbora Republike Slovenije, čezmejne obdelave in prenosi.

50. člen

(položaj pooblaščen osebe)

(1) Upravljavac ali obdelovalec pooblaščen osebi zagotovita pogoje za učinkovito in neodvisno opravljanje njenih nalog po 48. členu tega zakona, zlasti:

1. je ustrezno in pravočasno vključena v vsa vprašanja in postopke, povezane z varstvom osebnih podatkov in ima možnost podati ustrezni nasvet, mnenje ali predlog,
2. ima dostop do osebnih podatkov ter dejanj obdelave,

3. ima na razpolago prostorska in tehnična sredstva, potrebna za izvajanje njenih nalog in za ohranjanje njenega strokovnega znanja,

4. lahko posamezniki, na katere se nanašajo osebni podatki, z njo v slovenščini ali v drugem uradnem jeziku Republike Slovenije vstopijo v stik in se posvetujejo glede vseh vprašanj, povezanih z obdelavo njihovih osebnih podatkov in uresničevanje njihovih pravic po Splošni uredbi, ter

5. da ima neposredni dostop do vodstva upravljavca ali obdelovalca, če oceni, da je to zaradi pomembnosti določene obdelave osebnih podatkov nujno potrebno, zlasti kadar gre za tvegane obdelave, obdelave posebnih vrst osebnih podatkov, množične obdelave in vpliv na človekove pravice, temeljne svoboščine ali interese posameznikov, na katere se nanašajo osebni podatki ali za očitno neustreznost ukrepov zavarovanja osebnih podatkov, neposredni dostop vključuje možnost predstavitve stališč ali ocen o neustreznosti varstva osebnih podatkov.

(2) Upravljavec ali obdelovalec zagotovi, da pooblaščen oseba pri izvajanju svojih nalog ne prejema nobenih navodil. Pooblaščen oseba o svojem izvedenem delu neposredno in neodvisno poroča vodstvu upravljavca ali obdelovalca.

(3) Upravljavec oziroma obdelovalec pooblaščen osebe za varstvo podatkov zaradi izvajanja njenih nalog ne sme razrešiti, je kaznovati ali je zapostavljati.

(4) Odpoved delovnega razmerja pooblaščen osebi ni dovoljena za čas njenega imenovanja in še eno leto po prenehanju imenovanja, razen v primeru redne odpovedi iz razloga nesposobnosti ali krivdnega razloga, izredne odpovedi, odpovedi v postopku prenehanja delodajalca, oziroma če v primeru poslovnega razloga odkloni ponujeno ustrezno zaposlitev pri delodajalcu. V primeru statusne spremembe delodajalca, pooblaščen oseba ohrani svoj položaj pooblaščen osebe, če pri delodajalcu prevzemniku še naprej obstaja obveznost določitve pooblaščen osebe v skladu s tem zakonom in če pri delodajalcu prevzemniku ni že določena pooblaščen oseba.

51. člen

(dolžnost varstva tajnosti osebnih podatkov)

(1) Pooblaščen oseba in v njenem imenu delujoče osebe so pri opravljanju nalog zavezani k varstvu tajnosti obdelovanih osebnih podatkov. Pooblaščen oseba in v njenem imenu delujoče osebe smejo informacije, ki so jim bile dane na razpolago, uporabljati izključno za opravljanje nalog, in so tudi po zaključku dejavnosti zavezane k varovanju tajnosti osebnih podatkov.

(2) To velja zlasti v zvezi z identiteto posameznika, na katerega se nanašajo osebni podatki, ki se je obrnil na pooblaščen osebo za varstvo podatkov.

(3) Če ima pooblaščen oseba za varstvo podatkov pri svoji dejavnosti vpogled v osebne podatke, v zvezi s katerimi ima oseba, ki je podvržena nadzoru pooblaščen osebe, pravico do molka, ta pravica velja tudi za pooblaščen osebo in za v njenem imenu delujoče osebe, in sicer do mere, v kateri je oseba, ki ima zakonsko pravico do molka, slednjo uveljavila.

2. poglavje

Kodeksi ravnanja in certificiranje

52. člen

(kodeksi ravnanja)

(1) Kodeksi ravnanja so podrobnejša pravila za uporabo Splošne uredbe na posameznih delovnih področjih oziroma s strani mikro, majhnih oziroma srednjih podjetij, ki jih na prostovoljni podlagi razvijajo in pripravljajo združenja ali drugi predstavniki obdelovalcev ali upravljavcev na določenem področju, potrjujejo pa Informacijski pooblaščenec, Odbor ter Evropska komisija.

(3) Združenja in drugi predstavniki upravljavcev ali obdelovalcev, ki želijo pripraviti, spremeniti ali razširiti kodeks ravnanja, na podlagi petega odstavka člena 40 Splošne uredbe predložijo osnutek kodeksa oziroma njegove spremembe ali razširitve v potrditev Informacijskemu pooblaščenču.

(4) Informacijski pooblaščenec po prejemu osnutka izvede ugotovitveni postopek, v okviru katerega pod pogoji iz petega odstavka člena 40 Splošne uredbe ugotovi, ali je predloženi osnutek kodeksa skladen s Splošno uredbo.

(5) Če Informacijski pooblaščenec v ugotovitvenem postopku z prejšnjega odstavka ugotovi, da osnutek kodeksa ni skladen s Splošno uredbo, izda o tem odločbo. Zoper odločbo pritožba ni dopustna, je pa dopusten upravni spor.

(6) Kodeksi ravnanja, ki jih potrdi Informacijski pooblaščenec, so za upravljavce in obdelovalce, na katere se nanašajo, obvezni. Kodeksi ravnanja, ki jih v okviru postopka pregleda po devetem odstavku v zvezi z drugim odstavkom člena 93 Splošne uredbe z izvedbenim aktom dodatno potrdi in objavi Evropska komisija, so splošno veljavni in s tem obvezni za vse upravljavce, na katere se nanašajo.

(7) Če Informacijski pooblaščenec v ugotovitvenem postopku iz prejšnjega odstavka ugotovi, da je osnutek kodeksa skladen s Splošno uredbo, pred izdajo ugotovitvene odločbe preveri, ali se kodeks nanaša na dejavnosti obdelave v več državah članicah Evropske unije. V kolikor ugotovi, da se osnutek ne nanaša na takšno obdelavo, z ugotovitveno odločbo potrdi kodeks, ga po ugotovitvi pravnomočnosti odločbe vpiše v seznam potrjenih kodeksov, ki ga upravlja na svoji spletni strani ter ga objavi v Uradnem listu Republike Slovenije. V kolikor pa ugotovi, da se osnutek nanaša na takšno obdelavo, pa v skladu s sedmim odstavkom člena 40 Splošne uredbe postopek prekine in osnutek kodeksa s sklepom predloži v potrditev Odboru iz člena 68 Splošne uredbe. Če Odbor osnutka kodeksa v svojem mnenju potem ne potrdi, Informacijski pooblaščenec nadaljuje postopek in z odločbo zavrne osnutek kodeksa. Če Odbor osnutek kodeksa potrdi, Informacijski pooblaščenec nadaljuje postopek, z odločbo potrdi kodeks, ga po ugotovitvi pravnomočnosti odločbe vpiše v seznam potrjenih kodeksov na svoji spletni strani, ter ga objavi v Uradnem listu Republike Slovenije.

(8) Evropska komisija lahko pod pogoji iz devetega odstavka člena 40 Splošne uredbe z izvedbenimi akti odloči, da naj bo odobreni kodeks splošno veljaven. V tem primeru ga v skladu z desetim odstavkom člena 40 Splošne uredbe ustrezno objavi.

(9) Spremljanje uporabe odobrenih kodeksov ravnanja izvaja Informacijski pooblaščenec. V primerih kršitve kodeksa s strani upravljavca ali obdelovalca sprejme ustrezne ukrepe, vključno z začasno ali dokončno prepovedjo uporabe kodeksa upravljavcu ali obdelovalcu. Zoper odločbo iz prejšnjega stavka pritožba ni dopustna, je pa dopusten upravni spor.

(10) Informacijski pooblaščenec za spremljanje uporabe kodeksov ne sme pooblastiti drugega organa.

53. člen

(certificiranje)

(1) Certificiranje za potrebe tega zakona je prostovoljni postopek ugotavljanja, ali so dejanja obdelave osebnih podatkov s strani upravljavcev in obdelovalcev skladna z merili iz določenega mehanizma certificiranja. O ugotovitvi takšne skladnosti se upravljavcu ali obdelovalcu izda certifikat.

(2) Merila posameznega certifikacijskega mehanizma odobri Informacijski pooblaščenec v skladu s petim odstavkom člena 42 Splošne uredbe ali Odbor v skladu s petim odstavkom člena 42 Splošne uredbe.

(3) Certifikat se lahko uporablja za izkazovanje, da so dejanja obdelave osebnih podatkov s strani upravljavca ali obdelovalca skladna s Splošno uredbo, tem zakonom ali drugim zakonom, pri čemer pa posedovanje certifikata ne posega v odgovornosti upravljavca ali obdelovalca za skladnost njunih delovanj obdelave osebnih podatkov s Splošno uredbo in ne posega v nadzorne pristojnosti Informacijskega pooblaščenca po določbah tega zakona ali Splošne uredbe.

(4) Informacijski pooblaščenec upravlja seznam odobrenih certifikacijskih mehanizmov ter ga sproti objavlja na svoji spletni strani.

54. člen

(postopek akreditiranja teles za certificiranje)

(1) Certificiranje izvajajo telesa, ki jih na podlagi njihove vloge za to akreditira nacionalni akreditacijski organ (Javni zavod Slovenska akreditacija), v skladu z določbami točke b prvega odstavka člena 43 Splošne uredbe in določbami zakona, ki ureja akreditacijo. Dodatne zahteve v skladu s točko b prvega odstavka in tretjim odstavkom člena 43 Splošne uredbe določi Informacijski pooblaščenec.

(2) Slovenska akreditacija izda akreditacijsko listino certifikacijskemu telesu in o tem dejstvu obvesti Informacijskega pooblaščenca. Zoper odločbo iz prejšnjega stavka se lahko vloži pritožbo po določbah zakona, ki ureja akreditacijo, zoper odločitev o pritožbi je dopusten upravni spor.

(3) Če Odbor ali Informacijski pooblaščenec spremenita merila iz drugega odstavka prejšnjega člena ali Informacijski pooblaščenec spremeni zahteve po drugem stavku prvega odstavka tega člena, o tem obvestita Slovensko akreditacijo, ki je na njih vezana v novih postopkih po drugem stavku prvega odstavka tega člena.

V. DEL

PRENOS OSEBNIH PODATKOV TRETJIM DRŽAVAM

ALI MEDNARODNIM ORGANIZACIJAM TER ČEZMEJNE OBDELAVE OSEBNIH PODATKOV

55. člen

(splošna pravila za prenos osebnih podatkov ter za čezmejno obdelavo)

(1) Določbe tega dela zakona veljajo za primere, ko osebne podatke obdelujejo pristojni državni organi ali organi samoupravnih lokalnih skupnosti ali nosilci javnih pooblastil za namene preprečevanja, preiskovanja, odkrivanja ali pregona kaznivih dejanj, izvrševanja nalog in pooblastil policije, varnosti države, obrambe države ter izvrševanja kazenskih sankcij, v skladu z določbami Direktive ter v zvezi z IX. delom tega zakona.

(2) Pristojni organ sme osebne podatke, ki so že obdelani ali naj bi se obdelali po prenosu tretji državi oziroma mednarodni organizaciji ali naj bi se čezmejno obdelovali, posredovati le, če so upoštevane določbe tega dela in:

1. je prenos potreben za namene iz 85. člena tega zakona;
2. se osebni podatki posredujejo upravljavcu v tretji državi ali mednarodni organizaciji, ki je pristojni organ za izpolnitev enega od namenov iz 85. člena tega zakona;
3. je pristojna država članica v primerih, ko se osebni podatki posredujejo iz druge države članice Evropske unije ali tej dajo na razpolago, prenos vnaprej odobrila;

4. je Evropska komisija v skladu s 56. členom tega zakona sprejela sklep o ustreznosti ali, če tak sklep ne obstaja, so bili predloženi oziroma obstajajo ustrezni ukrepi v smislu 57. člena tega zakona ali je, če ne obstaja sklep o ustreznosti in niso predložena ustrezna zagotovila, možno v skladu s 58. členom tega zakona uporabiti izjeme za določene primere in

5. je zagotovljeno, da je nadaljnji prenos tretji državi ali drugi mednarodni organizaciji dovoljen le na podlagi predhodne odobritve pristojnega organa, ki je izvedel prvotni prenos podatkov, in ob primernem upoštevanju vseh tehničnih meril, vključno z naravo ali težo kaznivega dejanja ali prekrška, namenom prvotnega prenosa osebnih podatkov in stopnjo varstva osebnih podatkov v tretji državi ali mednarodni organizaciji, ki se ji posredujejo osebni podatki oziroma jih posreduje naprej.

(3) Prenos brez prehodne odobritve v skladu s 3. točko prejšnjega odstavka je dovoljen le, če je prenos potreben za odvrnitev neposredne in resne nevarnosti za javno varnost države članice ali tretje države ali zaradi enakovrednega pomembnega interesa države članice ter če predhodne odobritve ni bilo mogoče pravočasno pridobiti. O tem je treba nemudoma obvestiti organ, pristojen za podelitev predhodne odobritve.

(4) Prenos osebnih podatkov tretjim državam ali mednarodnim organizacijam iz razlogov varnosti države se uredi v zakonih, ki urejajo izvajanje obveščevalnih in protiobveščevalnih nalog države.

(5) Dosedanje odločitve Evropske komisije ali Informacijskega pooblaščenca o ustreznosti varstva osebnih podatkov v tretjih državah in prenosov osebnih podatkov ostanejo v veljavi, dokler niso spremenjene.

56. člen

(prenos osebnih podatkov na podlagi sklepa o ustreznosti varstva osebnih podatkov)

(1) Prenos osebnih podatkov v tretjo državo ali mednarodno organizacijo je dovoljen, če je Evropska komisija v skladu s tretjim odstavkom člena 36 Direktive na podlagi izvedbenega akta odločila, da zadevna tretja država, njena regija oziroma eden ali več specifičnih sektorjev v tej tretji državi ali zadevna mednarodna organizacija nudi ustrezno stopnjo varstva osebnih podatkov. Za tak prenos podatkov ni potrebna posebna odobritev. Določbe prejšnjega stavka ne posegajo v obveznost pridobitve dovoljenja v skladu s 3. točko prvega odstavka prejšnjega člena tega zakona.

(2) Sklep Evropske komisije, sprejet v skladu s petim odstavkom člena 36 Direktive o preklicu, spremembi ali odložitvi sklepa po tretjem odstavku člena 36 Direktive ne vpliva na prenose osebnih podatkov tretji državi, regiji oziroma enemu ali več specifičnim sektorjem v tretji državi oziroma mednarodni organizaciji v skladu s 58. in 59. členom tega zakona.

57. člen

(prenos osebnih podatkov z uveljavljanjem ustreznih ukrepov varstva osebnih podatkov)

(1) Če ne obstaja sklep v skladu s 56. členom tega zakona, je prenos osebnih podatkov v tretjo državo ali mednarodno organizacijo dopusten, če:

1. so v ustreznem pravnem aktu, zlasti zakonu ali pravnem aktu Evropske unije, ki je pravno obvezujoč za upravljavca, obdelovalca ali uporabnika, določeni ustrezni ukrepi za varstvo osebnih podatkov ali

2. je upravljavec po oceni vseh okoliščin, ki so pri prenosu pomembne, ugotovil, da dejansko obstajajo ustrezni ukrepi za varstvo osebnih podatkov.

(2) Če v skladu z 2. točko prvega odstavka obstajajo ustrezni ukrepi za določene vrste prenosov, mora upravljavec o njih obvestiti Informacijskega pooblaščenca, ki lahko odredi prepoved prenosa osebnih podatkov.

(3) Prenose v skladu z 2. točko prvega odstavka je treba dokumentirati, dokumentacijo, ki vključuje datum in čas prenosa, informacije o pristojnemu organu - uporabniku, pravno podlago in razloge prenosa ter opis prenešenih osebnih podatkov, pa je treba na zahtevo dati na razpolago Informacijskemu pooblaščenču.

58. člen

(Izjeme za posamezne primere)

(1) Če ne obstajata ne sklep o ustreznosti v skladu s 56. členom tega zakona in tudi ne primeren ukrep v skladu s 57. členom tega zakona, je prenos osebnih podatkov tretji državi ali mednarodni organizaciji dopusten le, če je prenos potreben v posameznem primeru:

1. za zaščito življenjsko pomembnih interesov posameznika;
2. če je to predvideno zaradi varovanja zakonitih interesov posameznikov, na katere se nanašajo osebni podatki;
3. za odvrnitev neposredne in resne nevarnosti za javno varnost države članice Evropske unije ali tretje države;
4. za namene iz 85. člena tega zakona, ali
5. za uveljavljanje, izvajanje ali obrambo pravnih zahtevkov v povezavi z nameni iz 85. člena tega zakona.

(2) V primerih iz 4. in 5. točke prvega odstavka je prenos dovoljen le, če ni kršena nobena od nad javnim interesom prevladujočih človekovih pravic ali temeljnih svoboščin posameznikov, na katere se osebni podatki nanašajo.

(3) Za prenose v skladu s prvim odstavkom veljajo določbe tretjega odstavka 57. člena tega zakona.

59. člen

(izjemni prenosi določenim uporabnikom v tretjih državah)

(1) Pristojni državni organi Republike Slovenije, ki so upravljavci, lahko izvedejo prenos osebnih podatkov v tretjo državo v posebnem posameznem primeru, tako da jih prenesejo neposredno uporabniku javnega ali zasebnega sektorja v tretji državi, če je prenos nujno potreben za opravljanje njegovih konkretnih zakonskih nalog, četudi to ni centralni pristojni organ tretje države in:

1. je prenos nujno potreben za izvajanje naloge upravljavca iz Republike Slovenije v skladu z zakonom ali pravnim aktom Evropske unije za namene iz 85. člena tega zakona,
2. v konkretnem primeru človekove pravice in temeljne svoboščine posameznika, na katerega se nanašajo osebni podatki, ne prevladujejo nad javnim interesom za prenos,
3. bi bil prenos po drugih določbah tega dela zakona neučinkovit ali neprimeren, zlasti ker ga ni mogoče izvesti pravočasno ter je centralni pristojni organ tretje države o tem obveščen brez odlašanja, razen če to ni učinkovito ali primerno in
4. upravljavec iz Republike Slovenije uporabniku sporoči dopustne namene obdelave in ga zaveže, da lahko te osebne podatke obdeluje samo za ta namen in v obsegu, v katerem je obdelava za te namene potrebna.

(2) Za prenose po prvem odstavku se uporabljata drugi in tretji odstavek 57. člena.

(3) Ne glede na določbe prvega in drugega odstavka tega člena se prenos osebni podatkov centralnim pristojnim organom in drugim organom tretje države lahko izvedejo v skladu z obvezujočimi mednarodnimi pogodbami s področja pravosodnega sodelovanja v kazenskih zadevah in policijskega sodelovanja.

VI. DEL

NADZORNI ORGAN ZA VARSTVO OSEBNIH PODATKOV REPUBLIKE SLOVENIJE

1. poglavje

Položaj in temeljne pristojnosti in naloge nadzornega organa za varstvo osebnih podatkov Republike Slovenije

60. člen

(nadzorni organ za varstvo osebnih podatkov Republike Slovenije)

(1) Nadzorni organ za varstvo osebnih podatkov Republike Slovenije je Informacijski pooblaščenec, kot ga določa zakon, ki ureja informacijskega pooblaščenca.

(2) Informacijski pooblaščenec je samostojni in neodvisni državni organ.

(3) Pri Informacijskem pooblaščenču delujejo državne nadzornice oziroma državni nadzorniki za varstvo osebnih podatkov (v nadaljnjem besedilu: nadzornik), ki opravljajo pristojnosti inšpekcijskega nadzora in druge naloge glede varstva osebnih podatkov po določbah Splošne uredbe, tega zakona in drugih zakonov ali predpisov.

(4) Informacijski pooblaščenec in namestniki informacijskega pooblaščenca imajo enaka pooblastila in pristojnosti, kot velja za nadzornike iz prejšnjega odstavka.

(5) Informacijskemu pooblaščenču, namestnikom informacijskega pooblaščenca in nadzornikom lahko pri izvajanju pristojnosti iz tretjega odstavka, zlasti ugotavljanju dejstev in okoliščin, pomembnih za odločanje, ter opravljanju strokovnih oziroma administrativnih opravil, po pooblastilu informacijskega pooblaščenca pomagajo drugi zaposleni pri Informacijskem pooblaščenču.

61. člen

(temeljne pristojnosti Informacijskega pooblaščenca)

(1) Informacijski pooblaščenec samostojno in neodvisno izvaja inšpekcijski nadzor nad izvajanjem določb Splošne uredbe, tega zakona in drugih zakonov, ki urejajo varstvo, obdelavo ali prenos osebnih podatkov oziroma prenos osebnih podatkov iz Republike Slovenije, ter opravlja druge naloge ali pooblastila, ki jih določajo ti predpisi.

(2) Informacijski pooblaščenec pri inšpekcijskem nadzoru iz prejšnjega odstavka izvaja tudi nadzor glede uporabe podzakonskih predpisov, ki so izdani na podlagi predpisov iz prejšnjega odstavka.

(3) Informacijski pooblaščenec je pristojen za izvajanje inšpekcijskih nadzorov nad vsemi obdelavami osebnih podatkov v Republiki Sloveniji, v skladu s 4. členom tega zakona.

(4) Informacijski pooblaščenec je prekrškovni organ, pristojen za nadzor glede izvajanja določb tega zakona, drugih zakonov ali uredb, ki urejajo varstvo osebnih podatkov ter kot prekrškovni organ pristojen za nadzor glede izvajanja določb Splošne uredbe v zvezi s prekrški iz člena 83 Splošne uredbe.

62. člen

(izjeme glede pristojnosti Informacijskega pooblaščenca)

(1) Ne glede na določbe drugega odstavka prejšnjega člena Informacijski pooblaščenec ni pristojen za inšpekcijski nadzor glede:

1. obdelav osebnih podatkov, izvršenih v okviru izvajanja neodvisnega sodniškega odločanja, kot to opredeljuje zakon, ki ureja sodišča ali odločanja strokovnih sodelavcev ali sodniških pomočnikov po odredbi sodnika, kot to opredeljuje zakon, ki ureja sodišča ali po določbah drugih zakonov, ki določajo njihovo samostojno delovanje,

2. obdelav osebnih podatkov, izvršenih v okviru opravljanja kazenskega pregona ali uporabe pravnih sredstev v skladu z zakonom, ki ureja državno tožilstvo,

3. obdelav osebnih podatkov, izvršenih v okviru sodniškega odločanja Ustavnega sodišča Republike Slovenije o ustavnosti, zakonitosti ali človekovih pravicah ali temeljnih svoboščinah, kot jih opredeljuje zakon, ki ureja ustavno sodišče ali drugi zakoni,

4. obdelav osebnih podatkov, izvršenih v okviru delovanja Varuha človekovih pravic, kot jih opredeljujejo zakoni, ki določajo njegove pristojnosti ali pooblastila, razen glede zadev obdelav osebnih podatkov s področja zagovornišva otrok,

5. obdelav osebnih podatkov na področjih predkazenskega postopka ali obveščevalno-varnostne dejavnosti, le v delih, iz katerih bi bilo lahko razvidno, da v postopku delujejo ali sodelujejo tajni delavci oziroma sodelavci po določbah zakona, ki ureja kazenski postopek, zakona, ki ureja obrambo ali zakona, ki ureja Slovensko obveščevalno-varnostno agencijo oziroma bi bila lahko razkrita identiteta teh posameznikov,

6. obdelav osebnih podatkov na področju zaščiteneh prič po določbah zakona, ki ureja zaščito prič, le v delu, iz katerega bi bila lahko razkrita identiteta teh posameznikov.

(2) Informacijski pooblaščenec je ne glede na prejšnji odstavek tega člena pristojen za opravljanje inšpekcijskega nadzora v zvezi z zadevami sodne uprave, državnotožilske uprave, sodne uprave Ustavnega sodišča Republike Slovenije, sekretariata Varuha človekovih pravic ter glede izvajanja ukrepov in postopkov s področja varnosti osebnih podatkov. Informacijski pooblaščenec je pristojen za opravljanje inšpekcijskega nadzora glede zadev iz prejšnjega stavka tudi glede sledljivosti obdelav in posredovanj osebnih podatkov po (f) točki drugega odstavka 34. člena in sedmem odstavku 40. člena tega zakona ter posredovanj osebnih podatkov in čezmejnih obdelav osebnih podatkov - vseh državnih organov iz prejšnjega odstavka tega člena, razen kadar gre za posredovanje osebnih podatkov med sodišči za potrebe odločanja v sodnih postopkih ali med državnimi tožilstvi za potrebe državnotožilskega odločanja.

63. člen

(naloge Informacijskega pooblaščenca glede posvetovanj o uvedbah obdelav osebnih podatkov)

(1) Informacijski pooblaščenec daje predhodna mnenja ministrstvu, državnemu zboru ter državnemu svetu, organom samoupravnih lokalnih skupnosti, drugim državnim organom ter nosilcem javnih pooblastil o skladnosti določb predlogov zakonov, podzakonskih predpisov ter drugih predpisov (v nadaljnjem besedilu: pravni akt) s tem zakonom, Splošno uredbo in drugimi zakoni ter predpisi, ki urejajo osebne podatke.

(2) Organi in nosilci javnih pooblastil iz prejšnjega odstavka so se dolžni pravočasno, v skladu z določbami o rokih iz drugega odstavka člena 36 Splošne uredbe, predhodno posvetovati z Informacijskim pooblaščencom po določbah prejšnjega odstavka glede skladnosti predlaganega pravnega akta iz prejšnjega odstavka. Kadar predlagani pravni akt predvideva tudi obdelave, glede katerih je v skladu s 37. členom tega zakona opraviti oceno učinka v zvezi z varstvom podatkov, mora predlagatelj predpisa v okviru posvetovanja Informacijskemu pooblaščenцу predložiti tudi oceno učinka.

(3) Kadar zakon določa, da Informacijski pooblaščenec poda soglasje k predlogu pravnega akta, se smiselno uporabljajo določbe prejšnjega odstavka.

(4) Mnenje Informacijskega pooblaščenca mora biti del javno dostopnega gradiva predloga pravnega akta iz prvega odstavka tega člena, skupaj z odzivom organa ali nosilca javnega pooblastila.

(5) Informacijski pooblaščenec lahko samostojno odloči, da posreduje tudi naknadno mnenje organu ali nosilcu javnega pooblastila iz prvega odstavka tega člena, če oceni, da je bilo njegovo mnenje neutemeljeno neupoštevano.

(6) Drugi upravljavci so se dolžni predhodno posvetovati z Informacijskim pooblaščencom, s smiselno uporabo določb prvega do četrtega odstavka tega člena, kadar je iz ocene učinka na varstvo osebnih podatkov iz 37. člena tega zakona razvidno, da bi obdelava osebnih podatkov povzročila veliko tveganje za posameznike, na katere se nanašajo osebni podatki, če upravljavec ne bi sprejel ukrepov za ublažitev tveganja.

64. člen

(sodelovanje z drugimi organi)

(1) Informacijski pooblaščenec pri svojem delu sodeluje z državnimi organi, Odborom, drugimi pristojnimi organi Evropske unije za varstvo posameznikov pri obdelavi osebnih podatkov ter podobnimi organi Sveta Evrope, drugimi mednarodnimi organizacijami, tujimi nadzornimi organi za varstvo osebnih podatkov, zavodi, združenji, nevladnimi organizacijami s področja varstva osebnih podatkov ali zasebnosti ter drugimi organizacijami in organi glede vseh vprašanj, ki so pomembna za varstvo osebnih podatkov.

(2) Informacijski pooblaščenec je pristojen tudi za skupno ukrepanje ali preiskovanje z drugimi nadzornimi organi držav članic po členu 62 Splošne uredbe.

(3) V okviru delovanja po prejšnjem odstavku so člani ali osebje drugega nadzornega organa dolžni izvajati nadzor tako, da nadzor vodi Informacijski pooblaščenec, če se nadzor izvaja na ozemlju Republike Slovenije ali v okviru pristojnosti Informacijskega pooblaščenca po tem zakonu, pri tem lahko uporabljajo le preiskovalna pooblastila po določbah tega zakona ali Splošne uredbe. Člani ali osebje drugega nadzornega organa krijejo svoje stroške.

(4) Če Informacijski pooblaščenec izvaja nadzor po drugem odstavku v drugi državi članici Evropske unije, ga izvaja tako, da nadzor vodi pristojni nadzorni organ druge države članice. Predstavniki Informacijskega pooblaščenca v okviru tega nadzora krijejo svoje stroške.

2. poglavje

Inšpekcijski nadzor in javnost delovanja

65. člen

(uporaba predpisov, ki urejajo opravljanje inšpekcijskega nadzora)

Za opravljanje inšpekcijskega nadzora po določbah tega zakona in po določbah Splošne uredbe se uporabljajo določbe Splošne uredbe in tega zakona ter določbe zakona, ki ureja inšpekcijski nadzor in določbe zakona, ki ureja splošni upravni postopek, kolikor Splošna uredba in ta zakon ne določata drugače.

66. člen

(obseg inšpekcijskega nadzora)

V okviru inšpekcijskega nadzora Informacijski pooblaščenec:

1. nadzoruje skladnost obdelave osebnih podatkov z določbami Splošne uredbe, tega zakona in drugih predpisov, ki urejajo obdelavo osebnih podatkov;
2. nadzoruje ustreznost postopkov in ukrepov za varnost osebnih podatkov ter njihovo izvajanje;
3. nadzoruje izvajanje določb Splošne uredbe in tega zakona glede prenosa osebnih podatkov v tretjo državo in o njihovem prenosu uporabnikom v tretji državi ter čezmejno obdelavo osebnih podatkov.

67. člen

(neposredno opravljanje inšpekcijskega nadzora)

(1) Inšpekcijski nadzor neposredno opravljajo nadzorniki, informacijski pooblaščenec in namestniki informacijskega pooblaščenca v mejah pristojnosti Informacijskega pooblaščenca.

(2) Nadzornik, informacijski pooblaščenec in namestnik informacijskega pooblaščenca izkazuje pooblastilo za opravljanje nalog inšpekcijskega nadzora s službeno izkaznico in značko, ki vsebuje fotografijo nadzornika, informacijskega pooblaščenca ali namestnika informacijskega pooblaščenca, njegovo osebno ime, strokovni ali znanstveni naslov ter navedbo organa in pooblastil. Obliko in vsebino službene izkaznice in značke podrobneje predpiše Informacijski pooblaščenec.

68. člen

(preiskovalna pooblastila)

(1) Pri opravljanju inšpekcijskega nadzora so nadzornik, namestniki informacijskega pooblaščenca in informacijski pooblaščenec upravičeni, poleg uporabe preiskovalnih pooblastil iz Splošne uredbe:

1. pregledovati vsebino zbirk ne glede na njihovo tajnost ali drugo vrsto zaupnosti;
2. pregledovati dokumentacijo, ki se nanaša na obdelavo osebnih podatkov, ne glede na njeno zaupnost ali tajnost, ter na prenos osebnih podatkov v tretjo državo in posredovanje uporabnikom osebnih podatkov iz tretjih držav, ne glede na njeno tajnost ali drugo vrsto zaupnosti;
3. brez predhodne najave in brez navzočnosti upravljavca ali obdelovalca, njegovega zakonitega zastopnika oziroma pooblaščenca opraviti pregled vsebine in preveriti način delovanja zavezančevih spletnih strani in drugih elektronsko dostopnih storitev, le če gre za domnevno manjše kršitve oziroma obdelave, ki niso tvegane narave ali ne vsebujejo posebnih vrst osebnih podatkov ali če je to potrebno za nujno predhodno ukrepanje;
4. preverjati postopke in ukrepe ter pregledovati dokumentacijo in akte, ki se nanašajo na varnost osebnih podatkov oziroma na njeno izvajanje;

5. pregledovati prostore, v katerih se obdelujejo osebni podatki, računalniško in drugo opremo ter tehnično dokumentacijo;

6. izvajati druga pooblastila, določena z zakonom, ki ureja inšpekcijski nadzor, ter zakonom, ki ureja splošni upravni postopek;

7. opravljati druga preiskovalna pooblastila, določena z zakonom.

(2) Kadar se izvaja ukrep iz 2. ali 5. točke prejšnjega odstavka brez privolitve upravljavca ali obdelovalca iz zasebnega sektorja in obstaja očitna možnost, da bi lahko prišlo do posega v pravice do komunikacijske zasebnosti ali prostorske zasebnosti ali v odvetniško zaupnost, sodišče, pristojno za kazenske zadeve, odloči, ali se pregled izvede, če obstaja utemeljen sum, da je upravljavec ali obdelovalec kršil ali krši določbe Splošne uredbe, tega zakona ali drugih zakonov ali predpisov, in je verjetno, da se bodo pri pregledu prostorov, dokumentacije in stvari v njem našli dokazi, ki so pomembni za odločanje v postopku inšpekcijskega nadzora ali prekrškovnem postopku. Pregled elektronskih naprav mora biti opravljen na način, s katerim se v najmanjši možni meri posega v pravice oseb, ki niso zavezanci za nadzor, in varuje tajnost oziroma zaupnost podatkov ter ne povzroča nesorazmerna škoda. Pregled se opravi ob navzočnosti dveh polnoletnih prič in zavezanca, če določeno elektronsko napravo iz prostora zavezanca uporablja oseba, ki upravičeno pričakuje zasebnost na njej, pa ima tudi ona pravico biti navzoča ob pregledu njene vsebine.

(3) Odločbo po prejšnjem odstavku izda sodišče najpozneje v 24 urah od vložitve predloga Informacijskega pooblaščenca. Odločba mora vsebovati:

- opredelitev prostorov oziroma elektronskih naprav, ki jih je treba pregledati;
- opredelitev razlogov za preiskavo;
- opredelitev dokazov oziroma vsebine podatkov, ki se iščejo;
- navedbo okoliščin za uporabo preiskovalnega dejanja in način njegove izvršitve.

(4) O opravljenem inšpekcijskem ogledu se sestavi zapisnik, ki se lahko ne glede na določbe zakonov, ki urejata upravni in inšpekcijski postopek, v primeru, ko ne gre za nujne in neodložljive ukrepe, sestavi v roku 15 dni od dneva opravljenega nadzora ter se vroči zavezancu. Zapisnik vsebuje ugotovljeno dejansko stanje, ki vključuje dejstva in okoliščine, pomembne za odločbo, vključno s posnetki in izpisi podatkov iz spletnih strani ter drugimi pridobljenimi podatki. Zavezanec lahko na zapisnik poda pripombe ter se o ugotovljenih dejstvih in okoliščinah pisno ali ustno izjavi v roku, ki ga določi nadzornik in ne sme biti krajši od 2 delovnih dni po vročitvi zapisnika, o čemer mora biti zavezanec v zapisniku izrecno poučen.

69. člen

(popravljalna pooblastila in ukrepi ter njihove omejitve)

(1) Nadzornik, informacijski pooblaščenec ali namestnik informacijskega pooblaščenca, ki pri opravljanju inšpekcijskega nadzora ugotovi kršitev določb Splošne uredbe, tega zakona ali drugega zakona ali predpisa, ki ureja varstvo osebnih podatkov, ima pristojnost, poleg uporabe popravljalnih pooblastil iz Splošne uredbe, takoj:

1. odrediti, da se nepravilnosti ali pomanjkljivosti, ki jih ugotovi, odpravijo na način in v roku, ki ga sam določi;

2. odrediti prepoved obdelave osebnih podatkov osebam javnega ali zasebnega sektorja, ki niso zagotovile ali ne izvajajo ukrepov in postopkov za varnost osebnih podatkov ali skladnost obdelave osebnih podatkov;

3. odrediti prepoved obdelave osebnih podatkov ter anonimiziranje, omejitev obdelave, psevdonimizacijo, brisanje ali uničenje osebnih podatkov, kadar ugotovi, da se osebni podatki obdelujejo v nasprotju z določbami Splošne uredbe, tega zakona in drugih zakonov;

4. odrediti prepoved prenosa osebnih podatkov v tretjo državo ali njihovega prenosa uporabnikom osebnih podatkov v tretji državi, če se posredujejo v nasprotju z določbami Splošne uredbe ali zakona;

5. odrediti druge ukrepe, določene z zakonom, ki ureja inšpekcijski nadzor, ter zakonom, ki ureja splošni upravni postopek.

(2) Ukrepov iz prejšnjega odstavka ni mogoče odrediti zoper ponudnike izključnega prenosa podatkov v komunikacijskem omrežju, če ti ne sprožajo prenosa, ne izbirajo naslovnika in prenesenih podatkov ne izberejo ali spreminjajo. Ukrepov iz prejšnjega odstavka tudi ni mogoče odrediti zoper ponudnika shranjevanja podatkov v predpomnilniku, če ta ne spreminja posredovanih podatkov in brez odlašanja odstrani ali onemogoči dostop do podatka, ki ga hrani, takoj ko je obveščen, da je bil vir podatka odstranjen iz omrežja ali da je bil dostop do njega onemogočen. Ukrepov iz prejšnjega odstavka prav tako ni mogoče odrediti zoper ponudnike gostovanja v zvezi s podatki, ki jih je zagotovil prejemnik storitve, ki ne deluje v okviru pooblastili ali pod nadzorom ponudnika gostovanja, dokler niso seznanjeni s protipravnostjo oziroma jim niso znana dejstva ali okoliščine iz katerih izhaja protipravnost tako hranjenih podatkov. Določbe prejšnjih stavkov ne vključujejo zahteve, da bi se ponudniki morali seznaniti z vsebino podatkov, če to prepoveduje drug zakon

70. člen

(odločitev, da se postopek ne uvede)

Nadzornik, namestnik informacijskega pooblaščenca ali informacijski pooblaščenec v primerih, kadar iz podatkov v prijavi, ki jo je podal posameznik, na katerega se nanašajo osebni podatki ali iz prijave druge osebe očitno, da glede na podatke iz prijave in glede na druge podatke ni možno sklepati na kršitev varstva osebnih podatkov po Splošni uredbi, tem zakonu ali drugem zakonu oziroma predpisu, ki ureja obdelavo in varstvo osebnih podatkov, s sklepom odloči, da se inšpekcijski postopek ne uvede. V obrazložitvi sklepa navedejo razloge za neuvedbo postopka.

71. člen

(pravice prijavitelja)

(1) Nadzornik, namestnik informacijskega pooblaščenca ali informacijski pooblaščenec so dolžni prijavitelja po opravljenem nadzoru in sprejetem zadnjem ukrepu oziroma ustavitvi postopka obvestiti o vseh pomembnejših ugotovitvah in dejanjih v postopku inšpekcijskega nadzora.

(2) Prijavitelj, ki meni, da obstaja kršitev varstva osebnih podatkov v zvezi z osebnimi podatki, ki se nanašajo nanj, lahko v skladu s prvim odstavkom člena 80 Splošne uredbe pisno pooblasti nevladno organizacijo s področja varstva osebnih podatkov ali zasebnosti, ki ima status nevladne organizacije v javnem interesu, da v njegovem imenu vloži prijavo pri Informacijskem pooblaščenca.

72. člen

(pravno sredstvo zoper odločitev Informacijskega pooblaščenca)

(1) Zoper odločbo ali sklep Informacijskega pooblaščenca ni dovoljena pritožba, dovoljen pa je upravni spor.

(2) V skladu s prvim odstavkom člena 80 Splošne uredbe lahko posameznik, na katerega se nanašajo osebni podatki in je bil prijavitelj, pisno pooblasti nevladno organizacijo s področja varstva osebnih podatkov ali zasebnosti, ki ima status nevladne organizacije v javnem interesu, da v njegovem imenu uveljavlja sodno varstvo po določbah prejšnjega odstavka.

73. člen

(ukrepanje ob zaznavi kaznivih dejanj ali prekrškov)

(1) Če nadzornik, namestnik informacijskega pooblaščenca ali informacijski pooblaščenec pri izvrševanju svojih pristojnosti ugotovijo, da obstaja sum storitve prekrška, ki je v pristojnosti Informacijskega pooblaščenca, izvedejo postopek po zakonu, ki ureja prekrške, po določbah Splošne uredbe ter v skladu z določbami IX. dela tega zakona.

(2) Če uradne osebe iz prejšnjega odstavka pri izvrševanju svojih pristojnosti ugotovijo, da obstaja sum storitve kaznivega dejanja ali prekrška iz pristojnosti drugega prekrškovnega organa, podajo kazensko ovadbo v skladu z zakonom, ki ureja kazenski postopek oziroma izvedejo postopke v skladu z zakonom, ki ureja prekrške.

(3) Ukrepov po zakonu o prekrških ni mogoče odrediti zoper ponudnike iz drugega odstavka 69. člena tega zakona. Določbe prejšnjih stavkov ne vključujejo zahteve, da bi se ponudniki morali seznaniti z vsebino podatkov, če to prepoveduje drug zakon.

(4) Če gre za posebej hudo kršitev tega zakona in je za izvedbo prekrškovnega postopka nujno potrebno pridobiti podatke o uporabniku storitev ponudnikov iz prejšnjega odstavka, pri tem pa je mogoče utemeljeno sklepati, da prekrška z drugimi ukrepi ne bi bilo mogoče odkriti ali dokazati oziroma bi bilo to povezano z nesorazmernimi težavami, lahko sodišče za prekrške na obrazložen predlog nadzornika, namestnika informacijskega pooblaščenca ali informacijskega pooblaščenca odredi ponudniku iz prejšnjega odstavka, da nadzorniku, namestniku informacijskega pooblaščenca ali informacijskemu pooblaščenču sporoči podatke, na podlagi katerih je mogoče identificirati tega uporabnika (osebno ime, naslov prebivališča, firma, naslov elektronske pošte).

(5) Kopija odredbe ter na njeni podlagi prejetih osebnih podatkov se posamezniku, katerega osebni podatki so bili na ta način pridobljeni, vročijo v roku osmih dni po njegovi identifikaciji oziroma najpozneje skupaj z obvestilom o prekršku.

74. člen

(varovanje tajnosti)

(1) Nadzornik, informacijski pooblaščenec in namestnik informacijskega pooblaščenca so dolžni varovati tajnost osebnih podatkov, s katerimi se seznanijo pri opravljanju inšpekcijskega nadzora, preiskovalnih pooblastil, popravljalnih ali prekrškovnih pooblastil tudi po prenehanju delovnega razmerja ali funkcije.

(2) Dolžnost iz prejšnjega odstavka velja tudi za vse javne uslužbence pri Informacijskem pooblaščenču ali druge osebe, ki sodelujejo pri postopkih po tem zakonu.

75. člen

(javnost dela in dodatna svetovanja)

(1) Informacijski pooblaščenec lahko:

1. izdaja notranje glasilo ter strokovno literaturo;

2. na spletni strani ali na drug primeren način pravočasno objavlja mnenja iz 60. člena tega zakona;
 3. na spletni strani oziroma na drug primeren način objavlja odločbe in sklepe Ustavnega sodišča Republike Slovenije o zahtevah ocene ustavnosti, ki jih je vložil Informacijski pooblaščenec ter odločitve Ustavnega sodišča Republike Slovenije o njih;
 4. na spletni strani oziroma na drug primeren način objavlja odločbe in sklepe sodišč s splošno pristojnostjo in upravnega sodišča, ki se nanašajo na varstvo osebnih podatkov, tako da iz njih ni možno razbrati osebnih podatkov strank, oškodovancev, prič ali izvedencev z uporabo psevdonimizacije;
 5. daje mnenja o skladnosti splošnih pogojev poslovanja oziroma njihovih predlogov s predpisi s področja varstva osebnih podatkov;
 6. daje neobvezna mnenja, pojasnila in stališča o vprašanjih s področja varstva osebnih podatkov in jih objavlja na spletni strani ali na drug primeren način;
 7. pripravlja in daje neobvezne smernice in priporočila glede varstva osebnih podatkov na posameznem področju;
 8. po potrebi daje izjave za javnost o izvedbi posamičnih zadev po tem zakonu;
 9. izvaja konference za medije v zvezi z delom Informacijskega pooblaščenca ter prepise izjav ali posnetke izjav s konferenc za medije objavi na spletni strani;
 10. obdeluje kontaktne podatke za izvajanje izobraževanj, posvetovanj, javnih dogodkov;
 11. na spletni strani objavlja druga pomembna obvestila.
- (2) Informacijski pooblaščenec lahko za opravljanje pristojnosti iz 5., 6., in 7. točke prejšnjega odstavka pozove k sodelovanju tudi predstavnike društev in drugih nevladnih organizacij s področja varstva osebnih podatkov, zasebnosti ter potrošnikov.

3. poglavje

Zunanji nadzor delovanja Informacijskega pooblaščenca in sodelovanje

76. člen

(letno poročilo Informacijskega pooblaščenca)

- (1) Informacijski pooblaščenec v svojem letnem poročilu poroča Državnemu zboru Republike Slovenije o stanju na področju varstva osebnih podatkov ter povezanih ugotovitvah, predlogih in priporočilih. Poročilo iz prejšnjega stavka je del skupnega letnega poročila po določbah zakona, ki ureja Informacijskega pooblaščenca.
- (2) Poročilo iz prejšnjega odstavka se posreduje tudi Evropski komisiji, Odboru ter je dostopno javnosti.

77. člen

(pristojnosti Varuha človekovih pravic)

- (1) Varuh človekovih pravic opravlja svoje naloge na področju varstva osebnih podatkov v razmerju do državnih organov, organov samoupravnih lokalnih skupnosti in nosilcev javnih pooblastil v skladu z zakoni, ki določajo njegove pristojnosti ali pooblastila.

(2) Varstvo osebnih podatkov je posebno delovno področje Varuha človekovih pravic.

78. člen

(pristojnosti Državnega zbora Republike Slovenije)

(1) Stanje na področju varstva osebnih podatkov in izvrševanje določb tega zakona, v skladu s prvim odstavkom 76. člena tega zakona, spremlja pristojno delovno telo državnega zbora.

(2) Pristojno delovno telo Državnega zbora Republike Slovenije za nadzor obveščevalnih in varnostnih služb lahko sodeluje z Informacijskim pooblaščencom, na lasten predlog ali na pobudo Informacijskega pooblaščenca, kadar je potrebna zaupna izmenjava informacij o ugotovitvah nadzornih postopkov ali glede sprememb zakonov ali drugih predpisov.

VII. DEL

POSEBNA PRAVILA GLEDE OBDELAVE OSEBNIH PODATKOV ZA ZNANSTVENE RAZISKOVALNE, ZGODOVINSKE RAZISKOVALNE, STATISTIČNE IN ARHIVSKE NAMENE

79. člen

(Obdelava osebnih podatkov v znanstvene raziskovalne, zgodovinske raziskovalne in statistične namene)

(1) Ne glede na prvotni namen obdelave lahko upravljavec osebne podatke nadalje obdeluje za znanstvene raziskovalne, zgodovinske raziskovalne in statistične namene, drug uporabnik osebnih podatkov pa za iste namene:

- če je posameznik, na katerega se osebni podatki nanašajo za takšno obdelavo podal predhodno pisno privolitev;
- če jih pridobi in nadalje obdeluje v anonimizirani obliki ali
- če tako določa drug zakon.

(2) Raziskovalne organizacije ter raziskovalci, vpisani v zbirko podatkov o izvajalcih raziskovalne in razvojne dejavnosti pri Agenciji za raziskovalno dejavnost Republike Slovenije, lahko za namen obdelave iz prejšnjega odstavka pri upravljavcu osebnih podatkov vpogledajo oziroma pridobijo posebne vrste osebnih podatkov ali druge osebne podatke praviloma v psevdonimizirani obliki, če predložijo predstavitveni elaborat raziskave, s katerim izkažejo:

- dejanski obstoj raziskave,
- da učinkovite izvedbe raziskave oziroma njenega namena ni mogoče doseči brez obdelave določenih osebnih podatkov ali bi bilo to povezano z nesorazmernim naporom ali stroški (potrebnost in primernost obdelave osebnih podatkov),
- da osebnih podatkov, ki so nujno potrebni za učinkovito izvedbo raziskave, ni mogoče pridobiti s privolitvijo posameznika.

(3) Uporabniku iz prejšnjega odstavka se praviloma omogoči vpogled, lahko pa tudi pridobitev podatkov s kopiranjem, prepisom ali izpisom, če se z vpogledom ne da doseči namena raziskave ali bi bila izvedba vpogleda povezana z nesorazmernim naporom ali stroški.

(4) Predstavitveni elaborat iz drugega odstavka zaradi varstva osebnih podatkov, ki bodo obdelovani po določbah tega dela zakona vsebuje naslednje podatke:

- o naslovu raziskave,
- o nosilcu raziskave,
- o neposrednih izvajalcih raziskave (osebno ime, naziv, prebivališče, razmerje do nosilca raziskave in šifra raziskovalca),
- o znanstveno-raziskovalnem področju (opisno in po klasifikaciji Agencije za raziskovalno dejavnost Republike Slovenije),
- o metodah dela v zvezi z obdelavo osebnih podatkov,
- o namenu oziroma cilju raziskave,
- o predvidenem času trajanja obdelave osebnih podatkov,
- o postopkih in ukrepih za zagotavljanje varnosti osebnih podatkov in
- o izpolnjevanju pogojev iz drugega in tretjega odstavka tega člena.

Elaboratu mora biti priložena ocena učinkov v zvezi z varstvom osebnih podatkov, kot je opredeljena v 37. členu tega zakona.

(5) Osební podatki, ki jih je uporabnik pridobil v skladu s 1. in 3. točko prvega odstavka in drugim odstavkom tega člena, se ob zaključku raziskave uničijo ali nepovratno anonimizirajo, če zakon ne določa drugače, če posameznik ni privolil v nadaljnjo hrambo osebnih podatkov ali če to ni pomembno za izvršitev namena raziskave. Uporabnik mora upravljavca, ki mu je posredoval osebne podatke, brez odlašanja po njihovem uničenju pisno obvestiti, kdaj in na kakšen način jih je uničil.

(6) Rezultati obdelave iz prejšnjih odstavkov se objavijo v anonimizirani obliki, razen če ta ali drug zakon določa drugače ali če je posameznik, na katerega se nanašajo osebni podatki, za objavo v neanonimizirani obliki podal pisno privolitev ali če je za takšno objavo v času po smrti posameznika podana pisna privolitev naslednjih oseb v izključujočem vrstnem redu: zakonec, zunajzakonski partner oziroma partner iz istospolne partnerske skupnosti, otroci ali starši umrlega posameznika. Upravljavec ne sme objaviti neanonimiziranih osebnih podatkov, če je to v nasprotju z interesom varovanja tajnosti ali zaupnosti postopkov odločanja, ali pa ti postopki še niso končani.

(7) Določbe tega člena ne posegajo v določbe glede obdelav osebnih podatkov po določbah zakona, ki ureja varstvo dokumentarnega in arhivskega gradiva ter arhive.

80. člen

(obdelava naslovov za kontaktiranje posameznikov v znanstvene raziskovalne, zgodovinske raziskovalne in statistične namene)

(1) V okviru obdelave osebnih podatkov za namene znanstvenega raziskovanja, zgodovinskega raziskovanja ali statističnega raziskovanja je upravljavcu izjemoma dovoljeno tudi obdelovati osebne podatke ciljne skupine posameznikov za potrebe pridobitve privolitve za obdelavo njihovih osebnih podatkov ali zaradi pridobitve dodatnih podatkov ali pojasnil za prej navedene namene.

(2) Upravljavec lahko na podlagi zbirk, s katerimi zakonito razpolaga v okviru zakonitega opravljanja dejavnosti, proti plačilu kontaktira posameznike z namenom pridobivanja privolitve za potrebe drugega uporabnika in za izvrševanje namenov iz prejšnjega odstavka:

- ki za obdelavo osebnih podatkov nima podlage v zakonu ali privolitvi in
- ki z elaboratom iz četrtega odstavka prejšnjega člena izkaže, da bo osebne podatke po pridobitvi privolitve obdeloval na znanstveno-raziskovalnem, zgodovinskem raziskovalnem ali statističnem področju.

(3) V okviru obdelave iz prvega in drugega odstavka tega člena se lahko za namen kontaktiranja obdelujejo samo osebno ime, naslov stalnega ali začasnega prebivališča, kontaktna telefonska številka ali kontaktni naslov elektronske pošte.

(4) Posredovani ali obdelani osebni podatki po tem členu se lahko obdelajo izključno za namen raziskave in jih je treba izbrisati takoj, ko niso več potrebni.

(5) Določbe tega člena ne posegajo v določbe glede obdelav osebnih podatkov po določbah zakona, ki ureja varstvo dokumentarnega in arhivskega gradiva ter arhive.

81. člen

(obdelava podatkov za namene arhiviranja v javnem interesu)

(1) Obdelava osebnih podatkov za namene arhivskega delovanja je dovoljena, če je v javnem interesu, v skladu z zakonom. Upravljevec mora v skladu z zakonom določiti ukrepe za varnost osebnih podatkov ter primerne in posebne ukrepe za varstvo interesov posameznika, na katerega se nanašajo osebni podatki, zlasti glede posebnih vrst osebnih podatkov.

