REPUBLIKA SLOVENIJA
MINISTRSTVO ZA PRAVOSODJE

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 4. 4. 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 – NOVO GRADIVO ŠT. 2

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, saj za delovanje države, kolikor le-ta nastopa kot upravljavec ali obdelovalec osebnih podatkov ali pa jih čezmejno posreduje (npr. na policijskem ali 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). V zvezi z izvedbenimi zakoni držav članic Evropske unije po Splošni uredbi o varstvu osebnih podatkov Evropske unije iz leta 2016 ter povezani Direktivi EU iz istega leta sicer v Evropski uniji obstaja splošna pravna ne-varnost za poslovanja z osebnimi podatki, saj so bili dosedaj sprejeti le trije izvedbeni zakoni (Avstrija, Nemčija, Slovaška ter na Danskem posebni zakon za izvedbo Direktive (EU) 2016/680), v Francoski republiki se predlog izvedbenega zakona tudi obravnava po nujnem zakonodajnem postopku (Predlog Zakona o varstvu osebnih podatkov Francoske republike – nujni zakonodajni postopek, z dne 14. 2. 2018), ostali naj bi bili pretežno (predvidoma) sprejeti aprila ter maja 2018, ko poteče rok za uveljavitev obeh pravnih aktov Evropske unije.

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

- mag. Goran Klemenčič, minister za pravosodje,

- Darko Stare, državni sekretar,

- Tina Brecelj, 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 Brecelj, 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 ozir. oblastna 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 (v prehodnih določbah) 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 pooblaščene osebe. Določena je tudi možnost, da imajo lahko organi v sestavi lastno pooblaščeno osebo.

Prav tako je glede na predloge prakse v ZVOP-2 še vedno podrobno urejeno neposredno trženje, četudi je z vidika Splošne uredbe morda nekoliko sporno – s stališča, da je bolje regulirati, kot prepustiti nejasni praksi, ki lahko področje čisto odpre ali pa pride dejansko celo 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 na primerljivo »naravo stvari« dopustno, npr. ne sme se posegati v neodvisnost sodstva, ne sme biti nadzorov na področju, kjer ga tudi Državni zbor RS izjemoma ne izvaja (Komisija za nadzor obveščevalno-varnostnih služb) ipd..

Določene so posebne določbe ozir. okrepljene obstoječe določbe iz ZVOP-2, kdaj Informacijski pooblaščenec ne sme sam ukrepati (s posegom v določene druge človekove pravice), ker ali potrebuje predhodno sodno odločbo ali pa je to pristojnost drugih organov ali druge zakonodaje – kadar bi šlo za neprimeren ali neustaven poseg v komunikacijsko zasebnost, prostorsko zasebnost

ali svobodo izražanja ali svobodo komuniciranja z vidika varstva osebnih podatkov.

V predlogu je razrešeno tudi razmerje med vrednotami s področij svobode izražanja do varstva osebnih podatkov in vrednotami dostopa do informacij javnega značaja do varstva osebnih podatkov, v korist svobode izražanja ter dostopa do informacij javnega značaja.

Obrazložitev Novega gradiva št. 2:
Po sprejetju Predloga Zakona o varstvu osebnih podatkov na Odboru za državno ureditev in javne zadeve Vlade Republike Slovenije dne 13. 3. 2018 in obravnavi na seji Vlade Republike Slovenije dne 29. 3. 2018 so bila izvedena še dodatna medresorska in strokovna usklajevanja, katerih rezultat je Predlog Zakona o varstvu osebnih podatkov – Novo gradivo št. 2. V Novem gradivu št. 2 so smiselno v okviru koncepta zakona upoštevane strokovne in redakcijske pripombe Informacijskega pooblaščenca z dne 4. 4. 2018, strokovne in redakcijske pripombe Službe Vlade Republike Slovenije za zakonodajo, večje število pripomb Ministrstva za zdravje, več pripomb Ministrstva za javno upravo glede uporabe eIDAS Uredbe, poštenega upravnega postopka, tri pripombe Ministrstva za notranje zadeve ter opravljeni še določeni redakcijski ali s prej navedenimi pripombami povezani vsebinski popravki. Z vidika pripomb večih ministrstev so bile opravljene spremembe 112. člena glede povezovanja uradnih evidenc in javnih knjig, tako da ni več potrebna predhodna odobritev (odločba) Informacijskega pooblaščenca, ampak se Informacijskega pooblaščenca le predhodno obvesti o nameravani uvedbi povezovanja.

Obrazložitev z vidika opravljanja tekočih poslov Vlade Republike Slovenije po 115. členu Ustave Republike Slovenije:

Predlog ZVOP-2 je lahko obravnavan in sprejet s strani Vlade Republike Slovenije v skladu z ustavno določbo o opravljanju tekočih poslov Vlade (115. člen Ustave Republike Slovenije), saj so bile bistvene politike glede vsebine nove pravne ureditve varstva osebnih podatkov odločene že maja 2016 na ravni Evropske unije v sprejeti Splošni uredbi o varstvu podatkov in povezani Direktivi in je predlagani ZVOP-2 pretežno izvedbene ozir. povezovalne narave. Prav tako je večina bistvenih politik glede področnih ureditev (npr. videonadzor, biometrija) samo nasledek ozir. delna posodobitev določb iz veljavnega ZVOP-1 iz leta 2004. Obveznost novega delovanja ozir. pravil na področju varstva osebnih podatkov nastopi s 25. majem 2018, vendar sistem varstva osebnih podatkov ne bo mogel ustrezno delovati (ne bo dovolj zagotovljena pravna varnost) brez izvedbenih ozir. povezovalnih določb ZVOP-2.

Pri Predlogu ZVOP-2 gre za zadevo Evropske unije ter istočasno tudi za nujni zakonodajni postopek, ki je bil potrjen na pristojnem odboru vlade Republike Slovenije dne 13. marca 2018, še pred nastankom stanja opravljanja tekočih poslov Vlade. Z vidika opravljanja tekočih poslov Vlade gre tudi za zagotavljanje kontinuiranega delovanja države.

V tej obrazložitvi se glede vključenosti tega predloga zakona na področje opravljanja tekočih poslov Vlade izhaja tudi iz Mnenja Službe Vlade Republike Slovenije za zakonodajo, št. 000-1/2014/23, z dne 15. 3. 2018 o »Opravljanje tekočih poslov predsednika vlade in ministrov v skladu s 115. členom Ustave Republike Slovenije« glede zakonov, potrebnih za prilagoditev naše zakonodaje pravu Evropske unije (str. 1) ter glede nujno potrebnih zakonov (str. 2).