(2) Posameznik, na katerega se nanašajo osebni podatki, nima pravice do seznanitve z lastnimi osebnimi podatki v arhivskem gradivu po členu 15 Splošne uredbe le, če bi dajanje informacij ali kopij njegovih osebnih podatkov zahtevalo očitno nesorazmeren napor, niti ne sme zahtevati popravka osebnih podatkov zaradi netočnosti ali neposodobljenosti v skladu s členom 16 Splošne uredbe. Posameznik, na katerega se nanašajo osebni podatki nima pravice zahtevati izvedbe izbrisa v skladu s pravico do pozabe iz člena 17 Splošne uredbe.

(3) Ne glede na določbe drugega stavka prejšnjega odstavka je treba v primeru, kadar posameznik, na katerega se nanašajo osebni podatki, navaja netočnost in neposodobljenih svojih osebnih podatkov, posamezniku dati na razpolago možnost za nasprotni prikaz dejstev. Pristojni arhiv mora nasprotni prikaz dejstev priložiti dokumentom ali ustrezno označiti na njih, kje se ta prikaz nahaja.

(4) Posameznik, na katerega se nanašajo osebni podatki, nima pravice zahtevati omejitev obdelave po členu 18, pravice do prenosljivosti osebnih podatkov po členu 20 ter izvajati pravice do ugovora po členu 21 Splošne uredbe.

VIII. DEL

VARSTVO SVOBODE IZRAŽANJA TER DOSTOPA DO INFORMACIJ V RAZMERJU DO VARSTVA OSEBNIH PODATKOV

82. člen

(varstvo svobode izražanja v razmerju do pravice do varstva osebnih podatkov)

(1) Zagotovljeno je uresničevanje svobode izražanja, kar vključuje svobodo izražanja misli, govora in javnega nastopanja, tiska in drugih oblik javnega obveščanja in izražanja v okvirih pravnega reda Republike Slovenije. Vsakdo lahko svobodno zbira, sprejema in širi vesti in mnenja ter v njih vsebovane osebne podatke, ki so v ta namen potrebni in upravičeno obdelovani.

(2) Svoboda izražanja v razmerju do varstva osebnih podatkov za namene obveščanja javnosti s strani medijev, književnega, umetniškega ali znanstvenega ustvarjanja, zaradi resne kritike, obrambe kakšne pravice ali varstva upravičene koristi ter izobraževanja, ki ga izvajajo izobraževalne organizacije ali izobraževanja preko javno dostopnih publikacij, vključuje pravice, da se osebni podatki

uporabijo, objavijo ali drugače razkrijejo za namene uresničevanja svobode izražanja pod naslednjimi pogoji:

1. če je posameznik za uporabo, objavo ali razkritje osebnih podatkov podal privolitev,
2. če je posameznik osebne podatke že javno objavil ali dal na razpolago javnosti,
3. če so osebni podatki na zakonit način že bili dostopni javnosti,
4. če so bili osebni podatki pridobljeni na podlagi prisotnosti posameznika na javno dostopnih krajih ali dogodkih, kjer posameznik glede na vse okoliščine ne more razumno pričakovati varstva zasebnosti ter na način, ki ne pomeni občutnega posega v razumno pričakovano zasebnost,
5. če gre za zakonito objavo mnenja ali vrednostne ocene, kjer je objava osebnih podatkov v njunem okviru nujna za utemeljitev mnenja ali vrednostne ocene,
6. če so bili osebni podatki pridobljeni na drug zakonit način,
7. če javni interes po obveščanju javnosti, pravica do obveščenosti ter svoboda izražanja prevladajo nad upravičenimi interesi varstva zasebnosti in drugih osebnostnih pravic posameznika, ali
8. če tako določa drug zakon.

(3) Uveljavljanje pravic v zvezi z določbami tega člena zagotavljajo sodišča v skladu z določbami zakonov, ki urejajo sodne postopke ali urejajo sodno varstvo.

(4) Nadzor nad zakonitostjo posredovanja, razkritja ali omogočanja nepooblaščenega dostopa do osebnih podatkov iz zbirke za namene iz drugega odstavka tega člena izvaja Informacijski pooblaščenec.

83. člen

(varstvo pravice do dostopa do informacij javnega značaja v razmerju do pravice do varstva osebnih podatkov)

(1) Zavezanci po zakonu, ki ureja dostop do informacij javnega značaja, javnosti posredujejo osebne podatke, če so ti po zakonu javni ali če je za njihovo razkritje podan prevladujoč javni interes po določbah zakona, ki ureja dostop do informacij javnega značaja in ne velja izjema iz navedenega zakona ali zakona, ki ureja zunanje zadeve.

(2) Zaradi uresničevanja javnega interesa na področju sodelovanja javnosti, zagotavljanja transparentnosti dela ali spremljanja njihove prakse, zavezanci iz prejšnjega odstavka po postopku iz zakona, ki ureja dostop do informacij javnega značaja proaktivno javno objavijo tudi dokumente, ki niso zajeti v prvem odstavku tega člena, in predstavljajo prosto dostopno informacijo javnega značaja, na način delnega dostopa praviloma v anonimizirani obliki. Kadar uresničevanja teh namenov na ta način ni mogoče zagotoviti, pa jih lahko javno objavijo v psevdonimizirani obliki v skladu s Splošno uredbo ter ob upoštevanju drugih zakonskih izjem v skladu z določbami zakona, ki ureja dostop do informacij javnega značaja.

(3) Uveljavljanje pravic v zvezi z določbami tega člena zagotavljajo Informacijski pooblaščenec v skladu z določbami zakona, ki ureja dostop do informacij javnega značaja in določbami zakona, ki ureja medije ter sodišča v skladu z določbami zakonov, ki urejajo sodne postopke ali urejajo sodno varstvo.

84. člen

(izjema glede obveščanja posameznika)

Če so osebni podatki javni na podlagi zakona, posameznika ni treba obveščati po členu 12. do 14. Splošne uredbe in po določbah zakona, ki ureja splošni upravni postopek.

IX. DEL

OBDELAVA OSEBNIH PODATKOV ZA NAMENE PREPREČEVANJA, PREISKOVANJA, ODKRIVANJA ALI PREGONA ZARADI KAZNIVIH DEJANJ, IZVRŠEVANJA NALOG IN POOBLASTIL POLICIJE, VARNOSTI DRŽAVE, OBRAMBE DRŽAVE TER IZVRŠEVANJA KAZENSKIH SANKCIJ

1. poglavje

Splošne določbe

85. člen

(področje uporabe tega dela zakona)

(1) Določbe tega dela zakona veljajo za primere, ko osebne podatke obdelujejo pristojni državni organi ali organi samoupravnih lokalnih skupnosti ali nosilci javnih pooblastil za namene preprečevanja, preiskovanja, odkrivanja ali pregona kaznivih dejanj, izvrševanja nalog in pooblastil policije, varnosti države, obrambe države ter izvrševanja kazenskih sankcij, v skladu z določbami Direktive.

(2) V kolikor posamezni zakoni s področij iz prejšnjega odstavka glede konkretnih vrst osebnih podatkov, konkretnih zbirk, obdelav osebnih podatkov ter njihovega posredovanja, prenosov in čezmejnih obdelav določajo drugače, se za ta področja uporabljajo določbe teh zakonov in ne določbe tega dela zakona.

(3) Konkretno vrste osebnih podatkov, konkretne zbirke, obdelave osebnih podatkov, nameni obdelave in roki hrambe osebnih podatkov ter njihova posredovanja, prenosi in čezmejne obdelave na področju varnosti države se določijo v zakonih, ki urejajo izvajanje obveščevalnih in protiobveščevalnih nalog države.

86. člen

(temeljna načela obdelave podatkov)

Osebni podatki:

1. se morajo obdelovati v skladu s I. delom tega zakona;
2. morajo biti točni in po potrebi posodobljeni; pri tem je treba sprejeti vse primerne ukrepe, da se osebni podatki, ki glede na namene njihove obdelave niso ustrezni, takoj izbrišejo ali popravijo ali ustrezno označijo;
3. se smejo hraniti v obliki, ki dopušča identifikacijo posameznikov, na katere se nanašajo osebni podatki, le toliko časa, kot je potrebno za namene, za katere se obdelujejo;
4. se morajo obdelovati na način, ki zagotavlja ustrezno varnost osebnih podatkov, vključno z ustreznimi tehničnimi in organizacijskimi ukrepi za zagotavljanje zaščite pred nedovoljeno ali nezakonito obdelavo, nenamerno izgubo, nedovoljenim uničenjem ali nedovoljenim poškodovanjem osebnih podatkov.

87. člen

(razvrščanje osebnih podatkov po vrstah ter kakovost osebnih podatkov)

(1) Če je to glede na dejanske okoliščine posamezne zadeve možno in v skladu z zakonom, je treba pri obdelavi osebnih podatkov razlikovati zlasti med različnimi položaji obdelav:

1. osumljenci storitve kaznivega dejanja;
2. osebe, zoper katere na podlagi določenih dejstev in v zvezi z uporabo prikritih preiskovalnih ukrepov obstaja utemeljen sum, da bodo predvidoma kmalu storile kaznivo dejanje;
3. obsojeni storilci kaznivih dejanj;
4. žrtve kaznivega dejanja ali osebe, pri katerih določena dejstva upravičujejo domnevo, da so žrtve kaznivega dejanja,
5. druge osebe, povezane s kaznivim dejanjem, zlasti osebe, ki pridejo v poštev kot priče, osebe, ki lahko podajo informacije o kaznivem dejanju, ali osebe, ki so v stiku ali povezane z osebami iz 1. in 2. točke;
6. osumljenci storitve prekrška;
7. osebe, zoper katere na podlagi določenih dejstev obstaja sum, da bodo predvidoma kmalu storile prekršek;
8. kaznovani ali obsojeni storilci prekrškov;
9. druge osebe, povezane s prekrškom, zlasti oškodovanci prekrška, udeleženci prekrška, osebe, ki pridejo v poštev kot priče, osebe, ki lahko podajo informacije o prekršku, ali osebe, ki so v stiku ali povezane z osebami iz 6. in 7. točke; in
10. osebe, ki prestajajo nadomestni zapor za storjeni prekršek.

(2) Če je to možno, je treba razlikovati podatke, ki temeljijo na dejstvih, od tistih, ki temeljijo na osebni oceni. Osebnih podatke, ki temeljijo na osebni oceni, je treba ustrezno označiti ter, če je to možno in dopustno, utemeljiti na način, ki omogoča naknadno preverjanje te ocene. Za izvajanje preverjanja po prejšnjem stavku je odgovoren upravljavec.

(3) Osebnih podatki, ki so netočni, nepopolni, ki niso posodobljeni ali jih je treba izbrisati, se ne smejo ne prenašati ne pripraviti za avtomatiziran priklic iz zbirk. Upravitelj mora v ta namen pred prenosom v skladu z razločljivimi možnostmi ustrezno preveriti kakovost podatkov. Glede osebnih podatkov, ki so že na razpolago za avtomatiziran priklic, je treba neprestano izvajati prizadevanja za ohranjanje njihove točnosti in posodobljenosti.

(4) Pri vsakem posredovanju, čezmejni obdelavi ali prenosu osebnih podatkov jim je treba, če je to glede na dejanske okoliščine posamezne zadeve možno, priložiti informacije, na podlagi katerih lahko uporabnik oceni oceno aktualnost, pravilnost, popolnost in zanesljivost.

(5) Če uporabnik, Informacijski pooblaščenec ali pooblaščen oseba na podlagi sporočila posameznika, na katerega se nanašajo osebni podatki, ugotovi, da so bili posredovani osebni podatki, ki ne ustrezajo zahtevam iz tretjega odstavka tega člena, mora pošiljatelj to nemudoma sporočiti uporabniku. Ta mora nemudoma izvesti izbris nezakonitih posredovanih podatkov, popravek netočnih podatkov, dopolnitev nepopolnih podatkov ali omejitev obdelave.

(6) Če imata pošiljatelj ali uporabnik verjeten razlog za domnevo, da so bili posredovani, preneseni ali čezmejno obdelani osebni podatki netočni ali niso bili posodobljeni, da bi jih bilo treba izbrisati ali omejiti njihovo obdelavo, je treba nemudoma izvesti medsebojno obveščanje. Pošiljatelj mora nemudoma sprejeti ustrezne ukrepe popravka ali izbriša če so dejstva o neustreznih osebnih podatkih potrjena, uporabnik je na to odločitev vezan, je pa dolžan označiti morebitno nestrinjanje v svoji zbirki.

88. člen

(zakonitost obdelave osebnih podatkov)

(1) Obdelava osebnih podatkov po tem delu zakona je zakonita le, če je določena z zakonom, ali če je potrebna zaradi varstva življenja ali telesa posameznika ter je potrebna in sorazmerna za izpolnitev določenih nalog, ki jih pristojni organ izvaja v skladu z nameni iz 85. člena tega zakona.

(2) Obdelava posebnih vrst osebnih podatkov dovoljena le v primerih iz točk c), d), i) in j) iz prvega odstavka 12. člena tega zakona.

89. člen

(posebne določbe o obdelavi osebnih podatkov za druge namene in prenos osebnih podatkov)

(1) Obdelava osebnih podatkov po določbah tega dela zakona s strani istega ali drugega upravljavca in za drug namen obdelave od tistega, za katerega so bili podatki pridobljeni, je dovoljena le, če ta drug namen spada na področje iz 85. člena ter izpolnjuje pogoje iz 86. in 87. člena tega zakona.

(2) Prenos, posredovanje ali čezmejna obdelava osebnih podatkov, obdelanih skladno z določbami tega glavnega dela, za namen, ki ni naveden v 85. členu tega zakona, so dovoljeni le, če je to izrecno določeno v zakonski podlagi ter je uporabnik po svojih predpisih pooblaščen za obdelavo teh osebnih podatkov za ta drug namen.

(3) Če za obdelavo osebnih podatkov veljajo posebni pogoji, mora pristojni pošiljatelj uporabnika osebnih podatkov obvestiti o teh pogojih in o tem, da jih je treba upoštevati. Pri čezmejni obdelavi podatkov uporabnikom v druge države članice Evropske unije ali v ustanove in druge organe, vzpostavljene skladno s 4. in 5. poglavjem V. naslova Pogodbe o delovanju Evropske unije, se ne smejo uveljavljati pogoji, ki za ustrezno posredovanje osebnih podatkov ne veljajo tudi v Republiki Sloveniji.

90. člen

(avtomatizirano odločanje v posameznem primeru)

(1) Odločitve, ki temeljijo izključno na avtomatizirani obdelavi, vključno z oblikovanjem profilov, ki imajo negativne pravne posledice za posameznika, na katerega se podatki nanašajo, oziroma lahko v večji meri vplivajo nanj, so dovoljene le, če so izrecno določene v zakonski podlagi.

(2) Odločitve iz prvega odstavka lahko v skladu z 85. členom tega zakona izjemoma temeljijo na posebnih vrstah osebnih podatkov samo, če so bili sprejeti posebni ustrezni ukrepi za varstvo človekovih pravic in temeljnih svoboščin ter upravičenih interesov posameznika, na katerega se nanašajo osebni podatki. Odločitve po prejšnjem stavku, ki bi lahko vodile do diskriminacije posameznika, na katerega se nanašajo osebni podatki, ali njemu bližnjih oseb, so prepovedane.

2. poglavje

Pravice posameznika, na katerega se nanašajo osebni podatki

91. člen

(splošna pravila)

(1) Upravljavec mora posamezniku, na katerega se nanašajo osebni podatki, posredovati informacije in sporočila, v skladu s 92. do 94. členom tega zakona, ki se nanašajo na obdelavo osebnih podatkov, podajati v čim bolj točni, razumljivi in lahko dostopni obliki ter v jasnem in preprostem jeziku, če to posameznik zahteva. Informacije in sporočila se posredujejo v posamezniku ustrezni obliki.

(2) Upravljavec mora posamezniku, na katerega se nanašajo osebni podatki, olajšati uveljavljanje njegovih pravic iz 92. do 94. člena tega zakona.

(3) Upravljavec mora posameznika, na katerega se nanašajo osebni podatki, v roku petih delovnih dni po prejemu zahtevka, pisno obvestiti o stanju obravnave zahtevka.

(4) Upravljavec mora posamezniku, na katerega se nanašajo podatki, informacije o ukrepih, ki so bili na podlagi zahtevka sprejeti, zagotoviti čimprej, najpozneje pa v enem mesecu od vložitve zahtevka. Ta rok se lahko podaljša za dva meseca, če je to potrebno zaradi zapletenosti zahtevka ali števila zahtevkov. Upravljavec mora posameznika, na katerega se nanašajo podatki, v enem mesecu od vložitve zahtevka obvestiti o podaljšanju roka in ob tem navesti razloge za zamudo. Če posameznik, na katerega se podatki nanašajo, zahtevo predloži elektronsko, mora biti po možnosti obveščen po isti elektronski poti, če ne navede drugega kontaktnega naslova. Določbe prejšnjih stavkov se ne uporabljajo, če se izvede ukrep začasne omejitve obveščanja po petem odstavku 89. člena tega zakona.

(5) Če upravljavec ne odgovori na zahtevo posameznika, na katerega se podatki nanašajo ali ne ukrepa drugače in o tem obvesti posameznika, mora posameznika, na katerega se podatki nanašajo, brez zavlačevanja, najpozneje pa v enem mesecu od vložitve zahtevka obvestiti o razlogih za to ter o možnosti vložitve pritožbe pri Informacijskem pooblaščenцу, navesti kontaktne podatke Informacijskega pooblaščenca ter navesti možnosti za uveljavljanju pravice do pravnega sredstva.

(6) Informacije iz 92. člena ter vsa sporočila in ukrepi v skladu s 93. in 94. členom tega zakona se zagotovijo brezplačno. Pri očitno neutemeljenih ali pretiranih zahtevah posameznika, na katerega se podatki nanašajo, zlasti če se zahteve pogosto ponavljajo, lahko upravljavec s posebno obrazložitvijo odkloni ukrepanje na podlagi zahtevka. Obrazložitev iz prejšnjega stavka mora vsebovati vsaj povzetek razlogov glede očitne neutemeljenosti ali pretirano narave zahtevka.

(7) Upravljavec lahko zaradi potrditve identitete posameznika, na katerega se nanašajo osebni podatki, ki je v skladu z 93. ali 94. členom tega zakona vložil zahtevek, zahteva dodatne potrebne informacije od posameznika, kar vključuje glede na konkretne okoliščine poleg osebnega imena tudi navedbo datuma rojstva oziroma navedbo enotne matične številke občana, zahtevek pa mora biti podpisan lastnoročno ali v elektronski obliki z ustreznim digitalnim potrdilom.

(8) V primerih iz četrtega odstavka 92. člena, tretjega odstavka 93. člena in četrtega odstavka 94. člena tega zakona ima posameznik, na katerega se podatki nanašajo, pravico, da zahteva preverjanje zakonitosti zadevne omejitve njegovih pravic s strani Informacijskega pooblaščenca. Upravljavec mora posameznika, na katerega se nanašajo osebni podatki, izrecno poučiti o tej pravici.

(9) Če se uveljavlja pravica, navedena v osmem odstavku, mora Informacijski pooblaščenec posameznika, na katerega se osebni podatki nanašajo, ne glede na določbe 91. člena tega zakona, obvestiti vsaj o tem, da so bila izvedena vsa potrebna preverjanja ali da je preverjanje izvedel Informacijski pooblaščenec. Poleg tega mora Informacijski pooblaščenec posameznika, na katerega se nanašajo osebni podatki, obvestiti o njegovi pravici do uporabe sodnega varstva po 28. členu tega zakona.

92. člen

(dajanje informacij posamezniku, na katerega se nanašajo osebni podatki)

(1) Upravljavec mora posamezniku, na katerega se nanašajo osebni podatki, na njegovo zahtevo zagotoviti najmanj naslednje informacije:

1. naziv in kontaktne podatke upravljavca;
2. po potrebi kontaktne podatke pooblaščen osebe;
3. navedbo namenov, v katere bodo osebni podatki obdelani;
4. obstoj pravice do vložitve prijave pri Informacijskem pooblaščenču in njegove kontaktne podatke;
5. obstoj pravice dostopa do vsebine osebnih podatkov in do tega, da upravljavec popravi ali izbriše podatke ali omeji obdelavo podatkov posameznika, na katerega se osebni podatki nanašajo.

(2) Poleg informacij, navedenih v prvem odstavku, mora upravljavec posamezniku, na katerega se nanašajo podatki, v posebnih primerih zagotoviti naslednje dodatne informacije, da s tem omogoči učinkovitejše uresničevanje pravic posameznika, na katerega se nanašajo osebni podatki:

1. pravno podlago obdelave;
2. rok hrambe osebnih podatkov ali, če to izjemoma ni možno, merila za določitev tega roka v skladu z 43. členom tega zakona;
3. po potrebi navesti kategorije uporabnikov osebnih podatkov, tudi uporabnikov v tretjih državah in mednarodnih organizacijah;
4. po potrebi druge informacije, zlasti če so bili osebni podatki pridobljeni brez vednosti posameznika, na katerega se nanašajo.

(3) V primeru, če so bili osebni podatki pridobljeni neposredno od posameznika, na katerega se nanašajo, je treba posamezniku, na katerega se podatki nanašajo, ob poizvedbi predložiti informacije v skladu z določbami prvega in drugega odstavka tega člena. Informacije iz prvega in drugega odstavka se ne podajo, če so bili osebni podatki pridobljeni s prenosom podatkov iz drugih področij nalog istega upravljavca ali iz uporabe zbirk drugega upravljavca in je obdelava podatkov zakonsko določena.

(4) Obveščanje posameznika, na katerega se osebni podatki nanašajo, se lahko v skladu s prejšnjim odstavkom opusti ali delno ali začasno omeji, če in dokler je to v posameznem primeru očitno sorazmerno ali posebej določeno v drugem zakonu:

1. da se onemogoči oviranje preprečevanja, preiskovanja, odkrivanja ali pregona kaznivih dejanj ali prekrškov, izvrševanja nalog in pooblastil policije, izvrševanja kazenskih sankcij, vključno s pridobivanjem ali prenosi osebnih podatkov za še nedokončane uradne postopke po tej točki;
2. zaradi zagotavljanja, da niso ovirani drugi uradni postopki, povezani s 1. točko;
3. zaradi varnosti države;
4. zaradi varstva obrambe države;
5. zaradi varstva človekovih pravic in temeljnih svoboščin tretjih oseb.

(5) Začasna omejitev obveščanja po prejšnjem odstavku lahko vključuje tudi podajo začasne izjave, da se osebnih podatkov, ki se nanašajo na posameznika, ne obdeluje.

93. člen

(pravica posameznika, na katerega se nanašajo osebni podatki, do pridobitve teh podatkov)

(1) Vsak posameznik, na katerega se nanašajo osebni podatki, ima pravico, da od upravljavca prejme potrdilo o tem, ali so v obdelavi osebni podatki, ki se nanašajo nanj; če se nanašajo nanj, ima pravico pridobiti naslednje informacije o:

1. namenih obdelave in njihovi pravni podlagi;
 2. vrstah osebnih podatkov, ki se obdelujejo;
 3. uporabnikih ali kategorijah uporabnikov, ki so jim bili podatki razkriti, zlasti če gre za uporabnike v tretjih državah ali mednarodnih organizacijah;
 4. če je mogoče, predvideni roku hrambe osebnih podatkov ali, če to izjemoma ni možno, merilih za določitev tega roka v skladu z 43. členom tega zakona;
 5. obstoju pravice, da upravljavec popravi ali izbriše podatke ali omeji obdelavo osebnih podatkov posameznika, na katerega se podatki nanašajo;
 6. obstoju pravice do vložitve prijave pri Informacijskem pooblaščenču in njegovih kontaktnih podatkih;
 7. sporočilih o osebnih podatkih, ki so predmet obdelave, in vseh razpoložljivih informacijah o viru osebnih podatkov, razen njegove konkretne identifikacije, če je identiteta vira varovana kot tajna ali zaupna po določbah drugega zakona.
- (2) Za informacije iz prvega odstavka veljajo roki po določbah člena 12 Splošne uredbe. Omejitve pravice do pridobitve informacij so dovoljene le pod pogoji, navedenimi v četrtem odstavku prejšnjega člena tega zakona.
- (3) V primeru neizdaje informacij v skladu z drugim odstavkom mora upravljavec posameznika, na katerega se nanašajo podatki, nemudoma pisno obvestiti o zavrnitvi ali omejitvi informacij in razlogih, na katerih to temelji. Ta določba se ne uporablja, če je zagotovitev teh informacij v nasprotju z enim od namenov iz četrtega odstavka prejšnjega člena tega zakona. Upravljavec mora posameznika, na katerega se nanašajo podatki, obvestiti o možnosti vložitve pritožbe na organ za varstvo podatkov.
- (4) Upravljavec mora dokumentirati razloge za odločitev o neizdaji informacij v skladu z drugim odstavkom. Ti podatki morajo biti dostopni Informacijskemu pooblaščenču in pooblaščenim osebam.
- (5) V obsegu, v katerem ima posameznik, na katerega se nanašajo osebni podatki, v drugem zakonu določeno zakonsko pravico do vpogleda v njegove osebne podatke, ki se obdelujejo, ima pravico pridobiti informacije v skladu z določbami drugega zakona, ki urejajo pravico do vpogleda.

94. člen

(pravica do popravka ali izbrisa osebnih podatkov in do omejitve obdelave)

- (1) Vsak posameznik, na katerega se nanašajo osebni podatki, ima pravico, da od upravljavca zahteva takojšnji popravek svojih netočnih osebnih podatkov in dopolnitev nepopolnih ali neposodobljenih osebnih podatkov. Popravek ali dopolnitev se lahko po potrebi izvede z dodatno priloženo izjavo ali zaznamkom, če je naknadna sprememba nezdružljiva z namenom dokumentiranja glede na fazo določenega postopka. Upravljavec je dolžan dokazati točnost ali posodobljenost osebnih podatkov, če osebni podatki niso bili pridobljeni izključno na podlagi navedb posameznika, na katerega se podatki nanašajo.
- (2) Upravljavec mora osebne podatke nemudoma izbrisati na lastno pobudo ali na podlagi zahtevka posameznika, na katerega se podatki nanašajo, če:
1. osebni podatki niso več potrebni za namene, za katere so bili pridobljeni ali drugače obdelani;
 2. so bili osebni podatki obdelani nezakonito ali
 3. je izbris osebnih podatkov potreben zaradi izpolnitve druge obveznosti po zakonu ali po pravnomočni sodni odločbi.
- (3) Namesto izbrisa osebnih podatkov lahko upravljavec njihovo obdelavo omeji, če:

1. posameznik, na katerega se podatki nanašajo, izpodbija točnost ali posodobljenost osebnih podatkov in pravilnosti ali nepravilnosti ni mogoče ugotoviti, vendar mora posameznika, na katerega se nanašajo osebni podatki, obvestiti pred razveljavitvijo omejitve, ali

2. je treba osebne podatke še nadalje hraniti za dokazne namene v okviru izvajanja zakonsko določene naloge.

(4) Upravljavec mora posameznika, na katerega se nanašajo osebni podatki, pisno obvestiti o zavrnitvi popravka ali izbrisa osebnih podatkov ali o omejitvi obdelave in o razlogih za zavrnitev. Upravljavec mora posameznika, na katerega se nanašajo podatki, obvestiti o možnosti vložitve prijave Informacijskemu pooblaščenču in o njegovih kontaktnih podatkih.

(5) Upravljavec mora popravek nepravilnih osebnih podatkov sporočiti pristojnemu organu, ki mu je prenesel ali drugače poslal te osebne podatke.

(6) V primerih popravka, izbrisa podatkov ali omejitve obdelave po prvem do tretjem odstavku mora upravljavec o tem obvestiti vse uporabnike osebnih podatkov. Uporabniki so zavezani osebne podatke, ki so v njihovi pristojnosti, nemudoma popraviti, izbrisati, ustrezno označiti ali omejiti njihovo obdelavo.

(7) Za druga vprašanja se smiselno uporablja člen 12 Splošne uredbe.

(8) Upravljavci ali obdelovalci, ki na podlagi zakona za izvajanje svojega delovanja pridobivajo osebne podatke iz registrov ali evidenc s področja upravnih notranjih zadev, so dolžni na lastne stroške vzpostaviti varnostne mehanizme, ki jih kot ukrepe ali postopke za izvajanje varnosti osebnih podatkov določi ministrstvo pristojno za notranje zadeve kot upravljavec registrov ali evidenc.

X.

DEL

PODROČNE UREDITVE OBDELAV OSEBNIH PODATKOV

1. poglavje

Neposredno trženje

95. člen

(pravice in dolžnosti upravljavca na področju neposrednega trženja)

(1) Upravljavec lahko uporablja osebne podatke posameznikov, 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 lahko upravljavec uporablja 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 ter številko telefaksa. Na podlagi privolitve posameznika lahko upravljavec obdeluje tudi druge osebne podatke, posebne vrste osebnih podatkov pa le, če ima za to pisno privolitev posameznika.

(3) Upravljavec mora neposredno trženje izvajati tako, da posameznika ob izvajanju neposrednega trženja jasno in ločeno od katerihkoli drugih informacij obvesti o njegovih pravicah iz členov 13, 15-22 in 34 Splošne uredbe ter 96. člena tega zakona.

(4) Če namerava upravljavec posredovati osebne podatke iz drugega odstavka tega člena drugim uporabnikom osebnih podatkov za namene neposrednega trženja, je dolžan o tem obvestiti posameznika in pred posredovanjem osebnih podatkov pridobiti njegovo pisno privolitev. Obvestilo posamezniku o nameravanem posredovanju osebnih podatkov mora vsebovati informacijo, katere podatke namerava posredovati, komu in za kakšen namen. Stroške obvestila krije upravljavec.

96. člen

(pravica posameznika glede prenehanja obdelave osebnih podatkov s področja neposrednega trženja)

(1) Posameznik lahko kadarkoli pisno ali na drug dogovorjen način brezplačno zahteva, da upravljavec trajno ali začasno preneha uporabljati ali drugače obdelovati njegove osebne podatke za namen neposrednega trženja. Upravljavec je dolžan v 15 dneh prenehati obdelovati osebne podatke za namen neposrednega trženja ter o tem v nadaljnjih 5 dneh pisno ali na drug dogovorjen način obvestiti posameznika, ki je to zahteval.

(2) Stroške vseh dejanj upravljavca osebnih podatkov v zvezi z zahtevo iz prejšnjega odstavka krije upravljavec.

2. poglavje

Videonadzor

97. člen

(splošne določbe o videonadzoru in varstvu osebnih podatkov)

(1) Videonadzor je tehnološki sistem za generiranje, prenos, prikazovanje in shranjevanje video slik ali video slik in video zvoka, ki se ne sme uporabljati za popolnoma osebno ali domačo dejavnost, z namenom opazovanj in spremljanja ali nadzorovanja varovanega območja, objektov in prostorov ter analiziranja dogajanja in ki omogoča prepoznavo posameznikov ali povezovanje posnetkov videonadzora s posamezniki. Če z zakonom ni drugače določeno, se določbe tega poglavja uporablja za vse vrste videonadzora, in tudi v primerih, ko se z videonadzorom zgolj spremlja neposredno dogajanje pred kamerami.

(2) Odločitev o uvedbi videonadzora sprejme pristojni funkcionar, predstojnik, direktor ali drugi pristojni oziroma pooblaščen posameznik osebe javnega sektorja ali osebe zasebnega sektorja. V pisni odločitvi morajo biti obrazloženi razlogi za uvedbo videonadzora. Uvedba videonadzora se lahko določi tudi z zakonom ali s predpisom, sprejetim na njegovi podlagi.

(3) Oseba javnega ali zasebnega sektorja, ki izvaja videonadzor, mora o tem objaviti obvestilo. Obvestilo mora biti vidno in razločno objavljeno na način, ki omogoča posamezniku, da se seznani z njegovim izvajanjem najkasneje, ko se nad njim začne izvajati videonadzor.

(4) Obvestilo iz prejšnjega odstavka mora vsebovati naslednje informacije:

1. pisno ali nedvoumno grafično opisano dejstvo, da se izvaja videonadzor;
2. naziv osebe javnega ali zasebnega sektorja, ki ga izvaja;
3. telefonsko številko za pridobitev informacije, kje in koliko časa se shranjujejo posnetki videonadzornega sistema.

(5) Šteje se, da je z obvestilom iz tretjega odstavka tega člena posameznik obveščen o obdelavi osebnih podatkov.

(6) Videonadzorni sistem, s katerim se izvaja videonadzor, mora biti zavarovan pred dostopom nepooblaščenih oseb.

(7) Posnetki videonadzora se lahko hranijo največ 6 mesecev od trenutka nastanka posnetka, če zakon ne določa drugače.

(8) Videonadzora ni dovoljeno izvajati v dvigalih, sanitarijah, slačilnicah in drugih podobnih prostorih, v katerih lahko posameznik utemeljeno pričakuje višjo stopnjo zasebnosti.

(9) Upravljavec videonadzora mora za vsak vpogled ali uporabo posnetkov zagotoviti, da je možno, da je naknadno ugotoviti, v katere posnetke je bilo vpogledano, so bili uporabljeno ali posredovani, kdo je v njih izvedel ta dejanja obdelave, kdaj in s kakšnim namenom ali po kateri pravni podlagi ter takšno revizijsko sled hraniti za obdobje petih let, razen, če drug zakon ne določa drugače,

98. člen

(uporaba videonadzora glede dostopa v uradne službene oziroma poslovne prostore)

(1) Javni in zasebni sektor lahko izvajata videonadzor dostopa v njihove uradne službene oziroma poslovne prostore, če je to potrebno za varnost ljudi ali premoženja, zaradi zagotavljanja nadzora vstopa ali izstopa v ali iz službenih oziroma poslovnih prostorov ali če zaradi narave dela obstaja možnost ogrožanja zaposlenih. Vpogled, uporaba ali posredovanje posnetkov je dopustno le za namene iz prejšnjega stavka, če drug zakon ne določa drugače.

(2) Videonadzor se lahko izvaja le na takšen način, da se ne izvaja niti snemanje notranjosti stanovanjskih stavb, ki nimajo vpliva na dostop do njihovih prostorov, niti snemanje vhodov v stanovanja.

(3) O izvajanju videonadzora je potrebno pisno obvestiti vse zaposlene v osebi javnega ali zasebnega sektorja, ki opravljajo delo v nadzorovanem prostoru.

(4) Zbirka osebnih podatkov po tem členu vsebuje posnetek posameznika (slika oziroma glas), datum in čas vstopa in izstopa iz prostora, lahko pa tudi osebno ime posnetega posameznika, naslov njegovega stalnega ali začasnega prebivališča, zaposlitev, številko in podatke o vrsti njegovega osebnega dokumenta ter razlogu vstopa, če se navedeni osebni podatki zbirajo poleg ali s posnetkom videonadzornega sistema.

99. člen

(videonadzor in večstanovanjske stavbe)

(1) Videonadzor se lahko v večstanovanjski stavbi uvede le, kadar je to potrebno za varnost ljudi in premoženja. Vpogled, uporaba ali posredovanje posnetkov je dopustno le za namene iz prejšnjega stavka, če drug zakon ne določa drugače.

(2) Videonadzor v večstanovanjskih stavbah je dovoljen samo, če za to obstaja privolitev lastnikov, ki imajo v lasti več kot 70 odstotkov solastniških deležev na skupnih delih.

(3) Privolitev iz drugega odstavka mora biti pisna, pri čemer je treba na listini izrecno navesti, kateri lastniki so podali privolitev k uvedbi videonadzora.

(4) Upravljavec po tem členu je upravnik večstanovanjske stavbe. Če večstanovanjska stavba nima upravnika, je upravljavec oseba, ki jo izmed sebe pisno določijo lastniki, ki so podali privolitev za uvedbo videonadzora in se ta oseba s tem pisno strinja.

(5) Če upravljavec oziroma oseba iz prejšnjega odstavka ni določen, se šteje, da je upravljavec videonadzora v večstanovanjski stavbi skupnost lastnikov, ki so privolili v izvajanje videonadzora. Pravice in obveznosti, ki izvirajo iz uvedbe videonadzora in prekrškovno odgovornost nosijo samo tisti lastniki, ki so se strinjali z uvedbo videonadzora.

(6) Prepovedano je omogočiti ali izvajati sprotno ali naknadno pregledovanje dogajanja v območju izvajanja videonadzora preko interne kableske televizije, javne kableske televizije, svetovnega spleta ali s pomočjo drugega elektronskega komunikacijskega sredstva, ki lahko prenaša te posnetke.

(7) Prepovedano je z videonadzornim sistemom snemati vhode v posamezna stanovanja. Prepovedano je izvajati videonadzor nad hišniškim stanovanjem ter delavnico za hišnika.

(8) Izjemoma je dovoljeno omogočiti združitev videonadzornega sistema z napravami, ki jih uporabljajo lastniki za potrebe vstopa v večstanovanjsko stavbo, kot sta na primer domofon ali video domofon, razen če te naprave omogočajo snemanje ali spremljanje dogajanja v območju izvajanja videonadzora na posamezni napravi. Spremljanje dogajanja v območju izvajanja videonadzora mora onemogočiti upravljavec videonadzora.

(9) Videonadzor je dovoljeno izvajati samo v skupnih prostorih po zakonu, ki ureja razmerja med lastniki v večstanovanjskih stavbah.

100. člen **(delovni prostori)**

(1) Izvajanje videonadzora znotraj delovnih prostorov se lahko izvaja le v izjemnih primerih, kadar je to nujno potrebno za varnost ljudi ali premoženja ali za varovanje tajnih podatkov ter poslovne skrivnosti, tega namena pa ni možno doseči z milejšimi sredstvi. Vpogled, uporaba ali posredovanje posnetkov je dopustno le za namene iz prejšnjega stavka, če drug zakon ne določa drugače.

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

(3) Spremljanje neposrednega dogajanja pred kamerami je pod pogoji iz prvega in drugega odstavka tega člena dopustno le, če ga izvaja pooblaščen varnostno osebje.

(4) Zaposleni morajo biti pred začetkom izvajanja videonadzora po tem členu vnaprej pisno obveščeni o njegovem izvajanju.

(5) Pred uvedbo videonadzora v osebi javnega ali zasebnega sektorja se mora delodajalec posvetovati z reprezentativnimi sindikati pri delodajalcu ter svetom delavcev ali delavskim zaupnikom.

(6) Na področju obrambe države, obveščevalno-varnostne dejavnosti države in varovanja tajnih podatkov dveh najvišjih stopenj tajnosti se ne uporabljata četrti in peti odstavek tega člena.

(7) Videonadzor v poslovnih zgradbah, kjer je več različnih lastnikov je dovoljen samo, če za to obstaja privolitev lastnikov, ki imajo v lasti več kot 70 odstotkov solastniških deležev na skupnih delih.

101. člen **(videonadzor na javnih površinah)**

(1) Videonadzor na javnih površinah je dovoljen le v izjemnih primerih, kadar je to nujno potrebno, ker obstaja resna in utemeljena nevarnost za življenje ali zdravje ljudi, varnost premoženja ali varovanje tajnih podatkov in tega namena ni mogoče doseči z milejšimi sredstvi, ali za potrebe varovanja prostorov, zgradb ali območij, ki jih je potrebno varovati na podlagi zakona in sicer samo v obsegu in trajanju, ki je za doseg te namene nujno potreben. Vpogled, uporaba ali posredovanje posnetkov je dopustno le za namene iz prejšnjega stavka, če drug zakon ne določa drugače.

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

(3) Videonadzor na javnih površinah lahko izvaja oseba javnega ali zasebnega sektorja, ki upravlja z javno površino ali na njej zakonito opravlja dejavnost.

3. poglavje

Obdelava osebnih podatkov z uporabo biometrije

102. člen

(biometrični ukrepi v javnem sektorju)

(1) Biometrične ukrepe v javnem sektorju se lahko izjemoma določi le z zakonom, če je to nujno potrebno za varnost ljudi ali premoženja ali za varovanje tajnih podatkov ali za identifikacijo pogrešanih ali umrlih posameznikov ter poslovne skrivnosti, tega namena pa ni možno doseči z milejšimi sredstvi.

(2) Ne glede na prejšnji odstavek se biometrične ukrepe lahko določi z zakonom, če gre za izpolnjevanje obveznosti iz obvezujoče mednarodne pogodbe ali za identifikacijo posameznikov pri prehajanju državnih meja.

103. člen

(biometrični ukrepi v zasebnem sektorju)

(1) Zasebni sektor lahko izvaja biometrične ukrepe le, če so nujno potrebni za opravljanje dejavnosti, za varnost ljudi ali premoženja ali za varovanje tajnih podatkov ali poslovne skrivnosti v skladu z določbami tega člena.

(2) Biometrične ukrepe lahko izvaja nad svojimi zaposlenimi ter nad tistimi osebami, ki so zaposlene pri pogodbenih partnerjih upravljavca, če je to potrebno za namene varovanja interesov iz prvega odstavka in so bili predhodno o tem pisno obveščeni.

(3) Zasebni sektor lahko izvaja biometrične ukrepe tudi nad svojimi strankami pod naslednjimi pogoji:, da tako za namene varovanja interesov iz prvega odstavka določa zakon in so stranke podale pisno privolitev ter se na ta način preprečuje nastanek hude škode.

(4) Upravljavca osebnih podatkov, ki namerava izvajati biometrične ukrepe, je dolžan pred uvedbo ukrepov posredovati Informacijskemu pooblaščenцу opis nameravanih ukrepov in razloge za njihovo uvedbo.

(5) Informacijski pooblaščenec je po prejemu posredovanih informacij iz prejšnjega odstavka dolžan v dveh mesecih odločiti, ali je nameravana uvedba biometričnih ukrepov v skladu s tem zakonom, predvsem s pogoji iz prvega stavka prvega odstavka tega člena. Rok se ob upoštevanju kompleksnosti predvidene obdelave lahko podaljša za največ dva meseca.

(6) Upravljavec osebnih podatkov sme izvajati biometrične ukrepe po prejemu odločbe iz prejšnjega odstavka, s katero je izvajanje biometričnih ukrepov dovoljeno.

(7) Zoper odločbo Informacijskega pooblaščenca iz petega odstavka tega člena ni pritožbe, dovoljen pa je upravni spor.

(8) Izjemoma upravljavcu ni potrebno pridobiti odločbe iz petega odstavka tega člena, če pri izvajanju biometričnih ukrepov ne nastaja zbirka biometričnih značilnosti ali matematičnih pretvorb biometričnih značilnosti in so te vedno pod nadzorom posameznika.

(9) Upravljavec mora pred začetkom uporabe biometričnih ukrepov posamezniku, nad katerim se bodo izvajali ti ukrepi, predložiti obvestilo o zakonski ureditvi izvajanja biometričnih ukrepov, ki ga izdela in na svoji spletni strani objavi Informacijski pooblaščenec.

104. člen

(prepoved trženja biometričnih osebnih podatkov v zasebnem sektorju)

Zasebni sektor ne sme v okviru trženja ali temu podobne druge poslovne dejavnosti zahtevati, pridobiti ali nadalje obdelovati biometričnih osebnih podatkov v zamenjavo za določene storitve, četudi so te storitve za posameznika, na katerega se nanašajo osebni podatki, brezplačne.

4. poglavje

Evidentiranje vstopov in izstopov

105. člen

(evidentiranje vstopov in izstopov iz službenih prostorov)

(1) Oseba javnega ali zasebnega sektorja lahko za zagotavljanje varnosti ljudi in premoženja, varovanja tajnih podatkov ter reda v njenih prostorih ali v prostorih, ki jih ima v uporabi od posameznika, ki namerava vstopiti ali izstopiti iz tega prostora, zahteva, da navede vse ali nekatere osebne podatke iz drugega odstavka tega člena ter razlog vstopa ali izstopa. Po potrebi lahko osebne podatke preveri tudi z vpogledom v osebni dokument posameznika.

(2) V zbirki o vstopih in izstopih iz službenih prostorov se lahko o posamezniku vodijo samo naslednji osebni podatki, kadar je to potrebno: osebno ime, številka in vrsta osebnega dokumenta, naslov prebivališča, zaposlitev, vrsta in registrska številka vozila ter datum, ura in razlog vstopa ali izstopa v ali iz prostorov.

(3) Evidenca iz prejšnjega odstavka velja za uradno evidenco v skladu z zakonom, ki ureja splošni upravni postopek, če je potrebno pridobiti podatke z vidika koristi mladoletnika ali za izvrševanje pristojnosti policije ter obveščevalno-varnostne dejavnosti.

(4) Osebni podatki iz evidence iz drugega odstavka tega člena se lahko hranijo največ tri leta od vpisa, nato se zbršejo ali na drug način uničijo, če drug zakon ne določa drugače.

5. poglavje

Javne knjige in varstvo osebnih podatkov

106. člen
(zakoniti namen javne knjige)

Osební podatki iz javne knjige, urejene z zakonom, se lahko uporabljajo le v skladu z namenom, za katerega so bili zbrani ali se obdelujejo, če je zakoniti namen njihovega zbiranja ali obdelave določen ali določljiv.

6. poglavje
Povezovanje zbirk osebnih podatkov

107. člen
(povezovanje uradnih evidenc in javnih knjig)

(1) Uradne evidence in javne knjige, v katerih se obdelujejo posebne vrste osebnih podatkov, podatki o dohodkih v skladu z zakonom, ki ureja dohodnino, podatki o premoženju posameznika v skladu z zakonom, ki ureja uveljavljanje pravic iz javnih sredstev, podatki o nepremičninah v lasti posameznika v skladu z drugimi zakoni, podatki oziroma informacije o kreditni sposobnosti v skladu z zakonom, ki ureja bančništvo, oziroma uradne evidence, ki jih določata zakona, ki urejata naloge in pooblastila policije oziroma preprečevanje pranja denarja in financiranja terorizma, se lahko povezuje med seboj ali z drugimi zbirkami samo, če takšno povezovanje izrecno določa zakon.

(2) Uradne evidence in javne knjige, ki ne vsebujejo podatkov iz prejšnjega odstavka, se lahko povezuje med seboj ali z drugimi zbirkami samo, če zakon določa pravico upravljavca uradne evidence, javne knjige ali druge zbirke, da pridobi osebne podatke iz uradne evidence ali javne knjige.

(3) Povezovanje zbirk po določbah prejšnjih odstavkov tega člena pomeni elektronsko povezovanje dveh ali več uradnih evidenc, javnih knjig ali drugih zbirk, ki se upravljajo pri različnih upravljavcih ali tudi pri istem upravljavcu na podlagi različnih pravnih podlag, in ki se, neodvisno od tehnične izvedbe, izvaja v obsegu ali na način, ki predstavlja ali bi lahko predstavljalo bistveno večje tveganje za pravice in svoboščine posameznikov kot obdelava osebnih podatkov v okviru ene same uradne evidence, javne knjige ali zbirke. Povezovanje zbirk pomeni tudi obdelavo dveh ali več zbirk osebnih podatkov od istega ali različnih upravljavcev pri istem obdelovalcu, če ni z organizacijskimi in tehničnimi ukrepi zagotovljena popolna ločitev obdelav osebnih podatkov iz navedenih zbirk.

(4) Pred začetkom povezovanja zbirk iz prvega odstavka tega člena je poleg izpolnjevanja pogojev iz prejšnjih odstavkov potrebno pridobiti še predhodno dovoljenje Informacijskega pooblaščenca, s katerim se potrdi, da upravljavci in obdelovalci vseh povezanih zbirk zagotavljajo skladnost obdelave osebnih podatkov tako povezanih podatkov s pravili tega zakona.

(5) Dovoljenje iz prejšnjega odstavka se izda v obliki upravne odločbe, na podlagi pisne vloge enega ali več upravljavcev, ki želijo izvesti zadevno povezovanje. Zoper izdano odločbo ni pritožbe, dovoljen pa je upravni spor.

7. poglavje
Strokovni nadzor

108. člen
(uporaba določb tega poglavja)

Če drug zakon ne določa drugače, se določbe tega poglavja uporabljajo za obdelavo osebnih podatkov pri strokovnem nadzoru, ki je določen z zakonom.

109. člen **(splošne določbe)**

(1) Oseba javnega sektorja, ki izvaja strokovni nadzor (v nadaljnjem besedilu: izvajalec strokovnega nadzora), lahko obdeluje osebne podatke, ki jih obdelujejo upravljavci osebnih podatkov, nad katerimi ima po zakonu pristojnost izvajati strokovni nadzor.

(2) Izvajalec strokovnega nadzora ima pravico do vpogleda, izpisa, prepisovanja ali kopiranja vseh osebnih podatkov iz prejšnjega odstavka, pri njihovi obdelavi za namene strokovnega nadzora in izdelave poročila ali ocene pa je dolžan varovati njihovo tajnost. V poročilu ali oceni ob zaključku strokovnega nadzora lahko izvajalec strokovnega nadzora zapiše le tiste osebne podatke, ki so nujni za doseg namena strokovnega nadzora.

(3) Stroške vpogleda, izpisa, prepisovanja ali kopiranja iz prejšnjega odstavka krije upravljavec osebnih podatkov.

110. člen **(strokovni nadzor in dodatna obdelava osebnih podatkov)**

(1) Izvajalec strokovnega nadzora lahko pri opravljanju strokovnega nadzora, pri katerem v skladu s prvim odstavkom prejšnjega člena tega zakona obdeluje osebne podatke, pisno obvesti posameznika, na katerega se nanašajo osebni podatki, da izvaja strokovni nadzor in ga obvesti, da lahko pisno ali ustno poda svoja stališča.

(2) Posameznik iz prejšnjega odstavka lahko posreduje izvajalcu strokovnega nadzora za namene izvajanja strokovnega nadzora osebne podatke drugega posameznika, ki bi lahko o zadevi, v kateri se izvaja strokovni nadzor, kaj vedel. Če izvajalec strokovnega nadzora ugotovi, da je to potrebno, opravi razgovor tudi z drugim posameznikom.

111. člen **(strokovni nadzor in posebne vrste osebnih podatkov)**

Če se pri izvajanju strokovnega nadzora obdelujejo podatki iz 12. ali 13. člena tega zakona, izvajalec strokovnega nadzora o tem naredi uradni zaznamek ali drug uradni zapis v spisu zadeve upravljavca osebnih podatkov.

8. poglavje **Objava sodnih odločb**

112. člen **(javna objava sodnih odločb)**

(1) Za namene zagotavljanja javnosti dela sodišč, zagotavljanja pravne varnosti ter zagotavljanja enotnosti sodne prakse Ministrstvo za pravosodje v sodelovanju z Vrhovnim sodiščem na svoji spletni strani objavlja sodno prakso sodišč Republike Slovenije.

(2) V zbirki iz prejšnjega odstavka se objavlja vse sodne odločbe na prvi stopnji o glavni stvari v kazenskih, civilnih, gospodarskih, nepravdnih, delovnih, socialnih, upravnih ter prekrškovnih pomembnejših zadevah, vse sodne odločbe na drugi stopnji o glavni stvari ter vse sodne odločbe glede izrednih pravnih sredstev, razen odločb v postopkih, kjer je bila javnost v celoti ali deloma izključena.

(3) Vrhovno sodišče ministrstvu preko programskega vmesnika in v strojno berljivi obliki zagotavlja posredovanje sodnih odločb iz prejšnjega odstavka, in sicer najkasneje v 15 dneh po odpremi odločbe vsem strankam. Vrhovno sodišče na isti način zagotovi tudi posredovanje morebitnih kasnejših popravnih sklepov.

(4) Vrhovno sodišče ministrstvu za namen priprave posredovanih sodnih odločb za objavo preko programskega vmesnika in v strojno berljivi obliki zagotavlja tekoči dostop do:

- seznama sodnikov pri posameznem sodišču (ime in priimek, naziv, naziv sodišča),

- razporeda glavnih obravnav pri posameznem sodišču za tekoči mesec ter preteklih šest mesecev (naziv sodišča, datum in ura obravnave, opravilna številka zadeve, ime in priimek sodnika posameznika oziroma imena in priimki ter vloge članov senata, opis zadeve, ime in priimek oziroma firma vsake od strank postopka);

- javno dostopnih podatkov iz vpisnikov sodišč (opravilna številka zadeve, datum vpisa zadeve, datum izbrisa zadeve, način rešitve zadeve).

(5) Način izvajanja tega člena se lahko uredi v Sodnem redu.

113. člen

(priprava sodnih odločb za javno objavo)

(1) Ministrstvo pred objavo sodnih odločb izvede razumna prizadevanja, da iz odločbe ne bi bili več neposredno razvidni osebni podatki, ki bi omogočali neposredno identifikacijo strank in drugih fizičnih oseb, ki so navedene v odločbi.

(2) Ministrstvo lahko v ta namen uporabi tudi sredstva za avtomatizirano sprejemanje odločitev, pri čemer mora pred začetkom njegove uporabe izvesti oceno učinkov v zvezi z varstvom osebnih podatkov ter glede nje pridobiti mnenje Informacijskega pooblaščenca.

114. člen

(pravice posameznika)

(1) Ministrstvo na podlagi prijave posameznika, da določena objavljena odločba posega v njegove človekove pravice ali temeljne svoboščine, začasno umakne to odločbo iz javne objave. Posameznik mora nato v roku 8 dni ministrstvu posredovati obrazloženo zahtevo za umik te odločbe oziroma njenih posameznih delov, sicer ministrstvo to odločbo ponovno objavi.

(2) Ministrstvo ugotovi zahtevo posameznika iz prejšnjega odstavka in v celoti ali deloma umakne zadevno sodno odločbo iz objave, če iz zahteve sklepčno izhaja, da bi nadaljnja objava odločbe povzročila veliko tveganje za posameznikove človekove pravice ali temeljne svoboščine, razen če iz objavljene odločbe ali drugih okoliščin izhaja, da obstajajo posebni razlogi, kot je vloga tega posameznika ali pravne osebe v javnem delovanju, zaradi katerih obstaja prevladujoči interes javnosti do dostopa do podatkov v odločbi, ki ne vključujejo podatkov iz prvega odstavka prejšnjega člena.