6. Presoja posledic za:		
a)	javnofinančna sredstva nad 40.000 EUR v tekočem in naslednjih treh letih	**NE**
b)	usklajenost slovenskega pravnega reda s pravnim redom	**DA**

	Evropske unije	
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 posredovan dne 23. 1. 2018.

Precejšnjo 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 še do 10. 2. 2018, ko so bile prejete še zadnje sistemsko pomembnejše pripombe.

Strokovno usklajevanje:

Bistvene pripombe Vrhovnega sodišča Republike Slovenije ter Vrhovnega državnega tožilstva Republike Slovenije so bile sprejete, dne 12. 3. 2018 pa smo prejeli še stališča Vrhovnega sodišča Republike Slovenije o novi področni ureditvi – »Pravosodni supervizor« v zvezi s katerimi smo opravili določene popravke na način, da je sedaj objavljanje sodnih odločb urejeno v členu o razmerju med varstvo osebnih podatkov in dostopom do informacij javnega značaja (drugi odstavek 83. člena). Določene bistvene pripombe Informacijskega pooblaščenca z dne 4. 4. 2018 so bile upoštevane (ne glede institutov povezovanja ter glede poglavja o objavah sodnih odločb ter ne glede izjem glede nadzorov s področij javne varnosti in varnosti države). Z Varuhom človekovih pravic je Predlog ZVOP-2 v tej fazi usklajen.

10. Pri pripravi gradiva so bile upoštevane zahteve iz Resolucije o normativni dejavnosti:	**DA**
11. Gradivo je uvrščeno v delovni program vlade:	**DA**

Darko STARE

državni sekretar

Priloge:

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

EVA: 2017-2030-0039

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 Slovenije[4], Direktive 95/46/ES[5], Okvirnega sklepa 2008/977/PNZ[6] in Konvencije o varstvu posameznikov glede na avtomatsko obdelavo osebnih podatkov[7] (Sveta Evrope).

---

[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.

[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.

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 pravnih aktov Evropske unije pretežno ali v celoti nasprotovala[8], 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 članek[9], 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.

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

[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.

[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.

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 podatkov[13], obstoječo ustavnosodno presojo Ustavnega sodišča Republike Slovenije glede človekove pravice do varstva osebnih podatkov od leta 1992[14] dalje ter tudi določbe še veljavne (še nespremenjene) Konvencije o varstvu posameznikov glede na avtomatsko obdelavo osebnih podatkov (Svet Evrope, Konvencija št. 108).

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).

Konkretneje: 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 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 podatkov[15].

[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.
[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 specifike 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.

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.).

Pomembno 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 zaobsežena 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) – da Republika Slovenija to ureja z ZVOP-2 ali s področnimi zakoni (in bo to urejala še naprej). 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 z drugimi zakoni vsaj glede posegov v osebne podatke ali glede obdelave osebnih podatkov, določiti uporabo ZVOP-2 (poleg že navedenih področnih ureditev varstva osebnih podatkov) – relevantno zlasti glede določb o definicijah, pravnih podlagah za obdelave 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 države Evropske unije, namreč Zvezna republika Nemčija[16], Republika Avstrija[17] in Slovaška republika[18] (države s primerljivim pravnim redom in ustavnopravnim oziroma ustavnosodnim razumevanjem pravice do varstva osebnih podatkov) v njihovih novih zakonih o varstvu osebnih

[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.

[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..

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 v njenem zakonu izhajala iz celovite uporabe pristopa klasičnega mednarodnega zasebnega prava in postopka.

Predlog ZVOP-2 delno 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 tudi v določenih delih Predloga ZVOP-2 (npr. posebne vrste osebnih podatkov v 12. členu).

Prav tako utegne na dokončnejšo vsebino ZVOP-2 vplivati tudi dejstvo, da je predvidena objava popravkov uradne slovenske inačice besedil Splošne uredbe in Direktive predvidoma šele v maju 2018, kar velja tudi za večino drugih jezikovnih inačic Splošne uredbe in Direktive. Vpliv na določbe ZVOP-2 utegne biti še nekoliko širši, saj utegnejo biti spremenjene tudi inačici besedil Splošne uredbe in Direktive v angleški jezikovni inačici, kar sicer 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.

Vse navedene informacije, od tega, da je primerjalnopravna izvedbena ureditev dokaj skopa, da bodo objavljeni popravki slovenske inačice Splošne uredbe, pa tudi dejstvo, da nekateri pojmi ali instituti v praksi še nekaj časa ne bodo razjasnjeni (npr. tudi možna nasprotja v interpretaciji med opredelitvami Evropske komisije ter Delovne skupine po členu 29 Direktive 95/46/ES) ter tudi izbira zakonodajne tehnike v tem zakonu (glejte obrazložitev pod 2. 3.) bodo v prihodnosti nedvomno pripeljale tudi do noveliranja ZVOP-2 – ko bodo določene interpretacije ali povezave pravno znatno jasnejše.

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 (vseobsežen) 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 le 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.

biometrija) ipd.. Zlasti z vidika spoštovanja načela pravne varnosti je tak pristop skupnega urejanja varstva osebnih podatkov na enem mestu (tradicionalen že od leta 1990[19]) – upravičen.

2. 3. O zakonodajni tehniki Predloga ZVOP-2

Zakonodajna tehnika Predloga ZVOP-2 je delno novota, glede na potrebo delne implementacije določb Splošne uredbe in implementacije določb 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 in to čimveč na enem mestu. 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 (delno podobna zakonodajna tehnika novemu zakonu Zvezne republike Nemčije).

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

<u>Načelo spoštovanja osebnosti in pravic človeka</u>

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, prenosi 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.

<u>Načelo zakonitosti</u>

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

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

obdelave konkretnih osebnih podatkov določa v podzakonskih predpisih (kar je nedopustno po ustaljeni ustavnosodni presoji Ustavnega sodišča Republike Slovenije od leta 1992 dalje[20]). Temu pristopu tako sledijo 9. 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) s strani javnega sektorja (javne oblasti) velja strogo načelo zakonitosti, za zasebni sektor pa je to 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, konkretneje, po ustavnosodni presoji z uporabo strogega testa sorazmernosti (predvsem odločba US, št. U-I-60/03, 4. 12. 2003[21], zlasti 30. točka 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 dosedanji 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 preldog zakona sledi dosedanjim dosežkom pravne ureditve (obligacijsko pravo, pravo dostopa do informacij

[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.

javnega značaja), ustavnosodne presoje (sicer s področja prikritih preiskovalnih ukrepov po Zakonu o kazenskem postopku) in sodne prakse (zlasti civilnopravne).