(3) Ministrstvo lahko ne glede na določbe prejšnjega odstavka zavrže prijavo oziroma zahtevo posameznika, če je ta očitno neutemeljena ali pretirana, še zlasti pa, če se ponavlja.

(4) Za obravnavo zahteve za umik sodbe se smiselno uporabljajo določbe tega zakona o zahtevi za dopolnitev, popravek ali izbris osebnih podatkov, razen kolikor ta člen določa drugače.

(5) V zvezi z objavo sodnih odločb na podlagi poglavja posamezniku ne pripadajo pravice po členih 12 do 22 Splošne uredbe, razen pravic do izbrisa in omejitve obdelave iz členov 17 in 18, ki se izvajata v skladu s tem členom.

XI. DEL

KAZENSKÉ DOLOČBE

115. člen

(uporaba določb Splošne uredbe glede upravnih kazni in glob ter odločanje o prekrških po tem delu zakona)

(1) V skladu s prvim odstavkom 73. člena tega zakona Informacijski pooblaščenec odloča o predpisanih kršitvah in upravnih globah iz člena 83 Splošne uredbe kot o prekrških v okviru pristojnosti prekrškovnega organa po določbah zakona, ki ureja prekrške, kolikor ta zakon ne določa drugače.

(2) Pri odločanju Informacijskega pooblaščenca o višini izrečene globe za kršitve, predpisane v členu 83 Splošne uredbe, se v skladu z določbami prvega odstavka člena 83 Splošne uredbe in zakona, ki ureja prekrške, ob obravnavanju konkretnih okoliščin posameznega primera tudi upošteva, da globa ne sme biti nesorazmerno breme ali neprimerljivo breme za upravljavce ali obdelovalce glede na druge primerljive kršitve človekovih pravic in temeljnih svoboščin, ki se kaznujejo za prekrške, ali je obstajal namen koristiljubnosti ali namen škodovanja posameznikom, na katere se nanašajo osebni podatki, v primeru izvajanja popravljalnih ukrepov s strani upravljavca ali obdelovalca njihovo učinkovitost ali samostojno ukrepanje še pred uvedbo nadzora, glede fizičnih oseb pa se zlasti upošteva splošna raven dohodkov v Republiki Sloveniji ter njihov ekonomski položaj. Prav tako je treba upoštevati pri tem odločanju za vse obdelovalce ali upravljavce ali gre za ponavljajoče kršitve in pomen, ki bi ga za odvrčanje teh kršitev imela izbira vrste ali višine globe.

(3) Višine in razponi upravnih glob, ki so za pravne osebe, samostojne podjetnike posameznike in posameznike, ki samostojno opravljajo dejavnost, za kršitve, predpisane v členu 83 Splošne uredbe, določene v 116. in 117. členu tega zakona, se uporabljajo ne glede na določbe o razponih glob iz zakona, ki ureja prekrške.

(4) Informacijski pooblaščenec odloča kot prekrškovni organ tudi o predpisanih prekrških po tem delu zakona in po določbah Splošne uredbe.

(5) Za prekrške po določbah Splošne uredbe in po določbah tega zakona sme Informacijski pooblaščenec v hitrem postopku izreči globo tudi v znesku, ki je višji od najnižje predpisane globe, določene s tem zakonom.

116. člen

(kršitve iz četrtega odstavka člena 83 Splošne uredbe)

(1) Z globo od 4.000 do 10.000.000 eurov ali v primeru gospodarske družbe v znesku 2 % skupnega svetovnega letnega prometa v preteklem proračunskem letu, odvisno, kateri je višji, se kaznuje za prekršek pravna oseba, samostojni podjetnik posameznik ali posameznik, ki samostojno opravlja dejavnost:

1. če krši obveznosti upravljavca in obdelovalca v skladu s členi 8, 11, 25 do 39 ter 42 in 43 Splošne uredbe;
 2. če krši obveznosti organa za potrjevanje v skladu s členoma 42 in 43 Splošne uredbe;
 3. če krši obveznosti organa za spremljanje v skladu s četrtem odstavkom člena 41 Splošne uredbe.
- (2) Z globo od 800 do 1.200 eurov se kaznuje za prekršek iz prejšnjega odstavka tudi odgovorna oseba pravne osebe, samostojnega podjetnika posameznika ali posameznika, ki samostojno opravlja dejavnost.
- (3) Z globo od 800 do 1.200 eurov se kaznuje za prekršek odgovorna oseba državnega organa ali organa samoupravne lokalne skupnosti, ki stori dejanje iz prvega odstavka tega člena.
- (4) Z globo od 200 do 800 eurov se kaznuje za prekršek posameznik, ki stori dejanje iz prvega odstavka tega člena.

117. člen

(kršitve iz petega odstavka člena 83 Splošne uredbe)

- (1) Z globo od 4.000 do 20.000.000 eurov ali v primeru gospodarske družbe v znesku 4 % skupnega svetovnega letnega prometa v preteklem proračunskem letu, odvisno, kateri je višji, se kaznuje za prekršek pravna oseba, samostojni podjetnik posameznik ali posameznik, ki samostojno opravlja dejavnost:
1. če krši temeljna načela za obdelavo, vključno s pogoji za privolitve, v skladu s členi 5, 6, 7 in 9 Splošne uredbe;
 2. če krši pravice posameznika, na katerega se nanašajo podatki, v skladu s členi 12 do 22 Splošne uredbe;
 3. če krši določbe v zvezi s prenosi osebnih podatkov uporabniku v tretji državi ali mednarodni organizaciji, v skladu s členi 44 do 49 Splošne uredbe;
 4. če ne upošteva odredbe ali začasne ali dokončne omejitve obdelave ali prekinitve prenosa podatkov, ki jo izda Informacijski pooblaščenec v skladu z drugim odstavkom člena 58 Splošne uredbe, ali če ne zagotovi dostopa, s čimer se krši prvi odstavek člena 58 Splošne uredbe.
- (2) Z globo od 800 do 1.200 eurov se kaznuje za prekršek iz prejšnjega odstavka tudi odgovorna oseba pravne osebe, samostojnega podjetnika posameznika ali posameznika, ki samostojno opravlja dejavnost.
- (3) Z globo od 800 do 1.200 eurov se kaznuje za prekršek odgovorna oseba državnega organa ali organa samoupravne lokalne skupnosti, ki stori dejanje iz prvega odstavka tega člena.
- (4) Z globo od 200 do 800 eurov se kaznuje za prekršek posameznik, ki stori dejanje iz prvega odstavka tega člena.

118. člen

(kršitve iz IX. dela tega zakona)

- (1) Z globo od 1.000 do 6.000 eurov se kaznuje za prekršek odgovorna oseba državnega organa ali organa samoupravne lokalne skupnosti:
1. če obdeluje osebne podatke nezakonito, ne da bi imel za to podlago v zakonu ali glede na potrebo varovanja življenja ali telesa (88. člen);

2. če avtomatizirano obdeluje osebne podatke v nasprotju s 90. členom;
3. če nezakonito dostopa do vsebine osebnih podatkov v nasprotju s pravili iz sedmega odstavka 40. člena tega zakona.

(2) Z globo od 1.000 do 4.000 eurov se kaznuje za prekršek odgovorna oseba pravne osebe, samostojnega podjetnika posameznika ali posameznika, ki samostojno opravlja dejavnost, ki stori dejanje iz prvega odstavka tega člena.

(3) Z globo od 200 do 1.000 eurov se kaznuje za prekršek posameznik, ki stori dejanje iz prvega odstavka tega člena.

119. člen

(kršitev določb o neposrednem trženju)

(1) Z globo od 2.000 do 4.000 eurov se kaznuje za prekršek pravna oseba, samostojni podjetnik posameznik ali posameznik, ki samostojno opravlja dejavnost, če v skladu s tem zakonom obdeluje osebne podatke za namene neposrednega trženja in ne ravna v skladu z 95. ali 96. členom tega zakona.

(2) Z globo od 400 do 1.200 eurov se kaznuje za prekršek iz prejšnjega odstavka tudi odgovorna oseba pravne osebe, samostojnega podjetnika posameznika ali posameznika, ki samostojno opravlja dejavnost.

(3) Z globo od 200 do 800 eurov se kaznuje za prekršek posameznik, ki stori dejanje iz prvega odstavka tega člena.

120. člen

(kršitev splošnih določb o videonadzoru)

(1) Z globo od 4.000 do 12.000 eurov se kaznuje za prekršek pravna oseba, samostojni podjetnik posameznik ali posameznik, ki samostojno opravlja dejavnost:

1. če ne objavi obvestila na način iz tretjega odstavka 97. člena tega zakona;
2. če obvestilo ne vsebuje informacij iz četrtega odstavka 97. člena tega zakona;
3. če ne zavaruje videonadzornega sistema, s katerim se izvaja videonadzor, v nasprotju s šestim odstavkom 97. člena tega zakona.

(2) Z globo od 800 do 1.200 eurov se kaznuje za prekršek iz prejšnjega odstavka tudi odgovorna oseba pravne osebe, samostojnega podjetnika posameznika ali posameznika, ki samostojno opravlja dejavnost.

(3) Z globo od 800 do 1.200 eurov se kaznuje za prekršek odgovorna oseba državnega organa ali organa samoupravnega lokalne skupnosti, ki stori dejanje iz prvega odstavka tega člena.

(4) Z globo od 200 do 800 eurov se kaznuje za prekršek posameznik, ki stori dejanje iz prvega odstavka tega člena.

(5) Z globo od 5.000 do 15.000 eurov se kaznuje za prekršek pravna oseba, samostojni podjetnik posameznik ali posameznik, ki samostojno opravlja dejavnost, če izvaja nedovoljeni videonadzor v nasprotju s sedmim ali osmim odstavkom 97. člena tega zakona.

(6) Z globo od 1.000 do 2.000 eurov se kaznuje za prekršek iz prejšnjega odstavka tudi odgovorna oseba pravne osebe, samostojnega podjetnika posameznika ali posameznika, ki samostojno opravlja dejavnost.

(7) Z globo od 1.000 do 2.000 eurov se kaznuje za prekršek odgovorna oseba državnega organa ali organa samoupravne lokalne skupnosti, ki stori dejanje iz petega odstavka tega člena.

(8) Z globo od 500 do 1.500 eurov se kaznuje za prekršek posameznik, ki stori dejanje iz petega odstavka tega člena.

121. člen

(kršitev določb o videonadzoru glede dostopa v uradne službene oziroma poslovne prostore)

(1) Z globo od 4.000 do 12.000 eurov se kaznuje za prekršek pravna oseba, samostojni podjetnik posameznik ali posameznik, ki samostojno opravlja dejavnost:

1. če izvaja videonadzor brez pravne podlage iz prvega odstavka 98. člena tega zakona;
2. če izvaja videonadzor tako, da izvaja snemanje notranjosti stanovanjskih stavb, ki nimajo vpliva na dostop do njihovih prostorov ali posnetke vhodov v stanovanja (drugi odstavek 98. člena tega zakona);
3. če pisno ne obvesti zaposlenih (tretji odstavek 98. člena tega zakona).

(2) Z globo od 800 do 1.200 eurov se kaznuje za prekršek iz prejšnjega odstavka tudi odgovorna oseba pravne osebe, samostojnega podjetnika posameznika ali posameznika, ki samostojno opravlja dejavnost.

(3) Z globo od 800 do 1.200 eurov se kaznuje za prekršek odgovorna oseba državnega organa ali organa samoupravne lokalne skupnosti, ki stori dejanje iz prvega odstavka tega člena.

(4) Z globo od 200 do 800 eurov se kaznuje za prekršek posameznik, ki stori dejanje iz prvega odstavka tega člena.

122. člen

(kršitev določb o videonadzoru pri večstanovanjskih stavbah)

(1) Z globo od 2.000 do 8.000 eurov se kaznuje za prekršek pravna oseba, samostojni podjetnik posameznik ali posameznik, ki samostojno opravlja dejavnost, ki izvaja videonadzor v nasprotju s 99. členom tega zakona.

(2) Z globo od 400 do 1.200 eurov se kaznuje za prekršek iz prejšnjega odstavka tudi odgovorna oseba pravne osebe, samostojnega podjetnika posameznika ali posameznika, ki samostojno opravlja dejavnost.

(3) Z globo od 800 do 1.200 eurov se kaznuje za prekršek odgovorna oseba državnega organa ali organa samoupravne lokalne skupnosti, ki stori dejanje iz prvega odstavka tega člena.

(4) Z globo od 200 do 400 eurov se kaznuje za prekršek posameznik, ki stori dejanje iz prvega odstavka tega člena.

123. člen

(kršitev določb o videonadzoru v delovnih prostorih)

(1) Z globo od 4.000 do 12.000 eurov se kaznuje za prekršek pravna oseba, samostojni podjetnik posameznik ali posameznik, ki samostojno opravlja dejavnost, ki izvaja videonadzor v delovnih prostorih v nasprotju s 100. členom tega zakona.

(2) Z globo od 1.200 do 2.000 eurov se kaznuje za prekršek iz prejšnjega odstavka tudi odgovorna oseba pravne osebe, samostojnega podjetnika posameznika ali posameznika, ki samostojno opravlja dejavnost.

(3) Z globo od 1.200 do 2.000 eurov se kaznuje za prekršek odgovorna oseba državnega organa ali organa samoupravne lokalne skupnosti, ki stori dejanje iz prvega odstavka tega člena.

(4) Z globo od 800 do 1.200 eurov se kaznuje za prekršek posameznik, ki stori dejanje iz prvega odstavka tega člena.

124. člen

(kršitev določb o videonadzoru na javnih površinah)

(1) Z globo od 4.000 do 12.000 eurov se kaznuje za prekršek pravna oseba, samostojni podjetnik posameznik ali posameznik, ki samostojno opravlja dejavnost, ki izvaja videonadzor na javnih površinah v nasprotju z 101. členom tega zakona.

(2) Z globo od 1.200 do 2.000 eurov se kaznuje za prekršek iz prejšnjega odstavka tudi odgovorna oseba pravne osebe, samostojnega podjetnika posameznika ali posameznika, ki samostojno opravlja dejavnost.

(3) Z globo od 1.200 do 2.000 eurov se kaznuje za prekršek odgovorna oseba državnega organa ali organa samoupravne lokalne skupnosti, ki stori dejanje iz prvega odstavka tega člena.

(4) Z globo od 800 do 1.200 eurov se kaznuje za prekršek posameznik, ki stori dejanje iz prvega odstavka tega člena.

125. člen

(kršitev določb o biometriji v javnem sektorju)

(1) Z globo od 4.000 do 12.000 eurov se kaznuje za prekršek pravna oseba javnega sektorja, ki izvaja biometrične ukrepe v nasprotju z 102. členom tega zakona.

(2) Z globo od 1.200 do 2.000 eurov se kaznuje za prekršek iz prejšnjega odstavka tudi odgovorna oseba pravne osebe javnega sektorja.

(3) Z globo od 1.200 do 2.000 eurov se kaznuje za prekršek iz prvega odstavka tega člena tudi odgovorna oseba državnega organa ali organa samoupravne lokalne skupnosti, ki stori dejanje iz prvega odstavka tega člena.

126. člen

(kršitev določb o biometriji v zasebnem sektorju)

(1) Z globo od 4.000 do 12.000 eurov se kaznuje za prekršek pravna oseba, samostojni podjetnik posameznik ali posameznik, ki samostojno opravlja dejavnost, ki izvaja biometrične ukrepe v nasprotju s 103. členom tega zakona.

(2) Z globo od 1.200 do 2.000 eurov se kaznuje za prekršek iz prejšnjega odstavka tudi odgovorna oseba pravne osebe, samostojnega podjetnika posameznika ali posameznika, ki samostojno opravlja dejavnost.

127. člen

(kršitev določb o prepovedi trženja biometričnih osebnih podatkov v zasebnem sektorju)

(1) Z globo od 8.000 do 20.000 eurov se kaznuje za prekršek pravna oseba, samostojni podjetnik posameznik ali posameznik, ki samostojno opravlja dejavnost, ki izvaja biometrične ukrepe v nasprotju s 104. členom tega zakona.

(2) Z globo od 4.000 do 6.000 eurov se kaznuje za prekršek iz prejšnjega odstavka tudi odgovorna oseba pravne osebe, samostojnega podjetnika posameznika ali posameznika, ki samostojno opravlja dejavnost.

128. člen

(kršitev določb o evidentiranju vstopov in izstopov)

(1) Z globo od 2.000 do 4.000 eurov se kaznuje za prekršek pravna oseba, samostojni podjetnik posameznik ali posameznik, ki samostojno opravlja dejavnost:

1. ki uporablja evidenco vstopov in izstopov kot uradno evidenco v nasprotju s tretjim odstavkom 105. člena tega zakona;

2. ki ravna v nasprotju s četrnim odstavkom 105. člena tega zakona.

(2) Z globo od 200 do 800 eurov se za prekršek kaznuje tudi odgovorna oseba pravne osebe, samostojnega podjetnika posameznika ali posameznika, ki samostojno opravlja dejavnost, ki stori prekršek iz prejšnjega odstavka.

(3) Z globo od 200 do 800 eurov se kaznuje za prekršek odgovorna oseba državnega organa ali organa samoupravne lokalne skupnosti, ki stori prekršek iz prvega odstavka tega člena.

(4) Z globo od 200 do 400 eurov se kaznuje za prekršek posameznik, ki stori prekršek iz prvega odstavka tega člena.

129. člen

(kršitev določb o javnih knjigah)

(1) Z globo od 2.000 do 4.000 eurov se kaznuje za prekršek pravna oseba, samostojni podjetnik posameznik ali posameznik, ki samostojno opravlja dejavnost, ki uporablja osebne podatke v nasprotju z zakonskim namenom iz 106. člena tega zakona.

(2) Z globo od 400 do 1.200 eurov se kaznuje za prekršek iz prejšnjega odstavka tudi odgovorna oseba pravne osebe, samostojnega podjetnika posameznika ali posameznika, ki samostojno opravlja dejavnost.

(3) Z globo od 400 do 2.000 eurov se kaznuje za prekršek odgovorna oseba državnega organa ali organa samoupravne lokalne skupnosti, ki stori prekršek iz prvega odstavka tega člena.

(4) Z globo od 200 do 1000 eurov se kaznuje za prekršek posameznik, ki stori dejanje iz prvega odstavka tega člena.

130. člen

(kršitev določb o povezovanju uradnih evidenc in javnih knjig)

(1) Z globo od 2.000 do 8.000 eurov se kaznuje za prekršek pravna oseba, samostojni podjetnik posameznik ali posameznik, ki samostojno opravlja dejavnost, ki poveže uradne evidence ali javne knjige brez zakonske podlage v nasprotju s prvim odstavkom 103. člena tega zakona ali jih povezuje ali poveže brez predhodnega obvestila ali določbe Informacijskega pooblaščenca, v nasprotju z drugim ali tretjim odstavkom 107. člena tega zakona.

(2) Z globo od 400 do 4.000 eurov se kaznuje za prekršek odgovorna oseba državnega organa ali organa samoupravne lokalne skupnosti, ki stori prekršek iz prvega odstavka tega člena.

131. člen

(kršitev določb o strokovnem nadzoru)

(1) Z globo od 4.000 do 8.000 eurov se kaznuje za prekršek pravna oseba:

1. če izvaja strokovni nadzor v nasprotju z drugim odstavkom 109. člena tega zakona;
2. če ne naredi uradnega zaznamka ali drugega uradnega zapisa iz 111. člena tega zakona.

(2) Z globo od 800 do 1.200 eurov se kaznuje za prekršek iz prejšnjega odstavka tudi odgovorna oseba pravne osebe.

(3) Z globo od 800 do 1.200 eurov se kaznuje za prekršek odgovorna oseba državnega organa ali organa samoupravne lokalne skupnosti, ki stori dejanje iz prvega odstavka tega člena.

(4) Z globo od 200 do 800 eurov se kaznuje za prekršek posameznik, ki stori dejanje iz prvega odstavka tega člena.

XII. DEL

PREHODNE IN KONČNE DOLOČBE

132. člen

(prehodne določbe)

(1) Upravitelji in obdelovalci v enem letu od začetka veljavnosti tega zakona izvedejo ustrezne ukrepe prilagoditve glede uporabe privolitve določbam tega zakona kot pravne podlage za obdelavo osebnih podatkov, ki so bile dane pred uveljavitvijo tega zakona v skladu z Zakonom o varstvu osebnih podatkov (Uradni list RS, št. 94/07 – uradno prečiščeno besedilo). Če upravljavec in obdelovalec v obdobju iz prejšnjega stavka izvajata ustrezne ukrepe prilagoditve iz prejšnjega stavka, to preprečuje nastanek kaznivosti za prekršek.

(2) Postopki odločanja ali inšpekcijskega nadzora, ki so se pred začetkom uporabe tega zakona začeli pri Informacijskem pooblaščenca ali se obravnavajo na sodiščih se nadaljujejo in končajo po določbah Zakona o varstvu osebnih podatkov (Uradni list RS, št. 86/04, 113/05 – ZInfP, 51/07 – ZUstS-A, 67/07 in 94/07 – uradno prečiščeno besedilo).

(3) Dejanja obdelave osebnih podatkov pri upraviteljih osebnih podatkov in pogodbenih obdelovalcih, se nadaljujejo po določbah Zakona o varstvu osebnih podatkov (Uradni list RS, št. 86/04, 113/05 – ZInfP, 51/07 – ZUstS-A, 67/07 in 94/07 – uradno prečiščeno besedilo) najpozneje do roka šest mesecev od začetka veljavnosti tega zakona. Za obdobje iz prejšnjega stavka se šteje, da če upravljavec in obdelovalec izvajata ustrezne ukrepe glede priprave na usklajitev z določbami Splošne uredbe in tega zakona, da gre za ustrezni prilagoditveni ukrep, ki preprečuje nastanek kaznivosti za prekršek.

(4) Upravitelji in obdelovalci so dolžni v roku devetih mesecev od začetka veljavnosti tega zakona izvesti ustrezne ukrepe prilagoditve glede določitve pooblaščenih oseb po določbah tega zakona. Za obdobje iz prejšnjega stavka se šteje, da če obdelovalec in upravljavec izvajata ustrezne ukrepe glede določitve pooblaščenih oseb in zagotavljata v tem obdobju skladnost obdelave osebnih podatkov po tem zakonu na drug način, da gre za ustrezni prilagoditveni ukrep, ki preprečuje nastanek kaznivosti za prekršek.

(5) Ne glede na določbe prejšnjega odstavka so občine in javni vzgojno-izobraževalni zavodi v roku dveh let od začetka veljavnosti tega zakona dolžni določiti pooblaščenih oseb, do poteka tega roka lahko njihove naloge zagotavljanja skladnosti obdelave osebnih podatkov po tem zakonu opravljajo druge osebe iz občinske uprave oziroma zavoda, ki so pristojne za izvajanje notranjih nadzorov ali revizij ali podobnih delovanj.

(6) Slovenska akreditacija začne izvajati postopke akreditacije od 1. januarja 2020 dalje.

(7) Povezovanja po določbah prvega odstavka 107. člena tega zakona je treba uskladiti s pogoji iz tega člena v roku 4 let od začetka veljavnosti tega zakona.

(8) Za izvrševanje osmega odstavka 38. člena tega zakona so upravitelji ali obdelovalci, ki za izvajanje svojega delovanja pridobivajo osebne podatke iz registrov ali evidenc s področja upravnih notranjih zadev, dolžni v roku dveh let po začetku veljavnosti tega zakona vzpostaviti ustrezne varnostne mehanizme po predhodnem soglasju ministrstva, pristojnega za notranje zadeve.

(9) Z dnem začetka veljavnosti tega zakona preneha delovati Register zbirk osebnih podatkov pri Informacijskem pooblaščenju, Informacijski pooblaščenec njegovo vsebino arhivira in preda v roku enega leta Arhivu Republike Slovenije, ki vsebino Registra hrani kot trajno arhivsko gradivo.

133. člen

(prenehanje veljavnosti zakona)

Z dnem uveljavitve tega zakona preneha veljati Zakon o varstvu osebnih podatkov (Uradni list RS, št. 86/04, 113/05 – ZInFP, 51/07 – ZUstS-A, 67/07 in 94/07 – uradno prečiščeno besedilo).

134. člen

(končna določba)

Ta zakon začne veljati 25. maja 2018.

III. Obrazložitev členov

Besedilo Predloga ZVOP-2 še ne upošteva sprememb (popravkov) v besedilu določb slovenskih inštitucij, ker le-te še niso objavljene v Uradnem listu Evropske unije ter tako tudi še niso mogle biti upoštevane v obrazložitvi členov. Kot je že navedeno v uvodni obrazložitvi, utegne biti vpliv na določbe Predloga ZVOP-2 še nekoliko širši, saj utegneta biti delno spremenjeni tudi inštitucije besedil Splošne uredbe in Direktive v angleški jezikovni inačici (objava v Uradnem listu Evropske unije predvidoma maja 2018).

1. K I. delu Predloga ZVOP-2:

K 1. členu:

Prvi odstavek predlaganega člena navaja, da je vsebina zakona najprej določanje pravic, obveznosti, upravičenj, načel, postopkov in ukrepov, s katerimi se preprečujejo neustavni, nezakoniti ali neupravičeni posegi v zasebnost oziroma dostojanstvo oziroma druge temeljne pravice posameznika oziroma posameznice pri obdelavi osebnih podatkov, tako da se varuje ali uresničuje pravico do varstva osebnih podatkov iz 1. člena ZVOP-2 oziroma njena področja iz prvega in drugega odstavka 2. člena ZVOP-2. Gre torej za nadaljevanje sistemskega pristopa glede osebne človekove pravice, kot je opredeljena v 1. členu predloga ZVOP-2.

V drugem odstavku je določeno, da se v pravni red Republike Slovenije prenašajo določbe Direktive (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 ter tudi prenašajo in zagotavlja izvajanje določb Uredbe (EU) 2016/679 Evropskega parlamenta in Sveta z dne 27. aprila 2016 o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem pretoku takih podatkov ter o razveljavitvi Direktive 95/46/ES (Splošna uredba o varstvu podatkov), ki se morajo ali smejo prenesti v pravni red Republike Slovenije ter tudi povezovalne določbe v zvezi s Splošno uredbo do določb Direktive. Navedena zapletena formulacija pove, da se določbe navedene Direktive izvršuje z zakonom, da delno podobno velja glede določb Splošne uredbe, ki se lahko izvršijo ali morajo izvršiti z zakonom Republike Slovenije, da pa za določene neposredno uporabne določbe Splošne uredbe (kadar se zlasti prekrivajo z določbami Direktive) velja sistem informativnega prepisa in ne neposredne uporabnosti, saj se jih načeloma ne razdeli, temveč le prepiše (npr. prvi odstavek 6. člena Predloga ZVOP-2 o splošnih definicijah). Namen tovrstnega prepisa v zvezi z razlago njegovega pomena ne predstavlja kršitve določb Splošne uredbe, niti ne z vidika uvodne navedbe št. 8 Splošne uredbe, temveč le zagotavljanje pravne varnosti, pa četudi le na informativni način (v tem primeru).

K 2. členu:

2. člen v prvem odstavku določa bistvo človekove pravice do varstva osebnih podatkov. Pravico oziroma skupek pravic iz varstva osebnih podatkov iz 38. člena Ustave Republike Slovenije določa kot osebno človekovo pravico posameznika ali posameznice do varstva njegovih ali njenih osebnih podatkov (poudarek glede osebne pravice kaže na njen poseben pomen za človeka, ni mišljeno v smislu, da ni kolektivna človekova pravica). Pri tem določba izhaja iz ti. »subjektivnega pristopa« in ne iz pristopa regulacije (zakonske ozir. upravne obveznosti), v središču te ene od najbolj bistvenih pravic je namreč človek. To izhaja tudi iz zadnjega dela določbe, po kateri se posameznikom in posameznikom zagotavljajo zasebnost (38. in 35. člen Ustave Republike Slovenije) oziroma (torej: in/ali) dostojanstvo (34. člen Ustave Republike Slovenije) ob upoštevanju podatkovne samoodločbe (38. člen Ustave Republike Slovenije). V primeru podatkovne samoodločbe (ki kaže, da gre za človekovo posebej poudarjeno osebno pravico razpolaganja svojimi osebnimi podatki) gre za to, da je

vsak posameznik »oblast« nad svojimi osebnimi podatki, da torej primarno sam odloča ali želi, da se njegove osebne podatke obdela, posreduje (npr. za izpolnitev pogodbe), izjeme pa so dopustne (ob spoštovanju testa stroge sorazmernosti), da se namreč določene podatke obdeluje proti njegovi volji – npr. če to določi zakon, ki preстане navedene pogoje presoje.

V drugem odstavku je določeno, da se v okviru osebne človekove pravice po prvem odstavku zagotavlja, da ima vsaka posameznica ali posameznik upravičenje, da se z zakonom ter pošteno in na pregleden način ureja in zagotavlja obdelava njenih ali njegovih osebnih podatkov, tajnost njenih ali njegovih osebnih podatkov, ter njene ali njegove pravice do seznanitve z lastnimi osebnimi podatki, do popravka lastnih podatkov oziroma do uresničevanja drugih pravic iz tega ali drugega zakona. Glede dela določbe o tajnosti osebnih podatkov določba izhaja iz drugega odstavka 38. člena Ustave Republike Slovenije, po katerem »varstvo tajnosti (!) osebnih podatkov določa zakon«.

Predlagani 2. člen predloga zakona je tudi primerljiv določbi 1. člena Zakona o varstvu osebnih podatkov Republike Avstrije, kot je bil spremenjen z Zveznim zakonom, s katerim se spreminja Zakon o varstvu osebnih podatkov iz leta 2000 (Zakon o prilagoditvi varstva osebnih podatkov 2018)³³. Z navedenim zakonom sicer ni bil izveden poseg v 1. člen veljavnega zakona, ki temeljno ureja človekovo pravico od varstva osebnih podatkov – zaradi neobstoja dvotretjinske ustavne večine za revizijo, kar pomeni, da je tudi Avstrija zadržala dosedanje širše opredelitev varstva osebnih podatkov kot temeljne človekove pravice (na ustavni ravni).

2. člen ima pomen za razlago vseh določb tega predloga zakona, področne zakonodaje glede varstva osebnih podatkov ter za uporabo določb Splošne uredbe, tako da mora osredotočeni naslovnik pravic biti posameznik, na katerega se nanašajo osebni podatki (subjekt varstva pravice do tajnosti osebnih podatkov).

Glede na dosedanje 1. člen ZVOP-1 novi 2. člen ZVOP-2 torej vsebuje posodobljene formulacije, s posebnim pomenom za interpretacijo ZVOP-2, kot je opisan zgoraj.

K 3. členu:

Predlagani 3. člen ureja prepoved diskriminacije glede varstva osebnih podatkov. Pri tem je pomembna povezava s 1. členom, da gre za osebno človekovo pravico, da je osredotočeni naslovnik pravic posameznik, na katerega se nanašajo osebni podatki ter glede razlagalne »moči« glede drugih zakonov ipd.. V 2. členu so glede na 14. člen Ustave Republike Slovenije ter glede na druge ustaljene formulacije pravnega reda Republike Slovenije (npr. prvi odstavek 131. člena Kazenskega zakonika³⁴ ter prvi odstavek 1. člena Zakona o varstvu pred diskriminacijo³⁵) navedene prepovedane okoliščine diskriminacije. Določbe so nekoliko posodobljene – dodana spolna identiteta po prvem odstavku 1. člena Zakona o varstvu pred diskriminacijo, dodana genska (ne genetska) predispozicija, beseda »barva« iz dosedanjega 4. člena ZVOP-1 je spremenjena v »barvo kože«, omenjeno je tudi zdravstveno stanje.

Predlagani člen pomeni, da se nikogar ne sme diskriminirati glede varstva osebnih podatkov, kar med drugim vključuje tudi prebivališče (vpliv glede 4. člena predloga zakona – ozemeljska veljavnost). Natančneje – med prepovedanimi kriteriji diskriminacije (razlikovanja) sta v praksi zlasti najbolj pomembna kriterija državljanstva in prebivališča, tudi glede na 1. člen Konvencije o varstvu posameznikov glede na avtomatsko obdelavo osebnih podatkov³⁶ (Sveta Evrope), ki se v tem delu v okviru še nedokončane reforme varstva osebnih podatkov v okviru Sveta Evrope ne spreminja.

K 4. členu:

³³ Objava: Bundesgesetzblatt I Nr. 120/2017, Teil I.

³⁴ Uradni list RS, št. 50/12 – uradno prečiščeno besedilo, 6/16 – popr., 54/15, 38/16 in 27/17.

³⁵ Uradni list RS, št. 33/16.

³⁶ Uradni list RS, št. 11/94 – Mednarodne pogodbe, št. 3/94 in 86/04 – ZVOP-1.

V navedenem členu je določena materialna veljava tega zakona, tj. za katere obdelave velja in za katere ne velja.

V prvem odstavku je tako določeno (glede na prvi odstavek člena 2 Splošne uredbe), da določbe ZVOP-2 veljajo za popolnoma ali delno avtomatizirano obdelavo osebnih podatkov ter za drugačne obdelave osebnih podatkov, ki so vključeni ali so namenjeni vključitvi v zbirko.

V drugem odstavku je določena splošna izjema od veljave zakona, namreč obdelava osebnih podatkov za domače potrebe, kar vključuje zlasti obdelave osebnih podatkov, ki jih izvajajo posamezniki izključno za osebno uporabo, družinsko življenje. Pri uporabi tega člena je treba biti pozoren v dve smeri – sicer široko tolmačiti domače potrebe, vendar v okviru besede »izključno« - da ne pride do kombinacije med domačo potrebo (uporabo) in poslovnim namenom. V trenutno vodilni literaturi s področja razlage Splošne uredbe je npr. podana takšna razlaga:

»Najbolj pomembna izjema z vidika ekonomičnosti je določena v c. točki, po kateri se »uredba ne uporablja za obdelavo osebnih podatkov s strani fizične osebe v okviru *izključno osebne ali domače dejavnosti*«. Ta koncept se mora razlagati na podlagi splošnega družbenega mnenja in vključuje osebne podatke, ki se obdelujejo za prostočasovne aktivnosti, hobije, počitnice ali aktivnosti zabave, za uporabo družbenih omrežij ali podatkov, ki so del osebne zbirke naslovov, rojstnih dneвов ali drugih podobnih datumov, kot so obletnice.

Mora se opozoriti, da če obdelava zadeva tako zasebne kot poslovne informacije, se izjema ne uporabi. Beseda »izključno« nakazuje na *ozko interpretacijo* te določbe, Poslovna aktivnost bi morala vključevati kakršnokoli aktivnost ne glede na to, ali je odplačna, kot tudi pripravljala delovanja za njo, kot so npr. ukrepi trženja ali trgovanje z osebnimi podatki za to, da se dobi storitev.«³⁷

V tretjem odstavku je določeno, da če V. in IX. del tega zakona ne določata drugače, določbe tega dela zakona veljajo tudi na področjih preprečevanja, preiskovanja, odkrivanja ali pregona kaznivih dejanj ali izvrševanja kazenskih sankcij ter varnosti države in obrambe države (področje izvrševanja določb »Direktive (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«).

K 5. členu:

5. člen je en od najpomembnejših členov predloga zakona, glede na to, da preko določanja jurisdikcije pravnega reda Republike Slovenije (prvi in tretji odstavek), njenega nadzornega organa (Informacijski pooblaščenec) ter sodnega varstva pred sodišči Republike Slovenije določa raven varstva pravic posameznikov glede njihovih osebnih podatkov.

Ozemeljska veljavnost določa, za katere obdelave osebnih podatkov (in s tem, za katere upravljavce oziroma obdelovalce osebnih podatkov) se uporablja določen predpis. Splošna uredba v skladu s členom 3 tako velja za tiste obdelave, ki jih izvajajo upravljavci in obdelovalci iz Evropske unije, ter v določenem delu tudi obdelave tujih upravljavcev in obdelovalcev, če imajo ti namen obdelovati osebne podatke prebivalcev Evropske unije. Predlog ZVOP-2 svojo veljavnost določa prav v teh okvirih, poleg tega pa jo v okviru pooblastil iz Splošne uredbe³⁸ določa tudi za nekatere posebne primere obdelav osebnih podatkov prebivalcev Republike Slovenije, za katere bi bila sicer podana veljavnost nacionalnega zakona katere druge države članice. Cilj tako široko začrtane veljavnosti je preprečiti, da bi bili prebivalci Evropske unije oziroma Republike Slovenije izključeni iz varstva, ki ga zagotavljata

³⁷ Glejte: Voigt, Paul, von dem Bussche, Axel, *The EU General Data Protection Regulation (GDPR) : A Practical Guide*, Springer International Publishing AG, Cham, 2017, str. 16-17.

³⁸ Npr. drugi stavek prvega odstavka člena 8 (privolitvena starost otrok), uvodna navedba št. 27 (obdelave osebnih podatkov umrlih oseb), četrti odstavek člena 9 (obdelave genskih, biometričnih ali podatkov v zvezi z zdravjem) ali člen 10 (obdelava osebnih podatkov v zvezi s kazenskimi obsodbami in prekrški).

Splošna uredba oziroma tak zakon, oziroma da bi upravljavec oziroma obdelovalec to varstvo zaobšla³⁹ z izbiro kraja ustanovitve.

Prvenstveno ta zakon v skladu s prvim odstavkom tega člena tako kot dosedaj velja za tiste obdelave osebnih podatkov, ki potekajo v okviru opravljanja dejavnosti upravljavca ali obdelovalca, ki ima sedež, hčerinsko družbo, podružnico ali drugačno poslovno enoto na ozemlju Republike Slovenije, in to ne glede na to, ali sama dejanja obdelave dejansko potekajo na ozemlju Republike Slovenije ali ne⁴⁰.

Gre za že obstoječe kriterije iz (a) točke prvega odstavka člena 4 Direktive o varstvu osebnih podatkov oziroma prvega odstavka 5. člena dosedanje ZVOP-1. Pri tem pri ugotavljanju, ali se neka obdelava izvaja v okviru dejavnosti določene poslovne enote, v skladu z sodno prakso Sodišča Evropske unije⁴¹ ni nujno, da ta poslovna enota tudi dejansko izvaja zadevno obdelavo (tj. zlasti, da je namesto nje ne opravlja druga, z njo lastniško ali drugače povezana poslovna enota), ampak zadostuje že, da so dejavnosti poslovne enote na bistven način povezane z obdelavo. Pri ugotavljanju tega, ali se določen subjekt šteje za takšnega, ki ima sedež, hčerinsko družbo, podružnico ali drugačno poslovno enoto na ozemlju Republike Slovenije, pa prav tako ni nujno, da je ta subjekt vpisan v poslovni register Republike Slovenije in organiziran v obliki katere od ustaljenih organizacijskih oblik (npr. s.p., d.o.o., d.d., o.p., idr. – za te je veljava tega zakona nesporna), ampak štejejo tudi drugi subjekti, vključno s fizičnimi osebami, ki dejavnosti obdelave izvajajo dejansko in učinkovito ter prek ustaljenih ustanovitev⁴², oziroma ki na ozemlju Republike Slovenije opravljajo dejansko in resnično, čeprav majhno, dejavnost, v okviru katere se izvaja ta obdelava⁴³.

Upravljavci in obdelovalci, ki so del javnega sektorja Republike Slovenije, so vključeni že po samem zakonu, brez potrebe po ugotavljanju njihovega sedeža. S tem so vključena tudi veleposlaništva, konzulati, stalna predstavništva in druge misije, za katere se slovensko pravo uporablja na podlagi mednarodnega prava (tretji odstavek 3. člena Splošne uredbe oziroma dosedaj tudi četrti odstavek 5. člena ZVOP-1).

Pravila za razmejevanje veljave zakonov posameznih držav članic so sicer podrobneje pojasnjena v mnenju Delovne skupine po členu 29 Direktive o varstvu osebnih podatkov št. 8/2010 o pravu, ki se uporablja⁴⁴, upošteva okolščino, da se kriterij opreme za obdelavo ((c) točka prvega odstavka člena 4 Direktive oziroma drugi odstavek 5. člena ZVOP-1) z začetkom uporabe Splošne uredbe ne uporablja več.

Dodatno ta zakon v skladu z drugim odstavkom tega člena velja tudi za obdelave osebnih podatkov prebivalcev Republike Slovenije, ki ne potekajo v okviru upravljavca s sedežem zunaj Evropske unije (ampak jih izvaja upravljavec iz tretje države), vendar se ponujajo slovenskih uporabnikom, oz. zadevajo profiliranje slovenskih uporabnikov. Navedena določba temelji na drugem odstavku člena 3 Splošne uredbe in cilja na to, da prebivalci Republike Slovenije ne bi bili prikrajšani za varstvo svojih osebnih podatkov samo zato, ker upravljavec ali obdelovalec osebnih podatkov nista ustanovljena znotraj Evropske unije⁴⁵ (in torej za nadzor nad njim ni že tako v skladu s prvim odstavkom člena 3 Splošne uredbe pristojen kateri od državnih nadzornih organov držav članic). Pri tem pa sama dostopnost spletne strani upravljavca, obdelovalca ali njenega posrednika za prebivalce Republike Slovenije še ne zadostuje za vzpostavitev veljave zakona; za to mora biti izkazano, da namerava upravljavec oziroma obdelovalec tudi dejansko nuditi storitve posameznikom iz Republike Slovenije,

³⁹ Glejte: razdelek št. 54 sodbe Sodišča EU v zadevi C-131/12 z dne 13. 5. 2014, *Google Spain SL, Google Inc. proti Agencia Española de Protección de Datos (AEPD)*.

⁴⁰ Uvodna navedba št. 22 Splošne uredbe.

⁴¹ Sodba Sodišča EU v zadevi C-131/12, tč. 52, 56 in 67.

⁴² Uvodna navedba št. 22 Splošne uredbe.

⁴³ 1. točka izreka sodbe Sodišča Evropske unije v zadevi C-230/14 z dne 1. 10. 2015, *Weltimmo s. r. o. proti Nemzeti Adatvédelmi és Információszabadság Hatóság*.

⁴⁴ http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2010/wp179_en.pdf

⁴⁵ Navedba št. 23 Splošne uredbe.

še zlasti tako, da pri tem uporablja slovenski jezik⁴⁶ oziroma da namerava slediti obnašanju prebivalcev Republike Slovenije na internetu, še zlasti tako, da oblikuje profile njihovega obnašanja, oziroma drugače zbira podatke o tem z namenom sprejemanja odločitev o njem oziroma za analiziranje ali predvidevanje njegovega osebnega okusa in vedenja⁴⁷. V takšnih primerih bo Informacijski pooblaščenec pristojen za nadzor skladnosti obdelave tujega upravljavca oz. obdelovalca s tem zakonom, ter za obravnavo pritožb posameznikov v zvezi s tem.

Končno posamezne določbe tega zakona v skladu s tretjim odstavkom tega člena veljajo tudi za obdelave osebnih podatkov, za katere bi po kriteriju ustanovitve iz prvega odstavka sicer v celoti veljal zakon druge države članice, vendar pa Splošna uredba pooblašča državo članico, da vseeno določi obvezno veljavo svojega zakona. To ti. »načelo rezidenčnosti« omogoča Republiki Sloveniji, da npr. glede starosti privolitve slovenskih mladoletnih oseb zahteva od upravljavcem na npr. Irskem, da upoštevajo pri nas določeno minimalno starost 15 let. Vse primeri rabe tega načela so v tem odstavku posebej naštet. V njih bo slovenski državni nadzorni organ za varstvo osebnih podatkov (Informacijski pooblaščenec) pristojen sprejeti pritožbe posameznika, ter na tej podlagi sprožiti sodelovanje s pristojnim državnim nadzornim organom druge države članice Evropske unije, zato, da pri tem doseže spoštovanje določb slovenskega zakona za obdelave osebnih podatkov prebivalcev Republike Slovenije. Smisel takšnega pristopa je, da se tudi za te obdelave zagotovi spoštovanje visoke ravni varstva osebnih podatkov, ki jo je že dosedaj določal ZVOP-1, kar je glede na občutljivost in tveganost izbranih področij po presoji predlagatelja nujno in tudi smiselno. Pri vsem tem velja dodati, da v teh primerih veljava tega zakona torej ne pomeni tudi izključne pristojnosti (jurisdikcije) slovenskega državnega nadzornega organa, Informacijskega pooblaščenca.

Med vrstami osebnih podatkov v tretjem odstavku niso določeni osebni podatki umrlih oseb (10. člen Predloga ZVOP-2), ker le-teh Splošna uredba ne ureja (na to področje ne posega), ampak prepušča to urejanju s strani držav članic samih (popolna jurisdikcija vsake države članice v polju njene proste zakonodajne presoje ozir. v okviru bistvenih osnov njenega pravnega reda – npr. raven varstva spoštovanja pravice do pietete) – glede na uvodno navedbo št. 27 Splošne uredbe.

Primer št. 1: italijanski zdravnik obdeluje zdravstvene podatke prebivalca Slovenije. Prebivalec Slovenije se pritoži pri italijanskem ali slovenskem nadzornem organu za varstvo osebnih podatkov. Informacijski pooblaščenec se mora vključiti v postopek in zahtevati uporabo slovenskega ZVOP-2.

Primer št. 2: upokojenec z začasnim prebivališčem v Sloveniji. O njem avstrijski medij piše nekaj neprijetnega. Ta posameznik se bo pritožil v Avstriji avstrijskemu nadzornemu organu za varstvo osebnih podatkov. Izdajatelj medija bo imel pravico zahtevati, da se Informacijski pooblaščenec Republike Slovenije vključi v postopek in zahteva uporabo bolj garantističnih določb slovenskega ZVOP-2 o razmerju svobode izražanja do varstva osebnih podatkov – v korist spoštovanja svobode izražanja.

Določbe dosedanjega tretjega odstavka 5. člena ZVOP-1 (predstavnik tujega upravljavca) so urejena neposredno v Splošni uredbi (člen 27).

K 6. členu:

V 6. členu je v prvem odstavku najprej zapisan dobessedni prepis temeljnih izrazov iz Splošne uredbe in iz Direktive, ki so zaradi prekrivanja med določbami obeh pravnih aktov Evropske unije, kot so osebni podatki, obdelava, zbirka, upravljavec, psevdonimizacija, oblikovanje profilov...

Dodane so le dokaj male dopolnitve, npr. nadzorni organ države je konkretiziran, kadar se nanaša na Republiko Slovenijo – določen je konkretno kot Informacijski pooblaščenec. Pomembno pa je, da je izjemoma že popravljen besedilo definicije privolitve, ne glede na besedilo veljavne slovenske inačice Splošne uredbe, saj bi zadržanje uradne inačice pomenilo drugačno pravno razumevanje privolitve kot

⁴⁶ Navedba št. 23 Splošne uredbe.

⁴⁷ Navedba št. 24 Splošne uredbe.

enega od bistvenih institutov / pravnih podlag za obdelavo osebnih podatkov. Tudi ta popravek bo moral biti upoštevan v popravljeni slovenski inačici Splošne uredbe.

Kot že navedeno, je dodana pomembna (bistvena) sprememba v definiciji privolitve (11. točka prvega odstavka 6. člena), katera se sedaj glasi: »privolitev posameznika, na katerega se nanašajo osebni podatki, pomeni: vsako prostovoljno, konkretno, informirano in nedvoumno ravnanje v obliki izjave ali drugačnega jasnega aktivnega delovanja, iz katerega je mogoče sklepati na želje posameznika, na katerega se nanašajo osebni podatki, s katero izrazi strinjanje z obdelavo osebnih podatkov, ki se nanašajo nanj«. Navedena določba je očitno drugačna od dosedanje uradno zapisane (11). točke člena 4 Splošne uredbe, ki se glasi: »„privolitev posameznika, na katerega se nanašajo osebni podatki“ pomeni vsako prostovoljno, izrecno, informirano in nedvoumno izjavo volje posameznika, na katerega se nanašajo osebni podatki, s katero z izjavo ali jasnim pritrdilnim dejanjem izrazi soglasje z obdelavo osebnih podatkov, ki se nanašajo nanj«⁴⁸. V tem primeru predlagatelj šteje, da ni imel druge izbire, kot da že v tem predlogu zakona popravi definicijo privolitve še preden pride do popravka besedila slovenske jezikovne inačice Splošne uredbe v tem delu. Če bi bilo prepisano sedanje objavljeno napačno besedilo glede definicije privolitve, bi to pomenilo škodo pravni varnosti.

Zapisi temeljnih definicij s področja varstva osebnih podatkov (npr. osebni podatki, obdelava...) – kolikor se nanašajo na definicije iz Splošne uredbe, so na koncu prvega odstavka pojasnjeni z navedbo, da gre (samo) za navedbo »v skladu z zavezujočimi določbami člena 4 Splošne uredbe«. To pomeni, da je navedeni zapis (prepis) le informativne ozir. povezovalne narave v korist pravne varnosti in ne pomeni reguliranja izven dometa Splošne uredbe (tudi glede na uvodno navedbo št. 8 Splošne uredbe). V delu, ko se isti zapisi temeljnih definicij nanašajo na Direktivo in so spet enaki določbam Splošne uredbe, pa je na koncu prvega odstavka za razliko od prej navedene zaključne formulacije glede Splošne uredbe navedeno, da [to pravno urejanje] »tudi pomeni izvajanje določb člena 3 Direktive«. Dodatno pa je upoštevana tudi mednarodna obveznost s področja Sveta Evrope - navedeno je, da ta člen pomeni tudi izvajanje določb 2. in 5. člena Konvencije o varstvu posameznikov glede na avtomatsko obdelavo osebnih podatkov (Sveta Evrope)⁴⁹. Za področja, katerih Splošna uredba ali Direktiva ne urejajo (npr. varstvo osebnih podatkov umrlih oseb, varnost države, obramba države...) prav tako v celoti veljajo te temeljne definicije (razlog pravne varnosti).

V delu, ko gre za prej navedeni prepis temeljnih definicij iz Splošne uredbe, primerjalnopravna ureditev trenutno kaže (ob upoštevanju, da so dosedaj sprejeti le trije izvedbeni zakoni – avstrijski, nemški in slovaški), da ima slovaški zakon z dne 29. 11. 2017 tudi v 2. in 5. členu prepis določb Splošne uredbe, vendar ne vsebuje zamejitev (glede uporabe Splošne uredbe), kot je predlagano na koncu besedila prvega odstavka 6. člena ZVOP-2.

V predlaganem drugem odstavku 6. člena so za potrebe izvrševanja IX. dela tega zakona določene definicije pristojnih organov.

V predlaganem tretjem odstavku 6. člena pa so določeni še nekateri izrazi, katere se lahko glede na specifičnosti pravnega reda Slovenije določi samostojno, npr. javni sektor, povezovalni znak (dosedaj isti povezovalni znak) ipd., ki ne odstopajo vsebinsko od dosedanjih definicij iz 6. člena ZVOP-1.

Izbrisa osebnih podatkov pomeni trajno odstranitev ali uničenje osebnega podatka, tako da ga več ni mogoče obnoviti, pri tem pa je zaradi zagotavljanja sledljivosti obdelave osebnih podatkov (sedmi odstavek 40. člena ZVOP-2) dopustno zabeležiti zaznamek, da je bil v zvezi osebnimi podatki določenega posameznika izveden izbris, pri čemer pa zaznamek ne sme vsebovati podatkov, ki bi omogočali obnovo izbrisanega podatka. Izraz trajna odstranitev pomeni elektronski izbris podatka, izraz uničenje pa pomeni fizično uničenje podatka v papirnati obliki. Z zakonom se sicer lahko določi drugačna uporaba instituta izbrisa (na izrecen način!), da se po izbrisu osebni podatek lahko arhivira v ti. neaktivno« arhivsko zbirko (evidenco).

⁴⁸ V angleščini se besedilo 11. točke glasi: »‘consent’ of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her«.

⁴⁹ Uradni list RS, št. 11/94 – Mednarodne pogodbe, št. 3/94 in 86/04 – ZVOP-1.

Skupni upravljavci pomenijo situacijo ali stanje ali odločitev ali odločanje, kadar dva ali več upravljavcev skupaj določijo namene in sredstva obdelave (za skupne ali ločene zbirke, z deljenimi vlogami upravljalvskega tipa), skupni upravljavci pa so podrobneje urejeni v 33. členu ZVOP-2.

Zakon pomeni glede na člen 6 Splošne uredbe, člen 4 Direktive ter a) in b) točko 5. člena Konvencije o varstvu posameznikov glede na avtomatsko obdelavo osebnih podatkov (Sveta Evrope) - ta zakon, druge zakone Republike Slovenije, obvezujoče (in torej ratificirane) mednarodne pogodbe, ki zavezujejo Republiko Slovenijo ter pravne akte ali odločitve Evropske unije, katerih določbe so enakovredne zakonom in neposredno uporabljive ali neposredno učinkovite (glede na tretji odstavek 3.a člena Ustave Republike Slovenije), v to definicijo pa niso vključeni podzakonski predpisi (ker ne smejo biti vključeni glede na drugi odstavek 38. člena Ustave Republike Slovenije ter z njim povezano ustaljeno ustavnosodno presojo Ustavnega sodišča Republike Slovenije od leta 1992 dalje⁵⁰).

Varnost države za uporabo po določbah ZVOP-2: gre le za del področja ti. notranje varnosti, ki torej po tej definiciji ne vključuje javne varnosti, temveč klasično varnost države (obveščevalno in protiobveščevalno delovanje). Ta definicija je pomembna za področje uporabe posebnih ureditev po ZVOP-2 (npr. osmi odstavek 31. člena, peti odstavek 38. člena, tretji odstavek 42. člena, sedmi odstavek 49. člena, peti odstavek 55. člena ipd. ZVOP-2).