Znatno je spremenjena definicija splošne 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 ((e) 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 pooblaščene 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 pooblaščene osebe. Določena je tudi možnost, da imajo lahko organi v sestavi lastno pooblaščeno 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 Slovenije[23].

[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 *Maximillian 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 pooblaščencu. 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 zaščitenih 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), kjer pa je tudi navedeno da I.-IV. del zakona veljajo tudi za to področje (načela, obravnavanje zahtev, sledljivost ipd.). Ustrezne specifike in izjeme, tako glede namenov obdelav osebnih podatkov, obveščanja posameznikov o njihovih osebnih podatkih, so seveda urejene specifično, glede na določbe Direktive. V povezavi s tem delom zakona so urejene tudi specifike glede obdelav osebnih podatkov na področjih varnosti države in obrambe države, sicer še vedno 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 tudi ureditev o objavljanju sob v okviru razmerja med varstvom osebnih podatkov in dostopom do informacij javnega značaja, vključno s psevodnimiziranimi objavami sodb prvostopenjskih sodišč.

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 1984[24]) – 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 (dosedanji 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 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 dosedanje organizacije dela bo sicer treba sistem prenoviti v še bolj »varovalno smer« - namreč vzpostaviti notranje ali zunanje (pogodbene) pooblaščene 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 pooblaščene 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 pooblaščene 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 javno 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 (poroštva): 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

Za izvajanje zakona so že zagotovljena dodatna sredstva v državnem proračunu. Dodatna sredstva so bila zagotovljena že v letu 2017 in sicer za obdobje 2018 in 2019 – za delovanje neodvisnega nadzornega in samostojnega organa (Informacijski pooblaščenec).

Za leto 2018 so zagotovljene naslednje proračunske postavke:

– proračunska postavka 1267 plače; na kateri so predvidena finančna sredstva za 10 novih državnih nadzornikov za varstvo osebnih podatkov (41. plačni razred in 10 let delovne dobe) - na letni ravni se za enega ocenjujejo finančna sredstva v višini 34.200,00 EUR, skupaj 342.000,00 EUR,

– proračunska postavka 1273 investicije; na kateri so zagotovljena finančna sredstva za osnovno opremo za 10 novo zaposlenih, skupaj 10.000,00 EUR

– proračunska postavka 1271; na kateri so predvidena finančna sredstva za materialne stroške, selitev, skupaj v znesku 20.000,00 EUR ter za najem poslovnih prostorov za obdobje 6 mesecev (15.300 EUR/mesec), skupaj 91.800,00 EUR.

Za leto 2018 so tako zagotovljena finančna sredstva skupaj v višini 463.800,00 EUR.

Za leto 2019 so zagotovljene naslednje proračunske postavke:

– proračunska postavka 1267 plače; na kateri so predvidena finančna sredstva za 5 novih državnih nadzornikov za varstvo osebnih podatkov (41. plačni razred in 10 let delovne dobe) - na letni ravni za enega ocenjujejo finančna sredstva v višini 34.200,00 EUR, skupaj 171.000,00 EUR in

– proračunska postavka 1273 investicije; na kateri so zagotovljena finančna sredstva za osnovno opremo za 5 novo zaposlenih, skupaj 5.000,00 EUR, najem poslovnih prostorov za 12 mesecev (15.300 EUR/mesec), skupaj 183.600,00 EUR.

Za leto 2019 so tako zagotovljena finančna sredstva skupaj v višini 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 pripravlja[25]. »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 2016[27] 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[28]. 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**) ter predosnutek zakona Kraljevine Belgije.

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)[29]. 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).

[25] Predosnutek Zakona o varstvu fizičnih oseb glede glede obdelave osebnih podatkov Kraljevine Belgije je bil tako objavljen 16. marca 2018 (o tem več v nadaljevanju).
[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 dosedanji 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] Predlog Zakona o varstvu osebnih podatkov Francoske republike – nujni zakonodajni postopek, z dne 14. 2. 2018.
[29] Zakon z dne 30. junija 2017, Bundesgesetzblatt Teil I, 2097.

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.

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 pregon[30] 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 pripravljeni) 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 sicer tudi, da je sprejeti Zakon o prilagoditvi in izvajanju zakonodaje o varstvu osebnih podatkov EU deležen (sicer neupoštevanih) kritik iz dela zasebnega sektorja in dela javnosti[31], češ da ni dovolj v skladu z določbami Splošne uredbe - da naj bi bile občasno njegove določbe prestroge ali preširoke. Za domnevati je, da je Nemčija glede teh vprašanj (vidiki domnevne neskladnosti določb Zakona o prilagoditvi in izvajanju zakonodaje o varstvu osebnih podatkov EU v razmerju do določb Splošne uredbe) izhajala iz podlage 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)[32].

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

[30] Zasebni sektor npr. uporablja videonadzor in bi hotel vložiti kazensko ovadbo, saj je ocenil, da obstaja sum storitve kaznivega dejanja.
[31] 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/
[32] Bundesgesetzblatt I Nr. 120/2017, Teil I.

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 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 upravljavca, 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 izrekati 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 privolitev 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. 2017[33]. 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 iz člena 4 Splošne uredbe za vsa zakonska področja (5. člen), kot so to npr. obdelava osebnih podatkov, privolitev 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 legitimne 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 prenosljivosti osebnih podatkov, s tem da je določeno, da ta pravica ne sme imeti

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

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.

5. 5. Kraljevina Belgija

Predosnutek Zakona o varstvu fizičnih oseb glede glede obdelave osebnih podatkov Kraljevine Belgije je bil objavljen 16. marca 2018 in vsebuje 287. členov. Zakonodajno smer Predosnutka je možno v tej fazi oceniti za garantistično (glede človekove pravice do varstva osebnih podatkov) in prepisovalno oziroma samostojno urejevalno. 1. člen predloga zakona določa posebno zakonodajno pristojnost s sklicem na Ustavo Kraljevine Belgije, 2. člen med drugim določa delno omejitev glede področja obrambe države – da se ne nanaša na uporabo oboroženih sil ali na pripravo na uporabo oboroženih sil. V 3. členu je najprej določeno, da prosti pretok osebnih podatkov na ozemlju Evropske unije ali Kraljevine Belgije ne more biti omejen iz razlogov varstva osebnih podatkov, nato pa je ta pristop zamejen s strogo določbo, da to ne posega v pristojnosti nadzornega organa za varstvo osebnih podatkov. Nadalje 5. člen določa, da so definicije iz tega zakona iste kot v Splošni uredbi in da kadar predosnutek zakona navede definicijo, da to pomeni, da je mišljen le sklic na definicijo iz Splošne uredbe (s formulacijo: »brez posega v definicije v tem zakonu…«). V 7. členu je določeno, da je privolitvena starost za otroke glede uporabe storitev informacijske družbe 13 let. Sistem uvedbe pooblaščenih oseb za varstvo osebnih podatkov je dokaj podrobno razdelan, glede na vse njihove možne uporabe z vidika zagotavljanja skladnosti obdelave osebnih podatkov, s tem, da bo tudi Kraljevina Belgija samostojno določila pogoje za določitev pooblaščene osebe – vendar na način, da je za to dano pooblastilo v obliki delegirane zakonodaje za Kraljevo (dejansko: vladno) uredbo v zakonu (peti odstavek 65. člena). Področja iz Direktive 2016/680/EU so urejena v II. Delu Predosnutka zakona, delno pa tudi v III. Delu Predosnutka zakona. Področja arhiviranja, znanstvenega in zgodovinskega raziskovanja ter statističnega delovanja so urejena v 4. Delu Predosnutka zakona. V 233. členu so podrobneje določeni sodelovanje in kvalifikacije nevladnih organizacij za (pooblastilno) zastopanje posameznikov pred sodišči, kadar posamezniki zatrjujejo kršitev svojih pravic s področja varstva osebnih podatkov, s tem da je izrecno podano pooblastilo tudi za možnost zastopanja v kazenskem postopku. V 235. členu in naslednjih členih so določeni prekrški za kršitve zakona in za njih predpisane globe očitno odstopajo (in so sorazmerne) od upravnih sankcij po Splošni uredbi – npr. globe za upravljavce in obdelovalce (pravne osebe) so pretežno predpisane od 250 do 15.000 evrov (EUR) oziroma od 500 do 30.000 evrov.

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. 207 ter ponovno (drugi krog) 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 Brecelj, 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

I. DEL

TEMELJNE DOLOČBE

1. člen

(vsebina)

(1) Ta zakon ureja pravice, obveznosti, upravičenja, načela, postopke in ukrepe, 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 izvaja 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) (UL L št. 119 z dne 4. 5. 2016, str. 1; v nadaljnjem besedilu: Splošna uredba) in prenaša 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 (UL L št. 119 z dne 4. 5. 2016, str. 89; v nadaljnjem besedilu: Direktiva).

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 uresničevanjem teh njegovih pravic.

3. člen

(prepoved diskriminacije glede varstva osebnih podatkov)

Varstvo osebnih podatkov je zagotovljeno vsaki posameznici ali posamezniku ne glede na narodnost, raso, barvo kože, veroizpoved, etnično pripadnost, spol, jezik, politično ali drugo prepričanje, spolno usmerjenost, spolno identiteto, premoženjsko stanje, kraj rojstva, izobrazbo, družbeni položaj, državljanstvo, kraj oziroma vrsto prebivališča, zdravstveno stanje 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 IX. del tega zakona ne določa drugače, določbe Splošne uredbe in 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 iz 85. člena tega zakona.

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, ali če so povezane s spremljanjem njihovega delovanja ali vedenja, če to poteka v Republiki Sloveniji.

(3) Določbe tega zakona o privolitvi mladoletnih oseb 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 s stalnim prebivališčem 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« pomenijo katerokoli 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 Evropske unije ali pravo države članice, se lahko upravljavec ali posebna merila za njegovo imenovanje določijo s pravom Evropske 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 Evropske 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 pooblaščene 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, nepooblaščeno razkritje ali dostop do osebnih podatkov, ki so poslani, shranjeni ali kako drugače obdelani;

13. »genski podatki« pomenijo 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 Evropski uniji ali, kadar se odločitve o namenih in sredstvih obdelave osebnih podatkov sprejemajo na drugem sedežu upravljavca v Evropski 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 Evropski uniji, ki jo pisno imenuje upravljavec ali obdelovalec v skladu s 27. členom Splošne uredbe in ki predstavlja upravljavca ali obdelovalca v zvezi z njegovimi obveznostmi iz Splošne 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

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

b) obdelavo osebnih podatkov, ki poteka v Uniji v okviru dejavnosti edinega sedeža upravljavca 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 Splošna uredba kršena, oziroma glede tega, ali je predvideno ukrepanje v zvezi z upravljavcem ali obdelovalcem v skladu s Splošno 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 Evropski uniji;

25. »storitev informacijske družbe« pomeni storitev, kakor je opredeljena v točki b) prvega odstavka 1. člena Direktive (EU) 2015/1535 Evropskega parlamenta in Sveta z dne 9. septembra 2015 o določitvi postopka za zbiranje informacij na področju tehničnih predpisov in pravil za storitve informacijske družbe (kodificirano besedilo) (UL L št. 241 z dne 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, ustanovljena 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 je:

1. katerikoli organ ali subjekt javnega prava Republike Slovenije, ki je pristojen za preprečevanje, preiskovanje, odkrivanje ali pregon kaznivih dejanj ali izvrševanje kazenskih sankcij, vključno s preprečevanjem pranja denarja ali financiranja terorizma, varnostjo države in obrambe države, varovanjem pred grožnjami javni varnosti in njihovim preprečevanjem, ali

2. katerikoli drug organ ali subjekt, ki v skladu z zakonom Republike Slovenije lahko opravlja javne funkcije ali izvaja javna pooblastila v zvezi s področji iz prejšnje točke.