K 7. členu:

V predlaganem 7. členu so določena temeljna načela za zakonito obdelavo osebnih podatkov, ki zlasti sledijo določbam člena 5 Splošne uredbe. V a) točki prvega odstavka so glede na načelo zakonitosti glede varstva osebnih podatkov iz drugega odstavka 38. člena Ustave Republike Slovenije v zvezi z 87. členom Ustave Republike Slovenije (ter glede na ustaljeno ustavnosodno presojo Ustavnega sodišča Republike Slovenije zlasti po 38. členu Ustave Republike Slovenije) določena obvezna merila za zakonodajno urejanje – kadar se obdelavo osebnih podatkov za javni sektor ali tudi za zasebni sektor ureja z zakonom, pri čemer je upoštevan zadnji del tretjega odstavka člena 6 Splošne uredbe. Točke b), c), č), in e) urejajo omejitve namena obdelave, vključno glede vprašanja nezdružljivosti, minimizacijo obdelave osebnih podatkov, točnost in posodobljenost (dosedanji izraz za posodobljenost: ažurnost), pri tem sledijo točkam iz prvega odstavka člena 5 Splošne uredbe. Načelo sorazmernosti je vsebovano v vsebinah c) točke v delni povezavi z b) in d) točkama in kot tako skupno poimenovano v tretjem odstavku. V e) točki je določen institut varnosti osebnih podatkov (dosedaj: zavarovanje osebnih podatkov), ki je nadalje razdelan v ZVOP-2 v členih o varnosti osebnih podatkov in je z vidika informacijske varnosti ključen.

V drugem odstavku je določena obveznost dokumentiranja skladnosti obdelav osebnih podatkov za upravljavca in obdelovalca z določbami prvega odstavka, katera morata v skladu s tem voditi tudi predpisano dokumentacijo v skladu z zakonom. Kar tudi pomeni, morata to izvajati tudi ko se odloča o obdelavi v druge namene – in ko se oceni, da je možna obdelava v druge namene, da je ta ocena del splošne dokumentacije o skladnosti obdelave. To se dokaže zlasti z izvedbo ocene učinkov ter notranjo sledljivostjo ((f) točka drugega odstavka 34. člena ZVOP-2) in zunanjo sledljivostjo obdelav osebnih podatkov (sedmi odstavek 40. člena ZVOP-2) po določbah tega zakona.

V tretjem odstavku je z vidika lažje povezave in uporabe določb zakona dodano, da je načelo sorazmernosti (poimenovano kot tako) vsebovano v c) točki, v delni povezavi z b) in d) točko prvega odstavka 7. člena ZVOP-2.

K 8. členu:

Predlagani 8. člen najprej določa pravne podlage za obdelavo osebnih podatkov v javnem sektorju in pri temu precej sledi smerem iz dosedanjega 9. člena ZVOP-1. Dejansko nove vsebine so v predlaganem drugem, petem in šestem odstavku.

⁵⁰ Odločba US, št. U-I-115/92, 24.12.1992; objava: OdlUS I, 105 in Uradni list RS, št. 3/93.

Predlagani prvi odstavek določa, kaj mora biti vsebina področnega zakona s področja osebnih podatkov, ki naj bi se obdelovali v javnem sektorju, glede na določbe drugega odstavka 38. člena Ustave Republike Slovenije v zvezi z 87. členom Ustave Republike Slovenije (ter glede na ustaljeno ustavnosodno presojo Ustavnega sodišča Republike Slovenije zlasti po 38. členu Ustave Republike Slovenije). Upošteva tudi merila iz drugega odstavka člena 6 Splošne uredbe ter drugega dela tretjega odstavka člena 6 Splošne uredbe ter drugega odstavka člena 23 Splošne uredbe. V razmerju med prvim in petim odstavkom 8. člena velja, da se podajanje kazenskih ovadb ali naznanitev kaznivih dejanj in s tem povezana posredovanja osebnih podatkov ne šteje za dodatni namen – na to namreč napotuje zadnja poved uvodne navedbe 50 Splošne uredbe. V Sloveniji je to urejeno načeloma na sistemski ravni: ovaditelj ima bodisi zakonsko pravico (145. do 147. člen Zakona o kazenskem postopku) ali posebne dolžnosti sporočanja kršitev (68.–69. člena Zakona o preprečevanju pranja denarja in financiranja terorizma) podaje kazenske ovadbe, če pa je morda na kakem področju nima določene, pa jo podaja na podlagi varstva upravičenih interesov (upravljavca ali obdelovalca) – glede javnega sektorja tudi po zadnjem delu določbe drugega odstavka 8. člena ZVOP-2.

Zadnji stavek prvega odstavka določa pravno podlago za razliko od dosedanjega drugega odstavka 9. člena ZVOP-1, tako da lahko ne samo nosilci javnih pooblastil, ampak izrecno celotni javni sektor po definiciji iz 5. člena ZVOP-2 delujejo tudi na podlagi privolitve⁵¹, ki pa mora biti določena v zakonu (npr. narodnost, verska pripadnost – 61. člen ter prvi in drugi odstavek 41. člena Ustave Republike Slovenije).

Predlagani drugi odstavek določa, da se lahko v javnem sektorju tudi obdelujejo osebni podatki, če ne gre za izvrševanje oblastvenih⁵² nalog ali pristojnosti javnega sektorja v smislu odločanja o človekovih pravicah ali temeljnih svoboščinah ali obveznostih, v okviru posameznikove podatkovne samoodločbe, da pač razkrije svoje osebne podatke določenemu krogu ljudi v določenem subjektu javnega prava ozir. le temu subjektu javnega prava. To prostovoljno razkritje, ki običajno ne zahteva podaje (izrecne) privolitve, je podobno določbi d) točke drugega odstavka predlaganega 12. člena ZVOP-2 – prostovoljno razkritje posebne vrste osebnih podatkov. V isti smeri je določeno, da so tej pravni podlagi enakovredni tudi osebni podatki, pridobljeni iz javnega vira ter osebni podatki, pridobljeni na drug zakonit ali običajen način (npr. izmenjava e-poštних naslovov z istega delovnega področja ipd.). Urejena je torej pravna podlaga za npr. zbiranje in obdelavo osebnih podatkov seznamov obiskovalcev državnih proslav, seznam novinarjev z elektronskimi naslovi, seznamov državljanov Republike Slovenije za udeležbo na prireditvah na diplomatsko-konzularnih predstavništvih ali drugih državljanov ali diplomatov za uradne sprejeme, vodenje osebnih imen staršev zaradi vabil na ti. »nadstandardne« šolske aktivnosti – npr. eAsistent. Običajni osebni podatki, ki se bodo zbirali in nadalje obdelovali v skladu z načelom sorazmernosti in glede na okoliščine posamezne situacije ozir. dogodka, so npr.: osebno ime, znanstveni ali strokovni naslov, naslov elektronske pošte, telefonska številka, naslov institucije ali izjemoma naslov domačega prebivališča, morebitna zaposlitev ali funkcija ali članstvo v določenem klubu ipd.). Navedeni osebni podatki se bodo zbirali z običajno prakso – posameznikom bo zlasti dana možnost, da se glede na običajno prakso samo-opredelijo – posredujejo svoje osebne podatke. Zbirke osebnih podatkov, ki nastanejo na tej podlagi pa morajo biti ločene od zbirk osebnih podatkov, ki nastanejo pri izvrševanju zakonitih pristojnosti, nalog ali obveznosti.

⁵¹ Z vidika, da je možno privolitev za obdelavo osebnih podatkov po določbi tretjega odstavka člena 7 Splošne uredbe kadarkoli umakniti, je Zvezno ministrstvo za notranje zadeve Zvezne republike Nemčije v smernicah za izvajanje novega zakona (opr. št. V II 4 - 20108/24#27, 31. 8. 2017) opozorilo: »Prav tako se je treba izogibati pravilom o privolitvi, zlasti v zvezi z javnimi organi, saj se privolitev lahko kadar koli umakne (člen 7 (3) Splošne uredbe) in ker Splošna uredba izrecno navaja, da privolitev ne more biti pravna podlaga, kadar ni bila svobodno podana, kadar je upravljavec [tak] organ (uvodna navedba 43 Splošne uredbe).«

⁵² Za okvirno opredelitev neoblastvenih delovanj glejte smiselno: Sklep Upravnega oddelka Vrhovnega sodišča RS, opr. št. I Up 231/2016, 1. 2. 2017: »11. Delovanje Varuha niti z vidika splošne opredelitve njegovih nalog in pristojnosti niti z vidika ravnanja v konkretnem primeru očitno ne ustreza značilnostim oblastvenega delovanja. Njegovo ravnanje je usmerjeno v nadzor nad delovanjem nosilcev oblasti in se tudi izraža v ukrepih, ki so usmerjeni prav zoper navedene oblastvene subjekte in ne druge osebe, nosilce človekovih pravic in temeljnih svoboščin. Še več, tudi samo delovanje Varuha je tako po zakonski kot po konceptualni opredelitvi neoblastno in le omejeno formalizirano [...]«.«

Predlagana določba torej pomeni neposredno pravno podlago za obdelavo osebnih podatkov v javnem sektorju.

Drugi del določbe drugega odstavka pomeni izvedbo (f) točke prvega odstavka člena 6 Splošne uredbe. Po njej se izjemoma, lahko obdelujejo neposredno na tej pravni podlagi, določeni v zakonu, osebni podatki, kadar je to nujno za izvrševanje drugih nalog javnega sektorja, drugi osebni podatki, ki niso določeni v zakonu – in se z obdelavo ne poseže v upravičen interes posameznika, na katerega se osebni podatki nanašajo, kar vključuje človekove pravice in temeljne svoboščine. Primera sta npr. podaja kazenske ovadbe (kadar tega zakon ne določa kot dolžnost subjekta javnega sektorja) ali pa kontaktiranje posameznika preko telefona za izvedbo določene storitve javnega sektorja. Zbirke, ki nastanejo na tej podlagi, morajo biti ločene od zbirk, ki nastanejo pri izvrševanju zakonskih nalog ali pristojnosti javnega sektorja. Predlagana določba pa ne omogoča niti začasnega omogočanja določanja osebnih podatkov v podzakonskih predpisih (zlasti v pravilnikih), je kvečjemu na njeno izjemnost lahko »sprožilec«, da pristojno ministrstvo po izvedeni začasni konkretni obdelavi osebnih podatkov, pripravi spremembe ali dopolnitve ustreznega zakona, tako da je spoštovano pravilo iz prvega odstavka 8. člena Predloga ZVOP-2 (in drugi odstavek 38. člena Ustave Republike Slovenije v zvezi s 87. členom Ustave Republike Slovenije)⁵³. Gre za nadgradnjo vsebine dosedanjega četrtega odstavka 9. člena ZVOP-1.

Predlagani tretji odstavek določa, da se ne glede na prvi odstavek 8. člena lahko v javnem sektorju obdelujejo tudi osebni podatki posameznika, ki je z javnim sektorjem sklenil pogodbo, ali pa je na podlagi zahteve tega posameznika v fazi pogajanj za sklenitev pogodbe z njim, če je obdelava osebnih podatkov potrebna in primerna za izvajanje ukrepov pred sklenitvijo pogodbe ali za izvajanje pogodbe.

Predlagani četrti odstavek določa, da se ne glede na prvi odstavek tega člena lahko v javnem sektorju izjemoma obdelujejo tisti osebni podatki, ki so potrebni za zaščito življenjskih interesov posameznika, na katerega se nanašajo osebni podatki, ali druge fizične osebe. Poudarek je na besedi »izjemoma«, življenjski interesi posameznika pa so nekoliko širši od samo varovanja življenja in telesa – primerljivo določbam 43. člena Zakona o nalogah in pooblastilih policije o iskanju oseb in delno primerljivo tudi določbam 153. člena Zakona o elektronskih komunikacijah, vendar tudi širše, saj gre lahko tudi za dajanje pravne pomoči neuki stranki, preprečevanje nastanka hujše škode (npr. nujna medsosedska pomoč, kolikor pride v poštev v javnem sektorju) ipd..

Predlagani peti odstavek določa obdelavo osebnih podatkov v druge namene⁵⁴ kot pravilo za delovanje (odločanje) javnega sektorja glede možnosti obdelav osebnih podatkov v druge namene po četrtem odstavku člena 6 Splošne uredbe. Po predlagani določbi 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 izvrševanja ciljev iz prvega odstavka člena 23 Splošne uredbe in pod pogoji iz prvega odstavka 8. člena določa drug področni zakon. Primeri so npr. zlasti arhiviranje po področni zakonodaji, znanstveno raziskovanje, statistično raziskovanje.

Predlagani šesti odstavek določa posebno pravilo glede uporabe privolitve v druge namene za potrebe javnega sektorja. Določeno je, da je obdelava osebnih podatkov v javnem sektorju za drug namen kot za tistega, za katerega so bili zbrani, prepovedana (ni dopustna) na podlagi prvotne privolitve, če je bila ta privolitev podana za določen namen, ki sicer lahko vsebuje eno ali več delovanj obdelave v skladu z **določenim namenom**. Če je načrtovana obdelava osebnih podatkov za drug (nov) namen na podlagi privolitve, se lahko izvede le na podlagi nove privolitve posameznika, na

⁵³ Glejte ustaljeno ustavnosodno presojo Ustavnega sodišča Republike Slovenije o nedopustnosti določanja osebnih podatkov, namenov obdelave ipd. v podzakonskih predpisih: Odločba US, št. U-I-115/92, 24. 12. 1992; objava: OdlUS I, 105 in Uradni list RS, št. 3/93; Odločba US, št. U-I-229/03, 9. 2. 2006; objava: OdlUS XV, 13 in Uradni list RS, št. 21/06; Odločba US, št. U-I-245/05, 7. 2. 2007; objava: Uradni list RS, št. 15/07; delno tudi Odločba US, št. U-I-463/06, 18. 1. 2007; objava: Uradni list RS, št. 8/07.

⁵⁴ Glede določb Splošne uredbe o obdelavi v druge namene ter glede povezanih pravnih nejasnosti glejte: Voigt, Paul, von dem Bussche, Axel, *The EU General Data Protection Regulation (GDPR) : A Practical Guide*, Springer International Publishing AG, Cham, 2017, str. 108-110, razdelek 4.2.2.5. Sprememba namena obdelave osebnih podatkov.

katerega se nanašajo osebni podatki, če druga zakonska podlaga izrecno (glede na načelo zakonitosti iz drugega odstavka 38. in 87. člena Ustave Republike Slovenije) ne določa drugače. To dodatno pravilo izhaja iz besedila Predloga Smernic glede privolitve po Uredbi 2016/679⁵⁵ z dne 28. 11. 2017, ki jih je pripravila Delovna skupina po členu 29 Direktive 95/46/ES (združenje evropskih nadzornih organov za varstvo osebnih podatkov Evropske unije). Gre za dodatno (originarno) razlago po kateri privolitev velja le za en namen, ki ima sicer lahko različne opcije obdelave – če so za isti namen, ni pa možna obdelava v druge namene – in nato je za obdelavo v drug namen potrebno pridobiti dodatno privolitev – skladno s členom 6, četrtem odstavkom Splošne uredbe ter členom 5, (b) točko prvega odstavka iste uredbe ter glede na uvodno navedbo št. 32 uredbe.

K 9. členu:

Predlagani 9. člen najprej določa pravne podlage za obdelavo osebnih podatkov v zasebnem sektorju in pri temu precej sledi smerem iz dosedanjega 10. člena ZVOP-1. Ob tem v petem odstavku določa tudi sistemsko pravilo glede obdelave v druge namene v zasebnem sektorju.

Prvi odstavek določa, da se osebni podatki v zasebnem sektorju 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 in vrste osebnih podatkov, ki se obdelujejo, kategorije posameznikov, na katere se nanašajo osebni podatki in rok hrambe. Zakon pa lahko, če je to potrebno, določi tudi morebitne druge ukrepe za zagotovitev zakonite, poštene in pregledne obdelave, omejitve namena in uporabnike in druge upravljavce osebnih podatkov, ki se jim osebni podatki lahko razkrijejo. Z zakonom se lahko določi, da se določeni osebni podatki za enega ali več določenih namenov obdelujejo le na podlagi privolitve posameznika. Bistvo glede prvega odstavka je seveda pravna podlaga privolitve, zakonska ureditev pride v poštev, kadar to zaradi varovanja javnega interesa (npr. tudi regulacija poklica, sporočanje kršitev zakona) predpiše zakonodajalec (npr. po c) točki prvega odstavka člena 6 Splošne uredbe).

Predlagani drugi odstavek določa, da se ne glede na prvi odstavek lahko v zasebnem sektorju obdelujejo osebni podatki posameznika, ki je z zasebnim sektorjem sklenil pogodbo, ali pa je na podlagi zahteve tega posameznika v fazi pogajanj za sklenitev pogodbe z njim, če je obdelava osebnih podatkov potrebna in primerna za izvajanje ukrepov pred sklenitvijo pogodbe ali za izvajanje pogodbe.

Predlagani tretji odstavek določa, da se ne glede na prvi odstavek 9. člena ZVOP-2 lahko v zasebnem sektorju obdelujejo tisti osebni podatki, ki so potrebni za zaščito življenjskih interesov posameznika, na katerega se nanašajo osebni podatki, ali druge fizične osebe – podobno kot v četrtem odstavku 8. člena ZVOP-2. Na ta način je podana paralelna obveznost, da je upravljavec ali obdelovalec v zasebnem sektorju dolžan posredovati osebne podatke za izvrševanje pristojnosti javnega sektorja po četrtem odstavku 8. člena ZVOP-2.

Predlagani četrti odstavek določa, da se ne glede na prvi odstavek tega člena lahko v zasebnem sektorju obdelujejo osebni podatki, če je obdelava potrebna zaradi uresničevanja zakonitih upravičenih interesov, 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, zlasti kadar je posameznik, na katerega se nanašajo osebni podatki, otrok. Npr. zasebni sektor lahko obdelava na tej podlagi osebne podatke, ki jih zakonito ima, za potrebe pravnega postopka, ne gre pa za obdelavo osebnih podatkov za namene neposrednega trženja, saj je to posebno (področno) urejeno v poglavju tega zakona.

Predlagani peti odstavek določa obdelavo v druge namene v zasebnem sektorju. Določeno je, da je obdelava osebnih podatkov za druge namene kot tiste, za katere so bili osebni podatki prvotno zbrani,

⁵⁵ »Guidelines on Consent under Regulation 2016/679«, 17/EN, WP259, Adopted on 28 November 2017, str. 12.

v zasebnem sektorju dovoljena le, kadar je združljiva z nameni, za katere so bili osebni podatki prvotno zbrani. Za ugotovitev, ali je namen nadaljnje obdelave združljiv z namenom, za katerega so bili osebni podatki prvotno zbrani, mora upravljavec, potem ko je izpolnil vse zahteve glede zakonitosti prvotne obdelave, opraviti presojo v skladu s četrnim odstavkom člena 6 Splošne uredbe. Presoja mora biti opravljena pred začetkom obdelave za druge namene, v pisni obliki, in je sestavni del dokumentacije po drugem odstavku člena 5 Splošne uredbe.

Predlagani šesti odstavek tudi določa dodatno pravilo glede uporabe privolitve v druge namene za potrebe zasebnega sektorja. Določeno je, da je obdelava osebnih podatkov v zasebnem sektorju za drug namen kot za tistega, za katerega so bili zbrani - prepovedana (ni dopustna) na podlagi prvotne privolitve, če je bila ta privolitev podana za določen namen, ki lahko vsebuje eno ali več delovanj obdelave v skladu z določenim namenom. Če je načrtovana obdelava za drug (torej nov) namen na podlagi privolitve, se lahko izvede le na podlagi nove privolitve posameznika, na katerega se nanašajo osebni podatki, če druga zakonska podlaga ne določa drugače. Enako kot pri sedmem odstavku 8. člena ZVOP-2 to dodatno pravilo izhaja iz Predloga Smernic glede privolitve po Uredbi 2016/679 z dne 28. 11. 2017, ki jih je pripravila Delovna skupina po členu 29 Direktive 95/46/ES. Gre za dodatno (originarno) razlago po kateri privolitev velja le za en namen⁵⁶, ki ima sicer lahko različne opcije obdelave – če so za isti namen, ni pa možna obdelava v druge namene – in nato je za obdelavo v drug namen potrebno pridobiti dodatno privolitev – skladno s členom 6, četrnim odstavkom Splošne uredbe ter členom 5, (b) točko prvega odstavka iste uredbe ter glede na uvodno navedbo št. 32 uredbe⁵⁷.

K 10. členu:

V 10. členu je predlagana posebna ureditev glede varstva osebnih podatkov umrlih posameznikov, na katere so se nanašali v preteklosti zbrani in obdelani osebni podatki. Gre že za tradicionalno slovensko ureditev (glejte veljavni 23. člen ZVOP-1) z vidika zadržanja dosedanje višje stopnje varstva osebnih podatkov. Podobna ureditev obstaja ali pa bo prenovljena vsaj v Avstriji in v Estoniji. Predlagana ureditev torej predstavlja zadržanje dosedanje ureditve, vendar z nekoliko posodobljena vsebino – tudi ob upoštevanju dejstva, da Splošna uredba določa, da ne posega v tovrstne nacionalne ureditve obdelave osebnih podatkov umrlih oseb (uvodna navedba št. 27 Splošne uredbe).

Predlagani prvi odstavek določa, da se osebni podatki umrlih posameznikov varujejo po tem zakonu in drugih zakonih (npr. Obligacijski zakonik, Zakon o varstvu dokumentarnega in arhivskega gradiva ter arhivih).

Predlagani drugi odstavek določa, da upravljavec podatke o umrlem posamezniku posreduje le tistim uporabnikom, ki so za obdelavo osebnih podatkov pooblaščen z zakonom (s področja javnega ali zasebnega sektorja) in tistim osebam, ki izkažejo pravni interes za uveljavljanje pravic pred osebami javnega sektorja.

Predlagani tretji odstavek določa, da ne glede na določbe drugega odstavka 10. člena ZVOP-2 upravljavec osebne podatke o umrlem posamezniku posreduje zakoncu, zunajzakonskemu partnerju ali partnerju iz partnerske zveze (izenačen s prej navedenimi), otrokom ali staršem ali drugim osebam, če izkažejo pravni interes. Upoštevano je z vidika interesov pietete bližnjih, da imajo dostop do teh podatkov.

⁵⁶ S tega vidika je morda relevantna tudi določba tretjega odstavka člena 7 Splošne uredbe, po kateri lahko posameznik uvede umik privolitve kadarkoli – glejte: Voigt, Paul, von dem Bussche, Axel, *The EU General Data Protection Regulation (GDPR) : A Practical Guide*, Springer International Publishing AG, Cham, 2017, str. 97, razdelek 4.2.1.5. Umik.

⁵⁷ Za nasprotno stališče glejte sodbo Sodišča EU v primeru *Tele2 (Netherlands) BV, Ziggo BV, Vodafone Libertel BV proti Autoriteit Consument en Markt (ACM)*, C 536/15; 15. 3. 2017 - o nepotrebnosti dajanja nove privolitve za objavo naročniških podatkov v drugem imeniku, predstavljeno v: Skubic, Zoran, *Čezmejna objava osebnih podatkov telefonskih naročnikov po pravu EU*, Pravna praksa, št. 23/2017, str. 32-33.

Predlagani četrti odstavek določa, da če drug zakon ne določa drugače, lahko upravljavec podatke o umrlem posamezniku posreduje tudi katerikoli drugi osebi, ki namerava te podatke uporabljati za zgodovinske raziskovalne, znanstvene raziskovalne, statistične ali arhivske namene pod pogoji iz 79. do 81. člena tega zakona.

Predlagani peti odstavek je neposredna pravna podlaga (upravičenje) za izjemno objavo podatkov umrlih v knjigah, učbenikih, enciklopedijah itd, se pa ne nanaša na klasične članke v medijih (za te primere načeloma velja svoboda izražanja po 79. členu predloga zakona).

K 11. členu:

Predlagani 11. člen določa v skladu s členom 8 Splošne uredbe (po vzorcu iz Zakona o zasebnosti otrok na spletu Združenih držav Amerike – (*Children's Online Privacy Protection Act - COPPA*) iz leta 1998) pogoje za obdelavo osebnih podatkov otrok v primeru uporabe storitev informacijske družbe (opredelitev storitev informacijske družbe je vsebovana v 25. točki prvega odstavka 6. člena Predloga ZVOP-2). Storitve informacijske družbe so opredeljene v 25. točki prvega odstavka 6. člena ZVOP-2, otrok pa je v tem primeru v skladu z odprtimi določbami Splošne uredbe naveden kot mladoletna oseba, ki je stara 15 let ali več. Kar tudi pomeni (glede na predlagani prvi odstavek 11. člena), da veljajo strogi pogoji v zvezi s privolitvijo po tem členu le za otroke, ki še niso stari 15 let. Starost 15 let je izbrana (določena) glede na sistemsko vodilo iz prvega odstavka 146. člena Družinskega zakonika⁵⁸: »Otrok, ki dopolni 15 let, lahko sam sklepa pravne posle, če zakon ne določa drugače.«.

Nadalje prvi odstavek določa, da gre za vprašanje urejanja privolitve mladoletne osebe za uporabo storitev informacijske družbe, ki se jih ponuja neposredno mladoletnim osebam oziroma za katere se lahko verjetno domneva, da jih bodo uporabljale mladoletne osebe – torej upravljavcu daje obveznost preverjanja in vzpostavljanja informacijskih sistemov, ki naj bi preprečili, da bi privolitev lahko podala mladoletna oseba, ki še ni stara 15 let. V primeru, če je mladoletna oseba mlajša od 15 let, je privolitev veljavna le, če jo poda ali odobri eden od staršev mladoletne osebe oziroma njen rejnik ali skrbnik.

Po predlaganem drugem odstavku je upravljavec dolžan ves čas nudenja storitve ob upoštevanju razpoložljive tehnologije v primerih iz drugega stavka prejšnjega odstavka izvajati dolžan izvajati razumna prizadevanja, s katerimi preveri, ali je starš, rejnik ali skrbnik za otroka mladoletno osebo podal ali odobril privolitev ter ali privolitev še velja (dokler imajo te osebe v razmerju do mladoletne osebe še ta status). Razumna prizadevanja so lahko različna, zakonska določba z uporabo besede »zlasti« (torej enumerativni - odprti pristop) omenja možnost kontaktiranja staršev, rejnikov ali skrbnikov.

Po predlaganem tretjem odstavku privolitev mladoletne osebe iz prvega odstavka 11. člena ZVOP-2 (ki je torej stara 15 let ali več) ne sme biti pogojevana s pretiranimi pogoji s strani upravljavca, zlasti da bi bila omogočena udeležba mladoletnih oseb v igri, ponujanje nagrade, vključitve v družbeno omrežje ali druge podobne dejavnosti, tako da bi mladoletna oseba morala posredovati več osebnih podatkov (kršitev načela sorazmernosti), kot je potrebno za namen opravljanje takšne dejavnosti. Prepoved velja tudi v primerih iz drugega stavka prvega odstavka 11. člena ZVOP-2.

Predlagani člen izhaja (enako tudi določbe člena 8 Splošne uredbe) iz COPPA, ki nima podrobnejših kriterijev, kaj se šteje za razumna prizadevanja, razen da gre (vsaj posredno) za kontaktiranje staršev ob uporabi razpoložljive tehnologije (SEC. 1302., deveti odstavek). Navedeni zakon sicer načeloma v praksi ni znan kot učinkovit zakon.

K 12. členu:

V 12. (dejansko pa tudi v povezanem 13.) členu se urejajo obdelave posebnih vrst osebnih podatkov (dosedaj: občutljivi osebni podatki).

⁵⁸ Uradni list RS, št. 15/17.

V predlaganem prvem odstavku je najprej podana stroga (tradicionalna) prepoved obdelave posebnih vrst osebnih podatkov, sedaj glede na prvi odstavek člena 9 Splošne uredbe ter smiselno (po zapisu drugače, rezultat pa je vsebinsko enak) iz člena 10 Direktive ter glede na še nespremenjeni 6. člen Konvencije o varstvu posameznikov glede na avtomatsko obdelavo podatkov (Sveta Evrope). Določeno je, da so posebne vrste osebnih podatkov naslednje: osebni podatki o rasnem ali etničnem poreklu, političnem mnenju, verskem ali filozofskem prepričanju ali članstvu v sindikatu, genski podatki, biometrijski podatki za namene edinstvene identifikacije posameznika, podatki v zvezi z zdravjem ali podatki v zvezi s posameznikovim spolnim življenjem ali spolno usmerjenostjo.

Drugi odstavek, podobno kot dosednji 13. člen ZVOP-1, določa pravne podlage za obdelavo posebnih vrst osebnih podatkov, z določenimi podrobnejšimi določbami. Tako je npr. določeno, da se posebne vrste osebnih podatkov lahko obdelujejo tudi, če je to potrebno zaradi uveljavljanja ali izvajanja pravnih zahtevkov ali obrambo pred njimi – vendar v okviru zakonsko določenih uradnih postopkov – torej, upravni postopki, sodni postopki, nadzorni postopki ipd., ki morajo biti urejeni z zakonom. V h) točki pa je razdelana tudi še dodatna omejitev, ki je usmerjena na področne zakone, namreč z vidika sorazmernosti je določeno, da lahko obdelavo posebnih vrst osebnih podatkov določi drug zakon zaradi izvrševanja bistvenega javnega interesa, kar mora biti sorazmerno z zastavljenim ciljem, spoštovati bistvo pravice do varstva podatkov ter zagotavljati ustrezne in posebne ukrepe za varstvo človekovih pravic in temeljnih svoboščin ali interesov posameznika, na katerega se nanašajo osebni podatki.

V tretjem odstavku je določeno, da je treba v primerih obdelav posebnih vrst osebnih podatkov po drugem odstavku poleg ukrepov iz 29. člena ZVOP-2 določiti in vzpostaviti in pisno opredeliti še primerne in posebne zaščitne ukrepe za varstvo pravic, svoboščin ali interesov posameznika, na katerega se nanašajo osebni podatki. Ob upoštevanju tehnološkega razvoja, stroškov izvajanja ter vrste, obsega, okoliščin in namenov obdelave ter različnih stopenj verjetnosti pojava tveganj, povezanih z obdelavo, za človekove pravice in temeljne svoboščine in interese posameznikov ter njihove resnosti, so ti zaščitni ukrepi najmanj tisti, ki so urejeni v točkah tretjega odstavka. Po točki a) so to politike, postopki in ukrepi za varnost osebnih podatkov (nekdanje zavarovanje osebnih podatkov), ki zagotavljajo, da obdelava poteka skladno z zahtevami iz 29. člena ZVOP-2. Za posebne vrste osebnih podatkov bodo torej veljala splošna pravila, za ti. navadne osebne podatke pa po 29. členu ter dodatni ukrepi varnosti osebnih podatkov po tem členu. V b) točki je naveden ukrep ozaveščanja oseb, udeleženih v postopkih obdelave, o varnostnih politikah, postopkih in ukrepih za zagotavljanje varnosti osebnih podatkov. V c) točki je za področje zagotavljanja elektronskih storitev javnega sektorja, ki vključujejo obdelavo posebnih vrst osebnih podatkov, določen ukrep, da je za dostop do teh storitev potrebno zagotoviti takšna sredstva elektronske identifikacije, kjer se ob izdaji zahteva osebno navzočnost posameznika in se njegovo identiteto preveri z vpogledom v uradni osebni dokument posameznika. V č) točki je določeno, da je treba pri prenosu posebnih vrst osebnih podatkov preko elektronskih omrežij te podatke šifrirati tako, da je zagotovljena njihova neprepoznavnost med prenosom in da so kontaktni podatki naslovnika predhodno preverjeni s potrditvenim sporočilom, s katerim naslovnik potrdi pravilnost podatkov za dostavo. Elektronski podpis ni več zahtevan, ker dejansko niti ne zagotavlja nečitljivosti podatkov.

Možni primer: pošiljanje izvidov pacientom po e-pošti.

V d) točki je določen ukrep ustreznega upravljanja uporabniških pooblastil pri upravljavcih in obdelovalcih, v e) točki pa – da, kjer je to ustrezno, tudi psevdonimizacija oziroma šifriranje osebnih podatkov.

Glede posebnega vidika glede podatkov o narodni pripadnosti - statistični namen zbiranja teh osebnih podatkov:

Republika Slovenija ima že ustavnopravno dokaj strogo pozicijo glede izražanja narodne pripadnosti – namreč v 61. členu Ustave Republike Slovenije, po katerem se narodno pripadnost izraža svobodno. Glede na navedeni člen Ustave mora biti vsak poseg v smer pridobivanja osebnega podatka o narodni pripadnosti razumno utemeljen, mora spoštovati svobodo človeka in biti v skladu s temeljnim ustavnim

načelom sorazmernosti (2. člen v zvezi s tretjim odstavkom 15. člena Ustave Republike Slovenije) – spoštovano mora biti torej strogo načelo sorazmernosti. Torej zbiranja in obdelave osebnih podatkov ni možno opravičiti s potrebami statističnega poročanja ali raziskovanja (izjema so glede na posebne varovalke lahko popisi prebivalstva – npr. Popis prebivalstva, gospodinjstev in stanovanj v Republiki Sloveniji leta 2002), če ni opravičen (utemeljen) že primarni namen za zbiranje podatka o narodni in etnični pripadnosti za potrebe določenega postopka ali odločanja (npr. prosilci za mednarodno zaščito – preganjanje zaradi narodne pripadnosti⁵⁹). Prav tako, če se odmisli prej navedeni primarni namen zbiranja (za potrebe postopka ozir. odločanja), bi bilo zbiranje in obdelava podatkov o pripadnosti na podlagi osebne privolitve načeloma nesmiselno, saj nikoli ne bi dovolj ljudi dalo privolitev za to, da bi vzorec dejansko bil reprezentativen, niti njihove dejanske pripadnosti ne bi bilo dopustno preverjati (svobodno opredeljevanje iz 61., člena Ustave) in lahko kaj pomenil z vidika ocene delovanj ali odločanj o ljudeh v raznih uradnih (zakonsko določenih) postopkih.

Seveda pa pravni red Republike Slovenije ne preprečuje, da nevladne organizacije ali raziskovalne organizacije ne raziskujejo same, na podlagi uporabe arhivskega gradiva, kakšna so določena razmerja/vpliv glede narodne pripadnosti v zvezi z uradnimi postopki, storitvami ipd. v Sloveniji.

K 13. členu:

V predlaganem 13. členu je določena dodatna vrsta posebne vrste osebnih podatkov, namreč podatkov o kazenskih obsodbah in kaznovanjih za prekrške – glede na člen 10 Splošne uredbe ter glede na uvodni navedbi št. 75 in 80, ki v zvezi s konceptom kazenske obtožbe iz prvega odstavka 6. člena Evropske konvencije omenja poleg kaznivih dejanj tudi prekrške (kar je del skupnega koncepta kaznivih ravnanj). V prvem odstavku je tako določeno, da za podatke o vpisu ali izbrisu v ali iz kazenske evidence ali evidenc, ki se upravljajo na podlagi Zakona o prekrških ter za prenose teh osebnih podatkov velja, da gre za osebne podatke, ki morajo biti varovani kot posebne vrste osebnih podatkov po drugem in tretjem odstavku 12. člena ZVOP-2.

Drugi odstavek najprej v prvem stavku določa, da za obdelave določenih (vrst) osebnih podatkov iz kazenskih evidenc ter njihove zakonsko določene namene obdelave, roke hrambe ter prenose osebnih podatkov javnemu ali zasebnemu sektorju iz teh evidenc veljajo pravila iz 250.a člena Zakona o izvrševanju kazenskih sankcij, 135. člena Zakona o kazenskem postopku ter 84. člena Kazenskega zakonika. Prav tako določa, da za obdelave določenih (kategorij) osebnih podatkov iz prekrškovnih evidenc po Zakonu o prekrških veljajo primerljiva pravila iz Zakona o prekrških glede zakonsko določenih namenov obdelave, rokov hrambe ter prenosov javnemu ali zasebnemu sektorju. Zaključno je za obe vrsti evidenc tudi določeno, da za prenose teh osebnih podatkov iz navedenih evidenc organom drugih držav ali mednarodnim organizacijam (za zakonsko določene namene) veljajo tudi pravila po drugih zakonskih podlagah. Glede na to, da je torej sistemska pravna ureditev glede osebnih podatkov o kazenskih obsodbah in kaznovanjih za prekrške dejansko izenačena s posebnimi vrstami osebnih podatkov, ostane v veljavi dosedanja višja raven njihovega varstva, vključno z omejitvami dostopa do njih, tudi po dosedanji praksi Informacijskega pooblaščenca⁶⁰.

Predlagani tretji in četrti odstavek določata, da se kazenske evidence in prekrškovne evidence lahko povezujejo s Centralnim registrom prebivalstva tako, da se zagotovi točnost in posodobljenost osebnih podatkov v kazenskih ali prekrškovnih evidencah ter da se povezovanje izvede tako, da je možno samodejno posodabljanje podatkov v evidencah oziroma na način, da povezovanje omogoča vsaj, da se v evidencah pri osebnih podatkih določenega ali določljivega posameznika pojavi samodejno opozorilo, da je pri njegovih podatkih v drugi zbirki osebnih podatkov prišlo do spremembe. V petem

⁵⁹ Podoben pristop ima tudi Francoska republika – ni zbiranja podatkov o narodni ali etnični pripadnosti, niti na podlagi privolitve, izjema so mednarodne migracije, če je to vprašanje bistveno glede odločanja v zadevi (razlog preganjanja prosilca za mednarodno zaščito).

⁶⁰ Glede na določbe Zakona o dostopu o informacijah javnega značaja in praksi Informacijskega pooblaščenca ti osebni podatki niso dostopni javnosti: odločba IP, št. 021-65/2008/4, 30. 6. 2008 in odločba IP, št. 090-111/2010/2, 5. 8. 2010.

odstavku je glede povezovanja zaključno določeno, da se za državljane Republike Slovenije ali osebe s prebivališčem v Republiki Sloveniji kot identifikacijska znaka uporabita osebno ime in njihova enotna matična številka, za tujca pa njegovo osebno ime in njegova enotna matična številka ali drug ustrezen identifikacijski znak iz kazenske evidence.

2. K II. delu Predloga ZVOP-2:

K 14. členu:

Splošna uredba določa okrepljeno odgovornost upravljavca za zagotavljanje informacij oziroma pravic posameznikom, katerih osebne podatke obdeluje. Navedeno temelji na premisi, da lahko le dobro informiran posameznik ustrezno zavaruje svoj pravice skozi postopke pred upravljavcem, Informacijskim pooblaščencom oziroma pred sodišči.

Člen v tem smislu najprej določa obveznost upravljavca, da vzpostavi ustrezne ukrepe in postopke za obveščanje posameznikov o obdelavi njegovih podatkov. Vsebina informacij, ki jih mora zagotoviti, ter roki, do kdaj jih mora zagotoviti, so določeni v členih 13 in 14 oziroma 34 Splošne uredbe. Način obveščanja je prepuščen upravljavcu in bo odvisen predvsem od načina, kako upravljavec stopa v stik s posamezniku. V primeru zbiranje podatkov neposredno od posameznikov bo to npr. mogoče uresničiti s predložitvijo ali omogočanjem vpogleda v pravilnik o varnosti osebnih podatkov.

Člen prav tako določa obveznost upravljavca, da vzpostavi ustrezne ukrepe in postopke za sprejem, obravnavo in odgovarjanja na zahteve posameznikov po členih 15 do 22 Splošne uredbe. Upravljavec mora ustrezno določiti in usposobiti osebje, ki bo opravljalo te naloge, ter določiti postopke za njihovo delo. V kolikor ima upravljavec imenovano pooblaščenca osebo za varstvo osebnih podatkov, lahko te naloge opravlja ta oseba.

Končno člen določa še, da mora upravljavec sprejeti ustrezne ukrepe, da posamezniku olajša uveljavljanje njegovih pravic. Navedeno še zlasti pomeni, da posamezniku posreduje ustrezna navodila ter obrazce za uveljavljanje zahtev. Pri tem pa mora upoštevati, da lahko posameznik, če želi, svojo zahtevo še vedno odda brez uporabe obrazca.

K 15. členu:

Navedeni ter sledeči členu po vzoru obstoječe ureditve iz 30. in sledečih členov ZVOP-1 urejajo postopek vložitve, obravnave ter odločitve o zahtevah posameznika. Pri tem smiselno izhaja iz ureditve obravnave vlog v Zakonu o splošnem upravnem postopku, seveda z ustreznimi prilagoditvami, ki upoštevajo, da številni upravljavci niso upravni organi oziroma zavezanci po navedenem zakonu.

Člen tako določa način vložitve zahteve (pisno ali ustno na zapisnik) ter dolžnost upravljavca, da pisno potrdi prejem zahteve.

K 16. členu:

Člen določa obvezne vsebine zahteve, kar so poleg same vsebine zahteve (za katero pravico gre, ter na katere osebne podatke se nanaša) še zlasti podatki, ki bodo upravljavcu potrebni, da enolično določi posameznika v svojih zbirkah. V kolikor zahteva ne vsebuje vseh teh elementov, mora upravljavec (v luči obveznosti olajšanja uveljavljanja pravic posamezniku omogočiti, da jo dopolni. Šele, če je posameznik tudi na poziv ne dopolni, lahko upravljavec zahtevo zavrže.

Člen določa tudi, da mora biti zahteva sestavljena tako, da lahko upravljavec potrdi identiteto posameznika. Navedeno lahko upravljavec stori na različne načine; od tega, da zahteva prejem zahteve z e-poštnega naslova, ki je že tako vezan na uporabnikov račun, do tega, da zahteva vložitve

K 17. členu:

Člen v skladu z okvirjem iz Splošne uredbe posamezniku prepoveduje pretirano ali šikanozno vlaganje zahtev, torej vlaganje zahtev, katerih edini ali prevladujoči cilj je povzročati stroške upravljavcu oziroma onemogočati njegovo siceršnje poslovanje, ne pa zagotoviti spoštovanje posameznikovih temeljnih pravic in svoboščin. V tem smislu so po vzoru obstoječe ureditve določene časovne omejitve vlaganja zahtevkov, ki so praviloma 1x na tri mesece, v utemeljenih primerih pa lahko tudi pogostejše. V kolikor posameznik krši te omejitve, lahko upravljavec zahtevo že na tej podlagi zavrže (tj. zavrne brez vsebinske obravnave).

Člen prav tako določa, da za uveljavljanje pravic na medicinski dokumentaciji veljajo specialne določbe zakona, ki ureja pravice pacientov.

K 18. členu:

Člen določa, da mora upravljavec odgovor zagotoviti brez nepotrebnega odlašanja, vendar v vsakem primeru v enem mestu po prejemu zahteve, razen če si v skladu s pravili Splošne uredbe izgovori podaljšanje tega roka. Kršitve teh rokov imajo za posledico, da se šteje, da je zahteva zavrnjena.

Navedeno ne pomeni, da lahko upravljavec izvajanje vseh pravic vedno zadrži do preteka meseca dni od prejema popolne zahteve. Takšno postopanje se šteje kot kršitev Splošne uredbe oziroma tega zakona in predstavlja osnovo za prekrškovno odgovornost upravjavca.

K 19. členu:

Upravljavci iz javnega sektorja morajo o zahtevi, kot že zgoraj v tretjem odstavku 15. člena, odločiti z upravno odločbo. Upravljavec iz zasebnega sektorja lahko odloči s pisnim dopisom, ki ga posamezniku vroči na način, kot ga je ta zahteval oziroma kot je glede na vse okoliščine primerno.

K 20. členu:

V 20. členu je določen ugovor v primeru nepopolne odločitve upravjavca glede posredovanja osebnih podatkov. Predlagano je, da če posameznik po prejeti odločitvi upravjavca meni, da osebni podatki, ki jih je prejel, niso osebni podatki, ki jih je zahteval, ali da ni prejel vseh zahtevanih osebnih podatkov, lahko pred vložitvijo pritožbe pri upravljavcu vloži obrazložen ugovor v roku 15 dni. Upravljavec mora o ugovoru odločiti kot o novi zahtevi v 5 delovnih dneh.

K 21. členu:

V 21. členu je določeno, da če upravljavec ne odloči o zahtevi posameznika v roku iz 19. člena ZVOP-2, lahko posameznik pri Informacijskem pooblaščenca vloži pritožbo zaradi molka. Če upravljavec zahtevo zavrne, lahko posameznik pri upravljavcu, če gre za javni sektor oziroma pri Informacijskem pooblaščenca, če gre za zasebni sektor vloži obrazloženo pritožbo v roku 15 dni od prejema obvestila ali odločbe upravjavca. Po drugem odstavku pravica strank do pregledovanja dokumentov v zadevah odločanja o posameznikovi pritožbi po določbah Zakona o splošnem upravnem postopku, do pravnomočnosti odločbe Informacijskega pooblaščenca - ne more vključevati pregledovanja upravne zadeve v delu, ki se nanaša na dokumente, ki so predmet zahteve in drugih dokumentov zadeve, iz katerih bi se dalo razbrati ali sklepati na vsebino zahtevanih osebnih podatkov. Smiselno enaka omejitev glede omejitev pravic do pregledovanja upravne zadeve velja tudi pri odločanju o zahtevi pri upravljavcu.

K 22. členu:

V 22. členu je določen postopek obravnavanja pritožbe, da namreč odloča Informacijski pooblaščenec ter kaj so dodatni možni pritožbeni razlogi.

K 23. členu:

V 23. členu so določena pooblastila Informacijskega pooblaščenca v pritožbenem postopku, konkretno glede državnih nadzornikov za varstvo osebnih podatkov, tako glede uporabe pooblastil iz Splošne uredbe, Zakona o inšpekcijskem nadzoru, dostopa do dokumentacije ipd. V šestem odstavku je določen možen ekonomičen pristop obravnavanja pritožb, za primere, ko tako narekuje učinkovitost postopka, lahko Informacijski pooblaščenec o pritožbi odloči z odločbo s skrajšano obrazložitvijo, v kateri poleg izreka navede le pravno podlago in temeljni razlog odločitve ter pravni pouk. Če po prejemu odločbe s skrajšano obrazložitvijo prosilec, organ ali stranski udeleženec najkasneje v 8 dneh neobvezujoče napove upravni spor zoper odločitev Informacijskega pooblaščenca, ta izda odločbo s polno obrazložitvijo v 15 dneh, s katero tudi razveljavi odločbo s skrajšano obrazložitvijo.

K 24. členu:

V 24. členu so določene izjeme glede uveljavljanja pravic posameznika preko zakonitega zastopnika na področju zdravstvene dokumentacije. Omejitve so dopustne glede na določbe tretjega odstavka 38. člena Ustave Republike Slovenije⁶¹.

K 25. členu:

25. člen določa, da je za izvedbe upravne izvršbe v zvezi z odločbami, izdanimi v postopku v pritožbenem postopku je pristojen Informacijski pooblaščenec. Po drugem odstavku se upravna izvršba opravi na predlog posameznika na podlagi izvršljive odločbe in sklepa o dovolitvi izvršbe, in sicer s prisilitvijo zoper upravljavca. Po tretjem odstavku zoper sklep o dovolitvi izvršbe ni pritožbe, dovoljen pa je upravni spor.

K 26. členu:

Bistvo 26. člena o zaračunavanju stroškov je, da se po prvem odstavku informacije in sporočila ter ukrepi iz II. dela zakona zagotavljajo brezplačno (kot to zahteva prvi stavek tretjega odstavka člena 15 Splošne uredbe). Po drugem odstavku pa so določene izjeme, da se v določenih primerih očitno neutemeljenih zahtev ali njihove pretiranosti lahko zaračunajo razumne pristojbine, pri čemer se upoštevajo administrativni stroški posredovanja informacij ali sporočila oziroma izvajanja zahtevanega ukrepa po tem delu zakona (npr. če se zahteva nanaša na posredovanje istih osebnih podatkov npr. trikrat v enem letu). V primerih, ko se izdaja kopija, ki ne vsebuje samo lastnih osebnih podatkov posameznika, ampak tudi osebne podatke drugih posameznikov (npr. posnetek videonadzora, ki ga je treba anonimizirati pred posredovanjem posamezniku, ker so na njemu tudi drugi posamezniki), ne gre več za (začetno) kopijo, ampak za dodatno kopijo, kjer je možno zaračunavanje.

Naslednji odstavki določajo, da izda pravilnik o zaračunavanju stroškov neodvisni in samostojni državni organ (Informacijski pooblaščenec), po predhodnem soglasju pristojnih ministrov (pravilnik je omenjen glede pritožbe tudi v 22. členu). Področje višine stroškov na področju seznanitve z lastno zdravstveno dokumentacijo in dokumentacijo umrlih pacientov ter povezana pravila o zaračunavanju bodo predpisana v istem pravilniku, jih je pa treba zaradi pravne varnosti in različnih pristojnosti ministrstev posebej omeniti glede na področno ureditev, namreč glede na četrty odstavek 41. člena Zakona o pacientovih pravicah⁶².

K 27. členu:

Predlagani 27. člen ZVOP-2 določa omejitve pravic posameznikov. Po prvem odstavku se pravice posameznika iz tega dela zakona je mogoče z zakonom izjemoma omejiti iz razlogov navedenih v

⁶¹ Glejte: odločba US, št. U-I 60/03, 4. 12. 2003, zlasti 30. točka; objava: Uradni list RS, št. 131/03 in OdlUS XII, 93.

⁶² Uradni list RS, št. 15/08 in 55/17.

prvem odstavku členu 23 Splošne uredbe. Omejitve pa se lahko določijo samo pod pogojem, da je zakonska določba, ki določa takšno omejitev, v skladu s prvim odstavkom 8. člena ZVOP-2 (zakonska določba). Prav tako je določena sistemska izjema, da se ne glede na določbe prvega odstavka in še zlasti v primerih obdelave osebnih podatkov v okviru strokovnih mnenj, izdelanih v skladu z določbami zakonov, ki urejajo sodne ali upravne ali nadzorne postopke, v primeru, kadar se posameznik, na katerega se nanašajo osebni podatki, navaja netočnost in neposodobljenih svojih osebnih podatkov, posamezniku dati na razpolago možnost za nasprotni prikaz dejstev, v okviru njegove pravice do ugovora. Upravljavec mora nasprotni prikaz dejstev priložiti dokumentom (posebni uradni zaznamek) ali ustrezno označiti na njih, kje se ta prikaz nahaja.

K 28. členu:

V 28. členu je posebej urejeno sodno varstvo posameznika. V prvem odstavku je določeno, da posameznik, ki ugotovi, da so kršene njegove pravice, določene s tem zakonom, lahko zahteva sodno varstvo ves čas, dokler kršitev traja. V drugem odstavku je določeno, da če je kršitev iz prvega odstavka prenehala, lahko posameznik vloži tožbo za ugotovitev, da je kršitev obstajala, če mu v zvezi s kršitvijo ni zagotovljeno drugo sodno varstvo. V tretjem odstavku je določeno, da v sodnem postopku odloča pristojno sodišče po določbah Zakona o upravnem sporu, kolikor ta zakon ali drug zakon ne določa drugače (zoper javnopravnega upravljavca se toži pred Upravnim sodiščem Republike Slovenije po določbah Zakona o upravnem sporu, zoper zasebnopravnega pa pred okrožnim ali okrajnim sodiščem in se uporabljajo določbe Zakona o pravdnem postopku ter deloma tudi določbe Obligacijskega zakonika). Po četrtem odstavku je možno izključiti javnost iz sodnega postopka, razen če sodišče na predlog posameznika, na katerega se nanašajo osebni podatki, iz utemeljenih razlogov ne odloči drugače. Po petem odstavku lahko posameznik, na katerega se nanašajo osebni podatki, v skladu s prvim odstavkom člena 80 Splošne uredbe, pisno pooblasti nevladno organizacijo s področja varstva osebnih podatkov ali zasebnosti, ki ima status nevladne organizacije v javnem interesu⁶³, da v njegovem imenu uveljavlja sodno varstvo po določbah tega člena. Sodni postopek je po predlaganem šestem odstavku prednosten (ni pa nujen).

5. K III. delu Predloga ZVOP-2:

K 29. členu:

Ena od ključnih novosti Splošne uredbe v primerjavi z veljavno Direktivo je uzakonitev obveznosti upravljavca, da ves čas izvajanja obdelav skrbi za skladnost teh obdelav s pravili te uredbe oziroma drugih predpisov o varstvu osebnih podatkov, ter da to izvajanje tudi ustrezno dokumentira.

Upravljavec mora v ta namen v svojih internih aktih določiti postopke in ukrepe za zagotovitev skladnosti (kar je dosedaj veljalo zgolj za ukrepe za zavarovanje osebnih podatkov oz. za pogodbeno obdelavo - drugi odstavek 25. člena oz. drugi odstavek 11. člena ZVOP-1). V primeru bolj tveganih obdelav mora določiti tudi splošno politiko varstva osebnih podatkov, ki naj vključuje ukrepe kot so ozaveščanje in usposabljanje svojih zaposlenih, upravljanje njihovih pooblastil za dostop do oz. za obdelavo podatkov, določitev odgovornih oseb za posamezne zbirke osebnih podatkov ter pravila za izvajanje revizij. Primerne postopek oziroma ukrepe, oziroma vsebino politike varstva osebnih podatkov določi na podlagi tveganosti posamezne obdelave, v skladu s kriteriji, kot so določeni v uvodnih navedbah št. 75 in 76 Splošne uredbe. Pri najbolj tveganih ukrepih se priporoča uporaba katerega od veljavnih mednarodnih standardov na tem področju.

Upravljavec mora tako predpisane ukrepe tudi ves čas izvajati in o tem voditi vso potrebno dokumentacijo, s katero lahko skladnost dokazuje tudi za nazaj. Ta dokumentacija naj vsebuje zlasti evidenco obdelav pri upravljavcu, oceno učinkov teh obdelav za varstvo osebnih podatkov (izdelano po ustrezni metodologiji, upošteva tveganost obdelave), popis sredstev obdelave, popis dostopnih

⁶³ Navedene organizacije bodo priznane oziroma jim bo podeljen zahtevani status v skladu z določbami bodočega Zakona o nevladnih organizacijah, ki je v drugi obravnavi v Državnem zboru Republike Slovenije (EPA 2300-VII).

pravic zaposlenih, pogodbenih partnerjev in drugih uporabnikov, ter rezultate rednih revizij skladnosti obdelave podatkov. Upravljavce lahko za pripravo in hrambo te dokumentacije pooblasti tudi pooblaščen osebno za varstvo osebnih podatkov, najame zunanje strokovnjake, oziroma pribavi ustrezno in za to namenjeno programsko opremo.

V skladu z usmeritvijo Splošne uredbe veljajo vse navedene obveznosti tudi za obdelovalce osebnih podatkov (glejte tudi obrazložitev k 31. členu). Obdelovalci glede njih odgovarjajo samostojno, ob tem pa za njih posebej odgovarja še upravljavce.

K 30. členu:

Upravljavce mora po novem že pri snovanju novih obdelav preveriti, katere podatke resnično potrebuje za učinkovito izvajanje posamezne obdelave, ter potem te obdelave zasnovati tako, da ne zahtevajo zbiranja dodatnih podatkov (vgrajeno varstvo osebnih podatkov).

Obenem mora upravljavce mora svoje obdelave v čim večji meri zasnovati tudi tako, da v vsakem posamičnem primeru pridobijo in obdelajo samo tiste podatke, ki so potrebni v tem primeru. To pri obdelavah, ki se izvajajo s sredstvi informacijske tehnologije pomeni še zlasti, da se pred začetkom vsake obdelave ne naloži vseh podatkov, ki bi bili potrebni za tipično obdelavo te vrste, ampak, kolikor je le mogoče, zgolj tiste podatke, ki jih potrebuje ta konkretna obdelava (privzeto varstvo osebnih podatkov).

K 31. členu:

Tako kot že dosedaj (11. člen ZVOP-1) lahko upravljavce posamezna opravila v zvezi z obdelavo osebnih podatkov pogodbeno preda (zaupa) obdelovalcu (dosedanjemu "pogodbenemu obdelovalcu"). Podobno kot dosedaj mora njuna medsebojna razmerja še vedno urediti v pisni pogodbi ali drugem podobnem sporazumu, pri čemer pa mora ta pogodba zdaj zagotoviti izvajanje vseh obveznosti po tem zakonu, ne zgolj obveznosti varstva (zavarovanja) obdelave, kot dosedaj. Po novem namreč za obdelovalca veljajo enake obveznosti kot za upravljavca, razen tistih obveznosti, ki so posebej pridržane upravljavcu.

Upravljavce ne sme skleniti takšnega sporazuma z obdelovalcem, ki ni sposoben dati zagotovil, da bo lahko zagotovil spoštovanje teh obveznosti. Prav tako obdelovalec ne sme dalje prenesti posameznih opravil na druge obdelovalce, brez da bi mu upravljavce do izrecno dovolil, ali vsaj bil s tem seznanjen in imel možnost izbiri podobdelovalca nasprotovati.

Določeno je tudi, da obdelovalec obvezno nudi pomoč upravljavcu glede zagotavljanje varnosti osebnih podatkov, sporočanja in urejanja problemov glede kršitve varnosti osebnih podatkov, pri izdelavo ocene učinka glede varstva osebnih podatkov ter glede posvetovanje z Informacijskim pooblaščenecem glede ocene učinkov. Ostale skladnostne obveznosti so na upravljavcu samem; če želi pomoč obdelovalca pri tem, se to seveda lahko dogovori v pogodbi, ne sem pa biti obdelovalec prisiljen, da skladnost varstva osebnih podatkov pretežno ali skoraj v celoti zagotavlja sam, v tem primeru dejansko postane obdelovalec.

Vsebina sporazuma med upravljavcem in obdelovalcem ostaja podobna kot dosedaj, seveda z dodanimi novostmi Splošne uredbe.

K 32. členu:

Splošna uredba prinaša pomembno administrativno razbremenitev za večino upravljavcev, in sicer, da Informacijskega pooblaščenca več ne bo potrebno vnaprej obveščati o vzpostavitvi novih zbirk osebnih podatkov oziroma spremembah obstoječih zbirk (dosedanji 25. in 26. člen ZVOP-1 v zvezi s 7. členom - izjeme za manjše upravljavce). Nova ureditev tako predvideva zgolj še obveznost vodenja evidence dejavnosti obdelav, pa še to zgolj za večje upravljavce (z vsaj 250 zaposlenimi) oziroma upravljavce, ki redno izvajajo tvegane obdelave. Obvezna vsebina evidence je zdaj bistveno ožja kot

prej, saj vsebuje le še 8 točk namesto prejšnjih 13, pri čemer gre pri vseh za že obstoječe kategorije, kar bo omogočalo migracijo obstoječih katalogov zbirk osebnih podatkov v novo evidenco.

Namen evidence je zlasti pomagati pri dokazovanju skladnosti obdelav (29. člen predloga ZVOP-2) v morebitnih kasnejših postopkih nadzora s strani Informacijskega pooblaščenca, prav tako pa ostaja koristna tako za lasten pregled dejavnosti obdelave osebnih podatkov, kot tudi za obravnavo zahtev posameznikov za pridobitev lastnih osebnih podatkov (17. člen).

Drugi odstavek jasno določa, da se obveznost iz prvega odstavka ne uporablja za upravljavce in obdelovalce, ki so fizične osebe ali ki so pravne osebe z manj kot 250 zaposlenimi (splošna izjema v korist gospodarstva). Nato so od tega pravila (splošne izjeme) določene tri alternativne in seveda obvezujoče izjeme⁶⁴ glede na tveganost obdelav osebnih podatkov ali pomen pravice posameznikov, da navedena splošna izjema ne velja za:

- tiste njihove obdelave, za katere je verjetno, da predstavljajo tveganje za človekove pravice ali temeljne svoboščine posameznikov, na katere se nanašajo osebni podatki,
- obdelave, ki niso le občasne obdelave osebnih podatkov, ali
- obdelave osebnih podatkov, ki vključujejo posebne vrste podatkov ali osebne podatke v zvezi s kazenskimi obsodbami ali prekrški.

Katerakoli od teh izjem povzroči, da ni možno uporabiti (se sklicevati) na splošno izjemo.

Pravne podlage za to rešitev so uvodna navedba št. 13 Splošne uredbe o varstvu podatkov vsebuje opis izjeme (»Za upoštevanje posebnega položaja mikro, malih in srednjih podjetij ta uredba vsebuje odstopanja glede vodenja evidenc za organizacije, ki zaposlujejo manj kot 250 oseb.«), nato člen 30, peti odstavek Splošne uredbe o varstvu podatkov (»5. Obveznosti iz odstavkov 1 in 2 se ne uporabljajo za podjetje ali organizacijo, ki zaposluje manj kot 250 oseb, razen če je verjetno, da obdelava, ki jo izvaja, predstavlja tveganje za pravice in svoboščine posameznikov, na katere se nanašajo osebni podatki, in ni občasna, ali obdelava vključuje posebne vrste podatkov iz člena 9(1) ali osebne podatke v zvezi s kazenskimi obsodbami in prekrški iz člena 10.«).

K 33. členu:

V 33. členu je urejen institut skupnih upravljavec osebnih podatkov, v skladu s členom 26 Splošne uredbe, ki pa je področno vezan tudi na IX. del zakona.

K 34. členu:

Predlagani člen nadomešča dosednji izraz "zavarovanje osebnih podatkov" (24. člen ZVOP-1) s pojmom "varnost osebnih podatkov". Sprememba seveda ni samo izrazoslovna, ampak je vezana zlasti na spremenjene tehnološke realnosti, ki so nastopile v času od uveljavitve ZVOP-1. Vsesplošna informatizacija postopkov obdelave osebnih podatkov je namreč poleg številnih prednosti prinesla tudi nekatere probleme, zlasti glede zagotavljanja varnosti obdelav.

Uvodna konstrukcija člena ostaja enaka kot pri dosedanjem ZVOP-1, in sicer se poudarja, da je skrb za varnost zaveza tako obdelovalca kot upravljavca, gre pa za to, da podvzameta ustrezne tehnične ukrepe, da se v čim večji meri prepreči kršitve varstva osebnih podatkov.

Drugi odstavek primeroma našteva nekatere najbolj tipične varnostne ukrepe, tj. uporabo psevdonimiziranja oziroma šifriranja, izvajanje glavnih premis informacijske varnosti (zaupnost, celovitost, dostopnost sistemov), izdelovanje varnostnih kopij in sposobnost njihove obnove, ter zavarovanje osebnih podatkov med prenosom po elektronskem komunikacijskem omrežju. Novi,

⁶⁴ Glede alternativnosti treh izjem napram splošni izjemi glejte: Voigt, Paul, von dem Bussche, Axel, *The EU General Data Protection Regulation (GDPR) : A Practical Guide*, Springer International Publishing AG, Cham, 2017, str. 46-47, naslov »Pogoji za uporabo izjeme«.

oziroma točneje, izrecno določeni sta tako zgolj alineja d), ki zahteva, da se navedene ukrepe varstva osebnih podatkov periodično pregleduje, ter tč. f) zadosti dolgo vodenje dnevnih sledi o dejanjih obdelave osebnih podatkov.

Konkretnije se varnostne ukrepe zagotavlja zlasti z namenskimi informacijskimi orodji, kot so

- orodja, tehnike in mehanizmov za zagotavljanje zaupnosti, celovitosti in razpoložljivosti komunikacijskih omrežij,
- orodja za preverjanje identitete uporabnikov,
- orodja za upravljanje pooblastil za dostop,
- orodja za zaščito pred zlonamernimi kodami,
- orodja za beleženje dejavnosti kritične informacijske infrastrukture in pomembnih informacijskih sistemov, njihovih uporabnikov in administratorjev,
- orodja za zaznavanje poskusov vdorov in preprečevanje incidentov,
- orodja za šifriranje, anonimiziranje ali psevdonimiziranje osebnih podatkov.

Zadnja navedena novost (ti. »notranja sledljivost« obdelav osebnih podatkov) se nahaja v (f) točki drugega odstavka je predlagana zlasti glede na izkušnje Informacijskega pooblaščenca iz prakse, kjer se pri številnih nadzornih postopkih pri večjih upravljavcih še vedno dogaja, da kljub izvajanju tveganih obdelav še vedno ne vodijo revizijskih sledi v takšni kvaliteti, ki bi v primeru zlorab omogočali odgovor na vprašanje, katera oseba je kdaj dostopala do katerih podatkov, kaj je z njimi naredila ipd.. Iz tega razloga se obveznost vodenja revizijskih sledi izrecno predpisuje v minimalnem roku 5 let od preteka leta, v katerem se je zgodila obdelava, razen če kakšen področni zakon določa drug rok. Predlagana določba tako pomeni izvedbo členov 32 (ukrepi varnosti obdelave), 33 (obveščanje o kršitvah varstva osebnih podatkov), 17 (izkazovanje dejanske izvršitve ali omogočanje izvrševanja pravice od izbrisa ozir. pravice do pozabe) in 25 (olajšanje izvajanje vgrajenega in privzetega varstva osebnih podatkov) Splošne uredbe.

K 35. členu:

Ti. "*breach notification*" (obvestilo o kršitvi) v slovensko zakonodajo o varstvu osebnih podatkov prihaja sorazmerno pozno (zvezna država Združenih držav Amerike Kalifornija je to za področje varstva osebnih podatkov uvedla že leta 2003⁶⁵). Poznata ga npr. že 81. člen (zlasti četrti odstavek) Zakona o elektronskih komunikacijah ozir. tudi novi Predlog Zakona o informacijski varnosti. Gre za pravilo da morajo upravljavci v primeru odkritih varnostnih napadov oz. drugih incidentov le te sporočiti Informacijskemu pooblaščenču, da ta lahko ukrepa in določi primerne ukrepe za ustavitev oziroma razrešitev varnostnega incidenta.

Pri tem Informacijskega pooblaščenca ne bo potrebno obveščati o vsakem odkritem (ali osumljenem) varnostnem incidentu, ampak zgolj o tistih, za katere je verjetno, da so oz. še bodo povzročili tveganje za posege v človekove pravice in temeljne svoboščine posameznikov. Ključna razlika bo zlasti v primerih napadov na dosegljivost informacijskega sistema (ti. »availability napadi«, med njimi zlasti DDOS), kjer gre za varnostni incident, ni pa nujno, da je prišlo tudi do kršitve varstva osebnih podatkov.

Rok za obveščanje je čim prej po odkritju incidenta ("brez nepotrebnega odlašanja"), vendar najkasneje v 72 urah, po tem pa le, če za zamik obstajajo opravičljivi razlogi. Bistvo tega roka je, da lahko Informacijski pooblaščenec čim prej odredi morebitne ukrepe za varstvo osebnih podatkov, kot tudi v tem, da v primeru najresnejših kršitev skupaj z upravljavcem oziroma obdelovalcem, pri katerem

⁶⁵ Glejte: Database Breach Notification Security Act ("SB 1386") iz leta 2003 (zadnjič spremenjen leta 2015).

je prišlo do incidenta, premisli, ali je potrebno o njem obvestiti tudi končne uporabnike, zato da lahko podvzamejo ustrezne ukrepe za zaščito njihovih osebnih podatkov.

Obveščati je zatoj treba tudi v primerih, ko upravljavec incidenta še ni povsem raziskal, in ko tudi morda še ne ve dokončno, ali sploh je, ter v kakšnem obsegu, prišlo do zlorabe (zlasti odtujitve) osebnih podatkov. Takšen pristop izvira iz izkušenj z informacijsko-varnostne sfere, saj bi čakanje na dokončno raziskanost incidenta lahko povzročilo znatno dodatno škodo posameznikom zaradi zlorab njihovih podatkov v vmesnem času.

Dodatna novost pa je še v tem, da mora upravljavec takoj po odkritju varnostne grožnje pristopiti k zavarovanju dokazov o dogodku, za primer, če bi bilo kasneje potrebno za ugotavljanje okoliščin in dometa vloma.

Dodajamo, da je posamezne vidike notifikacijske dolžnosti že obravnavala Delovna skupina po členu 29 Direktive 95/46/ES, in o tem izdala svoje mnenje⁶⁶.

K 36. členu:

V primerih suma hujših incidentov, tj. ko je med preiskavo incidenta verjetno, da če da so ozir. bodo nas tala velika tveganja za človekove pravice in temeljne svoboščine posameznikov, mora upravljavec o incidentu obvestiti tudi svoje uporabnike, zato da lahko podvzamejo ustrezne zaščitne ukrepe.

K 37. členu:

Za večje in z vidika obdelave osebnih podatkov bolj intenzivne nove projekte bo v skladu s Splošno uredbo potrebno že v fazi načrtovanja pripraviti poseben dokument z oceno vseh učinkov na pravice posameznikov, katerih podatki se bodo obdelovali. Takšnemu dokumentu se pravi Ocena učinkov v zvezi z varstvom osebnih podatkov, oz. angl. Data Protection Impact Assessment - DPIA). Gre za ukrep, ki se močno povezuje z obveznostjo vgrajenega in privzetega varstva osebnih podatkov (30. člen), zato ga je treba izvesti še v fazi načrtovanja projekta obdelave osebnih podatkov.

DPIA ni obvezna za vse projekte. Dobro pravilo je, da bodo upravljavci, ki bomo morali imeti pooblaščenca osebo za varstvo osebnih podatkov, za vsaj nekatere od svojih projektov potrebovali tudi DPIA-o. Splošna uredba to izrecno pripoznava in upravljavca napotuje, da pri sestavi pridobi pomoč te osebe.

Bistvo DPIA-e ni v popisu obdelav osebnih podatkov oziroma iskanju pravne podlage za njih, ampak v identifikaciji, kategorizaciji ter ovrednotenju tveganj, ki bi lahko nastala pri obdelavah, ter potem iskanju rešitev, ki bi, vsaka posebej oziroma vse skupaj, prispevale k zmanjšanju tako najdenih tveganj.

Podrobnosti za izvedbo ocene razlaga Informacijski pooblaščenec v svojih smernicah iz novembra 2017⁶⁷.

K 38., 39. in 40. členu:

Navedeni trije členi urejajo vprašanje posredovanja osebnih podatkov drugemu upravljavcu, zaradi namenov, ki so pod njegovo kontrolo. V praksi gre pri tem zlasti za zahteve odvetnikov, policije, tožilstva in sodišč za posredovanje podatkov, relevantnih v tej ali oni zadevi.

Izhodiščno pravilo za posredovanje je, da gre zgolj za eno od oblik obdelave osebnih podatkov, in da mora torej zanj obstajati veljavna pravna podlaga, ki upravljavca zavezuje ali mu vsaj dovoljuje posredovanje. Naloga, da določi to pravno podlago, ter njeno podanost ustrezno izkaže, je na prosilcu za podatke. Ta mora imetniku podatkov poslati zahtevek, v katerem utemelji svojo pravno podlago.

⁶⁶ Glejte: WP250 z dne 3.10.2017, Guidelines on Personal data breach notification under Regulation 2016/679.

⁶⁷ Glejte: https://www.ip-rs.si/fileadmin/user_upload/Smernice_o_ocenah_ucinka__DPIA__nov2017.pdf

Šele na podlagi takšnega dopisa pa je potem mogoče pripraviti zaprošene podatke in jih tudi posredovati.

V sedmem odstavku 40. člena so določena pravila glede ti. »zunanje sledljivosti« obdelave osebnih podatkov, namreč glede posredovanj osebnih podatkov s strani upravljavcev uporabnikom. Po sedmem odstavku mora upravljavec za vsako posredovanje osebnih podatkov zagotoviti, da je mogoče pozneje ugotoviti, kateri osebni podatki so bili posredovani, komu, kdaj in po kateri pravni podlagi, za kateri namen oziroma iz katerih razlogov oziroma za potrebe katerega postopka, razen če drug zakon za posredovanje posameznih vrst podatkov ne določa drugače. Ureditev je podobna kot v dosedanjem tretjem odstavku 22. člena ZVOP-1. Predlagana določba je tako izvedba členov 32 (ukrepi varnosti obdelave), 33 (obveščanje o kršitvah varstva osebnih podatkov), 17 (izkazovanje dejanske izvršitve ali omogočanje izvrševanja pravice od izbrisa ozir. pravice do pozabe) in 25 (olajšanje izvajanje vgrajenega in privzetega varstva osebnih podatkov) Splošne uredbe. V zvezi z navedenim se v osmem odstavku izvedbeno zahteva tudi vodenje revizijskih sledi o posredovanjih.

Deveti odstavek 40. člena določa, da določbe sedmega in osmega odstavka o zunanji sledljivosti ter revizijski sledi veljajo tudi za obdelovalce, če so z zakonom ali pogodbo zavezani posredovati določene osebne podatke, kar pa vključuje tudi sodne odredbe ali inšpektorske ali druge nadzorne odredbe na podlagi zakona.

K 41. členu:

V navedenem členu se ohranja obstoječa pravica iz drugega odstavka 18. člena ZVOP-1. Pravica do vpogleda v osebni dokument tako ostaja definirana sorazmerno široko (vedno, ko je potrebno potrditi identiteto posameznika), medtem ko pravica fotokopiranja tega dokumenta ostaja pridržana bankam in drugim finančnim institucijam.

Po predlagani določbi lahko (občasno po drugem zakonu: mora⁶⁸) upravljavec osebnih podatkov pred vnosom določenih podatkov ali njihovo spremembo ali dopolnitvijo v zbirki (osebnih podatkov) preveriti točnost identifikacijskih osebnih podatkov z vpogledom v osebno izkaznico, potni list, vozniško dovoljenje ali drug osebni dokument ali drugo ustrezno javno listino posameznika, na katerega se nanašajo, ki vsebuje tudi fotografijo posameznika. Kot je razvidno, je krog dokumentov načeloma določen (razširijo jih lahko drugi zakoni), pomembno je, da je sedaj izrecno omenjeno vozniško dovoljenje. Te določbe ne posegajo v določbe zakonov, ki urejajo posamezne osebne dokumente glede dopustnosti kopiranja osebnega dokumenta.

K 42. členu:

V navedenem členu se ohranja obstoječe omejitve pri povezovanju z nekaterimi evidencami posebnih vrst osebnih podatkov, in sicer, da je treba poleg EMŠO-a ozir. davčne številke kot vezni kriterij vnesti vsaj še en drug podatek (priimek, rojstni datum, idr.). navedeno služi kot varovalka pred prehitrim in napačnim pripisovanjem dejstev iz teh evidenc napačni osebi.

K 43. členu:

V navedenem členu se konkretizira obveznosti upravljavca do spoštovanja načela najkrajšega roka hrambe oziroma do spoštovanja obveznosti vgrajenega in privzetega varstva osebnih podatkov. Upravljavec je zlasti dolžan redno preverjati, ali sta nabor in rok hrambe podatkov še vedno sorazmerna, ter o tem voditi dokumentacijo za potrebe nadzor s strani Informacijskega pooblaščenca.

K 44. členu:

⁶⁸ Npr. drugi odstavek 39. člena Zakona o notariatu (Uradni list RS, št. 2/07 – uradno prečiščeno besedilo, 33/07 – ZSReg-B, 45/08 in 91/13).

V 1. poglavju IV. delu Predloga ZVOP-2 se urejajo novi subjekti na področju varstva osebnih podatkov - pooblaščenice osebe za varstvo podatkov (*»data protection officers«*) ter certificiranje obdelav osebnih podatkov. Obveznost imenovanja pooblaščenice osebe za varstvo podatkov, njene naloge, ter njen položaj so urejeni v členih 37 do 39 Splošne uredbe. Določbe so v določenem delu neposredno uporabljive oziroma učinkovite, v določenem delu pa zahtevajo oziroma dovoljujejo podrobnejše urejanje v nacionalnih zakonih o varstvu osebnih podatkov. Glede pooblaščenih oseb za varstvo podatkov se najprej podrobno ureja delo in vloga oseb, ki znotraj upravljavcev ali obdelovalcev zagotavljajo varstvo osebnih podatkov, zlasti ko gre za tvegane ali množične obdelave osebnih podatkov. V skladu s prenovljenim pravnim okvirom varstva osebnih podatkov v Evropski uniji bodo upravljavci in obdelovalci primorani vprašanju skladnosti njihovih obdelav osebnih podatkov s pravili varstva osebnih podatkov namenjati več pozornosti in sredstev - še zlasti pa bodo morali v primerih, ko izvajajo večje število bolj tveganih obdelav osebnih podatkov, imenovati tudi osebo (zaposlenega ali zunanjo osebo), katere glavna (ne pa nujno edina) naloga bo skrbeti za izvajanje te skladnosti, odgovarjati na zahteve posameznikov v zvezi z obdelavami njihovih podatkov, ter vzdrževati določeno pojasnjevalno komunikacijo z državnim nadzornim organom za varstvo osebnih podatkov (Informacijskim pooblaščencom) – sodelovanje nižje intenzitete.

S predlagano ureditvijo se ne vzpostavlja reguliran poklic, temveč neodvisne osebe znotraj upravljavca ali obdelovalca, ki naj identificirajo ali pomagajo pri obvladovanju tveganj ali kršitev varstva osebnih podatkov. Te pooblaščenice osebe so individualne osebe, delajo neodvisno, lahko jim pomagajo druge osebe, vendar je vedno lahko le ena oseba odgovorna za ti. notranje varstvo osebnih podatkov. Zakon tudi omogoča izbiro (imenovanje) zunanjih pooblaščenih oseb, omogoča tudi fleksibilnost, da lahko skupine gospodarskih družb, društva ipd. določijo eno pooblaščenico osebo, ki skrbi za notranje varstvo osebnih podatkov v več institucijah. Ta nova oseba bo po svojem delovanju in vplivu podobna dosedanjim notranjim revizorjem ali pooblaščenim osebam za skladnost poslovanja (*»compliance officer«*), delno pa tudi uradnim osebam za dostop do informacij javnega značaja.

Imenovanje pooblaščenice osebe vsebinsko in stroškovno ni nujno (in zato tudi ne smiselno) za vse upravljavce in obdelovalce. Temu primerno Predlog ZVOP-2 v 45. členu (po vzoru člena 37 Splošna uredba) imenovanje pooblaščenice osebe zahteva zgolj za upravljavce in obdelovalce v javnem sektorju (katerih obdelave se, ker se izvajajo neodvisno od privolitve posameznika, že na splošno morajo presojati stroške), ter za tiste upravljavce iz zasebnega sektorja, ki izvajajo bolj tvegane obdelave osebnih podatkov. Pod slednjim so mišljene takšne obdelave, ki zajemajo obsežno in številčno profiliranje ali podobno sledenje večjega števila posameznikov, oziroma v večjem obsegu obdelujejo posebne vrste osebnih podatkov (nekdanji občutljivi osebni podatki). Primeri takšnih obdelav bi lahko zajemali zlasti oblikovanje profilov obiskovalcev spleta za potrebe oglaševanja, spremljanje nakupovalnih navad potrošnikov na podlagi kartic zvestobe, ali obdelava zdravstvenih podatkov posameznika v okviru zdravstvene dejavnosti.

V 44. členu ZVOP-2 so določene splošne (sistemske) opredelitve pomena (poslanstva) pooblaščenih oseb za varstvo podatkov. Pooblaščenica oseba za varstvo podatkov je tako le oseba z ustreznimi poklicnimi odlikami in zlasti strokovnim znanjem ter dejanskimi izkušnjami o zakonodaji in praksi na področju varstva osebnih podatkov ali na primerljivem področju (npr. varstvo ali uresničevanje osebnostnih pravic), ki upravljavcu ali obdelovalcu na neodvisen način pomaga pri zagotavljanju skladnosti obdelave osebnih podatkov s pravili Splošne uredbe ter določbami tega zakona in drugih zakonov, ki urejajo obdelavo in varstvo osebnih podatkov. Po drugem odstavku dejanske izkušnje iz prvega odstavka vključujejo vsaj tri leta delovnih izkušenj s področja varstva osebnih podatkov ali področja informacijske varnosti ali področja poslovne skrivnosti po zakonu, ki ureja gospodarske družbe ali zaupnih podatkov po zakonu, ki ureja bančništvo. Predlog, ki ne določa samo delovne izkušnje s področja varstva osebnih podatkov, upošteva tudi sorodna področja, če so le-ta zadevala tudi področje varstva osebnih podatkov. Pri tem upošteva usmeritev iz petega odstavka člena 37 Splošne uredbe, po katerem se pooblaščenica oseba imenuje na podlagi poklicnih odlik in zlasti (!) strokovnega znanja o zakonodaji in praksi na področju varstva podatkov ter zmožnosti za izpolnjevanje nalog iz člena 39 in del določbe uvodne navedbe št. 97, kjer je določeno: »Določiti bi bilo

treba stopnjo potrebnega strokovnega znanja, zlasti glede na izvedena dejanja obdelave podatkov in varstvo, ki je potrebno pri osebnih podatkih, obdelanih s strani upravljavca ali obdelovalca.«

V 44. členu je tako podana opredelitev pooblaščenice osebe, pri čemer je jasno poudarjeno, da gre za osebo, ki zgolj pomaga upravljavcu ali obdelovalcu zagotavljati skladnost njegovih obdelav osebnih podatkov z določbami Splošne uredbe. Obveznost zagotavljanja skladnosti obdelave osebnih podatkov z določbami Splošne uredbe, Direktive, ZVOP-2, področnih zakonov tako ostaja na upravljavcu oziroma obdelovalcu, oziroma se ta odgovornosti za kršitve skladnosti ne more rešiti s sklicevanjem na neustrezno delo pooblaščenice osebe.

K 45. členu:

45. člen ZVOP-2 določa v prvem odstavku, da morajo pooblaščenice osebo za varstvo podatkov imenovati vsi upravljavci ali obdelovalci v javnem sektorju (1. točka) – tukaj gre za pristop pomena oblastvene funkcije (pa četudi gre za nosilce javnih pooblastil). Po 2. točki istega odstavka morajo to osebo imenovati tudi tisti upravljavci ali obdelovalci v zasebnem sektorju, katerih temeljne dejavnosti zajemajo takšne obdelave osebnih podatkov, ki zaradi svoje narave, obsega oziroma namenov vključujejo redno, sistematično in obsežno spremljanje posameznikov, na katere se nanašajo osebni podatki. Presoja, ali gre za takšne obdelave, je treba posebej opraviti pri upravljavci in pri obdelovalcu. Tako je možno, da bosta k imenovanju pooblaščenice osebe zavezana oba, lahko pa samo eden od njiju. Npr. v primeru, ko manjši upravljavec uporablja določeno storitev obdelovalca, ki sicer je invazivna, vendar je ne uporablja v velikem obsegu, ta upravljavec ne bo zavezan k imenovanju pooblaščenice osebe, obdelovalec, ki pa isto storitev ponuja številnim upravljavcem in jo zato opravlja v velikem obsegu, pa bo.

Natančnejša merila glede tega, kdaj se določene obdelave štejejo v temeljne dejavnosti, ter kdaj gre za obsežne in bolj invazivne obdelave, so podrobneje pojasnjena v Smernicah Delovne skupine po členu 29 Direktive 95/46/ES⁶⁹ na to temo.

Velika večina upravljavcev in obdelovalcev bo torej prosta te obveznosti. Bodo pa še vedno lahko pooblaščenice osebo imenovali na prostovoljni podlagi, torej v primeru, če ocenjujejo, da jo potrebujejo. Zakon tudi ne predvideva dodatnih primerov, ko bi bilo imenovanje obvezno, lahko pa takšno možnost določijo posamezni področni zakoni.

Po 3. točki prvega odstavka morajo pooblaščenice osebo imenovati tudi tisti upravljavci ali obdelovalci osebnih podatkov, katerih temeljne dejavnosti zajemajo obsežne obdelave posebnih vrst osebnih podatkov ali obsežne obdelave osebnih podatkov v zvezi s kazenskimi obsodbami in prekrški.

Po drugem odstavku lahko tudi ostali upravljavci ali obdelovalci prostovoljno imenujejo pooblaščenice osebo in na ta način izkažejo kakovost njihovih obdelav osebnih podatkov.

Po tretjem odstavku morata upravljavec ali obdelovalec, ki sta imenovala pooblaščenice osebo, v roku osmih dni od imenovanja vpisati njene kontaktne podatke po členu 30 Splošne uredbe v svoji evidenci dejanj obdelave, jih javno objaviti na primeren način ter jih sporočiti Informacijskemu pooblaščenicu, ki teh podatkov ne objavi. Prav tako morata upravljavec ali obdelovalec s temi kontaktnimi podatki pod pogoji iz členov 13 ali 14 Splošne uredbe seznaniti posameznike, na katere se nanašajo osebni podatki – katerih osebne podatke obdeluje.

K 46. členu:

V 46. členu ZVOP-2 so določeni pogoji za imenovanje pooblaščenice osebe za varstvo podatkov. Po prvem odstavku je za pooblaščenice osebo lahko določen posameznik ali posameznica, ki izpolnjuje pogoje iz petega odstavka člena 37 in drugega stavka šestega odstavka člena 38 Splošne uredbe in drugega odstavka 42. člena tega zakona.

⁶⁹ Glejte: WP 243 rev.01, 5. 4. 2017, dostopne na: http://ec.europa.eu/newsroom/document.cfm?doc_id=44100

Po drugem odstavku je dodatno za javni sektor določeno, da je pooblaščen osebo lahko imenovan posameznik, ki poleg pogojev iz prvega odstavka izpolnjuje še naslednje pogoje, da je namreč:

1. državljan Republike Slovenije ali države članice Evropske unije ali države članice Evropskega gospodarskega prostora in aktivno obvlada slovenski jezik,
2. poslovno sposoben,
3. ima vsaj univerzitetno izobrazbo ali končan magistrski študijski program
4. ima vsaj tri leta delovnih izkušenj s področja varstva osebnih podatkov ali področja informacijske varnosti ali področja poslovne skrivnosti po zakonu, ki ureja gospodarske družbe⁷⁰ po zakonu, ki ureja gospodarske družbe ali zaupnih podatkov po zakonu, ki ureja bančništvo.
ali zaupnih podatkov po zakonu, ki ureja bančništvo (podobno kot v drugem odstavku 42. člena ZVOP-2),
5. je zaposlen v javnem sektorju, ter
6. ni bil pravnomočno obsojen na kazen najmanj šestih mesecev zapora, oziroma ni bil pravnomočno obsojen za kaznivo dejanje glede zlorabe osebnih podatkov ali kraje identitete.

Za javni sektor torej drugi odstavek 32. člena v skladu s splošno pooblastilno klavzulo iz drugega odstavka člena 6 Splošne uredbe določa še nekatere dodatne pogoje za imenovanje pooblaščen oseb.

V tretjem odstavku je določena razumna področna ureditev za področje vzgoje in izobraževanja, po kateri se v primeru, če se za pooblaščen osebo na področju vzgoje in izobraževanja določi osebo, ki izpolnjuje pogoje za strokovnega delavca, se šteje da izpolnjuje pogoj iz 4. točke prejšnjega odstavka (pogoji glede delovnih izkušenj z določenega področja).

V četrtem odstavku je določena razumna izjema za javni sektor glede zaposlitve pooblaščenih oseb v javnem sektorju, da lahko namreč javni sektor lahko za pooblaščen osebo izjemoma s pogodbo v pisni obliki imenuje tudi posameznika ali posameznico iz zasebnega sektorja, ali pravno osebo zasebnega sektorja, če ta subjekt javnega sektorja nima več kot 20 zaposlenih (varianta: 30 zaposlenih) ter če njegovo delovanje ne vsebuje visoke stopnje tveganj obdelave osebnih podatkov za človekove pravice in temeljne svoboščine in interese posameznikov, ne gre za množične avtomatične obdelave osebnih podatkov, ne gre za redno, sistematično in obsežno spremljanje posameznikov ali njihovo profiliranje ter tudi za obdelavo posebnih vrst osebnih podatkov kot del primarne dejavnosti subjekta javnega sektorja. Pogoji so torej kumulativne narave. Izjema od te izjeme je določena v tretjem odstavku 47. člena Predloga ZVOP-2 – za ministrstva.

Po petem odstavku lahko zasebni sektor za pooblaščen osebo upravljavca ali obdelovalca s pogodbo v pisni obliki imenuje tudi posameznika ali posameznico, ki ni zaposlena pri upravljavcu ali obdelovalcu, ali pravno osebo, podano je torej splošno pooblastilo za zunanje izvajalce.

Po šestem odstavku je obveznost, da morajo v primerih, kadar se v skladu s tretjim ali četrtem odstavkom 44. člena ZVOP-2 imenuje pravno osebo, vsi zaposleni in drugi sodelavci in pravne osebe, kateri bodo opravljali naloge pooblaščen oseb, izpolnjevati pogoje za imenovanje v pooblaščen osebo. Prav tako mora biti v pogodbi s pravno osebo določen vodilni član (zaposleni) pravne osebe, ki odgovarja za delo pravne osebe in katerega kontaktni podatki bodo objavljeni v skladu določbami tretjega odstavka 43. člena tega zakona.

Predlagani sedmi odstavek določa, da lahko pooblaščen osebi pri opravljanju njenih nalog pomagajo tudi druge osebe, ki so pri tem vezane na njena navodila. Te osebe morajo izpolnjevati pogoje za imenovanje za pooblaščen osebo. To pomeni, da je pooblaščen oseba funkcionalno in

⁷⁰ Za pomen in poslanstvo klasičnega instituta poslovne skrivnosti glejte: odločba US, št. U-I-201/14, U-I-202/14, 19. 2. 2015; objava: Uradni list RS, št. 72/14 in Uradni list RS, št. 19/15.

organizacijsko vedno le ena (ima lahko namestnika, ki jo v času odsotnosti polno nadomešča), je ti. »vodilna oseba« in da torej tudi ni možno ustanoviti kolektivne pooblaščen osebe (kolegijski subjekt ali kolegijski »organ«). Ta vodilna oseba je hierarhično nadrejena ostalim članom skupine in odgovorna za delo. Seveda za pooblaščen osebo ne more biti imenovana oseba, ki ima konflikt interesov, tj. še zlasti, da v organizaciji, ki jo nadzira, opravlja druge naloge v zvezi z obdelavo osebnih podatkov. V teh primerih bi ta oseba namreč nadzirala samo sebe, kar bi izničilo namen instituta. Takšna oseba torej ne sme biti imenovana, seveda pa jo je treba tudi razrešiti, če ti pogoji nastopijo naknadno.

V osmem odstavku je določena sistemska prepoved, po kateri za pooblaščen osebo in osebe, ki ji pomagajo pri opravljanju njenih nalog ne smejo biti imenovane osebe, ki imajo konflikt interesov z upravljavcem ali obdelovalcem. Npr. to ne more biti oseba iz kadrovske službe določenega upravljavca, lahko je, če je posebej izkazano, da ni konflikta interesov – oseba iz službe za informacijsko podpora...

V devetem odstavku je prepoved iz sedmega odstavka podrobneje razdelana. Po njej se za javni sektor šteje, da ima določena oseba konflikt interesov, če ima položaj predstojnika ali drugega funkcionarja v subjektu javnega sektorja, če je član organov upravljanja ali nadzora pri upravljavcu ali obdelovalcu, če njene druge naloge vključujejo odločanje o obdelavi osebnih podatkov pri upravljavcu ali obdelovalcu, ali če zastopa upravljavca oziroma obdelovalca v sodnih ali arbitražnih postopkih v zvezi z vprašanji varstva osebnih podatkov. V primeru, da pooblaščen oseba izve za situacijo, ki predstavlja ali bi lahko predstavljala konflikt interesov, mora o tem takoj pisno obvestiti upravljavca oziroma obdelovalca. Upravljavec oziroma obdelovalec mora v tem primeru bodisi odpraviti konflikt bodisi pooblaščen osebo razrešiti ob upoštevanju določb tretjega in četrtega odstavka 50. člena ZVOP-2. Enako ravna v primeru, če se na drug način seznanijo z obstojem ali verjetnostjo obstoja konflikta interesov. Vse navedeno velja tudi za osebe, ki pooblaščen osebi pomagajo pri opravljanju njenih nalog.

Po predlaganem desetem odstavku veljajo določbe devetega odstavka smiselno tudi za zasebni sektor.

K 47. členu:

V 47. členu je določena možnost imenovanja skupne pooblaščen osebe za varstvo podatkov. Več upravljavcev iz javnega sektorja ali več upravljavcev iz zasebnega sektorja lahko, upošteva njihovo delovno področje, organizacijsko strukturo in velikost, imenuje tudi skupno pooblaščen osebo (ne more pa del javnega sektorja skupaj z delom zasebnega sektorja imenovati skupne pooblaščen osebe). Pri tem morajo zagotoviti, da je pooblaščen oseba še vedno sposobna opravljati svoje naloge v zvezi z vsemi upravljavci ali obdelovalci, za katere je imenovana. Upoštevana je torej možnost, da zaradi strogosti pogojev in pa zahtevnosti nalog pooblaščen osebe obstaja skrb, da bodo morale pooblaščen osebo za polni delovni čas imenovati tudi takšni subjekti, ki je v resnici ne rabijo večino časa v letu. Zato se daje družbam v povezani družbi, državnim organom, ter društvom ipd. možnost, da določijo skupno pooblaščen besedo.

Zakon torej z vidikov ekonomičnosti (stroški) in racionalnosti (izkušnje) omogoča izbiro (imenovanje) zunanjih pooblaščenih oseb. Tako omogoča tudi fleksibilnost, da lahko zlasti skupine gospodarskih društev, društva ipd. določijo eno pooblaščen osebo, ki skrbi za notranje varstvo osebnih podatkov v več subjektih.

K 48. členu:

48. člen Predloga ZVOP-2 določa naloge pooblaščen osebe za varstvo podatkov. Po prvem odstavku pooblaščen oseba opravlja naloge iz člena 39 Splošne uredbe. Po drugem odstavku pooblaščen oseba opravlja navedene naloge iz člena 39 Splošne uredbe v zvezi z vsemi obdelavami

osebnih podatkov, ki jih izvaja upravljavec oziroma obdelovalec, pri katerem je imenovana. Po tretjem odstavku pooblaščen oseba sodišča ali državnega tožilstva ne sme opravljati navedenih nalog v zvezi z obdelavami osebnih podatkov, izvršenih v okviru izvajanja neodvisnega sodniškega odločanja (125. člen, prvi odstavek 23. člena Ustave Republike Slovenije, prvi odstavek 6. člena Evropske konvencije o človekovih pravicah) ali samostojnega opravljanja državnotožilske funkcije odločanja (135. člen Ustave Republike Slovenije), kot ju opredeljujeta Zakon o sodiščih⁷¹ (3. člen) in Zakon o državnem tožilstvu⁷² (19. člen). Pooblaščen oseba sme opravljati te naloge samo glede zadev sodne uprave (npr. kadri, finance, poslovna razmerja) in državnotožilske uprave ter glede izvajanja varnosti osebnih podatkov.

Za Ustavno sodišče Republike Slovenije je primerljivo (kot za neodvisna sodišča) v četrtem odstavku določeno, da pooblaščen oseba Ustavnega sodišča Republike Slovenije ne sme opravljati navedenih nalog v zvezi z obdelavami osebnih podatkov, izvršenih v okviru odločanja Ustavnega sodišča Republike Slovenije, kot jih opredeljujejo Zakon o ustavnem sodišču ali drugi zakoni (npr. drugi odstavek 5.č člena Zakona o referendumu in ljudski iniciativi). Pooblaščen oseba sme opravljati te naloge samo glede zadev uprave Ustavnega sodišča (pretežno zadeve s področja odločanja upravne seje Ustavnega sodišča) ter glede izvajanja varnosti osebnih podatkov.

Po petem odstavku pooblaščen oseba Varuha človekovih pravic ne sme opravljati navedenih nalog v zvezi z obdelavami osebnih podatkov, izvršenih v okviru delovanja Varuha človekovih pravic, kot jih opredeljuje Zakon o varuhu človekovih pravic ali drug zakon, ki ureja pristojnosti ali naloge varuha človekovih pravic (npr. 5. člen izvedbenega dela Zakona o ratifikaciji Opcijskega protokola h Konvenciji proti mučenju in drugim krutim, nečloveškim ali poniževalnim kaznim ali ravnanju⁷³). Varuh ima namreč položaj posebnega ustavnega organa (159. člen Ustave Republike Slovenije) ki kot *sui generis* ustavni organ izven trodelbe vej oblasti neoblastveno izvaja nadzor glede uresničevanja in varstva človekovih pravic ter temeljnih svoboščin v Republiki Sloveniji in to neodvisno in samostojno (4. člen Zakona o varuhu človekovih pravic). Pooblaščen oseba za varstvo podatkov Varuha človekovih pravic sme opravljati te naloge samo glede zadev obdelav osebnih podatkov s področja zagovornišva otrok – 25.a-25.d člen Zakona o varuhu človekovih pravic (glede na posebno občutljivost področja ter dejstvo, da ne gre za običajno nadzorno vlogo Varuha človekovih pravic, ampak za ti. »upravno pomožno delovanje« Varuha človekovih pravic) ter glede izvajanja varnosti osebnih podatkov.

K 49. členu:

V 49. členu Predloga ZVOP-2 so glede na posebne ustavne položaje ali določene ustavne vrednote določena pravila glede določitve pooblaščenih oseb za varstvo osebnih podatkov.

V prvem odstavku najprej določeno, da na Ustavnem sodišču Republike Slovenije Ustavno sodišče kot celota (plenarna seja) določi eno pooblaščen osebo, ki opravlja naloge v skladu s četrtem odstavkom 48. člena tega zakona. V drugem odstavku je določeno, da mora Vrhovno sodišče Republike Slovenije določiti (le) eno pooblaščen osebo, ki opravlja naloge v skladu s tretjim odstavkom 46. člena tega zakona za vsa sodišča s splošno pristojnostjo in specializirana sodišča v Republiki Sloveniji – torej centralizirani pristop. V tretjem odstavku je določen centraliziran pristop tudi za vsa državna tožilstva, da namreč Vrhovno državno tožilstvo Republike Slovenije določi eno pooblaščen osebo, ki opravlja naloge v skladu s tretjim odstavkom 46. člena tega zakona za vsa državna tožilstva v Republiki Sloveniji. V četrtem odstavku je določeno, da Varuh človekovih pravic (kot državni organ) določi eno pooblaščen osebo, ki opravlja naloge v skladu s petim odstavkom 46. člena tega zakona. V petem odstavku je določeno, da Ustavno sodišče Republike Slovenije, Vrhovno sodišče Republike Slovenije, Vrhovno državno tožilstvo Republike Slovenije ter Varuh človekovih

⁷¹ Uradni list RS, št. 94/07 – uradno prečiščeno besedilo, 45/08, 96/09, 86/10 – ZJNepS, 33/11, 75/12 – ZSPDLS-A, 63/13, 17/15 in 23/17 – ZSSve.

⁷² Uradni list RS, št. 58/11, 21/12 – ZDU-1F, 47/12, 15/13 – ZODPol, 47/13 – ZDU-1G, 48/13 – ZSKZDČEU-1, 19/15 in 23/17 – ZSSve.

⁷³ Uradni list RS, št. 114/06 – Mednarodne pogodbe, št. 20/06.

pravic lahko določijo namestnike pooblaščenih oseb, ki opravljajo naloge pooblaščenih oseb le za čas njene odsotnosti ali zadržanosti, kateri mora izpolnjevati pogoje iz drugega odstavka 44. člena tega zakona, razen pogoja iz 4. točke, kjer velja pogoj dveh let delovnih izkušenj.

V šestem odstavku je določeno strogo pravilo, po katerem mora vsak minister ali ministrica določiti svojo pooblaščenico osebo, ki je zaposlena na tem ministrstvu – v tem primeru se upošteva pravilo ministrske odgovornosti ter povezane parlamentarne odgovornosti ministrov (drugi stavek 110. člena in drugi stavek prvega odstavka 114. člena Ustave Republike Slovenije in 4. člen Zakona o Vladi Republike Slovenije⁷⁴). Za organe v sestavi ministrstev je določeno, da se lahko določi posebno pooblaščenico osebo, kar bo v praksi verjetno veljalo le za večje organe v sestavi.

Za področja obveščevalno-varnostne dejavnosti je v sedmem odstavku določeno, da predstojnik organizacije (Slovenska obveščevalno-varnostna agencija, Obveščevalno varnostna služba Ministrstva za obrambo) s tega področja določi eno pooblaščenico osebo in njenega namestnika znotraj organizacije s tega področja, ki opravljajo tiste naloge iz člena 39 Splošne uredbe, za katere tako določi predstojnik, med njih pa so obvezno vključene naloge glede izvajanja varnosti osebnih podatkov ter posredovanja osebnih podatkov Vladi Republike Slovenije, Predsedniku Republike Slovenije, policiji, državnim tožilstvom ali sodiščem ali pristojnemu delovnemu telesu Državnega zbora Republike Slovenije, čezmejne obdelave in prenosi.

K 50. členu:

Prvi odstavek določa, da morata upravljavec ali obdelovalec pooblaščenici osebi zagotoviti pogoje za učinkovito in neodvisno opravljanje njenih nalog po 48. členu ZVOP-2, zlasti, da je pooblaščenica oseba:

1. ustrezno in pravočasno vključena v vsa vprašanja in postopke, povezane z varstvom osebnih podatkov in ima možnost podati ustrezni nasvet, mnenje ali predlog,
2. ima dostop do vseh osebnih podatkov ter dejanj obdelave,
3. ima na razpolago sredstva, potrebna za izvajanje njenih nalog in za ohranjanje njenega strokovnega znanja,
4. lahko posamezniki, na katere se nanašajo osebni podatki, z njo v slovenščini ali v drugem uradnem jeziku Republike Slovenije vstopijo v stik in se posvetujejo glede vseh vprašanj, povezanih z obdelavo njihovih osebnih podatkov in uresničevanje njihovih pravic po Splošni uredbi, ter
5. da ima neposredni dostop do vodstva upravljavca ali obdelovalca, če oceni, da je to zaradi pomembnosti določene obdelave osebnih podatkov nujno potrebno, zlasti kadar gre za tvegane obdelave, obdelave posebnih vrst osebnih podatkov, množične obdelave in vpliv na človekove pravice, temeljne svoboščine ali interese posameznikov, na katere se nanašajo osebni podatki ali za očitno neustreznost ukrepov zavarovanja osebnih podatkov, neposredni dostop vključuje možnost predstavitve stališč ali ocen o neustreznosti varstva osebnih podatkov.

Po drugem odstavku morata upravljavec ali obdelovalec zagotoviti, da pooblaščenica oseba pri izvajanju svojih nalog ne prejema nobenih navodil. Pooblaščenica oseba o svojem izvedenem delu neposredno in neodvisno poroča vodstvu upravljavca ali obdelovalca (omogočen torej neposreden neoviran pristop ter zagotovljen neodvisen način dela).

Po tretjem odstavku upravljavec oziroma obdelovalec pooblaščenih oseb za varstvo podatkov zaradi izvajanja njenih nalog ne sme razrešiti, je kaznovati ali je zapostavljati (kar je del jamstva neodvisnosti iz drugega odstavka).

⁷⁴ Uradni list RS, št. 24/05 – uradno prečiščeno besedilo, 109/08, 38/10 – ZUKN, 8/12, 21/13, 47/13 – ZDU-1G, 65/14 in 55/17.

Po četrtem odstavku je odpoved delovnega razmerja pooblaščenim osebam prepovedana za čas njenega imenovanja in še eno leto po prenehanju imenovanja, razen v primeru redne odpovedi iz razloga nesposobnosti ali krivdnega razloga, izredne odpovedi, odpovedi v postopku prenehanja delodajalca, oziroma če v primeru poslovnega razloga odkloni ponujeno ustrezno zaposlitev pri delodajalcu. V primeru statusne spremembe delodajalca, pooblaščen ohrani svoj položaj pooblaščen osebne, če pri delodajalcu prevzemniku še naprej obstaja obveznost določitve pooblaščen osebne v skladu s tem zakonom, razen če ima delodajalec prevzemnik že lastno pooblaščen osebno. Na ta način je ponovno zagotovljena neodvisnost pooblaščen osebne, njen položaj je urejen primerljivo oziroma ima določena podobna jamstva kot za sindikalnega zaupnika po določbah Zakona o delovnih razmerjih.

K 51. členu:

V 51. členu Predloga ZVOP-2 je v prvem in drugem odstavku posebej urejena dolžnost varovanja tajnosti osebnih podatkov (glede na drugi odstavek 1. člena ZVOP-2, ki izhaja iz drugega odstavka 38. člena Ustave Republike Slovenije), še posebej v razmerju do varovanja identitete posameznikov in posameznic, katerih pritožbe obravnava pooblaščen osebna.

Tretji odstavek predlaganega člena določa, da če ima pooblaščen osebna pri svoji dejavnosti vpogled v osebne podatke, v zvezi s katerimi ima osebna, ki je podvržena nadzoru pooblaščen osebne, pravico do molka, ta pravica velja tudi za pooblaščen osebno in za v njenem imenu delujoče osebe, in sicer do mere, v kateri je osebna, ki ima zakonsko pravico do molka, slednjo uveljavila. Gre za smiselni in delni element privilegija zoper samoobtožbo.

K 52. členu:

V 2. poglavju IV. dela Predloga ZVOP-2 so od 52. do 54. člena določena pravila glede samoregulacije (kodeksi ravnanja) na področju varstva osebnih podatkov, njihove veljavnosti, certifikacijskega postopka ter pristojnost certificiranja (Slovenska akreditacija).

Modernizacija pravil varstva osebnih podatkov ima za posledico tudi, da so postala ta pravila znatno številčnejša, obsežnejša in vse bolj zapletena. Temu primerno se povečuje tudi potreba po nadzoru nad izvrševanjem teh pravil, ki pa jih, glede na vseprisotnost in obsežnost obdelav osebnih podatkov v današnji družbi, ni v celoti več mogoče zagotoviti skozi delo državnega nadzornega organa (Informacijski pooblaščenec).

Posledično se po zgledu številnih drugih področjih državno regulacijo dopolnjuje z instrumenti samoregulacije, kot so prostovoljne zaveze podjetij, da bodo pri svojem poslovanju spoštovala določene kodekse ravnanja, oziroma, da bodo svoje poslovne procese predala v neodvisno zunanjo revizijo certifikacijski agenciji, ki jim bo v primeru skladnosti tudi izdala ustreznega certifikat. Takšna potrdila imajo številne prednosti; poleg olajšanega izvajanja inšpekcijskega nadzora predvsem vzbujajo zaupanje posameznikov, na katere se nanašajo osebni podatki, da upravljavci oziroma obdelovalci njihove podatke obdelujejo v skladu s pravili, ter da temu posvečajo zadostna sredstva.

Ta razdelek Predloga ZVOP-2 ureja obe pojavi obliki takšne samoregulacije, in sicer tako kodekse ravnanja kot tudi certifikacijo. Pri kodeksih ravnanja sicer ne implementira možnosti zunanjega nadzora s strani pooblaščenih organizacij. Pri certifikaciji to prepušča tako Informacijskemu pooblaščenec kot morebitnim zunanjim certifikacijskim organizacijam, ki jih za to pooblasti nacionalni akreditacijski organ (Slovenska akreditacija). Za vsebine certifikacij (standarde) se v veliki meri zanaša na standarde, sprejete na evropski ravni, in odobrene s strani Informacijskega pooblaščenca.