(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 2. členu Zakona o sistemu plač v javnem sektorju (Uradni list RS, št. 108/09 – uradno prečiščeno besedilo, 13/10, 59/10, 85/10, 107/10, 35/11 – ORZSPJS49a, 40/12 – ZUJF, 46/13, 25/14 – ZFU, 50/14, 95/14 – ZUPPJS15, 82/15, 23/17 – ZDOdv in 67/17);

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

4. »povezovalni znak« pomeni osebno identifikacijsko številko 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 druge podobne znake v javnem sektorju, 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 ni več mogoče obnoviti; pri tem je zaradi zagotavljanja sledljivosti obdelave osebnih podatkov v skladu s sedmim odstavkom 40. člena tega zakona dopustno tudi zabeležiti zaznamek, da je bil v zvezi z osebnimi podatki določenega posameznika izveden izbris, pri čemer pa zaznamek ne sme vsebovati podatkov, ki bi omogočali obnovo izbrisanega 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 iz 68. člena Splošne uredbe;

9. »zakon« pomeni 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;

11. »sorazmernost obdelave« pomeni obdelavo v skladu z b), c) in d) točkami prvega odstavka 7. člena tega zakona.

(4) Izrazi, uporabljeni v tem členu, se uporabljajo za izvajanje tega zakona ter pomenijo tudi spoštovanje obveznosti iz drugega odstavka 1. člena tega zakona in obvezujočih mednarodnih pogodb za Republiko Slovenijo.

7. člen

(temeljna načela varstva osebnih podatkov)

(1) Osebni podatki:

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

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

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

č) so 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) se 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) se 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) Upravljavec in obdelovalec morata biti vedno biti zmožna dokazati skladnost svojih obdelav osebnih podatkov z določbami prejšnjega odstavka ter morata v skladu s tem voditi tudi predpisano dokumentacijo v skladu z zakonom.

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 ter 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 tudi na podlagi privolitve posameznika.

(2) Ne glede na prejšnji odstavek se lahko v javnem sektorju obdelujejo osebni podatki le na podlagi privolitve posameznika, če ne gre za izvrševanje zakonitih pristojnosti, nalog ali obveznosti javnega

sektorja. Zbirke osebnih podatkov, ki nastanejo na tej podlagi, morajo biti ločene od drugih zbirk osebnih podatkov, ki nastanejo pri izvrševanju zakonitih pristojnosti, nalog ali obveznosti.

(3) Ne glede na prvi odstavek tega člena se lahko v javnem sektorju izjemoma obdelujejo tisti osebni podatki, ki so nujni za izvrševanje zakonitih pristojnosti, nalog ali obveznosti javnega sektorja, če se s to obdelavo ne poseže v upravičen interes posameznika, na katerega se nanašajo osebni podatki. Zbirke osebnih podatkov, ki nastanejo na tej podlagi, morajo biti ločene od drugih zbirk osebnih podatkov, ki nastanejo pri izvrševanju drugih zakonitih pristojnosti, nalog ali obveznosti.

(4) 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 takšne pogodbe, če je obdelava osebnih podatkov potrebna in primerna za izvajanje ukrepov pred sklenitvijo pogodbe ali za izvajanje pogodbe.

(5) 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.

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

(7) 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 drug zakon 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 ter 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 zasebnemu 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 ter zakonitih interesov, ki so opredeljeni v oceni učinka na varstvo osebnih podatkov ter za katere si prizadeva upravljavec ali tretja oseba,

razen kadar nad takimi interesi prevladajo interesi ali človekove pravice in temeljne svoboščine posameznika, na katerega se nanašajo osebni podatki, ki zahtevajo varstvo osebnih podatkov.

(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 nezdružljiva 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, upravljavec, potem ko je izpolnil vse zahteve glede zakonitosti prvotne obdelave, opravi presojo v skladu s četrtim odstavkom 6. člena Splošne uredbe. Presoja se opravi pred začetkom obdelave za druge namene v pisni obliki in je sestavni del dokumentacije po drugem odstavku 7. člena tega zakona.

(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 v skladu s tem zakonom in drugimi zakoni.

(2) Upravljavec podatke o umrlem posamezniku posreduje le tistim uporabnikom, ki so za obdelavo osebnih podatkov pooblaščeni 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, partnerju v zunajzakonski skupnosti ter partnerjem z njima izenačenih skupnosti, otrokom ali staršem, dedičem ali drugim osebam, čeumrli posameznik ni pisno prepovedal posredovanja njegovih osebnih podatkov.

(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 tako določa zakon, če je privolitev pred smrtjo dal posameznik sam ali če je za takšno objavo v času po smrti posameznika podana pisna privolitev naslednjih oseb v izključujočem vrstnem redu: zakonec ali partner iz zunajzakonske skupnosti ali partner z njima z zakonom izenačene skupnosti, otroci ali starši umrlega posameznika.

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, če jo da mladoletna oseba, stara 15 let ali več. Če je mladoletna oseba mlajša od 15 let, je privolitev veljavna le, če jo da ali odobri eden od staršev mladoletne osebe ali njen rejnik ali skrbnik.

(2) Upravljavec ves čas nudenja storitve ob upoštevanju razpoložljive tehnologije v primerih iz drugega stavka prejšnjega odstavka izvaja razumna prizadevanja, zlasti s kontaktiranjem staršev, rejnikov ali

skrbnikov, s katerimi preveri, ali je starš, rejnik ali skrbnik za mladoletno osebo dal 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 na podlagi privolitve 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 opravljanja takšne dejavnosti.

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 o zdravstvenem stanju posameznika ali podatkov v zvezi s posameznikovim spolnim življenjem ali spolno usmerjenostjo (v nadaljnjem besedilu: posebne vrste osebnih podatkov), je prepovedana.

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

a) je posameznik za to dal izrecno privolitev, ki je pisna, in je bila privolitev dana 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 povezanih pravic, ki izhajajo iz zakonov s področja socialno varstvene dejavnosti ali zakona, ki ureja kolektivne pogodbe, ter za izpolnjevanje obveznosti v zvezi s tem, v skladu z drugim zakonom, ki določa tudi ustrezna jamstva človekovih pravic, temeljnih svoboščin ali interesov posameznika, na katerega se nanašajo osebni podatki,

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 odstavka,

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, ter če se ti podatki ne posredujejo drugim posameznikom ali osebam javnega ali zasebnega sektorja brez privolitve posameznika, na katerega se nanašajo,

d) je posameznik, na katerega se nanašajo posebne vrste osebnih podatkov, 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 zdravstvene dejavnosti ali ocene delovne sposobnosti s področja zaposlovanja obdelujejo zdravstveni delavci in zdravstveni sodelavci v skladu z zakonom in druge pooblaščeno osebje, če je to nujno za opravljanje njihovih nalog,