V predlaganem 50. členu se tako ureja kodekse ravnanja - podana je pravna podlaga, ki omogoča uporabo kodeksov ravnanja, tj. pravil dobre prakse na področju posameznih vrst obdelav osebnih podatkov, ki jih pripravijo relevantna domača ali tuja združenja podjetij v določenem sektorju, in so že

prilagojena posebnostim manjših, srednjih oziroma večjih podjetij. Člen predvideva uporabo kodeksov, ki so potrjeni na različnih nivojih nadzornih organov; tako s strani posameznega državnega nadzornega organa, kot tudi širše, s strani Evropskega Odbora za varstvo osebnih podatkov po členu 68 Splošne uredbe kot s strani Evropske komisije. Pri tem Evropska komisija potrjuje tiste kodekse, ki se nanašajo na obdelave, ki potekajo v več državah članicah, pri čemer mora predhodno pridobiti tudi mnenje Odbora.

Člen hkrati omogoča, da lahko Informacijski pooblaščenec razveljavi uporabo določenega kodeksa, če oceni, da ni oziroma da ni več ustrezen. Navedeno izhaja iz sodbe Sodišča Evropske unije v *primeru Maximilian Schrems* (ozir. ti. *Facebook primer*)⁷⁵, v kateri je Sodišče Evropske unije pojasnilo, da pooblastila Evropske komisije za izdajanje delegirane zakonodaje ne morejo voditi v pripravo takšnih pravil varstva osebnih podatkov, na katere bi bili državni nadzorni organi dokončno vezani. Državni nadzorni organi za varstvo osebnih podatkov lahko tako v vsakem primeru suspendirajo rabo kodeksov ravnanja, za katere ugotovijo, da niso skladni z določbami Splošne uredbe.

K 53. členu:

V 53. členu Predloga ZVOP-2 se ureja certificiranje obdelav osebnih podatkov. V prvem odstavku je tako določena definicija certificiranja, ki za potrebe tega zakona pomeni prostovoljni postopek ugotavljanja, ali so dejanja obdelave osebnih podatkov s strani upravljavcev in obdelovalcev skladna z merili iz določenega mehanizma certificiranja (vsebinski kriterij) ter da se o ugotovitvi takšne skladnosti se upravljavcu ali obdelovalcu izda certifikat (oblastveni kriterij). Predmet certificiranja je lahko zbirka, njena delovanja obdelave ter informacijski sistem - Klub zvestobe trgovinske gospodarske družbe, sistem SISBON, eAsistent informacijski sistem za šole, informacijski sistem za bolnišnico.

Po drugem odstavku merila posameznega certifikacijskega mehanizma pripravi upravljavec ali obdelovalec. Odobri jih z odločbo Informacijski pooblaščenec v skladu s petim odstavkom člena 42 Splošne uredbe ali Evropski Odbor za varstvo osebnih podatkov v skladu s petim odstavkom člena 42 Splošne uredbe ter v zvezi s členom 63 Splošne uredbe. Zoper odločbo Informacijskega pooblaščenca iz prejšnjega stavka pritožba ni dopustna, je pa dopusten upravni spor pred Upravnim sodiščem Republike Slovenije.

Po predlaganem tretjem odstavku se izdani certifikat lahko uporabi za izkazovanje, da so dejanja obdelave osebnih podatkov s strani upravljavca ali obdelovalca skladna s Splošno uredbo, pri čemer pa sklicevanje na certifikat ne posega v odgovornosti upravljavca ali obdelovalca za skladnost njunih delovanj obdelave osebnih podatkov s Splošno uredbo in ne posega v naloge in pristojnosti Informacijskega pooblaščenca za ugotavljanje te skladnosti.

Po predlaganem četrtem odstavku se certifikat izda upravljavcu ali obdelovalcu za obdobje največ treh let in se pod enakimi pogoji lahko tudi podaljša, če so zahtevani pogoji certifikacijskega mehanizma še naprej izpolnjeni.

Po petem odstavku mora upravljavec ali obdelovalec, ki svoje obdelave osebnih podatkov predloži v mehanizmu certifikacije, telesu, ki izvaja certifikacijo, zagotoviti dostop do vseh informacij oziroma dostope do svojih dejanj obdelave, ki so potrebne za izvedbo postopka certifikacije.

Po šestem odstavku lahko Informacijski pooblaščenec z odločbo po uradni dolžnosti razveljavi certifikat, če ugotovi, da zahteve v zvezi z njim niso bile ali niso več izpolnjene. Zoper to odločbo pritožba ni dopustna, je pa dopusten upravni spor.

Po sedmem odstavku Informacijski pooblaščenec pripravlja in upravlja seznam pravnomočnih certifikacijskih mehanizmov, ki jih je odobril in ta seznam sprotno objavlja na svoji spletni strani.

⁷⁵ Sodba SEU, C-362/14, 6. 10.2015.

K 54. členu:

V predlaganem 54. členu se glede na 121. člen Ustave Republike Slovenije smiselno predaja javno pooblastilo za izvajanje certificiranja telesom, ki jih na podlagi njihove vloge za to akreditira (ne pa izrecno pooblasti) nacionalni akreditacijski organ – to je Javni zavod Slovenska akreditacija, v skladu z določbami točke b prvega odstavka člena 43 Splošne uredbe in Zakona o akreditaciji⁷⁶ (torej tudi pooblastilo na podlagi zakona). Dodatne zahteve glede certifikacije v skladu s točko b prvega odstavka in tretjim odstavkom člena 43 Splošne uredbe določi Informacijski pooblaščenec.

Po drugem odstavku pred izdajo pooblastila zunanjemu certifikacijskemu telesu Slovenska akreditacija v skladu s prvim odstavkom člena 43 Splošne uredbe o vlogi zainteresiranega subjekta obvesti Informacijskega pooblaščenca, ki preveri izpolnjevanje dodatnih zahtev v skladu s točko b prvega odstavka in tretjim odstavkom člena 43 Splošne uredbe in o tem izda odločbo. Zoper to odločbo pritožba ni dopustna, je pa dopusten upravni spor pred Upravnim sodiščem Republike Slovenije.

Po tretjem odstavku Slovenska akreditacija na lastno pobudo ali na predlog Informacijskega pooblaščenca prekliče pooblastilo za certificiranje zunanjemu certifikacijskemu telesu, če je ugotovljeno, da pogoji za pooblastilo niso ali niso več izpolnjeni, ali, da so bili ukrepi, ki jih je v postopku certifikacije izvedlo pooblaščenno certifikacijsko telo, v neskladju s Splošno uredbo.

Predlagan je torej spodbujevalni mehanizem za varstvo osebnih podatkov, ki je le na razpolago in katerega je šteti, da utegne trajati daljše obdobje, preden bo v Republiki Sloveniji dejansko uporaben.

5. K V. delu Predloga ZVOP-2:

V. del Predloga ZVOP-2 je povezan (le) z IX. delom Predloga ZVOP-2, namreč potrebe (nameni) obdelave osebnih podatkov s strani pristojnih državnih organov ali organov samoupravnih lokalnih skupnosti ali nosilcev javnih pooblastil za namene preprečevanja, preiskovanja, odkrivanja ali pregona kaznivih dejanj ali prekrškov, izvrševanja nalog in pooblastil policije, varnosti države, obrambe države ter izvrševanja kazenskih sankcij, v skladu z določbami Direktive. Za druga področja prenosov ali čezmejnih obdelav veljajo neposredno določbe Splošne uredbe (členi 44. do 49.).

K 55. členu:

V predlaganem 55. členu ZVOP-2 so določena splošna pravila za prenos osebnih podatkov ter glede čezmejne obdelave (za posredovanja osebnih podatkov med državami članicami Evropske unije). Po prvem odstavku določbe tega dela ZVOP-2 veljajo za primere, ko osebne podatke obdelujejo pristojni državni organi ali organi samoupravnih lokalnih skupnosti ali nosilci javnih pooblastil za namene preprečevanja, preiskovanja, odkrivanja ali pregona kaznivih dejanj ali prekrškov, izvrševanja nalog in pooblastil policije, varnosti države, obrambe države ter izvrševanja kazenskih sankcij, v skladu z določbami Direktive ter v zvezi z IX. delom tega zakona. Po drugem odstavku sme pristojni organ osebne podatke, ki so že obdelani ali naj bi se obdelali po prenosu tretji državi oziroma mednarodni organizaciji ali naj bi se čezmejno obdelovali, posredovati le, če so upoštevane določbe tega dela zakona in:

1. je prenos potreben za namene iz 85. člena tega zakona;
2. se osebni podatki posredujejo upravljavcu v tretji državi ali mednarodni organizaciji, ki je pristojni organ za izpolnitev enega od namenov iz 85. člena tega zakona;
3. je pristojna država članica v primerih, ko se osebni podatki posredujejo iz druge države članice Evropske unije ali tej dajo na razpolago, prenos vnaprej odobrila;

⁷⁶ Uradni list RS, št. 59/99.

4. je Evropska komisija v skladu s 56. členom tega zakona sprejela sklep o ustreznosti ali, če tak sklep ne obstaja, so bili predloženi oziroma obstajajo ustrezni ukrepi v smislu 57. člena tega zakona ali je, če ne obstaja sklep o ustreznosti v skladu s 56. členom tega zakona in niso predložena ustrezna zagotovila v smislu 55. člena tega zakona, možno v skladu z 58. členom tega zakona uporabiti izjeme za določene primere in

5. je zagotovljeno, da je nadaljnji prenos tretji državi ali drugi mednarodni organizaciji dovoljen le na podlagi predhodne odobritve pristojnega organa, ki je izvedel prvotni prenos podatkov, in ob primernem upoštevanju vseh tehničnih meril, vključno z naravo ali težo kaznivenga dejanja ali prekrška, namenom prvotnega prenosa osebnih podatkov in stopnjo varstva osebnih podatkov v tretji državi ali mednarodni organizaciji, ki se ji posredujejo osebni podatki oziroma jih posreduje naprej.

Po tretjem odstavku je prenos brez prehodne odobritve v skladu s 3. točko prejšnjega odstavka dovoljen le, če je prenos potreben za odvrnitev neposredne in resne nevarnosti za javno varnost države članice ali tretje države ali zaradi enakovrednega pomembnega interesa države članice ter če predhodne odobritve ni bilo mogoče pravočasno pridobiti. O tem je treba nemudoma obvestiti organ, pristojen za podelitev predhodne odobritve.

K 56. členu:

V 56. členu je urejen sistem prenosa osebnih podatkov na podlagi sklepa o ustreznosti varstva osebnih podatkov, ki ga izda Evropska komisija na podlagi tretjega odstavka člena 36 Direktive (izvedbeni akt), če pač odloči, da zadevna tretja država, njena regija oziroma eden ali več specifičnih sektorjev (javni sektor, zasebni sektor, deli zasebnega sektorja, deli javnega sektorja) v tej tretji državi ali zadevna mednarodna organizacija nudi ustrezno stopnjo varstva osebnih podatkov. Za tak prenos podatkov ni potrebna posebna odobritev nobenega drugega organa (ni potrebna naknadna odobritev). Ta Sklep Evropske komisije, sprejet v skladu s petim odstavkom člena 36 Direktive, ki se nanaša na preklic, spremembo ali odložitev izvajanja že izdanega sklepa po tretjem odstavku člena 36 Direktive ne vpliva na prenose osebnih podatkov tretji državi, regiji oziroma enemu ali več specifičnim sektorjem v tretji državi oziroma mednarodni organizaciji v skladu s 57. in 58. členom tega zakona.

K 57. členu:

Po 57. členu se lahko izvaja tudi prenos osebnih podatkov z uveljavljanjem ustreznih ukrepov varstva osebnih podatkov, namreč če ne obstaja sklep Evropske komisije v skladu s prvim odstavkom 54. člena tega zakona, je prenos osebnih podatkov v tretjo državo ali mednarodno organizacijo dopusten, če:

1. so v ustreznem pravnem aktu, ki je pravno obvezujoč, določeni ustrezni ukrepi za varstvo osebnih podatkov ali
2. je upravljavec po oceni vseh okoliščin, ki so pri prenosu pomembne, ugotovil, da dejansko obstajajo ustrezni ukrepi za varstvo osebnih podatkov.

V predlaganem drugem odstavku je določeno, da če v skladu z 2. točko prvega odstavka obstajajo ustrezni ukrepi za določene vrste prenosov, mora upravljavec o teh kategorijah prenosov obvestiti Informacijskega pooblaščenca, ki lahko odredi prepoved prenosa osebnih podatkov. Po tretjem odstavku je treba prenose v skladu z 2. točko prvega odstavka dokumentirati, dokumentacijo, ki vključuje datum in čas prenosa, informacije o pristojnemu organu uporabniku, utemeljitev prenosa in prenešene osebne podatke, pa je treba na zahtevo dati na razpolago Informacijskemu pooblaščenču.

K 58. členu:

V 58. členu so določene izjeme (glede na člen 38 Direktive), ki urejajo dodatne možnosti prenosa osebnih podatkov, če ne obstajajo podlage po 54. in 55. členu ZVOP-2. Po prvem odstavku je prenos osebnih podatkov tretji državi ali mednarodni organizaciji dopusten le, če je prenos potreben:

1. za zaščito življenjsko pomembnih interesov posameznika (življenje in telo);
2. če je to predvideno zaradi varovanja zakonitih interesov posameznikov, na katere se nanašajo osebni podatki (obramba pred tožbo);
3. za odvrnitev neposredne in resne nevarnosti za javno varnost države članice Evropske unije ali tretje države (ne gre samo za varnost države);
4. v posameznem primeru za namene, navedene v 85. členu ZVOP-2, ali
5. v posameznem primeru za uveljavljanje, izvajanje ali obrambo pravnih zahtevkov v povezavi z nameni, navedenimi v 85. členu ZVOP-2.

Po drugem odstavku je v primerih iz 4. in 5. točke prvega odstavka prenos osebnih podatkov dovoljen le, če ni kršena nobena od nad javnim interesom prevladujočih temeljnih pravic in svoboščin posameznikov, na katere se osebni podatki nanašajo. Po tretjem odstavku za prenose v skladu s prvim odstavkom veljajo določbe tretjega odstavka 57. člena tega zakona (obveznost dokumentiranja).

K 59. členu:

Predlagani 59. člen izvršuje člen 39 Direktive glede izjemnih prenosov osebnih podatkov določenim uporabnikom v tretjih državah – in to neposredno, mimo običajnega sodelovanja (posredništva) preko centralnega pristojnega organa tretje države (pot centralnega pristojnega organa). Prvi odstavek v uvodnem besedilu definira prenosnike osebnih podatkov le kot upravljavce (torej ne gre za obdelovalce), znotraj njih pa gre lahko le za pristojne državne organe Republike Slovenije. Uvodni kriterij je, da mora biti prenos nujno potreben za opravljanje konkretnih nalog uporabnika v tretji državi (npr. nujni prenos policijske informacije za takojšnjo policijsko akcijo v tretji državi, akcija banke glede preprečevanja pranja denarja ipd.). V 1. do 4. točki so določeni kumulativni pogoji, ki omogočajo tovrsten izjemni prenos, s tem da 4. točka določa, da mora upravljavec (državni organ) iz Republike Slovenije določiti vezanost organa (uporabnika) iz tretje države, da bo osebne podatke uporabil le za določen namen in tudi sorazmerno v okviru tega namena.

Drugi odstavek določa, da se za prenose iz prvega odstavka uporabljajo pogoji iz drugega in tretjega odstavka 57. člena.

Tretji odstavek pa določa še dodatno izjemno pot prenosa osebnih podatkov – obvezujoče (ratificirane in objavljene) mednarodne pogodbe s področja pravosodnega sodelovanja v kazenskih zadevah in policijskega sodelovanja.

6. K VI. delu Predloga ZVOP-2:

1. poglavje VI. dela Predloga ZVOP-2 ureja položaj in temeljne pristojnosti in naloge Informacijskega pooblaščenca kot nadzornega organa za varstvo osebnih podatkov Republike Slovenije.

K 60. členu:

Predlagani 60. člen ZVOP-2 ponovno potrjuje obstoječe in ustrezno stanje, da je nadzorni organ za varstvo osebnih podatkov Republike Slovenije Informacijski pooblaščenec, kot ga določa Zakon o

informacijskem pooblaščenju⁷⁷. Nato ponovi iz obstoječe ureditve, da je Informacijski pooblaščenec (javnopravno) samostojni in neodvisni državni organ (ki pa nima funkcije tribunala, saj o njegovih odločitvah razsojajo Upravno sodišče Republike Slovenije ali prekrškovni oddelki okrajnih sodišč). Nadalje je v tretjem odstavku določeno, da pri Informacijskem pooblaščenju delujejo poleg informacijskega pooblaščenca in namestnikov tudi državne nadzornice oziroma državni nadzorniki za varstvo osebnih podatkov, ki opravljajo pristojnosti inšpekcijskega nadzora in druge naloge glede varstva osebnih podatkov po določbah Splošne uredbe, ZVOP-2 in drugih zakonov ali predpisov. V četrtem odstavku je določeno, da imajo informacijski pooblaščenec (funkcionar, predstojnik tega državnega organa) in njegovi namestniki enaka pooblastila in pristojnosti, kot velja za nadzornike iz prejšnjega odstavka – torej vsi lahko izvajajo nadzore glede varstva osebnih podatkov. Po petem odstavku informacijskemu pooblaščenju, namestnikom informacijskega pooblaščenca in državnim nadzornikom lahko pri izvajanju pristojnosti iz tretjega odstavka, zlasti ugotavljanju dejstev in okoliščin, pomembnih za odločanje, ter opravljanju strokovnih oziroma administrativnih opravil, po pooblastilu informacijskega pooblaščenca pomagajo drugi zaposleni pri Informacijskem pooblaščenju.

K 61. členu:

V 61. členu ZVOP-2 so določene temeljne pristojnosti Informacijskega pooblaščenca. V prvem odstavku je določeno, da Informacijski pooblaščenec samostojno in neodvisno⁷⁸ izvaja inšpekcijski nadzor nad izvajanjem določb Splošne uredbe, ZVOP-2 in drugih zakonov, ki urejajo varstvo, obdelavo ali prenos osebnih podatkov oziroma prenos osebnih podatkov iz Republike Slovenije, ter opravlja druge naloge ali pooblastila, ki jih določajo ti predpisi. Po drugem odstavku Informacijski pooblaščenec pri inšpekcijskem nadzoru iz prvega odstavka izvaja tudi nadzor glede uporabe podzakonskih predpisov, ki so izdani na podlagi predpisov iz prejšnjega odstavka (ki pa ne smejo glede na drugi odstavek 38. člena in 87. člen Ustave Republike Slovenije originarno urejati obdelave konkretnih osebnih podatkov). Po tretjem odstavku je Informacijski pooblaščenec pristojen za izvajanje inšpekcijskih nadzorov nad vsemi obdelavami osebnih podatkov v Republiki Sloveniji (torej tudi področja varstva osebnih podatkov umrlih oseb, obveščevalno-varnostne dejavnosti, obrambe države ipd.), razen glede obdelav, za katere je po določbah Splošne uredbe pristojen nadzorni organ druge države članice Evropske unije. V četrtem odstavku je uvodno določeno, da je Informacijski pooblaščenec prekrškovni organ, ki je pristojen za nadzor glede izvajanja določb ZVOP-2, drugih zakonov, ki urejajo varstvo osebnih podatkov ter je kot prekrškovni organ pristojen za nadzor glede izvajanja določb Splošne uredbe v zvezi s prekrški iz člena 83 Splošne uredbe. Navedeni odstavek je povezan s 108. členom ZVOP-2.

K 62. členu:

V predlaganem 62. členu so določene izjeme glede pristojnosti Informacijskega pooblaščenca glede dometa inšpekcijskih nadzorov na določenih sistemskih področjih. Namreč glede tistih obdelav osebnih podatkov, izvršenih v okviru izvajanja neodvisnega sodniškega odločanja, kot to opredeljuje Zakon o sodiščih (3. člen), odločanja strokovnih sodelavcev in sodniških pomočnikov po odredbah sodnika, kot to tudi opredeljuje Zakon o sodiščih (53.a člen in drugi odstavek 54. člena)⁷⁹ ali po določbah drugih zakonov, ki določajo njihovo samostojno delovanje (brez posebne odredbe sodnika), nato obdelav osebnih podatkov, izvršenih v okviru opravljanja samostojne državnotožilske funkcije po Zakonu o državnem tožilstvu (19. člen v zvezi s 3. členom), obdelav osebnih podatkov, izvršenih v okviru odločanja Ustavnega sodišča Republike Slovenije, kot jih opredeljujejo Zakon o ustavnem

⁷⁷ Uradni list RS, št. 113/05 in 51/07 – ZUstS-A.

⁷⁸ Glejte: Pirc Musar, Nataša, *Neodvisni nadzor in varstvo osebnih podatkov*, Pravna praksa, št. 35/2016, str. 6-10.

⁷⁹ Tudi v skladu z omejitvami ne-sodniškega odločanja v razmerju do pristojnosti neodvisnih sodnikov iz sodbe Evropskega sodišča za človekove pravice v primeru *Ezgeta proti Hrvaški*, št. 40562/12, 7. 9. 2017, zlasti razdelki 38.-45. sodbe.

sodišču (21. člen) ter obdelav osebnih podatkov, izvršenih v okviru delovanja Varuha človekovih pravic, kot jih opredeljuje Zakon o varuhu človekovih pravic (zlasti v zvezi s 6.a členom) ali drug zakon, ki ureja pristojnosti ali naloge varuha človekovih pravic, razen novega področja zagovornišva otrok ter glede obdelav osebnih podatkov na področjih predkazenskega postopka ali obveščevalno-varnostne dejavnosti, iz katerih bi bilo lahko razvidno, da v postopku delujejo ali sodelujejo tajni delavci oziroma sodelavci po določbah Zakona o kazenskem postopku, Zakona o obrambi ali Zakona o Slovenski obveščevalno-varnostni agenciji oziroma bi bila lahko razkrita identiteta teh posameznikov⁸⁰ ter podobno tudi glede tistih obdelav osebnih podatkov na področju zaščitenih prič po določbah Zakona za zaščito prič, iz katerih bi bila lahko razkrita identiteta teh posameznikov.

Glede sodne oblasti nadzor glede varstva osebnih podatkov v zvezi s sodnim odločanjem preprečujejo ustavne določbe, konvencijske določbe ter določbe Splošne uredbe – namreč neodvisno odločanje sodstva (prvi odstavek 23. člena in 125. člen Ustave Republike Slovenije, prvi odstavek 6. člena Evropske konvencije o človekovih pravicah ter tretji odstavek člena 55 Splošne uredbe). Podobno (primerljivo) velja za državna tožilstva glede na samostojnost državnih tožilcev po 135. členu Ustave Republike Slovenije, saj gre po ustavnosodni presoji za delno primerljiv (funkcionalno) samostojni sistem⁸¹ napram sistemu neodvisnega sodnega odločanja – zlasti v delu, ki se nanaša na kazenski pregon.

Pri izjemah glede nadzora v zvezi z varstvom osebnih podatkov v razmerju do Varuha človekovih pravic se izhaja iz spoštovanja *sui generis* ustavnega položaja Varuha človekovih pravic po 159. členu Ustave Republike Slovenije in njegove neoblastne nadzorne funkcije⁸².

Po drugem odstavku je Informacijski pooblaščenec ne glede na prvi odstavek tega člena pristojen za opravljanje inšpekcijskega nadzora v zvezi z zadevami sodne uprave, državnotožilske uprave, uprave Ustavnega sodišča Republike Slovenije, uprave Varuha človekovih pravic ter glede izvajanja ukrepov in postopkov s področja varnosti osebnih podatkov ter sledljivosti obdelav in posredovanj osebnih podatkov po sedmem odstavku 40. člena in (f) točki drugega odstavka 32. člena tega zakona glede vseh državnih organov iz prvega odstavka tega člena, razen če gre za izmenjave podatkov med sodišči in med državnimi tožilstvi. Navedena področja ne spadajo med temeljna delovna področja navedenih državnih organov oziroma so nekoliko bolj tehnične narave in je ta zakonodajni pristop (polna nadzorna pristojnost Informacijskega pooblaščenca) upravičen. Prav tako ni za področja, ki so izločena po prvem odstavku, predlagan kakšen poseben (*sui generis*) nadomestni nadzorni sistem (mehanizem) glede varstva osebnih podatkov, saj se npr. za sodstvo šteje, da je presoja zakonitosti obdelave določenih osebnih podatkov v sodnih postopkih del običajne postopkovne zakonodaje v zvezi z uporabo pravnih sredstev oziroma vprašanje dokaznega prava.

K 63. členu:

V predlaganem 63. členu so določene naloge Informacijskega pooblaščenca glede posvetovanj o uvedbah obdelav osebnih podatkov. Po prvem odstavku Informacijski pooblaščenec daje predhodna mnenja ministrstvu Vlade Republike Slovenije, Državnemu zboru Republike Slovenije ter Državnemu svetu Republike Slovenije, nato organom samoupravnih lokalnih skupnosti, drugim

⁸⁰ Primerljiva omejitev parlamentarnega nadzora glede tajnih delavcev in tajnih sodelavcev je že od leta 2007 določena v drugem odstavku 25. člena Zakona o parlamentarnem nadzoru obveščevalnih in varnostnih služb (Uradni list RS, št. 93/07 – uradno prečiščeno besedilo), namreč:

»(2) Ne glede na določbe prejšnjega odstavka pooblaščenca skupina ne sme vpogledati v tisti del dokumentacije nadzorovane službe, iz katerega bi bilo lahko razvidno, da v postopku delujejo ali sodelujejo tajni delavci oziroma sodelavci po določbah ZKP, ZObr in ZSOVA oziroma bi bila lahko razkrita identiteta teh tajnih delavcev ali sodelavcev.«

⁸¹ Odločba US, št. U-I-42/12, 7. 2. 2013; objava: Uradni list RS, št. 17/13 in OdlUS XX, 1.

⁸² Sklep Upravnega oddelka Vrhovnega sodišča RS, opr. št. I Up 231/2016, 1. 2. 2017: »11. Delovanje Varuha niti z vidika splošne opredelitve njegovih nalog in pristojnosti niti z vidika ravnanja v konkretnem primeru očitno ne ustreza značilnostim oblastvenega delovanja. Njegovo ravnanje je usmerjeno v nadzor nad delovanjem nosilcev oblasti in se tudi izraža v ukrepih, ki so usmerjeni prav zoper navedene oblastvene subjekte in ne druge osebe, nosilce človekovih pravic in temeljnih svoboščin. ...«

državnim organom ter nosilcem javnih pooblastil o usklajenosti določb predlogov zakonov, podzakonskih aktov ter drugih predpisov z ZVOP-2, Splošno uredbo in drugimi zakoni ter predpisi, ki urejajo osebne podatke. Po drugem odstavku so se organi in nosilci javnih pooblastil iz prvega odstavka dolžni pravočasno, v skladu z določbami o rokih iz drugega odstavka člena 36 Splošne uredbe, predhodno posvetovati z Informacijskim pooblaščencom po določbah prejšnjega odstavka, kadar je v predlaganem predpisu določena vzpostavitev nove zbirke, njena sprememba ali prenos osebnih podatkov iz obstoječe zbirke. Kadar se vrste obdelav, ki jih ureja predlagani predpis, nanašajo na situacije iz 41. člena ZVOP-2, mora predlagatelj predpisa v okviru posvetovanja Informacijskemu pooblaščenцу predložiti oceno učinka iz sedmega odstavka člena 25. člena Splošne uredbe. V tretjem odstavku je določeno, da kadar zakon določa, da Informacijski pooblaščenec poda soglasje k predlogu predpisa, se smiselno uporabljajo določbe drugega odstavka. V četrtem odstavku je z vidikov načel transparentnosti in legitimnosti določeno, da mora biti Mnenje Informacijskega pooblaščenca del javno dostopnega gradiva predloga predpisa iz prvega odstavka tega člena, skupaj z odzivom organa ali nosilca javnega pooblastila. V petem odstavku je določeno, da lahko Informacijski pooblaščenec samostojno odloči, da posreduje tudi naknadno mnenje organu ali nosilcu javnega pooblastila iz prvega odstavka tega člena, če oceni, da je bilo njegovo mnenje neutemeljeno neupoštevano (npr. v postopku obravnave predloga zakona v Državnem zboru Republike Slovenije). V šestem odstavku je določeno, da so se drugi upravljalci dolžni predhodno posvetovati z Informacijskim pooblaščencom, s smiselno uporabo določb prvega do četrtega odstavka tega člena, kadar je iz ocene učinka na varstvo osebnih podatkov iz 41. člena ZVOP-2 razvidno, da bi obdelava osebnih podatkov povzročila veliko tveganje za posameznike, na katere se nanašajo osebni podatki, če upravljavec ne bi sprejel ukrepov za ublažitev tveganja.

K 64. členu:

Predlagani 64. člen določa sistem sodelovanja Informacijskega pooblaščenca z drugimi nadzornimi in podobnimi organi, nevladnimi organizacijami ipd. Po prvem odstavku ima Informacijski pooblaščenec možnost, da pri svojem delu sodeluje z državnimi organi, Evropskim odborom za varstvo podatkov, drugimi pristojnimi organi Evropske unije za varstvo posameznikov pri obdelavi osebnih podatkov ter podobnimi organi Sveta Evrope, drugimi mednarodnimi organizacijami, tujimi nadzornimi organi za varstvo osebnih podatkov, zavodi, združenji, nevladnimi organizacijami s področja varstva osebnih podatkov ali zasebnosti ter drugimi organizacijami in organi glede vseh vprašanj, ki so pomembna za varstvo osebnih podatkov.

Po drugem odstavku je Informacijski pooblaščenec je pristojen tudi za skupno ukrepanje ali preiskovanje z drugimi nadzornimi organi držav članic po členu 62 Splošne uredbe, torej za izvajanje skupnega nadzora glede varstva osebnih podatkov.

V tretjem odstavku sta določena ti. kriterij »vrhovne oblasti« ter stroškovno pravilo, namreč če se skupni nadzor izvaja na ozemlju Republike Slovenije ali v okviru pristojnosti Informacijskega pooblaščenca po tretjem odstavku 4. člena ZVOP-2. Tako so člani (vodstvo, funkcionarji) ali strokovno osebje (javni uslužbenci) nadzornega organa druge države članice Evropske unije dolžni izvajati nadzor tako, da nadzor vodi Informacijski pooblaščenec (so začasno del njegove »ekipe«). Člani ali osebje drugega nadzornega organa krijejo svoje stroške.

V četrtem odstavku je urejena nasprotna situacija, če Informacijski pooblaščenec (funkcionar, namestniki ali državni nadzorniki) izvajajo skupni nadzor na ozemlju druge države članice Evropske unije ali v okviru njenih pristojnosti (pristojnosti njenega nadzornega organa za varstvo osebnih podatkov). Tudi v tem primeru vodi nadzor nadzorni organ druge (pristojne) države članice. In predstavniki Informacijskega pooblaščenca krijejo svoje stroške.

V 2. poglavju VI. dela ZVOP-2 sta urejeni področji sistema inšpekcijskega nadzora glede varstva osebnih podatkov ter tudi javnost delovanja nadzornega organa.

K 65. členu:

Predlagani 65. člen ureja uporabo predpisov, ki urejajo opravljanje inšpekcijskega nadzora, tako določa, da se za opravljanje inšpekcijskega nadzora in drugih nalog po določbah ZVOP-2 in po določbah Splošne uredbe uporabljajo določbe Splošne uredbe, ZVOP-2, Zakona o inšpekcijskem nadzoru ter Zakona o splošnem upravnem postopku. V primeru neskladnosti med določbami Zakona o inšpekcijskem nadzoru ter Zakona o splošnem upravnem postopku v razmerju do določb ZVOP-2 ter določb Splošne uredbe veljajo določbe ZVOP-2 ter določbe Splošne uredbe.

K 66. členu:

V 66. členu je določen obseg inšpekcijskega nadzora, po katerem v njegovem okviru nadzorni organ Informacijski pooblaščenec (torej informacijski pooblaščenec, njegovi namestniki in državni nadzorniki za varstvo osebnih podatkov – glejte tudi prvi odstavek 64. člena ZVOP-2) izvajajo naslednja delovanja:

1. nadzorujejo skladnost obdelave osebnih podatkov z določbami Splošne uredbe, tega zakona in drugih predpisov, ki urejajo obdelavo osebnih podatkov;
2. nadzorujejo ustreznost postopkov in ukrepov za varnost osebnih podatkov ter njihovo izvajanje;
3. nadzorujejo izvajanje določb Splošne uredbe in tega zakona glede prenosa osebnih podatkov v tretjo državo in o njihovem prenosu uporabnikom v tretji državi ter čezmejno obdelavo osebnih podatkov.

K 67. členu:

V 67. členu je določeno neposredno opravljanje inšpekcijskega nadzora s strani državnih nadzornikov, informacijski pooblaščenec in namestniki informacijskega pooblaščenca v mejah pristojnosti Informacijskega pooblaščenca (kot državnega nadzornega organa po tem zakonu, Zakonu o Informacijskem pooblaščenču in drugih zakonov). Po drugem odstavku državni nadzornik, informacijski pooblaščenec in namestnik informacijskega pooblaščenca izkazujejo pooblastilo (namen obdelave osebnih podatkov) za opravljanje nalog inšpekcijskega nadzora s službeno izkaznico in značko, ki vsebuje fotografijo nadzornika, informacijskega pooblaščenca ali namestnika informacijskega pooblaščenca, njegovo osebno ime, strokovni ali znanstveni naslov ter navedbo organa in pooblastil. Obliko in vsebino službene izkaznice in značke podrobneje predpiše Informacijski pooblaščenec v podzakonskem predpisu.

K 68. členu:

V 68. členu so glede na 65. člen ZVOP-2 podrobneje urejena preiskovalna pooblastila Informacijskega pooblaščenca. Po prvem odstavku so državni nadzornik, namestniki informacijskega pooblaščenca ter informacijski pooblaščenec upravičeni:

1. pregledovati vsebino zbirk ne glede na tajnost ali drugo vrsto zaupnosti;
2. pregledovati dokumentacijo, ki se nanaša na obdelavo osebnih podatkov, ne glede na njeno zaupnost ali tajnost, ter na prenos osebnih podatkov v tretjo državo in posredovanje uporabnikom osebnih podatkov iz tretjih držav, ne glede na njeno tajnost ali drugo vrsto zaupnosti;

3. brez predhodne najave in brez navzočnosti zavezanca, njegovega zakonitega zastopnika oziroma pooblaščenca opraviti pregled vsebine in preveriti način delovanja zavezančevih spletnih strani in drugih elektronsko dostopnih storitev;
4. preverjati postopke in ukrepe ter pregledovati dokumentacijo in akte, ki se nanašajo na varnost osebnih podatkov oziroma na njeno izvajanje;
5. pregledovati prostore, v katerih se obdelujejo osebni podatki, računalniško in drugo opremo ter tehnično dokumentacijo;
6. izvajati druga pooblastila, določene z zakonom, ki ureja inšpekcijski nadzor, ter zakonom, ki ureja splošni upravni postopek;
7. opravljati druga preiskovalna pooblastila, določena z zakonom.

V drugem odstavku so določena pravila glede morebitnih posegov v pravice s področja komunikacijske zasebnosti⁸³ (37. člen Ustave Republike Slovenije), prostorske zasebnosti⁸⁴ (36. člen Ustave Republike Slovenije) ali v odvetniško zaupnost⁸⁵ v zvezi s prostorsko ali komunikacijsko zasebnostjo (137. člen ter 36. in 37. člen Ustave Republike Slovenije), ki se lahko zgodijo v okviru izvajanja inšpekcijskih nadzorov po ZVOP-2 ali vsaj v primerih, ko zavezanec inšpekcijskega nadzora ugovarja po kakem od navedenih razlogov. Drugi odstavek izvedbeno določa, da se lahko izvaja ukrep iz 2. točke (pregled dokumentacije, ki se nanaša na obdelavo osebnih podatkov) ali 5. točke (pregled prostorov, v katerih se obdelujejo osebni podatki, računalniško in drugo opremo ter tehnično dokumentacijo) prvega odstavka najprej na podlagi privolitve upravljavca ali obdelovalca iz zasebnega sektorja, ki se pač odpove varovanju prej navedenih pravic s področja zasebnosti ali zaupnosti (poda privolitev). Če se temu ne odpove, sodišče, pristojno za kazenske zadeve (pristojno okrožno sodišče), odloči, ali se pregled izvede, če obstaja utemeljen sum, da je upravljavec ali obdelovalec kršil ali krši določbe Splošne uredbe, tega zakona ali drugih zakonov ali predpisov, in je verjetno, da se bodo pri pregledu prostorov, dokumentacije in stvari v njem našli dokazi, ki so pomembni za odločanje v postopku inšpekcijskega nadzora ali prekrškovnem postopku. Pregled elektronskih naprav mora biti opravljen na način, s katerim se v najmanjši možni meri posega v pravice oseb, ki niso zavezanci za nadzor, in varuje tajnost oziroma zaupnost podatkov ter ne povzroča nesorazmerna škoda. Pregled se opravi ob navzočnosti dveh polnoletnih prič in zavezanca, če določeno elektronsko napravo iz prostora zavezanca uporablja oseba, ki upravičeno pričakuje zasebnost na njej, pa ima tudi ona pravico biti navzoča ob pregledu njene vsebine.

Po tretjem odstavku sodišče odločbo o preiskavi iz prejšnjega odstavka izda najpozneje v 24 urah od vložitve predloga Informacijskega pooblaščenca. Odločba mora vsebovati:

- opredelitev prostorov oziroma elektronskih naprav, ki jih je treba pregledati;
- opredelitev razlogov za preiskavo;
- opredelitev dokazov oziroma vsebine podatkov, ki se iščejo;
- navedbo okoliščin za uporabo preiskovalnega dejanja in način njegove izvršitve.

Na ta način se varujejo vrednote komunikacijske zasebnosti, prostorske zasebnosti ter odvetniške zaupnosti.

⁸³ Glejte: odločba US, št. U-I-40/12, 11. 4. 2013, zlasti 40. točka odločbe; objava: Uradni list RS, št. 39/13 in OdlUS XX, 5.

⁸⁴ Glejte: odločba US, št. U-I-40/12, 11. 4. 2013, zlasti 38. in 39. točka odločbe; objava: Uradni list RS, št. 39/13 in OdlUS XX, 5.

⁸⁵ Glejte: odločba US, št. U-I-115/14, Up-218/14, 21. 1. 2016, zlasti 24.-34. in 52. točka odločbe; objava: Uradni list RS, št. 8/16 in OdlUS XXI, 20.

Po četrtem odstavku se o opravljenem inšpekcijskem ogledu sestavi zapisnik, ki se lahko ne glede na določbe zakonov, ki urejata upravni in inšpekcijski postopek, v primeru, ko ne gre za nujne in neodložljive ukrepe, sestavi v roku 15 dni od dneva opravljenega nadzora ter se vroči zavezancu. Zapisnik vsebuje ugotovljeno dejansko stanje, ki vključuje dejstva in okoliščine, pomembne za odločbo, vključno s posnetki in izpisi podatkov iz spletnih strani ter drugimi pridobljenimi podatki. Zavezanec lahko na zapisnik poda pripombe ter se o ugotovljenih dejstvih in okoliščinah pisno ali ustno izjavi v roku, ki ga določi nadzornik in ne sme biti krajši od 2 delovnih dni po vročitvi zapisnika, o čemer mora biti zavezanec v zapisniku izrecno poučen⁸⁶.

K 69. členu:

V 69. členu so urejena popravljalna pooblastila in ukrepi državnega nadzornika za varstvo osebnih podatkov, namestnika informacijskega pooblaščenca in samega informacijskega pooblaščenca (predstojnika Informacijskega pooblaščenca). V prvem odstavku je urejeno, da imajo navedene uradne osebe, ki pri opravljanju inšpekcijskega nadzora ugotovijo kršitev določb Splošne uredbe, ZVOP-2 ali drugega zakona ali predpisa, ki ureja varstvo osebnih podatkov, pristojnost, poleg uporabe popravljalnih pooblastil iz Splošne uredbe, takoj:

1. odrediti, da se nepravilnosti ali pomanjkljivosti, ki jih ugotovi, odpravijo na način in v roku, ki ga nadzornik sam določi;
2. odrediti prepoved obdelave osebnih podatkov osebam javnega ali zasebnega sektorja, ki niso zagotovile ali ne izvajajo ukrepov in postopkov za varnost osebnih podatkov ali skladnost obdelave osebnih podatkov;
3. odrediti prepoved obdelave osebnih podatkov ter anonimiziranje, omejitev obdelave, psevdonimizacijo, brisanje ali uničenje osebnih podatkov, kadar ugotovi, da se osebni podatki obdelujejo v nasprotju z določbami Splošne uredbe, tega zakona in drugih zakonov;
4. odrediti prepoved prenosa osebnih podatkov v tretjo državo ali njihovega prenosa uporabnikom osebnih podatkov v tretji državi, če se posredujejo v nasprotju z določbami Splošne uredbe ali zakona;
5. odrediti druge ukrepe, določene z zakonom, ki ureja inšpekcijski nadzor, ter zakonom, ki ureja splošni upravni postopek.

Predlagani drugi odstavek pomeni nadgradnjo določb dosedanjega drugega odstavka 54. člena ZVOP-1⁸⁷. Po predlaganem drugem odstavku ukrepov iz prvega odstavka ni mogoče odrediti zoper osebo, ki v elektronskem komunikacijskem omrežju opravlja storitev izključnega prenosa podatkov, vključno z začasnim shranjevanjem podatkov in drugimi delovanji v zvezi s podatki, ki so izključno v funkciji opravljanja ali olajšanja prenosa podatkov po omrežjih, če ta oseba sama nima interesa, povezanega z vsebino teh podatkov, in ne gre za osebo, ki lahko sama ali skupaj z omejenim krogom z njo povezanih oseb učinkovito nadzoruje dostop do teh podatkov, kot je bilo že dosedaj določeno v drugem odstavku 54. člena ZVOP-1. Ukrepa prav tako ni mogoče odrediti zoper ponudnika gostovanja, če le-ta ni bil predhodno seznanjen s protipravnostjo vsebine, ki so jo zagotovili njegovi uporabniki. Zadnji stavek še posebej poudarja zaupnost (in posredno tudi svobodo) komuniciranja, saj določa, da prejšnje določbe ne vključujejo zahteve, da bi se ponudniki gostovanja, shranjevanja ipd. morali seznaniti z vsebino podatkov, če to prepoveduje drug zakon.

⁸⁶ Glejte: odločba US, št. U-I-252/00, 8. 10. 2003, 15. točka; objava: Uradni list RS, št. 105/03 in OdlUS XII, 80,

⁸⁷ Drugi odstavek 54. člena ZVOP-1 je bil predpisan leta 2004 kot reakcija na nekdanjo »afero udba.net« iz leta 2003 – kot ukrep preprečevanja vzpostavljanja cenzure ali preprečevanja nastanka samocenzure (ker to nedopustno posega v svobodo izražanja in v svobodo komuniciranja). Glejte tudi: Makarovic, Bostjan, *Foreign Internet content restriction in the Republic of Slovenia: Artificial borders within the Internet to protect personal data?*, Journal of Computer, Media and Telecommunications Law, Volume 8, Number 5, 2003, str. 371-374.

Predlagana je torej ureditev, ki naj bi preprečevala nastanek zlasti slučajnega vzpostavljanja cenzure ozir. spodbujanja samocenzure (svoboda izražanja in svoboda komuniciranja)⁸⁸, posredno pa gre tudi ukrep proti vzpostavljanju ti. totalne nadzorovalne družbe. Ta varovalni ukrep je tudi nekoliko povezan z 9., 10. in 11. členom Zakona o elektronskem poslovanju na trgu⁸⁹ – sodno odrejeni »take down« sistem ter tudi novejša praksa na ravni Evropske unije na področjih odgovornosti ponudnikov družbenih omrežij za ti. lažne novice (»fake news«) in ti. prirejanje volitev preko njih (»election rigging«).

K 70. členu:

V prvem odstavku 70. člena je določen postopek odločitve, da se postopek nadzora ne uvede. Nadzornik v primerih, kadar je iz prijave posameznika, na katerega se nanašajo osebni podatki očitno, da glede na podatke iz prijave ni možno sklepati na kršitev varstva osebnih podatkov po Splošni uredbi, tem zakonu ali drugem zakonu oziroma predpisu, ki ureja obdelavo in varstvo osebnih podatkov, s sklepom odloči, da se inšpekcijski postopek ne uvede. Enako velja, ko je prijavo podala druga oseba. Nadzornik v obrazložitvi sklepa navede razloge za neuvedbo postopka. Pri tem predlagatelj izhaja iz pomena varstva osebnih podatkov kot osebne človekove pravice (1. člen Predloga ZVOP-2) in zagotavljanja pravne varnosti ter enakega obravnavanja (22. člen Ustave Republike Slovenije⁹⁰), člen pa je povezan tudi z 72. členom Predloga ZVOP-2, ki določa sodno (upravnosodno) varstvo.

K 71. členu:

Predlagani 71. člen določa pravice prijavitelja. V prvem odstavku je določeno obveščanje prijavitelja, po določbi morajo nadzornik, namestnik informacijskega pooblaščenca in informacijski pooblaščenec vsakega prijavitelja po opravljenem nadzoru in sprejetem zadnjem ukrepu oziroma ustavitvi postopka obvestiti o vseh pomembnejših ugotovitvah in dejanjih iz postopka inšpekcijskega nadzora.

Po drugem odstavku lahko prijavitelj, ki meni, da obstaja domnevna kršitev varstva osebnih podatkov v zvezi z osebnimi podatki, ki se nanašajo nanj, v skladu s prvim odstavkom člena 80 Splošne uredbe pisno pooblasti nevladno organizacijo s področja varstva osebnih podatkov ali zasebnosti, ki ima status nevladne organizacije v javnem interesu, da v njegovem imenu vloži prijavo po prejšnjem členu tega zakona.

K 72. členu:

V prvem odstavku 72. člena ZVOP-2 je določeno splošno pravno sredstvo zoper odločitve Informacijskega pooblaščenca, da namreč zoper odločbo ali sklep Informacijskega pooblaščenca ni dovoljena pritožba, dovoljen pa je upravni spor. Informacijski pooblaščenec kot samostojni in

⁸⁸ Glejte: Makarovic, Bostjan, *The new Slovenian personal data protection act: Statutory limits to injunctive regulation of the internet*, Computer & Security Law Report (2005), 21, Elsevier Ltd., str. 322-327, še posebej str. 326-327, mag. Makarovič, Boštjan, *Ustavno varstvo zasebnosti komunikacijskih naprav v inšpekcijskih in prekrškovnih postopkih*, Zbornik - 6. dnevi prekrškovnega prava - DPP, 2011, str. 151 ter *Komentar Ustave Republike Slovenije – Dopolnitev A*, ur.: prof. dr. Šturm, Lovro, Fakulteta za državne in evropske študije, Ljubljana, 2011 (*Komentar 37. člena Ustave Republike Slovenije*, mag. Klemenčič, Goran, str. 522-524, robne št. 4-6, str. 529-530, robne št. 17-18).

⁸⁹ Uradni list RS, št. 96/09 – uradno prečiščeno besedilo in 19/15.

⁹⁰ Glede obrazložitve sklepa se smiselno sledi sicer odločitvi o obrazložitvi državnega organa glede na zavezo iz 22. člena Ustave Republike Slovenije iz najnovejše odločbe Ustavnega sodišča RS, št. Up-326/14, 6. 12. 2017, zlasti 16. točka odločbe; objava: Uradni list RS, št. 6/18.

neodvisni državni organ za varstvo osebnih podatkov torej ne sme imeti (nad seboj) drugostopenjskega upravnega organa, torej pritožbenega organa⁹¹.

Po drugem odstavku lahko v skladu s prvim odstavkom člena 80 Splošne uredbe posameznik, na katerega se nanašajo osebni podatki in je bil prijavitelj, pisno pooblasti nevladno organizacijo s področja varstva osebnih podatkov ali zasebnosti, ki ima status nevladne organizacije v javnem interesu, da v njegovem imenu uveljavlja sodno varstvo po določbah prvega odstavka 72. člena ZVOP-2.

K 73. členu:

V 73. členu ZVOP-2 je urejeno ukrepanje ob zaznavi kaznivih dejanj ali prekrškov. V prvem odstavku je določeno, da če nadzornik pri izvrševanju svojih pristojnosti ugotovi, da obstaja sum storitve prekrška, ki je v pristojnosti Informacijskega pooblaščenca, izvede postopek po zakonu, ki ureja prekrške, po določbah Splošne uredbe ter v skladu z določbami IX. dela tega zakona. V drugem odstavku je določeno, da če nadzornik pri izvrševanju svojih pristojnosti ugotovi, da obstaja sum storitve kaznivnega dejanja ali prekrška iz pristojnosti drugega prekrškovnega organa, poda kazensko ovadbo v skladu z Zakonom o kazenskem postopku oziroma izvede ustrezne postopke v skladu z Zakonom o prekrških.

Predlagani tretji odstavek vzpostavlja podobne omejitve kot v inšpekcijskem postopku (drugi odstavek 69. člena ZVOP-2) tudi za prekrškovni postopek. Tako nadzornik, namestnik informacijskega pooblaščenca in informacijski pooblaščenec zaradi ugotavljanja dejstev in okoliščin oziroma zbiranja dokazov v prekrškovnem postopku ne smejo uporabiti svojih pooblastil zoper tretje osebe (ponudniki storitev gostovanja ipd., kot so navedeni v drugem odstavku 69. člena ZVOP-2), ki so zgolj ponujale posredovalne storitve osebi, osumljeni storitve prekrška.

Predlagani četrti odstavek nadzorniku, namestniku informacijskega pooblaščenca in informacijskemu pooblaščenču v primeru obravnave posebej hudih kršitev zakona oziroma Splošne uredbe omogočata prebitje komunikacijske zasebnosti posameznika (37. člen Ustave Republike Slovenije) na podlagi odredbe sodnika s sodišča za prekrške (pristojnega sodnika okrajnega sodišča). Predlagana ureditev tako določa, da morajo ponudniki prenosa (ISP), začasnega shranjevanja, oziroma gostovanja ne odgovarjajo za kršitve, ki so jih povzročili njihovi uporabniki (prejemniki storitev), Informacijskemu pooblaščenču, če le-ta pridobi sodno odredbo, predati določene identifikacijske podatke o teh uporabnikih po vsebinskih določbah drugega zakona (Zakon o elektronskem poslovanju na trgu⁹²) in ustaviti kršitev, pod pogojem predhodne odredbe prekrškovnega sodišča. Informacijski pooblaščenec lahko torej od ponudnikov prenosa (ISP), začasnega shranjevanja, oziroma gostovanja s sodno odredbo zgolj zahteva identifikacijske podatke o dejanskem kršitelju (tiste s katerimi razpolagajo). Ker je iz narave ureditve jasno, da se podatki vedno pridobivajo v zvezi z neko določljivo komunikacijo, se za pridobitev podatkov zahteva sodna odredba, kjer sodišče za vsak primer posebej preverja nujnost, primernost in sorazmernost ukrepa v luči 37. in 38. člena Ustave Republike Slovenije (glejte tudi odločbo Ustavnega sodišča RS iz leta 2013⁹³). Takšna sodna odredba temu primerno tudi ne more biti izdana v inšpekcijskem postopku, ampak le v prekrškovnem postopku, in še to le, če gre za prekrške, se glede na vrednote, katere varujejo, štejejo za hude prekrške.

Peti odstavek ureja obvezno (in ustrezno) obveščanje posameznika, čigar podatki so bili tako pridobljeni, o tem, da so bili osebni podatki pridobljeni.

K 74. členu:

⁹¹ Glejte: odločba US, št. P-5/11, 2. 6. 2011; objava: Uradni list RS, št. 52/11.

⁹² Uradni list RS, št. 96/09 – uradno prečiščeno besedilo in 19/15.

⁹³ Odločba US, št. U-I-40/12, 11. 4. 2013; objava: Uradni list RS, št. 39/13.

V 74. členu je določeno varovanje tajnosti osebnih podatkov, v okviru nadzornih postopkov Informacijskega pooblaščenca. Po prvem odstavku so dolžni državni nadzornik za varstvo osebnih podatkov, informacijski pooblaščenec in namestnik informacijskega pooblaščenca dolžni varovati tajnost osebnih podatkov, s katerimi se seznanijo pri opravljanju inšpekcijskega nadzora, preiskovalnih pooblastil, popravljalnih ali prekrškovnih pooblastil tudi po prenehanju delovnega razmerja ali funkcije. Po drugem odstavku dolžnost iz prvega odstavka velja tudi za vse javne uslužbence pri Informacijskem pooblaščenču ali druge osebe, ki sodelujejo pri postopkih po tem zakonu.