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 zdravilih in

medicinskih pripomočkih in te podatke obdelujejo zdravstveno osebje ali druge osebe, ki so zavezane 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 sodnih in drugih uradnih postopkov,

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

j) je potrebna za namene arhiviranja v javnem interesu, za znanstvenorazioskovalne ali zgodovinskoraziskovalne namene ali statistične namene v skladu s tem ali drugim zakonom, kar mora biti sorazmerno z zastavljenim ciljem, spoštovati bistvo pravice do varstva osebnih podatkov ter zagotavljati ustrezne in posebne ukrepe za varstvo človekovih pravic in temeljnih svoboščin ali interesov posameznika, na katerega se nanašajo osebni podatki, ali

k) tako določajo zakoni, ki urejajo izvajanje obveščevalnih in protiobveščevalnih dejavnosti države, kadar gre za izvrševanje bistvenega javnega interesa in je to sorazmerno z zastavljenim ciljem, spoštuje bistvo pravice do varstva osebnih podatkov ter zagotavlja ustrezne in posebne ukrepe za varstvo človekovih pravic in temeljnih svoboščin ali interesov posameznika.

(3) V primerih obdelav posebnih vrst osebnih podatkov iz prejšnjega odstavka se poleg ukrepov iz 34. člena tega zakona določi in vzpostavi in pisno opredeli 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) varnostne politike, postopki in ukrepi za varstvo osebnih podatkov, ki zagotavljajo, da obdelava poteka skladno z zahtevami iz 34. 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, se za dostop do teh storitev zagotovi takšna sredstva elektronske identifikacije, kjer se ob njihovi izdaji zahteva osebna navzočnost posameznika in njegova identiteta preveri z vpogledom v uradni osebni dokument posameznika,

č) pri posredovanju, prenosu ali čezmejni obdelavi posebnih vrst osebnih podatkov preko elektronske pošte se ti podatki šifrirajo tako, da je zagotovljena njihova neprepoznavnost med prenosom, razen če gre za posredovanja, prenose ali čezmejne obdelave posebnih vrst osebnih podatkov preko omrežij, ki so pod nadzorom upravljavca,

d) ustrezno upravljanje uporabniških pooblastil pri upravljavcih in obdelovalcih.

13. člen

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

(1) Podatki 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 prenosi teh podatkov se obravnavajo kot posebne vrste osebnih podatkov v skladu s prvim in tretjim odstavkom prejšnjega člena.

(2) Za obdelave osebnih podatkov iz kazenskih 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 tudi določbe zakona, ki ureja izvrševanje kazenskih sankcij, zakona, ki ureja kazenski postopek, kazenskega zakonika, zakona, ki ureja prekrške, ter mednarodne pogodbe, 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 iz drugih zakonov.

(3) Kazenske 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 mogoče avtomatično posodabljanje podatkov v evidencah oziroma tako, 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 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, da lahko učinkovito uveljavlja pravice iz 12. člena Splošne uredbe, vse informacije iz 13. in 14. člena Splošne uredbe ter vsa sporočila in odgovori iz 15. do 22. člena in 34. člena Splošne uredbe, tako da je to zagotovljeno v jedrnati, pregledni, razumljivi in lahko dostopni obliki ter v jasnem in preprostem jeziku.

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

15. člen

(vložitev zahteve)

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

(2) Za obravnavo zahtev s strani upravljavcev iz javnega sektorja, se glede vprašanj, ki niso urejena v tem delu zakona, subsidiarno 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, na katerega se nanašajo osebni podatki, naslov, morebitni naslov elektronske pošte in druge njegove nujne podatke, potrebne za iskanje in za določitev osebnih podatkov, na katere se zahteva nanaša, oziroma za rešitev zahteve, morebitne podatke o pooblaščencu ali zastopniku posameznika, opredelitev oblike, v kateri želi prejeti odgovor, ter opredelitev zahtevanih osebnih podatkov.

(2) Če je zahteva nepopolna ali nerazumljiva, upravljavec v petih delovnih dneh zahteva, da se pomanjkljivosti odpravijo, in določi vložniku rok za odpravo pomanjkljivosti. Če posameznik, na katerega se nanašajo osebni podatki, v tem roku, ki ne more biti krajši od petih delovnih dni, pomanjkljivosti ne odpravi, upravljavec zavrže njegovo zahtevo oziroma mu pisno sporoči, da je ne bo obravnaval.

17. člen

(preverjanje istovetnosti posameznika)

Upravljavec lahko zaradi potrditve točnosti identitete posameznika, na katerega se nanašajo osebni podatki, zahteva dodatne potrebne informacije. Ugotavljanje identitete posameznika pri zahtevah, vloženih po elektronski pošti, se lahko izvaja tudi:

– v javnem ali zasebnem sektorju z elektronskim podpisom, ki je izenačen z lastnoročnim poddpisom in velja v skladu z Uredbo (EU) št. 910/2014,

– s potrditvijo zahteve 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.

18. člen

(odločitev o zahtevi)

(1) Upravljavec o zahtevi posameznika, na katerega se nanašajo osebni podatki, odloči 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 v skladu s tem ali drugim zakonom.

(2) Če upravljavec o zahtevi ne ravna skladu s prejšnjim odstavkom, se šteje, da je zahtevo zavrnil.

(3) Stranke in stranski udeleženci do sprejema odločitve upravljavca oziroma če je bila zoper to odločitev vložena pritožba, do dokončnosti odločitve Informacijskega pooblaščenca o pritožbi, nimajo pravice do pregledovanja dokumentacije, ki je predmet zahteve.

19. člen

(oblika odgovora)

Upravljavec o zahtevi posameznika, na katerega se nanašajo osebni podatki, odloči z upravno odločbo oziroma v obliki pisnega obvestila, ki vsebuje obrazložitev razlogov za odločitev in informacijo o možnosti pritožbe v skladu s tem zakonom.

20. člen

(ugovor v primeru nepopolne odločitve upravljavca)

Če posameznik, na katerega se nanašajo osebni podatki, po prejeti odločitvi upravljavca meni, da upravljavec ni v celoti odločil o njegovi zahtevi, še zlasti če 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 osmih dneh od prejema odločitve upravljavca. Upravljavec o ugovoru odloči v petih delovnih dneh, o ugovoru glede osebnih podatkov s področij v skladu s 85. členom tega zakona pa v petnajstih delovnih dneh. Rok za pritožbo začne v primeru vložitve ugovora teči po prejemu odločitve o ugovoru oziroma preteku roka za odločitev.

21. člen

(pritožba)

(1) Če upravljavec ne odloči o zahtevi posameznika, na katerega se nanašajo osebni podatki, v roku iz prvega odstavka 18. člena tega zakona oziroma o ugovoru v roku iz prejšnjega člena, lahko posameznik pri Informacijskem pooblaščencu vloži pritožbo zaradi molka upravljavca. Če upravljavec zahtevo oziroma ugovor zavrne, lahko posameznik pri upravljavcu, če gre za javni sektor, oziroma pri Informacijskem pooblaščencu, če gre za zasebni sektor, vloži pritožbo v 15 dneh od prejema obvestila oziroma odločbe upravljavca.

(2) Pravica strank in stranskih udeležencev do pregledovanja dokumentov v zadevah odločanja o posameznikovi pritožbi v skladu z zakonom, ki ureja splošni upravni postopek, do dokončnosti 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.

(3) Po dokončnosti odločbe Informacijskega pooblaščenca o pritožbi pravica oseb iz prejšnjega odstavka vključuje pregled zadeve v obsegu, dovoljenem z dokončno odločbo Informacijskega pooblaščenca ali 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 odloča Informacijski pooblaščenec v skladu z subsidiarno uporabo zakona, ki ureja splošni upravni postopek, razen če je v tem delu zakona določeno drugače.

(2) Posameznik, na katerega se nanašajo osebni podatki, se lahko pritoži tudi zoper:

– višino zaračunane razumne pristojbine iz iz 26. člena tega zakona in

– odločitev upravljavca o podaljšanju roka za obravnavo zahtevkov posameznika iz prvega odstavka 18. člena tega zakona.

23. člen

(pooblastila Informacijskega pooblaščenca v pritožbenem postopku)

(1) V postopku iz prejšnjega člena ima pooblaščena uradna oseba Informacijskega pooblaščenca, ki mora izpolnjevati pogoje za nadzornika, poleg preiskovalnih pooblastil iz prvega odstavka 58. člena Splošne uredbe oziroma 68. člena tega zakona tudi pooblastila iz zakona, ki ureja inšpekcijski nadzor. Druga postopkovna dejanja v upravnem postopku, vključno z dejanji iz drugega in tretjega odstavka tega člena, lahko opravlja in v njih dokončno odloči tudi pooblaščena uradna oseba, ki ne izpolnjuje pogojev za nadzornika.

(2) V postopkih iz prejšnjega člena lahko pooblaščena 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 pooblaščena 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 pooblaščene 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 lahko pooblaščena uradna oseba Informacijskega pooblaščenca namesto izdaje upravne odločbe upravljavcu z ureditvenim predlogom predlaga prostovoljno rešitev posameznikove pritožbe v postavljenem roku, ki ne sme biti daljši od enega meseca, če se z ureditvenim predlogom predhodno strinja posameznik, na katerega se nanašajo osebni podatki in je to smiselno zaradi učinkovitega uresničevanja njegovih pravic. 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 mogoče rešiti v skladu s prejšnjim odstavkom, o pritožbi odloči z odločbo. Zoper odločbo ni dovoljena pritožba, je pa dopusten upravni spor.

(5) Informacijski pooblaščenec lahko za potrebe opravljanja dejanj v pritožbenem postopku tudi brezplačno in neposredno elektronsko dostopa do osebnih podatkov v uradnih evidencah ali javnih knjigah.

24. člen

(izjema glede uveljavljanja pravic posameznika preko zakonitega zastopnika)

Upravljavec lahko izjemoma zavrne zahtevo posameznika iz tega dela zakona ali dostop do posameznikove 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, in če 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 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 prisilitvijo 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 in odgovori upravljavca 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 vsaj petkrat v enem letu), lahko upravljavec s posebno obrazloženo odločitvijo:

– zavrne ukrepanje v zvezi z zahtevo, ali

– zahtevi ugodi, če je po vsebini utemeljena, in posamezniku zaračuna razumno pristojbino, pri čemer upošteva administrativne stroške posredovanja informacij ali sporočila oziroma izvajanja zahtevanega ukrepa v skladu s tem delom zakona.

(3) V primerih iz prejšnjega odstavka upravljavec obrazloži tudi razloge glede očitne neutemeljenosti ali pretiranosti zahteve.

(4) Višino pristojbine iz druge alineje drugega odstavka tega člena ter iz tretjega odstavka 15. člena Splošne uredbe glede dodatnih kopij osebnih podatkov, pravila o zaračunavanju, višino stroškov na področju seznanitve z lastno zdravstveno dokumentacijo in dokumentacijo umrlih pacientov ter povezana pravila o zaračunavanju predpiše Informacijski pooblaščenec, po predhodnem soglasju ministra, pristojnega za pravosodje in ministra, pristojnega za zdravje.

(5) Stroške priprave podatkov za seznanitev, stroške 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 23. členu Splošne uredbe.

(2) Ne glede na določbe prejšnjega odstavka in še zlasti v primerih obdelave osebnih podatkov v okviru strokovnih mnenj, izdelanih v skladu z določbami zakonov, ki urejajo uradne postopke, se, kadar posameznik, na katerega se nanašajo osebni podatki, navaja netočnost in neposodobljenost svojih osebnih podatkov, posamezniku da na razpolago možnost za nasprotni prikaz dejstev. Upravljavec mora nasprotni prikaz dejstev priložiti dokumentom ali, če to ni primerno ali enostavno izvedljivo, ustrezno označiti na njih, kje se ta prikaz nahaja.

28. člen

(sodno varstvo pravic posameznika)

(1) Ne glede na določbe tega zakona lahko posameznik, ki ugotovi, da so kršene njegove pravice, določene s tem zakonom, zahteva sodno varstvo tudi v skladu z zakonom, ki ureja obligacije, pred pristojnim sodiščem, ki odloča po zakonu, ki ureja pravdni postopek.

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

(4) V skladu s prvim odstavkom 80. člena 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 v skladu s tem členom.

(5) Postopek iz tega člena je nujen in prednosten.

III. DEL

UPRAVLJAVEC IN OBDELOVALEC

1. poglavje
Splošne obveznosti

29. člen

(odgovornost za skladnost obdelav osebnih podatkov)

(1) Upravljavec izvaja ustrezne tehnične in organizacijske ukrepe za zagotovitev skladnosti obdelave s Splošno uredbo, tem zakonom in drugimi predpisi, 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 se tudi pregleduje in dopolnjuje, kadar je to potrebno.