K 75. členu:

V predlaganem 75. členu so določeni javnost dela Informacijskega pooblaščenca, informiranje javnosti ter dodatna svetovanja. Po prvem odstavku Informacijski pooblaščenec lahko:

1. izdaja notranje glasilo ter strokovno literaturo;
2. na spletni strani ali na drug primeren način pravočasno objavlja mnenja iz 44. člena tega zakona;
3. na spletni strani oziroma na drug primeren način objavlja odločbe in sklepe Ustavnega sodišča Republike Slovenije o zahtevah ocene ustavnosti, ki jih je vložil Informacijski pooblaščenec ter odločitve Ustavnega sodišča Republike Slovenije o njih;
4. na spletni strani oziroma na drug primeren način objavlja odločbe in sklepe sodišč s splošno pristojnostjo in upravnega sodišča, ki se nanašajo na varstvo osebnih podatkov, tako da iz njih ni možno razbrati osebnih podatkov strank, oškodovancev, prič ali izvedencev z uporabo psevdonimizacije;
5. daje mnenja o skladnosti kodeksov poklicne etike, splošnih pogojev poslovanja oziroma njihovih predlogov s predpisi s področja varstva osebnih podatkov;
6. daje neobvezna mnenja, pojasnila in stališča o vprašanih s področja varstva osebnih podatkov in jih objavlja na spletni strani ali na drug primeren način;
7. pripravlja in daje neobvezne smernice in priporočila glede varstva osebnih podatkov na posameznem področju;
8. po potrebi daje izjave za javnost o izvedbi posamičnih zadev po tem zakonu;
9. izvaja konference za medije v zvezi z delom Informacijskega pooblaščenca ter prepise izjav ali posnetke izjav s konferenc za medije objavi na spletni strani;
10. obdeluje kontaktne podatke za izvajanje izobraževanj, posvetovanj, javnih dogodkov;
11. na spletni strani objavlja druga pomembna obvestila.

Po drugem odstavku lahko Informacijski pooblaščenec za opravljanje pristojnosti iz 5., 6., in 7. točke prvega odstavka pozove k sodelovanju tudi predstavnike društev in drugih nevladnih organizacij s področja varstva osebnih podatkov, zasebnosti ter potrošnikov.

V 3. poglavju VI. dela ZVOP-2 so urejeni kontrolni mehanizmi (poročanje ipd.) glede delovanja Informacijskega pooblaščenca.

K 76. členu:

Po prvem odstavku Informacijski pooblaščenec v svojem letnem poročilu poroča Državnemu zboru Republike Slovenije o stanju na področju varstva osebnih podatkov ter povezanih ugotovitvah,

predlogih in priporočilih. Poročilo iz prejšnjega stavka je del skupnega letnega poročila po določbah zakona, ki ureja Informacijskega pooblaščenca. Po drugem odstavku se poročilo posreduje tudi Evropski komisiji, Odboru ter je dostopno javnosti. To je prvi zunanji kontrolni mehanizem parlamentarne vrste, nekako analogno zgodovinskemu izvoru »ombudsmanov«, ki so nastali kot parlamentarni organ (Informacijski pooblaščenec je v manjšem delu primerljiv s klasičnim ombudsmanom).

K 77. členu:

Dodatni (drugi) zunanji kontrolni mehanizem določa pristojnosti Varuha človekovih pravic. Določeno je da Varuh človekovih pravic opravlja svoje naloge na področju varstva osebnih podatkov v razmerju do državnih organov, organov samoupravnih lokalnih skupnosti in nosilcev javnih pooblastil v skladu z Zakonom o varuhu človekovih pravic – torej gre za rezervni (generalni) kontrolni mehanizem, ki deluje neoblastno z lastnimi nadzori na področju varstva osebnih podatkov kot ene od človekovih pravic iz Ustave Republike Slovenije. V drugem odstavku je določeno, da je varstvo osebnih podatkov posebno delovno področje varuha.

K 78. členu:

Kot dodatna izpeljava kontrolnega mehanizma (kot tretji zunanji kontrolni mehanizem) je določeno glede pristojnosti zakonodajne oblasti, da stanje na področju varstva osebnih podatkov in izvrševanje določb tega zakona, v skladu s 76. členom tega zakona, spremlja pristojno delovno telo državnega zbora.

Po drugem odstavku pristojno delovno telo Državnega zbora Republike Slovenije za nadzor obveščevalnih in varnostnih služb (Komisija za nadzor obveščevalnih in varnostnih služb Državnega zbora Republike Slovenije) lahko sodeluje z Informacijskim pooblaščencom, na lasten predlog ali na pobudo Informacijskega pooblaščenca, kadar je potrebna zaupna izmenjava informacij o ugotovitvah ločenih nadzornih postopkov (iz pristojnosti Informacijskega pooblaščenca ali iz pristojnosti Komisije) ali glede sprememb zakonov ali drugih predpisov (iz delovnega področja Informacijskega pooblaščenca ali Komisije).

7. K VII. delu Predloga ZVOP-2:

K 79. členu:

Predlagani 79. člen ureja obdelava osebnih podatkov v znanstvene raziskovalne, zgodovinske raziskovalne in statistične namene. Ta področja so načeloma z vidika varstva osebnih podatkov dobro urejena v področni zakonodaji – v Zakonu o varstvu dokumentarnega in arhivskega gradiva ter arhivih⁹⁴, v Zakonu o državni statistiki⁹⁵ (kjer bi morda vseeno bilo potrebno urediti področno povezovanje zbirk) ter v Zakonu o raziskovalni in razvojni dejavnosti⁹⁶ (ki pa bi ga bilo treba širše spremeniti ozir. dopolniti z vidika urejanja varstva osebnih podatkov).

⁹⁴ Uradni list RS, št. 30/06 in 51/14.

⁹⁵ Uradni list RS, št. 45/95 in 9/01.

⁹⁶ Uradni list RS, št. 22/06 – uradno prečiščeno besedilo, 61/06 – ZDru-1, 112/07, 9/11 in 57/12 – ZPOP-1A.

Po prvem odstavku lahko upravljavec ne glede na prvotni namen zbiranja osebne podatke nadalje obdeluje za znanstvene raziskovalne, zgodovinske raziskovalne in statistične namene, drug uporabnik osebnih podatkov pa za iste namene. Urejena je torej obdelava v druge namene glede na določbe (b) točke prvega odstavka člena 5 in člena 89 Splošne uredbe. Obdelava za te druge namene, ki so v posebnem javnem interesu, je dopustna v okviru naslednjih pravnih podlag:

- če je posameznik, na katerega se osebni podatki nanašajo za takšno obdelavo podal predhodno pisno privolitve (torej posebna vrsta privolitve, določena na sistemski način v ZVOP-2),
- če jih pridobi in nadalje obdeluje v anonimizirani obliki (tako da torej ne veljajo več za osebne podatke) ali
- če tako določa področni zakon (torej posebna zakonska podlaga).

V drugem odstavku je določen strog sistem, kdo lahko izvaja delovanja za namene iz prvega odstavka, namreč registrirane znanstveno-raziskovalne organizacije ali registrirani raziskovalci po zakonu, ki ureja raziskovalno in razvojno dejavnost. Nato je določeno da lahko za namen obdelave iz prvega odstavka tega člena pri upravljavcu osebnih podatkov vpogledajo oziroma pridobijo posebne vrste osebnih podatkov ali druge osebne podatke praviloma v psevdonimizirani obliki, če predložijo predstavitveni elaborat raziskave, s katerim izkažejo:

- dejanski obstoj raziskave,
- da učinkovite izvedbe raziskave oziroma njenega namena ni mogoče doseči brez obdelave določenih osebnih podatkov ali bi bilo to povezano z nesorazmernim naporom ali stroški (potrebnost in primernost obdelave osebnih podatkov),
- da osebnih podatkov, ki so nujno potrebni za učinkovito izvedbo raziskave, ni mogoče pridobiti s privolitvijo posameznika (kar mora organizacija ali raziskovalec izkazati).
-

Predlagani so torej kumulativni strogi pogoji, kdaj lahko pridobijo osebne podatke brez privolitve, posebnega (področnega) zakona, brez anonimizacije.

Po tretjem odstavku se uporabniku (organizaciji ali raziskovalcu) iz drugega odstavka praviloma omogoči vpogled, lahko pa tudi pridobitev podatkov s kopiranjem, prepisom ali izpisom, če se z vpogledom ne da doseči namena raziskave ali bi bila izvedba vpogleda povezana z nesorazmernim naporom ali stroški.

Četrty odstavek določa stroge pogoje za vsebino elaborata ter nujnost (priložene) izvedbe ocene učinka v zvezi z varstvom osebnih podatkov po 37. členu ZVOP-2. Po petem odstavku se osebne podatke po opravljeni raziskavi praviloma uniči, so pa možne izjeme, namreč osebni podatki, ki jih je uporabnik pridobil v skladu s 1. in 3. točko prvega odstavka in drugim odstavkom tega člena, se ob zaključku raziskave uničijo ali nepovratno anonimizirajo, če zakon ne določa drugače, če posameznik ni privolil v nadaljnjo hrambo osebnih podatkov ali če to ni pomembno za izvršitev namena raziskave. Uporabnik osebnih podatkov pa mora upravljavca, ki mu je posredoval osebne podatke, brez odlašanja po njihovem uničenju pisno obvestiti, kdaj in na kakšen način jih je uničil.

Šesti odstavek je en od najpomembnejših odstavkov tega člena, določa namreč objave rezultatov raziskav praviloma v anonimizirani obliki (uporabljeno načelo sorazmernosti). Določeno je, da se rezultati obdelave objavijo v anonimizirani obliki, razen če ZVOP-2 ali drug zakon določa drugače ali če je posameznik, na katerega se nanašajo osebni podatki, za objavo v neanonimizirani obliki podal

pisno privolitev ali če je za takšno objavo v času po smrti posameznika podana pisna privolitev določenih oseb v izključujočem vrstnem redu (zakonec, zunajzakonski partner oziroma partner iz istospolne partnerske skupnosti, otroci ali starši umrlega posameznika). Upravljavec pa ne sme objaviti neanonimiziranih osebnih podatkov, če je to v nasprotju z interesom varovanja tajnosti ali zaupnosti postopkov odločanja, ali pa ti postopki še niso končani. V sedmem odstavku je določeno, da določbe 76. člena ZVOP-2 ne posegajo v (področne) določbe Zakona o varstvu dokumentarnega in arhivskega gradiva ter arhivih⁹⁷,

K 80. členu:

V 80. členu je določena obdelava naslovov za kontaktiranje posameznikov v znanstvene raziskovalne, zgodovinske raziskovalne in statistične namene. Po prvem odstavku se v okviru obdelave osebnih podatkov za namene znanstvenega raziskovanja, zgodovinskega raziskovanja ali statističnega raziskovanja upravljavcu izjemoma dovoljuje tudi obdelovati osebne podatke ciljne skupine posameznikov za potrebe pridobitve privolitev za obdelavo njihovih osebnih podatkov ali zaradi pridobitve dodatnih podatkov ali pojasnil za prej navedene namene.

Po drugem odstavku lahko upravljavec lahko na podlagi zbirk, s katerimi zakonito razpolaga v okviru zakonitega opravljanja dejavnosti, proti plačilu kontaktira posameznike z namenom pridobivanja privolitev za potrebe drugega uporabnika in za izvrševanje namenov iz prejšnjega odstavka:

- ki za obdelavo osebnih podatkov nima podlage v zakonu ali privolitvi in
- ki z elaboratom iz četrtega odstavka prejšnjega člena izkaže, da bo osebne podatke po pridobitvi privolitve obdeloval na znanstveno-raziskovalnem, zgodovinskem raziskovalnem ali statističnem področju.

Gre torej za primere, ko uporabnik želi pridobiti privolitev, pa nima osebnih podatkov, zato kontaktiranje posameznika, na katerega se nanašajo osebni podatki, za njega izvede upravljavec iz javnega sektorja in to proti plačilu stroškov ter le za namene iz prvega in drugega odstavka.

Po tretjem odstavku se v okviru obdelave iz prvega in drugega odstavka lahko za namen kontaktiranja obdelujejo samo osebno ime, naslov stalnega ali začasnega prebivališča, kontaktna telefonska številka ali kontaktni naslov elektronske pošte (uporabljeno načelo sorazmernosti ter določen namen obdelave).

Po četrtem odstavku se posredovani ali obdelani osebni podatki lahko obdelajo izključno za namen raziskave in jih je treba izbrisati takoj, ko niso več potrebni (namenska obdelava osebnih podatkov ter definicija izbrisa iz 6. točke tretjega odstavka 6. člena ZVOP-2).

V petem odstavku je določeno, da določbe 80. člena ZVOP-2 ne posegajo v (področne) določbe Zakona o varstvu dokumentarnega in arhivskega gradiva ter arhivih⁹⁸ (podobno kot to velja za določbe 76. člena ZVOP-1), za področje arhivov namreč tudi veljajo (podrejeno) možnosti npr. znanstvenega raziskovanja ter zgodovinskega raziskovanja.

K 81. členu:

V predlaganem 81. členu je določena obdelava podatkov za namene arhiviranja v javnem interesu. Po prvem odstavku je obdelava osebnih podatkov za namene arhivskega delovanja je dovoljena, če je v javnem interesu in določeno z zakonom. Upravljavec mora v skladu z zakonom določiti ukrepe za

⁹⁷ Uradni list RS, št. 30/06 in 51/14.

⁹⁸ Uradni list RS, št. 30/06 in 51/14.

varnost osebnih podatkov ter primerne in posebne ukrepe za varstvo interesov posameznika, na katerega se nanašajo osebni podatki, zlasti glede posebnih vrst osebnih podatkov.

Po drugem odstavku posameznik, na katerega se nanašajo osebni podatki, nima pravice do seznanitve z lastnimi osebnimi podatki v arhivskem gradivu po členu 15 Splošne uredbe le, če bi dajanje informacij ali kopij njegovih osebnih podatkov zahtevalo očitno nesorazmeren napor, niti ne sme zahtevati popravka osebnih podatkov zaradi netočnosti ali neposodobljenosti v skladu s členom 16 Splošne uredbe⁹⁹. Posameznik, na katerega se nanašajo osebni podatki nima pravice zahtevati izvedbe izbrisa v skladu s pravico do pozabe iz člena 17 Splošne uredbe.

Po tretjem odstavku se ne glede na določbe drugega stavka prejšnjega odstavka v primeru, kadar posameznik, na katerega se nanašajo osebni podatki in le-ta navaja netočnost in neposodobljenosti svojih osebnih podatkov, posamezniku dati na razpolago možnost za nasprotni prikaz dejstev. Pristojni arhiv mora nasprotni prikaz dejstev priložiti dokumentom ali ustrezno označiti na njih, kje se ta prikaz nahaja (posebna vrsta uradnega zaznamka).

Po četrtem odstavku posameznik, na katerega se nanašajo osebni podatki, nima pravice zahtevati omejitev obdelave po členu 18, pravice do prenosljivosti osebnih podatkov po členu 20 ter izvajati pravice do ugovora po členu 21 Splošne uredbe.

8. K VIII. delu Predloga ZVOP-2:

K 82. členu:

V 82. členu Predloga ZVOP-2 je primarno poudarjen pomen svobode izražanja v razmerju do varstva osebnih podatkov, tako da je omogočeno zadržanje dosedanje visoke ravni uresničevanja svobode izražanja v okviru pravnega reda Republike Slovenije¹⁰⁰. Treba je upoštevati, da je področje svobode izražanja eno od tistih, ki ni najbolj primerno za podrobno regulacijo (za razliko od varstva pravice do osebnih podatkov) in je torej z vidika varovanih ustavnih vrednot (npr. prvi odstavek 39. člena Ustave Republike Slovenije, 10. člen Evropske konvencije o človekovih pravicah¹⁰¹) področje, ki ga je treba nekoliko bolj varovati pred posegi države.

V prvem odstavku je glede na določbe prvega odstavka 39. člena Ustave Republike Slovenije zagotovljeno uresničevanje svobode izražanja, kar vključuje svobodo izražanja misli, govora in javnega nastopanja, tiska in drugih oblik javnega obveščanja in izražanja v okvirih pravnega reda Republike Slovenije. Vsakdo lahko svobodno zbira, sprejema in širi vesti in mnenja ter v njih vsebovane osebne podatke, ki so v ta namen potrebni in upravičeno obdelovani. Prvi odstavek (ozir. določbe celotnega člena) so formulirane tako, da se ne nanašajo samo na registrirane medije ali npr.

⁹⁹ Glejte: Sklep Višjega sodišča v Ljubljani, opr. št. I Cp 490/2000, 11. 4. 2001.

¹⁰⁰ Ko se je leta 2012 začelo obravnavanje takratnega Predloga Splošne uredbe, je Republika Slovenija navedla znatno število sistemskih pomislekov (Stališče Državnega zbora Republike Slovenije z dne 23. 3. 2012, št. EPA 191-VI, EU U 393), med drugim tudi z vidika varstva svobode izražanja v razmerju do varstva osebnih podatkov, zlasti:

»Republika Slovenija se načeloma strinja z določbami člena 80 glede razmerja med varstvom osebnih podatkov in svobodo izražanja. Bo pa v zakonodajnem postopku podrobneje proučila navedene določbe z vidika, če niso morda z vidika ostalih določb predloga pravnega akta preskope in je morda treba bolj aplikativno razmišljati o varstvu svobode izražanja, tudi z vidika razmerja do nove pravice "biti pozabljen" iz člena 17 predloga pravnega akta....«.

¹⁰¹ Uradni list RS št. 33/94 – Mednarodne pogodbe, št. 7/94, Uradni list RS, št. 102/03 – Mednarodne pogodbe, št. 22/03, Uradni list RS, št. 49/05 – Mednarodne pogodbe, št. 7/05, Uradni list RS, št. 48/09 – Mednarodne pogodbe, št. 12/09, Uradni list RS, št. 46/10 – Mednarodne pogodbe, št. 8/10 in Uradni list RS, št. 1/15 – Mednarodne pogodbe, št. 1/15.

akreditirane novinarje, ampak na celotno skupnost, ki izvaja svobodo izražanja (npr. tudi delovanje blogerjev, pisma bralcev, pisanje knjig...), torej ni mišljeno samo izvajanje svobode izražanja po določbah Zakona o medijih¹⁰². Posredno (posledično) pa pokriva predlagani člen tudi področje svobode komuniciranja¹⁰³ po 37. členu Ustave Republike Slovenije.

V drugem odstavku je natančneje določena varstvo svobode izražanja v razmerju do varstva osebnih podatkov za namene obveščanja javnosti s strani medijev, književnega, umetniškega ali znanstvenega ustvarjanja, zaradi resne kritike, obrambe kakšne pravice ali varstva upravičene koristi ter izobraževanja, ki ga izvajajo izobraževalne organizacije ali izobraževanja preko javno dostopnih publikacij, kar vključuje pravice medijev in drugih, da se osebni podatki uporabijo, objavijo ali drugače razkrijejo za namene uresničevanja svobode izražanja pod naslednjimi pogoji:

1. če je posameznik za uporabo, objavo ali razkritje podal privolitev (ki se dokazuje po določbah ZVOP-2 o dokumentiranju delovanj obdelave),
2. če je posameznik osebne podatke že javno objavil (uporaba pravice do informacijske samoodločbe),
3. če so osebni podatki na zakonit način že bili dostopni javnosti (npr. starejše objave v okviru izvrševanja svobode izražanja),
4. če so bili osebni podatki pridobljeni na podlagi prisotnosti posameznika na javno dostopnih krajih (npr. javno zbiranje) ali dogodkih, kjer posameznik glede na vse okoliščine ne more razumno pričakovati varstva zasebnosti ter na način, ki ne pomeni občutnega posega v razumno pričakovano zasebnost (koncept utemeljenega pričakovanja zasebnosti),
5. če gre za zakonito objavo mnenja ali vrednostne ocene, kjer je objava osebnih podatkov v njunem okviru nujna za utemeljitev mnenja ali vrednostne ocene¹⁰⁴ (ta določba ne posega nujno v pravico do pozabe – če gre za zelo staro objavo),
6. če so bili osebni podatki pridobljeni na drug zakonit način (jih npr. nekdo drug zakonito objavil, raziskovalno novinarstvo, povzetek objave iz čezmejne obdelave ipd.),
7. če javni interes po obveščanju javnosti, pravica do obveščenosti ter svoboda izražanja prevladajo nad upravičenimi interesi varstva zasebnosti in drugih osebnostnih pravic posameznika (zlasti določbe Zakona o dostopu do informacij javnega značaja), ali
8. če tako določa drug zakon (npr. drugi in tretji odstavek 178. člena Zakona o državnem tožilstvu¹⁰⁵).

Po tretjem odstavku uveljavljanje pravic v zvezi z določbami 79. člena ZVOP-2 zagotavlja samo sodna oblast (sodišča) v skladu z določbami zakonov, ki urejajo sodne postopke ali urejajo sodno varstvo (po splošnih določbah Zakona o pravnem postopku, Zakona o kazenskem postopku, delno pa tudi Zakona o upravnem sporu – ne gre pa več za posebno upravnosodno varstvo kot je to v 34. členu ZVOP-1).

¹⁰² Uradni list RS, št. 110/06 – uradno prečiščeno besedilo, 36/08 – ZPOmK-1, 77/10 – ZSFCJA, 90/10 – odl. US, 87/11 – ZAvMS, 47/12, 47/15 – ZZSDT, 22/16 in 39/16.

¹⁰³ Glejte: Komentar Ustave Republike Slovenije – Dopolnitev A, ur.: *prof. dr. Lovro Šturm*, Fakulteta za državne in evropske študije, Ljubljana, 2011 (komentar 37. člena Ustave Republike Slovenije, *mag. G. Klemenčič*, str. 522-524, robne št. 4-6, str. 529-530, robne št. 17-18).

¹⁰⁴ Glede pomembnosti osebnih podatkov, ki so vsebovani v mnenjih v okviru svobode izražanja ter načelni neprimernosti uporabe pravic izbrisa ali do pozabe po Splošni uredbi v takih primerih glejte: Voigt, Paul, von dem Bussche, Axel, *The EU General Data Protection Regulation (GDPR) : A Practical Guide*, Springer International Publishing AG, Cham, 2017, str. 159-160, razdelek 5.5.2.3..

¹⁰⁵ Uradni list RS, št. 58/11, 21/12 – ZDU-1F, 47/12, 15/13 – ZODPol, 47/13 – ZDU-1G, 48/13 – ZSKZDČEU-1, 19/15 in 23/17 – ZSSve.

Le v četrtem odstavku je zadržana pristojnost Informacijskega pooblaščenca – da nadzor nad zakonitostjo posredovanja, razkritja ali omogočanja nepooblaščenega dostopa do osebnih podatkov iz zbirke za namene iz uvodnega dela besedila drugega odstavka tega člena izvaja Informacijski pooblaščenec.

K 83. členu:

Podobno kot za varstvo svobode izražanja v 82. členu Predloga ZVOP-2 je v predlaganem 82. členu ZVOP-2 določena posebna ureditev tudi za varstvo ozir. uresničevanje druge človekove pravice, namreč dostopa do informacij javnega značaja (drugi odstavek 39. člena Ustave Republike Slovenije) v razmerju do človekove pravice do varstva osebnih podatkov, povzeto: obveljajo dosedanja pravila iz Zakona o dostopu do informacij javnega značaja¹⁰⁶.

Po prvem odstavku 83. člena ZVOP-2 lahko zavezanci po Zakonu o dostopu do informacij javnega značaja javnosti posredujejo osebne podatke, če so ti po zakonu javni ali če je za njihovo razkritje podan prevladujoč javni interes ali ne obstaja zakonsko določena izjema po določbah Zakonu o dostopu do informacij javnega značaja ali npr. Zakona o zunanjih zadevah (drugi odstavek 45.a člena)¹⁰⁷.

Po drugem odstavku za namene uresničevanja javnega interesa na področju sodelovanja javnosti, zagotavljanja transparentnosti dela ali spremljanja njihove prakse, zavezanci iz prvega odstavka po postopku iz Zakona o dostopu do informacij javnega značaja zakona, lahko proaktivno javno objavijo tudi dokumente, ki niso zajeti v prvem odstavku tega člena, in predstavljajo informacijo javnega značaja, na način delnega dostopa praviloma v anonimizirani obliki. V primerih, kjer zasledovanje navedenih ciljev na ta način ni mogoče, pa jih objavijo v psevdonimizirani obliki v skladu s Splošno uredbo upoštevajoč druge zakonske izjeme v skladu z določbami Zakona o dostopu do informacij javnega značaja zakona.

Po predlaganem tretjem odstavku uveljavljanje pravic v zvezi z določbami 83. člena ZVOP-2 zagotavljajo najprej Informacijski pooblaščenec v skladu z določbami Zakona o dostopu do informacij javnega značaja, Zakona o medijih, nato pa sodišča (zlasti po določbah Zakona o upravnem sporu, lahko pa tudi po določbah Zakona o pravnem postopku, Zakona o kazenskem postopku).

K 84. členu:

V predlaganem 84 členu ZVOP-2 je za upravljavce in obdelovalce določeno, da če so osebni podatki javni na podlagi zakona (npr. po določbah ZVOP-2, Zakona o medijih, Zakona o nalogah in pooblastilih policije, Zakona o sistemu plač v javnem sektorju ipd.), posameznika, na katerega se nanašajo osebni podatki, ni treba obveščati po členih 13. ali 14. Splošne uredbe, po 15. do 17. členu ZVOP in po določbah Zakona o splošnem upravnem postopku¹⁰⁸ (npr. šesti odstavek 143. člena o vabljenju k stranski udeležbi).

9. K IX. delu Predloga ZVOP-2:

Posebni IX. del ZVOP-2 pomeni izvrševanje določb Direktive za namene preprečevanja, preiskovanja, odkrivanja ali pregona kaznivih dejanj ali prekrškov, izvrševanja nalog in pooblastil policije, varnosti

¹⁰⁶ Uradni list RS, št. 51/06 – uradno prečiščeno besedilo, 117/06 – ZDavP-2, 23/14, 50/14, 19/15 – odl. US in 102/15.

¹⁰⁷ Uradni list RS, št. 113/03 – uradno prečiščeno besedilo, 20/06 – ZNOMCMO, 76/08, 108/09, 80/10 – ZUTD in 31/15.

¹⁰⁸ Uradni list RS, št. 24/06 – uradno prečiščeno besedilo, 105/06 – ZUS-1, 126/07, 65/08, 8/10 in 82/13.

države, obrambe države ter izvrševanja kazenskih sankcij. Zakonodajni pristop, da se področje ureja v posebnem delu systemskega Zakona o varstvu osebnih podatkov, je podoben zakonodajnim pristopom Nemčije, Avstrije, Slovaške, izhaja pa tudi iz pristopa Republike Slovenije iz časa priprave Predloga Direktive. Vsebinski pristop, da se v tem »policijsko ter kazensko pravosodnem« delu zakona izhaja iz uporabe določenih standardov (določb) Splošne uredbe sledi pristopu Zvezne republike Nemčije, ki je v Zakonu o prilagoditvi in izvajanju zakonodaje o varstvu osebnih podatkov EU (iz leta 2017) izvedla razširitev določb Splošne uredbe na določena vprašanja, ki jih ureja sicer Direktiva (zaradi pravne varnosti in enakosti na področju varstva osebnih podatkov), v III. Delu zakona Nemčije je namreč določena izvedba določb Direktive (EU) 2016/680 in določbe v njem, ki so enake ali podobne istim, ki so v Splošni uredbi ali v predhodnih delih zakona izhajajo iz pristopa, po katerem je nacionalnemu zakonodajalcu prepuščeno, kako bo izvedel določbe navedene Direktive in lahko tako tudi uporabi (z vidika pravne varnosti) splošni sistem (splošno systemsko raven) urejanja varstva osebnih podatkov po (nekoliko prilagojenih) določbah iz Splošne uredbe. To je tudi pristop predlagatelja ZVOP-2. K temu delu zakona spada tudi V. del Predloga ZVOP-2 o prenosu osebnih podatkov tretjim državam ali mednarodnim organizacijam ter glede čezmejne obdelave.

K 85. členu:

V 85. členu je določeno področje uporabe IX. dela zakona. Po njem določbe tega dela zakona veljajo za primere, ko osebne podatke obdelujejo pristojni državni organi ali organi samoupravnih lokalnih skupnosti ali nosilci javnih pooblastil za namene preprečevanja, preiskovanja, odkrivanja ali pregona kaznivih dejanj ali prekrškov, izvrševanja nalog in pooblastil policije, varnosti države, obrambe države ter izvrševanja kazenskih sankcij, v skladu z določbami Direktive. Dodano je systemsko napotilo (ne systemska varovalka) glede določb področnih zakonov, da če posamezni zakoni s področij iz prvega odstavka tega člena glede konkretnih vrst osebnih podatkov, konkretnih zbirk, obdelav osebnih podatkov ter njihovega posredovanja, prenosov in čezmejnih obdelav določajo drugače, se za ta področja uporabljajo določbe teh zakonov in ne določbe tega dela zakona. IX. del zakona bo torej v praksi v precej primerih uporabljen le kot pravna podlaga za delovanje, kadar obstajajo pravne praznine.

K 86. členu:

V 86. členu so podarjeno določena temeljna načela obdelave osebnih podatkov za področja (namene) iz 85. člena ZVOP-2, najprej na način systemskega sklica na I. del ZVOP-2, ki velja »nadrejeno« (1. točka), v nadaljevanju pa je dan poudarek, da morajo biti osebni podatki (še posebej) točni in po potrebi posodobljeni ter da je pri tem je treba sprejeti vse primerne ukrepe, da se osebni podatki, ki glede na namene njihove obdelave niso ustrezni (ni uporabljen izraz: točni), takoj izbrišejo ali popravijo ali ustrezno označijo. Nato je določeno, da se smejo osebni podatki hraniti v obliki, ki dopušča identifikacijo posameznikov, na katere se nanašajo osebni podatki, le toliko časa, kot je potrebno za namene, za katere se obdelujejo ter da se morajo obdelovati na način, ki zagotavlja ustrezno varnost osebnih podatkov, vključno z ustreznimi tehničnimi in organizacijskimi ukrepi za zagotavljanje zaščite pred nedovoljeno ali nezakonito obdelavo, nenamerno izgubo, nedovoljenim uničenjem ali nedovoljenim poškodovanjem osebnih podatkov.

K 87. členu:

Predlagani 87. člen ZVOP-2 določa razvrščanje osebnih podatkov po vrstah ter kakovost osebnih podatkov, ob upoštevanju realnih (tudi tehničnih zmožnosti), kakovosti virov podatkov ipd.. V bistvu gre za razlikovanje med različnimi postopkovnimi položaji posameznikov (faza postopka, oznaka kakovosti podatkov glede na zgodnjo ali poznejšo fazo), kar ne vključuje samo osumljencev, tudi žrtve kaznivih dejanj, udeležence prekrška ipd. Drugi odstavek podrobneje določa, da če je to možno, je

treba razlikovati podatke, ki temeljijo na dejstvih, od tistih, ki temeljijo na osebni oceni, nato da je osebne podatke, ki temeljijo na osebni oceni, je treba ustrezno označiti ter, če je to možno in dopustno, utemeljiti na način, ki omogoča naknadno preverjanje te ocene ter zaključno je določeno, da je za izvajanje tega preverjanja je odgovoren upravljavec. Po tretjem odstavku se osebni podatki, ki so netočni, nepopolni, ki niso posodobljeni ali jih je treba izbrisati, se ne smejo ne prenašati ne pripraviti za avtomatiziran priklic iz zbirk, upravljavci pa morajo v ta namen pred prenosom v skladu z razložljivimi možnostmi ustrezno preveriti kakovost podatkov. Glede osebnih podatkov, ki so že na razpolago za avtomatiziran priklic, se je treba neprestano prizadevati za ohranjanje njihove točnosti in posodobljenosti. Po četrtem odstavku je pri vsakem posredovanju, čezmejni obdelavi ali prenosu osebnih podatkov treba po možnosti osebnim podatkom priložiti informacije, na podlagi katerih lahko uporabnik oceni oceno aktualnost, pravilnost, popolnost in zanesljivost. V petem odstavku je določeno, da če uporabnik, Informacijski pooblaščenec ali pooblaščen oseba za varstvo osebnih podatkov na podlagi sporočila posameznika, na katerega se nanašajo osebni podatki, ugotovijo (katerikoli od njih), da so bili posredovani osebni podatki, ki ne ustrezajo zahtevam iz tretjega odstavka tega člena, mora pošiljatelj to nemudoma sporočiti uporabniku. Ta pa mora nemudoma izvesti izbris nezakonito posredovanih podatkov, popravek netočnih podatkov, dopolnitev nepopolnih podatkov ali omejitev obdelave.

Po šestem odstavku velja, da če imata pošiljatelj ali uporabnik verjeten razlog za domnevo (nadpolovična verjetnost), da so posredovani osebni podatki netočni ali da niso bili posodobljeni, da bi jih bilo treba izbrisati ali omejiti njihovo obdelavo, je treba nemudoma izvesti medsebojno obveščanje. Pošiljatelj pa mora nemudoma sprejeti ustrezne ukrepe popravka ali izbrisa če so dejstva o neustreznih osebnih podatkih potrjena, uporabnik je na to odločitev vezan, je pa dolžan označiti morebitno nestrinjanje v svoji zbirki.

K 88. členu:

V predlaganem prvem odstavku 88. člena je določena zakonitost obdelave osebnih podatkov, po kateri je obdelava osebnih podatkov po IX. delu ZVOP-2 zakonita le - če je določena z zakonom, ali če je potrebna zaradi varstva življenja ali telesa posameznika ter je potrebna in sorazmerna za izpolnitev določenih nalog, ki jih pristojni subjekt izvaja v skladu z nameni iz 85. člena tega zakona. Primer (sicer zakonsko določen) glede varstva življenja ali telesa posameznika so npr. določbe o posredovanju prometnih in lokacijskih podatkov za varovanje življenja in telesa po določbah 153. in 153.a člena Zakona o elektronskih komunikacijah¹⁰⁹.

Po drugem odstavku je obdelava posebnih vrst osebnih podatkov dovoljena le v primerih iz točk c) (je obdelava osebnih podatkov nujno potrebna za varovanje življenja ali telesa ali zdravja posameznika, na katerega se osebni podatki nanašajo, ali druge osebe, kadar posameznik, na katerega se osebni podatki nanašajo, fizično ali poslovno ni sposoben dati svoje privolitve iz a) točke prvega odstavka 12. člena ZVOP-2), d) (je posameznik, na katerega se nanašajo občutljivi osebni podatki, te javno objavil, brez očitnega ali izrecnega namena, da omeji namen obdelave osebnih podatkov), i) (tako določa drug zakon zaradi izvrševanja bistvenega javnega interesa, kar mora biti sorazmerno z zastavljenim ciljem, spoštovati bistvo pravice do varstva podatkov ter zagotavljati ustrezne in posebne ukrepe za varstvo človekovih pravic in temeljnih svoboščin ali interesov posameznika, na katerega se nanašajo osebni podatki) in j) (tako določajo zakoni, ki urejajo izvajanje obveščevalnih in protiobveščevalnih dejavnosti države¹¹⁰) iz prvega odstavka 12. člena ZVOP-2.

K 89. členu:

¹⁰⁹ Uradni list RS, št. 109/12, 110/13, 40/14 – ZIN-B, 54/14 – odl. US, 81/15 in 40/17.

¹¹⁰ Zakon o Slovenski obveščevalno-varnostni agenciji (Uradni list RS, št. 81/06 – uradno prečiščeno besedilo) in 32.-34. ter 36. člen Zakona o obrambi (Uradni list RS, št. 103/04 – uradno prečiščeno besedilo in 95/15).

V 89. členu ZVOP-2 so določene posebne določbe o obdelavi osebnih podatkov za druge namene ter prenos osebnih podatkov. Po prvem odstavku je obdelava osebnih podatkov po določbah tega dela zakona s strani istega ali drugega upravljavca in za drug namen obdelave od tistega, za katerega so bili podatki pridobljeni, je dovoljena le, če ta drug namen spada na področje iz 85. člena ZVOP-2 ter izpolnjuje pogoje iz 87. in 88. člena ZVOP-2. Prenos, posredovanje ali čezmejna obdelava osebnih podatkov, obdelanih skladno z določbami tega dela, za namen, ki ni naveden v 85. členu tega zakona, je dovoljeno le, če je to izrecno določeno v zakonu (zakon, obvezujoča mednarodna pogodba ali pravni akt ali odločitev Evropske unije, ki sta enakovredna zakonu in se v Republiki Sloveniji uporabljata neposredno) ter je uporabnik po svojih predpisih pooblaščen za obdelavo teh osebnih podatkov za ta drug namen.

Po tretjem odstavku mora v primeru, če za obdelavo osebnih podatkov veljajo posebni pogoji, mora pristojni pošiljatelj uporabnika osebnih podatkov obvestiti o teh pogojih in o tem, da jih je treba upoštevati. Pri čezmejni obdelavi uporabnikom v druge države članice Evropske unije ali v ustanove in druge organe, vzpostavljene skladno s 4. in 5. poglavjem V. naslova Pogodbe o delovanju Evropske unije, se ne smejo uveljavljati pogoji, ki za ustrezni prenos podatkov ne veljajo tudi v Republiki Sloveniji.

K 90. členu:

Predlagani 90. člen ZVOP-2 določa posebne pogoje za avtomatizirano odločanje v posameznem primeru. Po prvem odstavku so odločitve, ki temeljijo izključno na avtomatizirani obdelavi, vključno z oblikovanjem profilov (obdelava osebnih podatkov z uporabo profiliranja), ki imajo negativne pravne posledice za posameznika, na katerega se podatki nanašajo, oziroma lahko v večji meri vplivajo nanj, dovoljene le, če so izrecno določeno v zakonski podlagi (zakon, obvezujoča mednarodna pogodba ali pravni akt ali odločitev Evropske unije, ki sta enakovredna zakonu in se v Republiki Sloveniji uporabljata neposredno). Po drugem odstavku lahko odločitve iz prvega odstavka v skladu z 85. členom ZVOP-2 izjemoma temeljijo na posebnih vrstah osebnih podatkov samo, če so bili sprejeti posebni ustrezni ukrepi za varstvo človekovih pravic in temeljnih svoboščin ter upravičenih interesov posameznika, na katerega se nanašajo osebni podatki. Odločitve, ki bi lahko vodile do diskriminacije posameznika, na katerega se nanašajo osebni podatki, ali njemu bližnjih oseb, so prepovedane.

K 91. členu:

V 91. členu se urejajo splošna pravila glede pravic posameznika, na katerega se nanašajo osebni podatki. Po prvem odstavku mora upravljavec posamezniku, na katerega se nanašajo osebni podatki, posredovati informacije in sporočila, v skladu z 92. do 94. členom ZVOP-2, ki se nanašajo na obdelavo osebnih podatkov, podajati v čim bolj točni, razumljivi in lahko dostopni obliki ter v jasnem in preprostem jeziku, če to posameznik zahteva. Informacije in sporočila se posredujejo v posamezniku ustrezni obliki. Po drugem odstavku mora upravljavec posamezniku, na katerega se nanašajo osebni podatki, olajšati uveljavljanje njegovih pravic iz 92. do 94. člena ZVOP-2 (pač vzpostaviti ustrezno prakso glede na zahteve prvega odstavka tega člena). Po tretjem odstavku mora upravljavec posameznika, na katerega se nanašajo osebni podatki, v roku petih delovnih dni po prejemu zahtevka, pisno obvestiti o stanju obravnave zahtevka (npr. da ga preučuje pooblaščen oseba, da bo zahtev ek odstopljen, da bo predvidoma odločeno v roku... dni). Po četrtem odstavku mora upravljavec posamezniku, na katerega se nanašajo podatki, informacije o ukrepih, ki so bili na podlagi zahtevka sprejeti, zagotoviti čimprej, najpozneje pa v enem mesecu od vložitve zahtevka. Ta rok se lahko podaljša za dva meseca, če je to potrebno zaradi zapletenosti zahtevka ali števila zahtevkov. Upravljavec mora posameznika, na katerega se nanašajo podatki, v enem mesecu od vložitve zahtevka obvestiti o podaljšanju roka in ob tem navesti razloge za zamudo. Če posameznik, na katerega se podatki nanašajo, zahtevo predloži elektronsko, mora biti po možnosti obveščen po isti elektronski poti, če ne navede drugega kontaktnega naslova. Po petem odstavku v primeru, če upravljavec ne odgovori na zahtevo posameznika, na katerega se podatki nanašajo ali ne ukrepa

drugače in o tem obvesti posameznika, mora posameznika, na katerega se podatki nanašajo, brez zavlačevanja, najpozneje pa v enem mesecu od vložitve zahtevka obvestiti o razlogih za to ter o možnosti vložitve pritožbe pri Informacijskem pooblaščenca, navesti kontaktne podatke Informacijskega pooblaščenca ter navesti možnosti za uveljavljanju pravice do pravnega sredstva. Po šestem odstavku morajo biti informacije iz 92. člena ZVOP-2 ter vsa sporočila in ukrepi v skladu s 93. in 94. členom ZVOP-2 zagotovljeni brezplačno. Pri očitno neutemeljenih ali pretiranih zahtevah posameznika, na katerega se podatki nanašajo, zlasti če se zahteve pogosto ponavljajo (elementi šikanoznosti), lahko upravljavec s posebno obrazložitvijo odkloni ukrepanje na podlagi zahtevka, obrazložitev pa mora vsebovati vsaj povzetek razlogov glede očitne neutemeljenosti ali pretirano narave zahtevka. Po sedmem odstavku lahko upravljavec zaradi potrditve identitete posameznika, na katerega se nanašajo osebni podatki, ki je v skladu z 93. ali 94. členom tega zakona vložil zahtevek, zahteva tudi dodatne potrebne informacije (če posameznika npr. ne pozna glede na stalnost obravnavanja/sodelovanja) od posameznika, kar vključuje glede na konkretne okoliščine zadeve poleg osebnega imena tudi navedbo datuma rojstva oziroma navedbo enotne matične številke občana, zahtevek pa mora biti podpisan lastnoročno (če je v papirnati obliki) ali v elektronski obliki z ustreznim digitalnim potrdilom (uporabljen splošna formulacija glede na to, da še niso v celoti sprejete odločitve glede ustrezne izvedbe E-IDAS Uredbe). Po osmem odstavku se v primerih iz četrtega odstavka 92. člena, tretjega odstavka 93. člena in četrtega odstavka 94. člena ZVOP-2 posluje tako, da ima posameznik, na katerega se podatki nanašajo, pravico, da zahteva preverjanje zakonitosti zadevne omejitve njegovih pravic s strani Informacijskega pooblaščenca. Upravljavec pa mora posameznika, na katerega se nanašajo osebni podatki, izrecno poučiti o tej pravici. Po devetem odstavku mora v primeru, če se uveljavlja pravica, navedena v osmem odstavku, Informacijski pooblaščenec posameznika, na katerega se osebni podatki nanašajo, ne glede na določbe 94. člena tega zakona, obvestiti vsaj o tem, da so bila izvedena vsa potrebna preverjanja ali da je preverjanje izvedel Informacijski pooblaščenec. Poleg tega mora Informacijski pooblaščenec posameznika, na katerega se nanašajo osebni podatki, obvestiti o njegovi pravici do uporabe sodnega varstva po 28. členu tega zakona.

K 92. členu:

V 92. členu ZVOP-2 je urejeno področje dajanja informacij posamezniku, na katerega se nanašajo osebni podatki. Uvodno besedilo prvega odstavka določa, da se informacije zagotovi na zahtevo posameznika. Zagotoviti je treba najmanj:

1. naziv in kontaktne podatke upravljavca;
2. po potrebi tudi kontaktne podatke pooblaščenih oseb (glede na konkretne okoliščine zadeve ali zahtevka);
3. navedbo namenov, v katere bodo osebni podatki obdelani;
4. obstoj pravice do vložitve prijave pri Informacijskem pooblaščenca ter kontaktne podatke Informacijskega pooblaščenca;
5. navesti obstoj pravice dostopa do vsebine osebnih podatkov in do tega, da upravljavec popravi ali izbriše podatke ali omeji obdelavo podatkov posameznika, na katerega se osebni podatki nanašajo.

Po drugem odstavku mora poleg informacij iz prvega odstavka upravljavec posamezniku, na katerega se nanašajo podatki, v posebnih primerih na njegovo zahtevo po prvem odstavku zagotoviti tudi določene (navedene) dodatne informacije, da lahko s tem omogoči izvajanje pravic tega posameznika:

1. pravno podlago obdelave;
2. rok hrambe osebnih podatkov ali, če to izjemoma ni možno, merila za določitev tega roka v skladu z 41. členom tega zakona;

3. po potrebi navesti kategorije uporabnikov osebnih podatkov, tudi uporabnikov v tretjih državah in mednarodnih organizacijah;

4. po potrebi druge informacije, zlasti če so bili osebni podatki pridobljeni brez vednosti posameznika, na katerega se nanašajo.

Po tretjem odstavku se v primeru, če so bili osebni podatki pridobljeni neposredno od posameznika, na katerega se nanašajo, je treba temu posamezniku, ob poizvedbi predložiti informacije v skladu z določbami prvega in drugega odstavka tega člena. Informacije iz prvega in drugega odstavka se ne podajo, če so bili osebni podatki pridobljeni s prenosom podatkov iz drugih področij nalog istega upravljavca ali iz uporabe zbirk drugega upravljavca in je ta obdelava podatkov zakonsko določena. Po četrtem odstavku se lahko obveščanje posameznika, na katerega se osebni podatki nanašajo, v skladu s tretjim odstavkom opusti ali delno ali začasno omeji, če in dokler je to v posameznem primeru očitno sorazmerno ali posebej določeno v drugem zakonu, za te primere (namene):

1. da se onemogoči oviranje preprečevanja, preiskovanja, odkrivanja ali pregona kaznivih dejanj ali prekrškov, izvrševanja nalog in pooblastil policije, izvrševanja kazenskih sankcij, vključno s pridobivanjem ali prenosi osebnih podatkov za še nedokončane uradne postopke po tej točki;

2. zaradi zagotavljanja, da niso ovirani drugi uradni postopki, povezani s prejšnjo točko;

3. zaradi varnosti države;

4. zaradi varstva obrambe države;

5. zaradi varstva človekovih pravic in temeljnih svoboščin tretjih oseb.

K 93. členu:

V 93. členu so določene posebne seznanitvene pravice posameznika, na katerega se nanašajo osebni podatki, do pridobitve posebnih informacij o vsebini teh podatkov. Po drugem odstavku za pridobitev informacij iz prvega odstavka veljajo roki po določbah člena 12 Splošne uredbe. Omejitve pravice do pridobitve informacij so dovoljene le pod pogoji, navedenimi v četrtem odstavku 92. člena ZVOP-2.

Nato je v tretjem odstavku določeno, da v primeru neizdaje informacij v skladu z drugim odstavkom mora upravljavec posameznika, na katerega se nanašajo podatki, nemudoma pisno obvestiti o zavrnitvi ali omejitvi informacij in razlogih, na katerih to temelji. Ta določba se ne uporablja, če je zagotovitev teh informacij v nasprotju z enim od namenov iz četrtega odstavka 92. člena ZVOP-2. Upravljavec mora posameznika, na katerega se nanašajo podatki, obvestiti o možnosti vložitve pritožbe na organ za varstvo podatkov. Po četrtem odstavku mora upravljavec dokumentirati razloge za odločitev o neizdaji informacij v skladu z drugim odstavkom. Ti podatki morajo biti dostopni Informacijskemu pooblaščenču in pooblašчени osebi. Po petem odstavku se v obsegu, v katerem ima posameznik, na katerega se nanašajo osebni podatki, v drugem zakonu določeno zakonsko pravico do vpogleda v njegove osebne podatke, ki se obdelujejo, pravico pridobiti informacije v skladu z določbami tega drugega zakona, ki urejajo pravico do vpogleda (navedeni drugi področni zakon torej prevlada – npr. Zakon o nalogah in pooblastilih policije).

K 94. členu:

V 94. členu je ločeno (področno) urejena pravica do popravka ali izbrisa osebnih podatkov in do omejitve obdelave. Po prvem odstavku ima vsak posameznik, na katerega se nanašajo osebni podatki, pravico, da od upravljavca zahteva takojšnji popravek svojih netočnih osebnih podatkov in dopolnitev nepopolnih ali neposodobljenih osebnih podatkov. Popravek ali dopolnitev se lahko po potrebi izvede z dodatno priloženo izjavo ali posebnim uradnim zaznamkom, če je naknadna

sprememba nezdržljiva z namenom dokumentiranja glede na fazo določenega postopka (podatkov se torej ne spremeni, ampak se jim le priloži uradni zaznamek o izjavi). Upravljavec je dolžan dokazati točnost ali posodobljenost osebnih podatkov, če osebni podatki niso bili pridobljeni izključno na podlagi navedb posameznika, na katerega se podatki nanašajo. Po drugem odstavku mora upravljavec osebne podatke nemudoma izbrisati na lastno pobudo ali na podlagi zahtevka posameznika, na katerega se podatki nanašajo, če:

1. osebni podatki niso več potrebni za namene, za katere so bili pridobljeni ali drugače obdelani;
2. so bili osebni podatki obdelani nezakonito ali
3. je izbris osebnih podatkov potreben zaradi izpolnitve druge obveznosti po zakonu ali po pravnomočni sodni odločbi (npr. pravnomočna oprostilna kazenska sodba). Po tretjem odstavku lahko namesto izbrisa osebnih podatkov upravljavec njihovo obdelavo omeji, če:
 1. posameznik, na katerega se podatki nanašajo, izpodbija točnost ali posodobljenost osebnih podatkov in pravilnosti ali nepravilnosti ni mogoče ugotoviti, vendar mora posameznika, na katerega se nanašajo osebni podatki, obvestiti pred razveljavitvijo omejitve, ali
 2. je treba osebne podatke še nadalje hraniti za dokazne namene v okviru izvajanja zakonsko določene naloge.

Po četrtem odstavku mora upravljavec posameznika, na katerega se nanašajo osebni podatki, pisno obvestiti o zavrnitvi popravka ali izbrisa osebnih podatkov ali o omejitvi obdelave in o razlogih za zavrnitev. Upravljavec mora posameznika, na katerega se nanašajo podatki, obvestiti o možnosti vložitve prijave Informacijskemu pooblaščenču in o njegovih kontaktnih podatkih. Po petem odstavku mora upravljavec morebitni popravek nepravilnih osebnih podatkov sporočiti pristojnemu organu, ki mu je prenesel ali drugače poslal (čezmejna obdelava, posredovanje) te osebne podatke. Po šestem odstavku se v primerih popravka, izbrisa podatkov ali omejitve obdelave po prvem do tretjem odstavku mora upravljavec o tem obvestiti vse uporabnike osebnih podatkov. Uporabniki so zavezani osebne podatke, ki so v njihovi pristojnosti, nemudoma popraviti, izbrisati, ustrezno označiti ali omejiti njihovo obdelavo. Po sedmem odstavku se za druga vprašanja smiselno uporablja člen 12 Splošne uredbe (Pregledne informacije, sporočila in načini za uresničevanje pravic posameznika, na katerega se nanašajo osebni podatki), npr. zaračunavanje razumne pristojbine pod pogoji iz tega člena.

10. K X. delu Predloga ZVOP-2:

X. del Predloga ZVOP-2 ureja določene pomembne področne ureditve obdelav in varstva osebnih podatkov, podobno kot je bilo dosedaj določeno v VI. delu ZVOP-1.

K 95. členu:

Predlagani 95. člen ZVOP-2 ureja pravice in dolžnosti upravljavca na področju neposrednega trženja, kar je posebna (področna obdelava v druge namene v zvezi z upravičenimi interesi upravljavca) - glede na možnosti iz zadnjega stavka uvodne navedbe št. 47, ki je načeloma opcиска («Obdelava osebnih podatkov za neposredno trženje se lahko šteje za opravljeno v upravičenem interesu.»). Drugi odstavek pa ne vsebuje (ne omogoča obdelave) osebnih podatkov s področja kazenskih obsodb in kaznovanj za prekrške (glejte 13. člen ZVOP-2). Predlagani člen je načeloma enak kot določbe dosedanjega 72. člena ZVOP-1 (z navedeno izjemo osebnih podatkov iz 13. člena ZVOP-2), s tem da so določeni izrazi usklajeni z izrazoslovjem Splošne uredbe.

Ureditev v besedilu v skladu z navedenimi pravnimi podlagami določa ti. »*soft opt-in*«, izhaja namreč iz dejstva, da če se je zakonito opravljala dejavnost, zlasti da je bila zakonito opravljena določena

storitev, so se v njenem okviru zakonito pridobili in obdelali osebni podatki na podlagi privolitve, posebne privolitve ali pogodbe (torej neposredno od posameznika, na katerega se nanašajo osebni podatki) in upošteva spremenjen (močnejši) koncept privolitve, kot ga določa 11. točka člena 4 Splošne uredbe in tudi kot je navedeno tudi v skladu z zavezujočimi določbami člena 4 Splošne uredbe v 11. točki prvega odstavka 6. člena ZVOP-2. Zato gre v osnovi za ti. »*soft opt-in*«, kjer pa ima posameznik, na katerega se nanašajo osebni podatki, možnost, da poda ugovor po 96. členu ZVOP-2 in se njegovi osebni podatki ne morejo več obdelovati (»*opt-out*«).

Urejanje pravne podlage za neposredno trženje v Predlogu ZVOP-2 je predlagano zaradi zagotovitve pravne varnosti (in poslovne varnosti), saj utegnejo biti razlike glede obravnavanja tega področja med državami članicami (prej navedena odprta določba uvodne navedbe št. 47). Ta zakonodajna odločitev pa ne pomeni, da je možnost uporabe (ali reguliranja) upravičenega interesa iz (f) točke prvega odstavka člena 6 Splošne uredbe izčrpana.

V tretjem odstavku so navedene pravice, ki jih lahko posameznik uveljavlja glede obdelave osebnih podatkov s področja neposrednega trženja, od informiranja o obdelavi osebnih podatkov, do sporočanja o kršitvah varstva osebnih podatkov, vključno s pravico do ugovora, katera je postopkovno nadalje urejena v 96. členu ZVOP-2.

K 96. členu:

Predlagani 96. člen določa posebno pravico do ugovora ozir. prekinitve dogovorjenega dela od upravljavca glede njegovih osebnih podatkov, ki se obdelujejo za namene neposrednega trženja. Enak člen je vsebovan v določbah dosedanjega 73. člena ZVOP-1. Po vsebini gre za »*opt-out*« določbo.

K 97. členu:

S 97. členom se začne posebno (drugo) poglavje X. dela Predloga ZVOP-2. V njem se urejajo splošne določbe o videonadzoru in obdelavi osebnih podatkov. Člen je pretežno enak določbam dosedanjega 74. člena ZVOP-1, z določenimi dodatnimi rešitvami (pravno-tehnična definicija videonadzora v prvem odstavku, trimesečni rok v sedmem odstavku).

K 98. členu:

Predlagani 98. člen določa uporabo videonadzora glede dostopa v uradne službene oziroma poslovne prostore. Gre za vsebino dosedanjega 95. člena ZVOP-1.

K 99. členu:

V 99. členu je urejen videonadzor v zvezi z večstanovanjskimi stavbami, podrobno kot je to določeno v dosedanjem 76. členu ZVOP-1. Tretji odstavek posebej poudarja pomen (pisne) privolitve, četrti in peti odstavek definirata za ta kontekst posebej kdo je upravljavec, osmi odstavek pa določa, da je izjemoma dovoljeno omogočiti združitev videonadzornega sistema z napravami, ki jih uporabljajo lastniki za potrebe vstopa v večstanovanjsko stavbo, kot sta na primer domofon ali video domofon, razen če te naprave omogočajo snemanje ali spremljanje dogajanja v območju izvajanja videonadzora na posamezni napravi. Spremljanje dogajanja v območju izvajanja videonadzora mora onemogočiti upravljavec videonadzora. V sedmem odstavku prepovedi videonadzora glede hišniškega stanovanja ter delavnice za hišnika ni dodana tudi prepoved videonadzora prostorov za čistilke in čistilce, saj v tem primeru ne gre za znatno polje utemeljenega pričakovanja zasebnosti, niti ne obstaja ustrežna

pravna ureditev prostorov za čistilke ali čistilce¹¹¹. Vendar to z vidika splošnega načela sorazmernosti ne preprečuje, da se pri oceni učinkov po 37. členu ZVOP-2 oceni, da ni primerno uporabiti videonadzornega sistema v zvezi s prostori za čistilke ali čistilce.

K 100. členu:

V predlaganem 100. členu ZVOP-2 je urejen videonadzor glede delovnih prostorov, gre za nekoliko drugačno ureditev glede vstopov v uradne službene oziroma poslovne prostore v 98. členu predloga ZVOP-2, tukaj gre namreč za snemanje znotraj delovnih prostorov. Člen je pretežno enak 77. členu dosedanjega ZVOP-1, s tem da je tretji odstavek dodal, da je spremljanje neposrednega dogajanja pred kamerami pod pogoji iz prvega in drugega odstavka 100. člena ZVOP-2 dopustno le, če ga izvaja pooblaščen varnostno osebje. Posebna dodana vrednost je v petem odstavku, kjer je določeno, da se mora pred uvedbo videonadzora v osebi javnega ali zasebnega sektorja delodajalec posvetovati z reprezentativnimi sindikati pri delodajalcu ter svetom delavcev ali delavskim zaupnikom (dosedaj je bilo to določeno le glede reprezentativnih sindikatov pri delodajalcu), kar je »jamštveni« prispevek k dodatnemu spoštovanju človeškega dostojanstva z uporabo mehanizmov participacije s področja socialne države (2. člen Ustave Republike Slovenije).

V sedmem odstavku je na podoben način kot pri videonadzoru in večstanovanjskih stavbah (99. člen) določen tudi način uvedbe videonadzora v poslovnih zgradbah, kjer je lahko več lastnikov.

K 101. členu:

V 101. členu je urejena nova vrsta videonadzora, namreč izvajanje videonadzora na javnih površinah, kar dosedaj ni bilo urejeno v ZVOP-1. Določbe so načeloma previdno in sorazmerno napisane, upoštevajo delno dejansko stanje, njihov namen pa ni podpiranje ali promocija ali razvoj ti. »totalne nadzorovalne družbe«. Po prvem odstavku je videonadzor na javnih površinah dovoljen le v izjemnih primerih, kadar je to nujno potrebno, ker obstaja resna in utemeljena nevarnost za življenje ali zdravje ljudi, varnost premoženja ali varovanje tajnih podatkov in tega namena ni mogoče doseči z milejšimi sredstvi (prvi strogi kriterij/skupek pogojev kumulativne narave). Prav tako je dovoljen za potrebe varovanja prostorov, zgradb ali območij, ki jih je potrebno varovati na podlagi zakona in sicer samo v obsegu in trajanju, ki je za dosego teh namenov nujno potreben (drugi in nekoliko milejši kumulativni kriterij). Po drugem odstavku se videonadzor lahko izvaja le glede tistih delov javne površine in v obsegu, kjer je potrebno varovati interese iz prvega odstavka 101. člena ZVOP-2. V tretjem odstavku je podana še organizacijska omejitev, po kateri lahko videonadzor na javnih površinah izvaja le oseba javnega ali zasebnega sektorja, ki upravlja z javno površino ali na njej zakonito opravlja dejavnost.

K 102. členu:

V 102. členu se začne 3. poglavje X. dela Predloga ZVOP-2 – urejanje biometrije oziroma biometričnih ukrepov. Kot že v ZVOP-1, je zakonodajni pristop glede biometrije dokaj zadržan in garantističen, kar pomeni – načeloma nenaklonjen uporabi biometrije. Ne glede na navedeno predlagane rešitve nekoliko omogočajo širšo uporabo biometrije (za zasebni sektor), kot je to dosedaj bila urejena v ZVOP-1.

99. člen ureja biometrične ukrepe v javnem sektorju. Biometrične ukrepe v javnem sektorju se lahko določi le z zakonom, če je to nujno potrebno za varnost ljudi ali premoženja ali za (dodatno) identifikacijo pogrešanih ali umrlih posameznikov ter poslovne skrivnosti, tega namena pa ni možno doseči z milejšimi sredstvi (načelo sorazmernosti). Po izjemi v drugem odstavku se ne glede na

¹¹¹ Glejte npr. prvi odstavek 5. člena Stanovanjskega zakona (Uradni list RS, št. 69/03, 18/04 – ZVKSES, 47/06 – ZEN, 45/08 – ZVEtL, 57/08, 62/10 – ZUPJS, 56/11 – odl. US, 87/11, 40/12 – ZUJF, 14/17 – odl. US in 27/17) o hišniških stanovanjih in delavnicah za hišnike.

prejšnji odstavek biometrične ukrepe lahko določi z zakonom, če gre za izpolnjevanje obveznosti iz obvezujoče mednarodne pogodbe ali za identifikacijo posameznikov pri prehajanju državnih meja. Predlagani člen ima določen tudi prekršek za kršitve v 125. členu ZVOP-2.

K 103. členu:

V predlaganem 103. členu se urejajo biometrični ukrepi v zasebnem sektorju. Po prvem odstavku lahko zasebni sektor izvaja biometrične ukrepe le, če so nujno potrebni za opravljanje dejavnosti, za varnost ljudi ali premoženja ali za varovanje tajnih podatkov ali poslovne skrivnosti v skladu z določbami tega člena. Po drugem odstavku sme biometrične ukrepe izvajati nad svojimi zaposlenimi ter nad tistimi osebami, ki so zaposlene pri pogodbenih partnerjih upravljavca, če je to potrebno za namene varovanja interesov iz prvega odstavka in so bili te osebe o tem predhodno pisno obveščene. Po tretjem odstavku zasebni sektor lahko izvaja biometrične ukrepe tudi nad svojimi strankami pod naslednjimi pogoji:, da tako za namene varovanja interesov iz prvega odstavka določa zakon in so stranke podale pisno privolitev ter se na ta način preprečuje nastanek hude škode, kar je pomembna izjema od strogega pristopa k dovoljeni uporabi biometrije. V četrtem odstavku je kot varovalni organizacijski ukrep določeno da mora upravljavec osebnih podatkov, ki namerava izvajati biometrične ukrepe, še pred uvedbo ukrepov posredovati Informacijskemu pooblaščenцу opis nameravanih ukrepov in razloge za njihovo uvedbo. V petem odstavku je določeno, da je Informacijski pooblaščenec dolžan po prejemu posredovanih informacij iz četrtega odstavka dolžan v dveh mesecih odločiti, ali je nameravana uvedba biometričnih ukrepov v skladu s tem zakonom, predvsem s pogoji iz prvega stavka prvega odstavka tega člena. Rok se ob upoštevanju zapletenosti predvidene obdelave lahko podaljša za največ dva meseca. Po šestem odstavku sme upravljavec osebnih podatkov izvajati biometrične ukrepe šele po prejemu odločbe iz petega odstavka, s katero je izvajanje biometričnih ukrepov dovoljeno. Po sedmem odstavku zoper odločbo Informacijskega pooblaščenca iz petega odstavka tega člena ni pritožbe, dovoljen pa je upravni spor. V osmem odstavku je določena večja izjema, po kateri upravljavcu izjemoma ni treba pridobiti odločbe iz petega odstavka tega člena, če pri izvajanju biometričnih ukrepov ne nastaja zbirka biometričnih značilnosti ali matematičnih pretvorb biometričnih značilnosti in so te vedno pod nadzorom posameznika. Po devetem odstavku mora upravljavec pred začetkom uporabe biometričnih ukrepov posamezniku, nad katerim se bodo izvajali ti ukrepi, predložiti splošno obvestilo o zakonski ureditvi izvajanja biometričnih ukrepov, ki ga izdela in na svoji spletni strani objavi Informacijski pooblaščenec.

Predlagani člen ima določen tudi prekršek za kršitve v 126. členu ZVOP-2.

K 104. členu:

Predlagani 104. člen določa posebno prepoved glede uporabe biometrije za zasebni sektor. Predlagano je, da zasebni sektor ne sme zahtevati, pridobiti ali nadalje obdelovati osebnih podatkov v zamenjavo za določene storitve, pa četudi so te storitve (npr. storitve informacijske družbe) brezplačne. Za javni sektor ni dane izrecne prepovedi v posebnem členu, saj predlagatelj ocenjuje, da je z vidika (vsaj) 34. in 38. člena Ustave Republike Slovenije nepredstavljivo, da bi javni sektor (pa četudi bi to vprašanje morda vseeno poskusil urediti v zakonu) lahko zahteval biometrične podatke od ljudi za določene komercialne (trženjske) storitve. Drugače seveda velja (je dopustno), ko gre za vprašanje izpolnjevanja zakonskih obveznosti (npr. s področja državne uprave – 120. člen Ustave Republike Slovenije) – dajanje fotografij za osebne dokumente ipd.

Določen je tudi ustrezen prekršek v 127. členu ZVOP-2.

Predlagana ureditev v tem členu ne pomeni, da je podana sistemska opredelitev glede vprašanja zamenjave osebnih podatkov za določene (četudi brezplačne) storitve - za področja varstva in obdelave osebnih podatkov. O teh vprašanjih se bo odločalo na podlagi splošnih pravil ZVOP-2 in Splošne uredbe (sorazmernost, poštenost, namenska obdelava...).

K 105. členu:

V 105. členu Predloga ZVOP-2 je določena obdelava osebnih podatkov v okviru evidentiranja vstopov in izstopov iz službenih prostorov, podobno kot je to že urejeno v 82. členu ZVOP-1. Po prvem odstavku oseba javnega ali zasebnega sektorja lahko za zagotavljanje varnosti ljudi in premoženja, ter reda v njenih prostorih ali v prostorih, ki jih ima v uporabi od posameznika, ki namerava vstopiti ali izstopiti iz tega prostora, zahteva, da navede vse ali nekatere osebne podatke iz drugega odstavka tega člena ter razlog vstopa ali izstopa. Po potrebi pa lahko osebne podatke preveri tudi z vpogledom v osebni dokument posameznika. Po drugem odstavku se v zbirki o vstopih in izstopih iz službenih prostorov lahko o posamezniku vodijo samo naslednji osebni podatki, kadar je to potrebno: osebno ime, številka in vrsta osebnega dokumenta, naslov prebivališča, zaposlitev, vrsta in registrska številka vozila ter datum, ura in razlog vstopa ali izstopa v ali iz prostorov. Po tretjem odstavku evidenca iz prejšnjega odstavka velja za uradno evidenco v skladu z Zakonom o splošnem upravnem postopku (drugi odstavek 179. člena), če je potrebno pridobiti podatke iz nje z vidika koristi mladoletnika ali za izvrševanje pristojnosti policije ter obveščevalno-varnostne dejavnosti. Po četrtem odstavku se osebni podatki iz evidence iz drugega odstavka tega člena se lahko hranijo največ tri leta (rok hrambe) od vpisa, nato se zbrišejo ali na drug način uničijo, če zakon ne določa drugače.

Predlagani člen ima določen tudi prekršek za kršitve v 128. členu ZVOP-2.

K 106. členu:

V 106. členu je določeno, da se lahko osebni podatki iz javne knjige, urejene z zakonom (npr. zemljiška knjiga), uporabljajo le v skladu z namenom¹¹², za katerega so bili zbrani ali se obdelujejo, če je zakoniti namen njihovega zbiranja ali obdelave določen ali določljiv (se da na njega iz vsebine zakona sklepati tako, da je določljiv – npr. varnost pravnega prometa, izkazovanje pravnih ali osebnih stanj ipd.). S tem členom je povezana tudi prekrškovna določba v 129. členu ZVOP-2.

K 107. členu

Posebno pravno urejanje povezovanja pomeni, da je sprejet pristop proti ti. »slučajnemu« nastanku/omogočanju »totalne nadzorovalne družbe« (ki v situacijah, ki niso izredno ali vojno stanje, niso dopustne, pa še takrat so dopustne le v skladu z načelom sorazmernosti in ne smejo pripeljati do »popolne« totalne nadzorovalne družbe). Ta pristop izhaja iz francoske »afere SAFARI« iz leta 1974¹¹³, ko so se v Francoski republiki izvrševale zakonodajne priprave, da se preko povezovanj množice informatiziranih zbirk osebnih podatkov doseže nastanek ene (centralne; centralizirane) zbirke osebnih podatkov (v smislu uradne evidence), za povezovanje pa bi se uporabila takratna francoska enotna matična številka občana (INSEE koda). S predlaganim pristopom glede povezovanja pa so delno povezana tudi definicija povezovalnega znaka v 4. točki tretjega odstavka 6. člena ter druga pravila po ZVOP-2 glede njegove uporabe (42. člen ZVOP-2).

Predlagani 107. člen tako ureja povezovanje uradnih evidenc oziroma javnih knjig med seboj oziroma z drugimi zbirkami osebnih podatkov. Ureditev je pretežno podobna kot že po dosedanjem zakonu, in sicer v tem, da zahteva, da bolj tvegana in obsežna povezovanja posebej odobrita najprej zakonodajalec (na načelni ravni) in potem (glede načina izvedbe) še Informacijski pooblaščenec.

¹¹² Glejte: odločba US, št. U-I-98/11, 26. 9. 2012, zlasti 17. točka in opomba št. 10; objava: Uradni list RS, št. 79/12.

¹¹³ Afero je razkril in kritiziral dnevnik Le Monde, Boucher, Philippe, *SAFARI ou la chasse aux Français*, 21. 3. 1974.

Razlog za tako strogo ureditev dostopa do uradnih evidenc oziroma javnih knjig v večjem obsegu je v posebnih tveganjih, ki bi pri tem lahko postala. Uradne evidence hranijo podatke, ki so pomembni za uveljavljanje pravic in pravnih koristi posameznikov, oziroma ki vsebujejo točne, ažurne in uradne podatke o posamezniku. Neupravičen dostop do njih, neupravičeno razkritje njih, oziroma njihova zloraba bi zatorej lahko imela znatne posledice za posameznika. Zato mora biti dostop, ki je po obsegu ali naravi tveganj zahtevnejše narave, ustrezno odobren in preverjen. Tovrstne tvegane situacije povezovanja zbirk osebnih podatkov lahko nastanejo zlasti, ko so zbirke osebnih podatkov medsebojno tehnološko tako povezane, da lahko uporabnik podatkov pri delu v svojem informacijskem okolju z enostavno poizvedbo (npr. z vnosom povezovalnih znakov/enoličnih identifikatorjev, kot je npr. enotna matična številka občana - EMŠO), pridobi osebne podatke posameznika iz večjega števila medsebojno povezanih zbirk (primer obsežnega povezovanja je sistem eSociala, ki povezuje 44 zbirk osebnih podatkov). Takšna enostavna dostopnost velikega obsega osebnih podatkov pomeni veliko razgaljenost posameznika in s tem veliko moč odločanja o posamezniku ter zaradi centralizacije večje možnosti zlorab (povišana tveganja za notranjo in zunanjo nenamensko uporabo, okrepljeni motivi za vdor v informacijski sistem, pridobitev velike količine podatkov idr.) ter tudi nevarnost profiliranja – kar očitno terja ustrezno stroge varovalke na drugi strani. Povezovanje je lahko izvedeno samodejno (npr. da informacijski sistemi medsebojno čez noč posodablajo osebne podatke ob spremembah kot v primeru Centralnega registra prebivalstva) ali pa na zahtevo uporabnika (primer eSociala, kjer sistem na zahtevo uporabnika z uporabo različnih centralnih gradnikov pridobi osebne podatke posameznika iz 44 zbirk) – posledice so za posameznika iste, v praksi pa celo več povezovanja poteka na zahtevo. Prav tako z vidika tveganj ni razlike, ali se podatki združijo šele pri uporabniku ali na kakšnem mestu pred njim (primer rešitve ti. »Pladenj«).

Definicija uradnih evidenc in javnih knjig je določena v drugem odstavku 179. člena Zakona o splošnem upravnem postopku. Definicija povezovanja le-teh oziroma drugih zbirk je določena v tretjem odstavku predlaganega člena, in to na način, ki je tehnološko nevtralen, tj. se namesto na način povezovanja osredotoča zlasti na obseg in pogostost povezovanja, ter tveganja, ki pri tem nastajajo. Definicija je tako bolj prilagojena modernemu informacijskemu okolju oziroma spremembam, ki se pojavljajo v tem. Prav tako je določeno, da se za povezovanje šteje tudi vodenje različnih zbirk pri istem upravljavcu ali obdelovalcu, razen če so organizacijsko in tehnično ustrezno ločene, saj bi sicer kršitev pravil varstva osebnih podatkov na eni od povezanih zbirk lahko imela posledice še za ostale povezane zbirke.

Podobno visoka tveganja za pravice posameznika lahko predstavlja tudi povezovanje zbirk na strani pogodbenega obdelovalca, ki za enega ali več upravljavce po pogodbi opravlja določene obdelave. Zato se za povezovanje štejejo tudi obdelave osebnih podatkov, kadar se osebni podatki iz zbirk osebnih podatkov različnih upravljavcev ali zbirk osebnih podatkov vodenih na različnih pravnih podlagah obdelujejo pri istem obdelovalcu in ni s tehničnimi sredstvi in organizacijskimi postopki zagotovljena popolna ločitev obdelav osebnih podatkov iz različnih zbirk.

Vendar pa za povezovanje ne bi smeli šteti primerov, ko se pooblaščen uporabnik v okviru upravnega ali drugega individualnega postopka prijavi v zbirko osebnih podatkov, iz katere je pooblaščen pridobiti osebne podatke posameznika (primeri aplikacij za posamične poizvedbe v centralnih registrih, kot je e-RISK v primeru Centralnega registra prebivalstva ali e-Poizvedbe na področju zdravstvenega zavarovanja). V takšnem primeru ni povečanih tveganj za pravice in svoboščine posameznika. Ključna razlika med povezovanjem zbirk osebnih podatkov in posameznim pridobivanjem osebnih podatkov je v tem, da se posamezniku v primeru povezanih zbirk podatkov pred vsako posamično poizvedbo v zbirko podatkov ni treba posebej prijavljati v vsako zbirko osebnih podatkov.

Vse navedeno za upravljavce, ki bi želeli povezovati svoje zbirke z uradnimi evidencami ali javnimi knjigami (kar vključuje tako povezavo med samimi uradnimi evidencami, povezavo med javnimi knjigami, povezavo med evidencami in javnimi knjigami, povezavo uradnih evidenc z drugimi zbirkami, povezavo javnih knjig z drugimi zbirkami kot tudi povezavo uradnih evidenc in javnih knjig z drugimi zbirkami), nalaga določene pripravljalne obveznosti. Intenzivnost teh obveznosti je odvisna od tveganosti podatkov zbirki, s katero se želi povezovati.

Četrty odstavek se sklicuje na posebno občutljiva področja iz prvega odstavka in pomeni, da je za ta področja potrebno imeti tako določbe v področnem zakonu glede povezovanja kot tudi odločbo (dovoljenje) Informacijskega pooblaščenca. Pri tem morajo biti spoštovani pogoji iz drugega in tretjega odstavka tega člena (tudi definicija povezovanja). V primerih, ki ne spadajo v prvi odstavek, se uporabijo le določbe drugega in tretjega odstavka in ni potrebna odločba Informacijskega pooblaščenca, povezovanje pa je dopustno izvesti (ob upoštevanju tudi pogojev informacijske varnost, ki vključujejo tudi zunanjo in notranjo sledljivost po tem zakonu) že v primerih, če področni zakon določa pravico do pridobitve določenih osebnih podatkov iz uradnih evidenc ipd. .

Ker obstajajo določeni režimi povezovanja s ključnimi uradnimi evidencami ipd., ki ne zadostijo tem pogojem, je v prehodnih določbah določeno štiriletno prehodno obdobje za uskladitev z novimi pravili.

Za povezovanje z drugimi uradnimi evidencami zadostuje, da možnost pridobivanja podatkov iz njih določa zakon.

Nekaj praktičnih primerov tega, kaj se šteje za povezovanje in kaj ne:

- eSociala I/O modul in namenski spletni servisi – JE POVEZOVANJE;
- eSociala asinhroni modul (uporabnik na CSD prek ISCS2 sistema in Pladnja posreduje zahtevo bankam, banke grede po zahtevku na pladenj, vsak zahtevek obdelajo ročno in poizvedbe ne spustijo v svoj sistem, pripravijo podatke in jih čez nekaj časa odložijo na Pladenj, kjer so na voljo uporabniku na CSD-ju) – JE POVEZOVANJE;
- aplikacije e-RISK, e-Poizvedbe, eMRVL - dostop do podatkov v registru MRVL – NI POVEZOVANJE;
- informacijski sistem TIRS, ki inšpektorju omogoča, da se posebej prijavi (avtenticira) v CRP in za posamezno osebo pridobi njene podatke – NI POVEZOVANJE;
- informacijski sistem TIRS, ki inšpektorju omogoča, da v tem sistemu brez posebne prijave v CRP za določeno osebo iz CRP pridobi njene podatke ali hkrati pridobi podatke za večje število oseb– JE POVEZOVANJE;
- spletni servis, kjer se uporabnik na občini pred poizvedbo posebej avtenticira za dostop do zbirke osebnih podatkov in dobi podatke hkrati za več posameznikov – paketna poizvedba (npr. vsi, ki imajo 50 let) – JE POVEZOVANJE;
- spletni servis, kjer se uporabnik na občini pred poizvedbo posebej avtenticira za dostop do zbirke osebnih podatkov in pridobi podatke za enega posameznika (posamična poizvedba) – NI POVEZOVANJE;
- spletni servis, kjer se uporabnik na občini pred poizvedbo posebej avtenticira za dostop do zbirke osebnih podatkov hkrati za več posameznikov (oseba na občini pripravi podatke, naredi izvoz, zapeče podatke na CD ali jih odloži na neko mesto za prevzem - JE POVEZOVANJE.

K 108. členu:

V 108. členu je določena uvodna določba za posebno poglavje (7. poglavje) X. dela Predloga ZVOP-2 o strokovnem nadzoru in obdelavi osebnih podatkov. V tem poglavju so določena pravila obdelave osebnih podatkov pri opravljanju strokovnega nadzora, če področni zakoni ne določajo drugače. S predlaganim poglavjem se upošteva možnost pravne praznine na tem področju, saj veljavni področni zakoni ne vsebujejo vedno določb o obdelavi osebnih podatkov pri opravljanju strokovnega nadzora.

Predlagano poglavje je uporabno predvsem na področju socialnega varstva in zdravstva, kjer imajo npr. državni organi ali nosilci javnega pooblastila v njihovih področnih zakonih običajno določeno le pristojnost oziroma obveznost opravljanja strokovnega nadzora, ni pa tudi nujno določeno vsebinsko (materialno), kaj konkretno lahko izvajalec strokovnega nadzora pri njegovem opravljanju opravi glede dostopa do vsebine osebnih podatkov, za kar pa je treba določiti ustrezno ureditev tudi v zvezi z 8. členom Predloga ZVOP-2.

K 109. členu:

V 109. členu so ponovljene dosedanje konkretne določbe o obdelavi osebnih podatkov v okviru strokovnega nadzora, kot je to določeno že v 88. členu ZVOP-1. S tem členom so povezane prekrškovne določbe v 131. členu ZVOP-2.

K 110. členu:

V 110. členu je določeno obveščanje posameznika in dodatna obdelava osebnih podatkov, kot je to določeno v 89. členu ZVOP-1.

K 111. členu:

V 111. členu so določeni strokovni nadzor in obdelava posebnih vrst osebnih podatkov, kot je to določeno v 90. členu ZVOP-2. S tem členom so povezane prekrškovne določbe v 131. členu ZVOP-2.

K osmemu poglavju X. dela (javna objava sodnih odločb)

Pomemben element sodnega sistema je tudi načelo javnosti sojenja. Kot določa Ustava Republike Slovenije v 24. členu, so sodne obravnave javne, sodbe pa se izrekajo javno (razen v izjemah, ki jih določa zakon). Javnost je pri tem pomemben garant neodvisnosti in nepristranskosti sodišč oziroma prispeva k večji pravni predvidljivosti in pravni varnosti glede sodnega odločanja. Čeprav sodna praksa sodišč v Republiki Sloveniji ni obvezen pravni vir, pa ni mogoče zanikati njenega vpliva: je namreč pomembno orodje pri vsakdanjem delu pravnikov, saj daje jasen vpogled v pomen in uporabo veljavne zakonodaje.

Javno objavljane sodb lahko obenem še posebej nazorno pokaže, da se v sodstvu dela veliko in dobro; torej da so sodne odločitve utemeljene na celovito ugotovljenih dejstvih, pridobljene skozi zakonit in pošten sodni postopek ter pravno dobro premišljene. Pri tem je proaktivna transparentnost eno najmočnejših orodij zoper širjenje morebitnih dezinformacij in ustvarjanje napačnih mnenj; še zlasti ustvarjanja preuranjenih zaključkov na podlagi posameznih problematičnih primerov, o katerih pa se sicer največ piše in s katerimi je javnost zatorej tudi najbolj seznanjena.

Iz teh razlogov je Vrhovno sodišče Republike Slovenije že pred tridesetimi leti začelo aktivno razvijati informacijski sistem za vodenje in distribucijo sodne prakse, sprva sicer predvsem za rabo znotraj sodišč samih. Z letom 2006 pa se je na spletni strani sodišč¹¹⁴ začelo objavljati izbrano sodno prakso višjih oziroma Vrhovnega sodišča. Število letno objavljenih odločb je bilo takrat okoli 2000, z naslednjimi leti se je postopoma večalo, do nekje 5000 v letu 2016. Sproti so bile te objave prenesene na namensko spletno stran¹¹⁵, ustrezno kategorizirane, povezane na člene zakonov ter opremljene z zmogljivim in enostavno uporabljivim spletnim iskalnikom. Skozi navedena orodja je javnost dobila podroben vpogled v delo sodnih instanc v zadnjih letih, še zlasti pa v to, kako zapolnjujejo pravne standarde in kako rešujejo posamezna sporna vprašanja.

¹¹⁴ Glejte: <http://www.sodisce.si>

¹¹⁵ Glejte: <http://sodnapraksa.si/>

Čeprav so navedeni trendi izjemno pozitivni, še vedno zajemajo zgolj manjši delež sodnih odločb, ki jih slovenska sodišča izdajo vsako leto. Glavna ovira za širšo objavo sodnih odločb je v naporu, ki ga je treba vložiti v pripravo sodbe za objavo. Navedeno zajema še zlasti prikritje osebnih podatke strank ter drugih posameznikov, omenjenih v sodbi, saj bistvo objave ni razkrivanje identifikacije strank sodnega postopka, ampak pravne logike, ki je sodišča vodila k njegovi odločitvi. To delo je ročno in časovno zamudno, zato se trenutno ne objavlja tudi prvostopenjskih sodb.

Cilj predlagatelja je razširiti obseg objave sodnih odločb na vse prvo-, drugo- in tretjestopenjske odločbe o glavni stvari, izvzemši odločitve v tistih zadevah, v katerih je bila javnost izključena.

S tem ciljem sta Ministrstvo za pravosodje in Vrhovno sodišče Republike Slovenije začela sodelovati na projektu »Pravosodni supervizor«, ki proces priprave sodnih odločb za javno objavo veliki meri avtomatizira, in s tem poenostavi. Ministrstvo za pravosodje je k projektu prvotno prispevalo rešitev za strojno anonimizacijo velikega števila sodnih odločb »Tacita«, razvito v sodelovanju z uglednim Inštitutom Jožef Štefan, ki je na podlagi dela, ki so ga sodišča do sedaj izvedla za sodno stran sodnapraks.si, pripravilo algoritme za avtomatizirano odločanje o tem, katere dele nov izdanih sodnih odločb je potrebno prikriti, in katere ne. Na podlagi sledečega dogovora med obema deležnikoma, kot je bil potem tudi urejen v novem Sodnem redu¹¹⁶ (6. člen), je potem Ministrstvo za pravosodje svoje naloge razširilo še na objavljane tega razširjenega nabora sodnih odločb, medtem ko sodišča poskrbijo zgolj za sprotno posredovanje sodnih odločb Ministrstvu za pravosodje. Vrhovno sodišče se je v ta namen odločilo istočasno izboljšati še svojo informacijsko infrastrukturo za odpremo sodnih odločb.

Predvidena informacijska rešitev bi skrbela za avtomatizirano posredovanje novo izdanih sodb Ministrstvu za pravosodje, za njihovo strojno anonimizacijo ter nekatere dodatne popravke, za njihovo javno objavo, ter za upravljanje z morebitnimi pritožbami in pripombami uporabnikov novonastalega spletnega portala sodne prakse.

K 112. členu (javna objava sodnih odločb)

Člen v prvih dveh odstavkih določa pravno podlago za javno objavo vseh prvo-, drugo- in tretjestopenjskih sodnih odločb o glavni stvari na spletu, z namenom zagotavljanja pravne varnosti, enotnosti sodne prakse ter transparentnost delovanja sodstva (sodišč s splošno pristojnostjo in specializiranih sodišč). Odločb, pri nastanku katerih je bila javnost v celoti ali vsaj deloma izključena, se ne objavlja. Prav tako se ne objavlja vmesnih in postopkovnih odločb, oziroma vsebine sodnega spisa. Z navedenim se po mnenju predlagatelja objavo omeji zgolj na tiste sodne dokumente, glede katerih obstaja največji interes in pričakovanje javnosti, da bodo javno dostopne.

Odločbe objavlja Ministrstvo za pravosodje, ki je tudi upravljavec navedene zbirke.

Predlagani tretji, četrti in peti odstavek določajo, da mora Vrhovno sodišče Republike Slovenije zagotoviti ažurno posredovanje navedenih odločb Ministrstvu za pravosodje, v načinu, primernem za obdelavo in objavo. Prav tako določa, da Vrhovno sodišče omogoči Ministrstvu za pravosodje dostop do ustreznih podpornih evidenc sodišč, ki so potrebna za lažje oziroma celovito pripravo in objavo sodnih odločb. S tem se Ministrstvu za pravosodje zagotovi dostop do sodnih odločb in drugih podatkov, potrebnih za izvedbo nalog po tem členu. Pri tem se Ministrstvu za pravosodje posredujejo zgolj tisti podatki iz evidenc sodišč, ki so že javni, točneje že javno dostopni na spletnih straneh sodišč.

K 113. členu (priprava sodnih odločb za javno objavo)

¹¹⁶ Uradni list RS, št. 87/16.

V členu so predlagana splošna pravila glede anonimizacije sodnih odločb, kar je obveznost Ministrstva za pravosodje, ki jo izvede že na podlagi obdelanih sodnih odločb, ki jih pridobi od Vrhovnega sodišča Republike Slovenije. Obveznost je določena specifično glede na zakonodajo s področja varstva osebnih podatkov – Ministrstvo za pravosodje je dolžno izvesti pred samo objavo odločb tiste ukrepe (merilo »razumna prizadevanja«), ki naj bi pretežno onemogočili, da bi bili iz odločbe neposredno razvidni osebni podatki, ki bi omogočali neposredno identifikacijo strank in drugih fizičnih oseb, ki so navedene v odločbi (neposredna prepoznavnost) – prvi odstavek. Pristop pri predlagani rešitvi je sorazmeren, ni možno in razumno (tudi ob upoštevanju delno relevantnega načela javnosti sojenja iz 24. člena Ustave Republike Slovenije) predpisati ozir. zahtevati, da se z anonimizacijo doseže popolna neprepoznavnost fizičnih oseb, katere so bile stranke ali stranski udeleženci, priče ipd. v sodni odločbi, torej lahko pride ti. posredne prepoznavnosti.

Drugi odstavek predlaganega člena določa pooblastilo, da lahko Ministrstvo za pravosodje pri izvajanju te upravne naloge uporabi tudi avtomatizirano odločanje, pri čemer mora pred začetkom njegove uporabe izvesti oceno vplivov na varstvo osebnih podatkov, ter glede nje pridobiti (pozitivno) mnenje Informacijskega pooblaščenca – namreč, če ta avtomatizirano odločanje zagotavlja izpolnjevanje meril iz prvega odstavka.

K 114. členu (pravice posameznika)

Predlagani člen določa posebno ureditev uresničevanja pravic posameznikov in posameznic glede njihovih osebnih podatkov, ki se objavi v okviru objavljenih sodnih odločb. Navedena ureditev upošteva specifične področja (tj., da so bili vsi podatki, ki so objavljeni v sodbi, že tako obravnavani na javni obravnavi) nadomešča splošni režim pravic posameznikov iz tretjega dela tega zakona.

Predlagana ureditev sledi rešitvam glede odgovornosti ponudnikov posredovalnih storitev po Zakonu o elektronskem poslovanju na trgu ter pravici do izbrisa ali omejitve objave. Posamezniku daje možnost, da brez posebne obrazložitve doseže hitri umik posamezne sodbe iz objave, za trajni umik oziroma spremembo vsebine objavljene sodbe pa mora potem vložiti utemeljeno zahtevo, iz katere mora sklepčno izhajati, da v sodbi objavljeni podatki nesorazmerno posegajo v njegovo pravico do varstva osebnih podatkov. Navedeno pa v skladu s sodno prakso Sodišča Evropske unije o dostopu do podatkov (informacije javnega značaja) ne bo držalo zlasti v primerih, če iz objavljene odločbe ali drugih okoliščin izhaja, da obstajajo posebni razlogi, kot je vloga tega posameznika ali pravne osebe v javnem življenju, zaradi katerih obstaja prevladujoči interes javnosti do dostopa do zadevnih podatkov, to pa vseeno ne vključuje identifikacijskih osebnih podatkov iz prvega odstavka 113. člena ZVOP-2.

Za obravnavo utemeljene zahteve se smiselno uporabljajo postopkovne določbe tega zakona glede pravic do izbrisa in omejitve obdelave.

11. K XI. delu Predloga ZVOP-2:

K 115. členu:

Predlagani 115. člen določa načine uporabe določb Splošne uredbe glede upravnih kazni in glob ter odločanje o prekrških po tem delu zakona. Predlagani člen je pomemben z vidika določitve nadzornega in prekrškovnega organa, prenosa (pretvorbe) upravnih glob v prekrške ter glede odločanja o (pre)visokih upravnih globah po Splošni uredbi. Preko njegove vsebine se zagotavlja pravna varnost na področju prekrškov kot dela kaznovalnega prava.

Po prvem odstavku mora Informacijski pooblaščenec (glede na prvi odstavek 73. člena ZVOP-2) odločati o predpisanih kršitvah in upravnih globah iz člena 83 Splošne uredbe kot o prekrških v okviru pristojnosti prekrškovnega organa po določbah Zakona o prekrških, kolikor ta zakon ne določa

drugače (pomeni: prilagojeno, npr. glede na drugi odstavek 115. člena ZVOP-2). ZVOP-2 torej predpisane (opise; znake) kršitev iz Splošne uredbe opredeli kot prekrške v smislu Zakona o prekrških, njihove sankcije pa kot sankcije za prekrške (slovensko kaznovalno pravo pozna v okviru kaznivih ravnanj le kazniva dejanja in prekrške).

V drugem odstavku je sistemsko določeno, da se pri odločanju Informacijskega pooblaščenca o višini izrečene globe za kršitve, predpisane v členu 83 Splošne uredbe, v skladu z določbami prvega odstavka člena 83 Splošne uredbe in Zakona o prekrških, ob obravnavanju konkretnih okoliščin posameznega primera tudi upošteva, da globa ne sme biti nesorazmerno breme ali neprimerljivo breme za upravljavce ali obdelovalce glede na druge primerljive kršitve človekovih pravic in temeljnih svoboščin, ki se kaznujejo za prekrške, ali je obstajal namen koristoljubnosti ali namen škodovanja posameznikom, na katere se nanašajo osebni podatki, v primeru izvajanja popravljalnih ukrepov s strani upravljavca ali obdelovalca njihovo učinkovitost ali samostojno ukrepanje še pred uvedbo nadzora, glede fizičnih oseb pa se zlasti upošteva splošna raven dohodkov v Republiki Sloveniji ter njihov ekonomski položaj. Prav tako je treba upoštevati pri tem odločanju za vse obdelovalce ali upravljavce ali gre za ponavljajoče kršitve in pomen, ki bi ga za odvratanje teh kršitev imela izbira vrste ali višine globe. Pri tem se upošteva pooblastilo iz uvodnega dela besedila drugega odstavka člena 83 Splošne uredbe ter zlasti (c) in (k) točke navedenega odstavka. Na ta način se onemogoča, da bi bile v neskladju s temeljnim ustavnim načelom sorazmernosti (2. v zvezi s tretjim odstavkom 15. člena Ustave Republike Slovenije) izrečene nesorazmerno visoke globe (kot že navedeno, je delno primerljiva ureditev zaradi pretiranosti glob v ustavnosodni presoji pred Ustavnim sodiščem Republike Avstrije).

V predlaganem tretjem odstavku je določeno, da višine in razponi upravnih glob, ki so za pravne osebe, samostojne podjetnike posameznike in posameznike, ki samostojno opravljajo dejavnost, za kršitve, predpisane v členu 83 Splošne uredbe ter določene v 109. in 110. členu ZVOP-2, se uporabljajo ne glede na določbe o razponih glob iz 17. člena Zakona o prekrških.

V predlaganem četrtem odstavku je ponovno določeno, da Informacijski pooblaščenec odloča kot prekrškovni organ tudi o predpisanih prekrških po tem delu ZVOP-2 in po določbah Splošne uredbe.

V predlaganem petem odstavku je določeno, da Informacijski pooblaščenec lahko za prekrške po določbah Splošne uredbe in iz ZVOP-2 v hitrem postopku izreče globo v kateri koli višini v razponu, kot je določena v določbah Splošne uredbe in ZVOP-2.

K 116. členu:

V predlaganem 116. členu so zaradi pravne varnosti in pravne jasnosti (uporaba s strani prekrškovnega organa) z vidika prava prekrškov določene kršitve iz četrtega odstavka člena 83 Splošne uredbe.

K 117. členu:

V predlaganem 117. členu so tudi zaradi pravne varnosti in pravne jasnosti (uporaba s strani prekrškovnega organa) z vidika prava prekrškov določene kršitve iz petega odstavka člena 83 Splošne uredbe.

K 118. členu:

V 118. členu so predpisani prekrški s področja IX. dela tega zakona, namreč bistvene kršitve glede nezakonite obdelave osebnih podatkov ter nezakonitega dostopanja do njihove vsebine.

K 119. členu:

V 119. členu so določeni prekrški glede kršitve splošnih določb prve področne ureditve po ZVOP-2, namreč določb o neposrednem trženju.

K 120. členu:

V 120. členu so določeni prekrški glede kršitve splošnih določb druge področne ureditve po ZVOP-2, namreč splošnih določb o videonadzoru, katere med drugim vključujejo ne-objavo obvestila o izvajanju videonadzora ipd. Globe so razumno (sorazmerno) predpisane.

K 121. členu:

V predlaganem 121. členu so določeni prekrški glede kršitev določb o videonadzoru glede dostopa v uradne službene oziroma poslovne prostore. Tudi v tem primeru so globe razumno (sorazmerno) predpisane.

K 122. členu:

V predlaganem 122. členu so določeni prekrški glede kršitev določb o videonadzoru pri večstanovanjskih stavbah. Tudi v tem primeru so globe razumno (sorazmerno) predpisane, so nekoliko nižje kot v primerih po 120. in 121. členu ZVOP-2, ker se upošteva pomembnejši zasebnopravni kontekst stanovanjskih razmerij.

K 123. členu:

V 123. členu so določeni prekrški glede kršitev določb o videonadzoru v delovnih prostorih. Tudi v tem primeru so globe razumno (sorazmerno) predpisane, so pretežno enake kot v primerih po 120. in 121. členu ZVOP-2, ker se upošteva pomembnejši kontekst varstva delavcev v delovnih prostorih.

K 124. členu:

V 124. členu so določeni prekrški glede kršitev določb o videonadzoru na javnih površinah (nov prekršek). Glede na kontekst (javne površine; javni prostor), kjer je večja nevarnost nastanka nadzorovalne države ozir. družbe je višina prekrškov nekoliko višja, vseeno pa primerljiva globam po 120. in 121. členu ZVOP-2.

K 125. členu:

V predlaganem 125. členu je določen prvi prekršek s področja tretje področne ureditve – biometrije. Globe so razumno (sorazmerno) predpisane za kršitve določb glede biometrije v javnem sektorju.

K 126. členu:

V predlaganem 126. členu je določen drugi prekršek s področja področne ureditve biometrije. Globe so razumno (sorazmerno) predpisane za kršitve določb glede biometrije v zasebnem sektorju.

K 127. členu:

Predlagani 127. člen določa poseben prekršek glede kršitev določb o prepovedi trženja biometričnih osebnih podatkov v zasebnem sektorju (104. člen Predloga ZVOP-2). Predpisane globe so opazno višje od drugih glob s področja biometrije, saj gre pri ukrepih »zamenjave biometričnih osebnih podatkov za storitve« za večjo nevarnost (tveganost) za pravice ljudi, za njihovo razosebljenje, krajo identitete ipd.

K 128. členu:

V predlaganem 128. členu je določen prekršek s področja četrte področne ureditve, namreč kršitev določb o evidenci vstopov in izstopov. Glede na kontekst (običajni vstopi in izstopi v prostore) so globe razumno (sorazmerno) predpisane – nižje kot npr. v 120. in 121. členu ZVOP-2.

K 129. členu:

V predlaganem 129. členu je določen prekršek s področja pete področne ureditve, namreč kršitev določb o javnih knjigah (njihovi namenski uporabi). Globe so razumno (sorazmerno) predpisane za kršitve določb.

K 130. členu:

V predlaganem 130. členu so določeni prekrški s področja šeste področne ureditve glede povezovanj uradnih evidenc in javnih knjig (glede na prvi odstavek, drugi odstavek in tretji odstavek 107. člena ZVOP-2). Globe so glede na kontekst predpisane v nekoliko večji višini (glede na 128. člen).

K 131. členu:

V 131. členu so predpisani prekrški glede na določbe 109. in 111. člena ZVOP-2, katere urejajo področje strokovnega nadzora in obdelavo osebnih podatkov (torej zadnja - šesta področna ureditev). Globe so razumno (sorazmerno) predpisane za kršitve navedenih določb.

12. K XII. delu Predloga ZVOP-2:**K 132. členu:**

V predlaganem 132. členu se urejajo prehodne določbe ZVOP-2, upoštevajoč zlasti načelo pravne varnosti in njegovo »pod-načelo« zaupanja v pravo.

Prvi in četrti odstavek določata začasno prilagoditveno obdobje (časovno zamejeno obdobje) za upravljavce in obdelovalce – glede na novote iz Splošne uredbe in ZVOP-2, kar v primeru, če izvajajo (so vsaj začeli) postopne prilagoditve – to onemogoča začasno nastanek kaznivosti za prekrške po določbah Splošne uredbe ali ZVOP-2, ne omogoča pa nadzorov Informacijskega pooblaščenca.

Delno primerljiva situacija nastaja tudi v drugih državah Evropske unije, tako je Državna Komisija za informatiko in svoboščine Francoske republike (državni nadzorni organ za varstvo osebnih podatkov - CNIL)¹¹⁷ dne 19. 2. 2018¹¹⁸ podala javno pojasnilo - napoved prehodne nadzorovalne politike - v zvezi

¹¹⁷ CNIL obstaja od leta 1980 (nasledek ti. »afere SAFARI« iz leta 1974) in je načeloma en najbolj prepoznavnih nadzornih organov za varstvo osebnih podatkov v Evropski uniji.

z izvajanjem novot iz Splošne uredbe ali nacionalne izvedbene zakonodaje, po kateri začasno (nekaj mesecev) ne bo kaznovala upravljavcev in obdelovalcev, kadar gre za nove obveznosti za njih, npr. pravico do prenosljivosti osebnih podatkov, oceno učinkov na varstvo osebnih podatkov ipd., vendar pod pogojem da upravljavci in obdelovalci že izvajajo ustrezne prilagoditve navedenim novim obveznostim in da glede morebitnih nadzorov CNIL glede teh vprašanj sodelujejo s CNIL.

Ta pristop omogoča drugačno začasno politiko (policy) CNIL brez izrecne podlage v zakonu, podobno utegne delovati tudi nekaj drugih nadzornih organov za varstvo osebnih podatkov držav članic Evropske unije.

Zlasti glede predlaganih določb prvega in četrtega odstavka 132. člena Republika Slovenija kot pravna država (2. in delno 87. ter 153. člen Ustave Republike Slovenije) ter ustavna demokracija (1. člen Ustave Republike Slovenije) ne more omogočiti podobnih začasnih prilagoditvenih izjem in povezane začasne (!) nekaznivosti kot to lahko druge države z drugačnimi ustavnimi sistemi. V Republiki Sloveniji se takšne začasne ureditve lahko določijo le v zakonu (87. člen, drugi odstavek 120. člena, 2. člen in 153. člena Ustave Republike Slovenije v delni povezavi s celotnim 38. členom Ustave Republike Slovenije) in le na tej izrecni zakonski podlagi lahko deluje Informacijski pooblaščenec »samostojno v okviru in na podlagi ustave in zakonov«¹¹⁹, kar je tudi predlagano v tem členu.

Predlagani prvi odstavek določa da so upravljavci (dosedanji upravljavci osebnih podatkov) in obdelovalci (dosedanji pogodbeni obdelovalci) dolžni v roku enega leta od začetka veljavnosti tega zakona (133. člen ZVOP-2) izvesti ustrezne ukrepe prilagoditve glede uporabe privolitve kot pravne podlage za obdelavo osebnih podatkov, če le te ne ustrezajo novi definiciji privolitve iz 11. točke člena 4 Splošne uredbe – glede na usmeritev iz drugega stavka uvodne navedbe št. 171 Splošne uredbe. Za navedeno obdobje velja, da če upravljavec ali obdelovalec izvajata ustrezne ukrepe prilagoditve (na novi sistem privolitve) in je bila dosedaj podana privolitev v skladu z dosedanjimi pravili iz ZVOP-1, da izvajata ustrezne popravilne ukrepe, ki za obdobje iz prvega stavka preprečujejo nastanek kaznivosti za prekršek po Zakonu o prekrških. Z vidika spoštovanja pravne in poslovne varnosti je torej določeno enoletno prehodno obdobje za pridobivanje novih privolitev za obdelavo osebnih podatkov po novem ZVOP-2.

Predlagani drugi odstavek določa, da se postopki odločanja ali obdelave osebnih podatkov, ki so se pred začetkom uporabe ZVOP-2 začeli pri Informacijskem pooblaščenču ali se obravnavajo na sodiščih (upravni spor, sodno varstvo glede prekrškov) nadaljujejo in končajo po določbah ZVOP-1. To pomeni, da je zagotovljena pravna varnost.

Predlagani tretji odstavek določa, da se dejanja obdelave pri dosedanjih upravljavcih osebnih podatkov in pogodbenih obdelovalcih nadaljujejo po določbah ZVOP-1 – za obdobje največ šest mesecev. Za to obdobje se šteje, da če upravljavec ali obdelovalec izvajata ustrezne prilagoditve za usklajitev z določbami Splošne uredbe in ZVOP-2, da gre za ustrezni prilagoditveni ukrep, ki preprečuje nastanek kaznivosti za prekršek in tako zagotavlja pravno in poslovno varnost.

Po četrtem odstavku so upravljavci in obdelovalci dolžni v roku devetih mesecev od začetka veljavnosti tega zakona izvesti ustrezne ukrepe prilagoditve glede določitve pooblaščenih oseb za varstvo osebnih podatkov po določbah ZVOP-2. Za obdobje iz prejšnjega stavka se šteje, da če obdelovalec in upravljavec izvajata ustrezne ukrepe glede določitve pooblaščenih oseb in zagotavljata v tem obdobju skladnost obdelave osebnih podatkov po tem zakonu na drug način (npr. preko posebne skupine informatikov in/ali pravnikov, ki preverja skladnost sistema obdelave osebnih podatkov, preko zunanega pravnega svetovalca ipd.), da gre za ustrezni prilagoditveni ukrep, ki preprečuje nastanek kaznivosti za prekršek. Na ta način se za določeno prehodno obdobje na poseben način zagotovita pravna in poslovna varnost.

V petem odstavku je določena posebna izjema za občine (kot samoupravne lokalne skupnosti) glede določitve pooblaščenih oseb za varstvo osebnih podatkov. Po predlagani določbi so ne glede na

¹¹⁸ Glejte: <https://www.cnil.fr/fr/rqpd-comment-la-cnil-vous-accompagne-dans-cette-periode-transitoire>

¹¹⁹ Ponovno drugi odstavek 120. člena Ustave Republike Slovenije.

določbe četrtega odstavka tega člena občine šele v roku dveh let od začetka veljavnosti tega zakona dolžne določiti pooblaščen osebe, do poteka tega roka lahko njihove naloge zagotavljanja skladnosti obdelave osebnih podatkov po tem zakonu opravljajo druge osebe iz občinske uprave, ki so pristojne za izvajanje notranjih nadzorov ali revizij ali podobnih delovanj.

Predlagani šesti odstavek določa posebne prehodne določbe za Slovensko akreditacijo glede začetka certificiranja (izvedbe postopkov akreditacije), namreč od 1. januarja 2020 dalje. Pred tem je namreč treba izdati merila iz drugega odstavka 53. člena ZVOP-2 oziroma dodatne zahteve iz drugega stavka prvega odstavka 54. člena ZVOP-2 – merila na ravni Evropske unije, ki se bodo še nekaj časa usklajevala ter merila, ki jih izda Informacijski pooblaščenec. Realno to pomeni približno nekaj manj kot dvoletni rok za začetek delovanja določb o postopkih akreditacije.

Predlagani sedmi odstavek določa, da se povezovanja v skladu s prvim odstavkom 107. člena ZVOP-2 uskladijo v skladu s pogoji iz 107. člena ZVOP-2 v roku štirih let od začetka veljavnosti zakona.

Po osmem odstavku so upravljavci ali obdelovalci, ki za izvajanje svojega delovanja pridobivajo osebne podatke iz registrov ali evidenc s področja upravnih notranjih zadev, dolžni v roku dveh let po začetku veljavnosti tega zakona vzpostaviti ustrezne varnostne mehanizme po predhodnem soglasju Ministrstva za notranje zadeve – zaradi izvrševanja osmega odstavka 94. člena ZVOP-2.

Predlagani deveti odstavek določa ukinitve dosedanjega Registra zbirk osebnih podatkov iz 28. člena ZVOP-1, ki po Splošni uredbi ne sme več obvezujoče obstajati. Nato je določeno, da Informacijski pooblaščenec njegovo vsebino arhivira in nato v roku enega leta preda Arhivu Republike Slovenije, ki vsebino Registra hrani kot trajno arhivsko gradivo (pomembno za zgodovino pravne države ter delno tudi za pravno varnost).

Prehodne določbe ne vsebujejo več rešitve, da se v Zakonu o spremembah in dopolnitvah Zakona o izvrševanju kazenskih sankcij (ZIKS-1F)¹²⁰ z dnem uporabe ZVOP-2 črta 88. člen iz ZIKS-1F, torej črtanje tam določene prehodne (začasne) določbe glede uporabe istega povezovalnega znaka iz ZIKS-1F, saj so rešitve iz njega že vključene v tretjem do petem odstavku 13. člena ZVOP-2.

K 133. členu:

Predlagani 133. člen določa prenehanje veljavnosti dosedanjega ZVOP-1 (iz leta 2004, s spremembami do leta 2007¹²¹).

K 134. členu:

V končni določbi je v 134. členu predlagano, da novi Zakon o varstvu osebnih podatkov (ZVOP-2) začne veljati dne 25. maja 2018.

¹²⁰ Uradni list RS, št. 54/15.

¹²¹ Uradni list RS, št. 86/04, 113/05 – ZInfP, 51/07 – ZUstS-A, 67/07 in 94/07 – uradno prečiščeno besedilo.