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

(3) Upravljavec mora biti sposoben dokazati, da obdelava poteka v skladu s Splošno uredbo, tem zakonom oziroma drugimi predpisi, ki urejajo varstvo osebnih podatkov. To dokazuje še zlasti z vodenjem ustrezne dokumentacije glede izvajanja obveznosti v skladu s tem poglavjem.

(4) Informacijski pooblaščenec izda smernice za izvajanje obveznosti iz tega člena, pri čemer upošteva tudi izdane smernice Odbora glede tega vprašanja ter okvirno opredeli tudi ukrepe za zagotavljanje varnosti osebnih podatkov.

30. člen

(vgrajeno varstvo osebnih podatkov)

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

31. člen

(obdelava s strani obdelovalcev)

(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, 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 upravljavec posebej presodi, ali lahko vključitev dodatnega obdelovalca vpliva na tveganost obdelave osebnih podatkov.

(4) Obdelava pri obdelovalcu poteka 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 zlasti določa, da obdelovalec:

1. osebne podatke obdeluje samo po izkazanih navodilih upravljavca, kar vključuje tudi prenos osebnih podatkov tretji državi ali mednarodni organizaciji, razen 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 z ustreznim potrdilom, ali izpisom iz pogodbe ali iz drugega dogovora, da so osebe, pooblaščene za obdelavo osebnih podatkov, zavezane k varovanju zaupnosti osebnih podatkov ali da za njih velja ustrezna zakonska dolžnost varovanja tajnosti osebnih podatkov;

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 zahtevke glede izvajanja 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 32. do 36. členu Splošne uredbe, ter po pogodbi ali dogovoru lahko tudi nudi pomoč pri izpolnjevanju drugih obveznosti po tem zakonu ali po Splošni uredbi;

7. po zaključku storitev v zvezi z obdelavo vrne vse osebne podatke upravljavcu ter uniči obstoječe kopije, razen če zanj velja zakonska 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 pooblaščena 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 dejanja 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 v skladu s tretjim in četrtim odstavkom tega člena je v pisni 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 zakon, pravo Evropske unije ali pravo druge države članice zahtevata drugačno ravnanje.

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

(9) Obdelovalec, ki bi ne glede na določbe tega zakona in Splošne uredbe 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 30. členom 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 pravne osebe z manj kot 250 zaposlenimi, razen za:

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

– obdelave, ki niso le občasne, ali

– obdelave, ki vključujejo posebne vrste podatkov ali osebne podatke iz 13. člena tega zakona.

(3) Obveznost iz prvega odstavka ne vključuje podatkov o evidencah s področja dela, kot jih določajo zakoni, ki določajo evidence s področja dela.

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

33. člen

(skupni upravljavci)

(1) Če dva ali več upravljavcev skupaj določijo namene in sredstva obdelave, so to skupni upravljavci. Skupni upravljavci z medsebojnim dogovorom določijo 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 iz 13. in 14. člena Splošne uredbe oziroma iz 92. člena tega zakona.

(2) V dogovoru se določi 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 zagotovita ustrezne tehnične in organizacijske ukrepe, s katerimi se varujejo osebni podatki ter preprečuje njihovo naključno, namerno ali drugače nezakonito uničenje, spremembo, izgubo, nepooblaščeno razkritje, dostop ali drugo nepooblaščeno obdelavo.

(2) Ukrepi iz prejšnjega odstavka 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. Upoštevaje te okoliščine, to zlasti vključuje:

a) psevdonimizacijo in šifriranje osebnih podatkov;

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

c) ukrepe za zmožnost pravočasne povrnitve razpoložljivosti osebnih podatkov v primeru varnostnega incidenta, ki je fizično ali tehnološko onemogočil razpoložljivost osebnih podatkov;

č) postopke rednega testiranja, ocenjevanja in vrednotenja učinkovitosti tehničnih in organizacijskih ukrepov;

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

e) 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 petih let od zaključka leta, v katerem je potekala obdelava, razen če za obdelave posameznih vrst osebnih podatkov drug zakon določa drugače.

(3) Upravljavec in obdelovalec zagotovita, da nobena fizična oseba, ki ukrepa pod vodstvom upravljavca ali obdelovalca, ki ima dostop do osebnih podatkov, slednjih ne obdela brez navodil upravljavca, razen če tega od nje ne zahteva zakon, pravo Evropske unije ali pravo druge države članice.

(4) Upravljavec in obdelovalec v svojih notranjih aktih določita 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 iz tega člena, pri čemer upošteva tudi smernice Odbora glede tega vprašanja.

35. člen

(obveščanja Informacijskega pooblaščenca o kršitvah varstva osebnih podatkov)

(1) V primeru kršitve varnosti osebnih podatkov upravljavec brez nepotrebnega odlašanja, po možnosti pa najpozneje v 72 urah po seznanitvi s kršitvijo, o njej v skladu s 33. členom Splošne uredbe uradno obvesti Informacijskega pooblaščenca, razen če ni verjetno, da bi bile s kršitvijo varstva osebnih podatkov ogrožene človekove pravice in temeljne svoboščine posameznikov.

(2) Upravljavec oziroma obdelovalec takoj po zaznavi kršitve zavarujeta dnevniške zapise in druge podatke, na podlagi katerih bi se dalo ugotoviti dejstva v zvezi s kršitvijo, ter jih na poziv predložita

Informacijskemu pooblaščencu. Navedena obveznost ne posega v obveznosti upravljavca oziroma obdelovalca do dokumentiranja kršitve v skladu s petim odstavkom 33. člena Splošne uredbe.

(3) Obdelovalec po seznanitvi s kršitvijo varstva osebnih podatkov brez nepotrebnega odlašanja obvesti upravljavca.

(4) Če je upravljavec osebne podatke prejel oziroma posredoval upravljavcu ali obdelovalcu v drugi državi članici, in je verjetno, da bi zaradi kršitve lahko nastala tveganja tudi za varnost osebnih podatkov pri tem upravljavcu oziroma obdelovalcu, upravljavec oziroma obdelovalec o kršitvi obvestita tudi upravljavca oziroma obdelovalca iz druge države članice.

36. člen

(obveščanje posameznikov o kršitvah varstva osebnih podatkov)

(1) Kadar je verjetno, da kršitev varstva osebnih podatkov povzroči veliko tveganje za pravice in svoboščine posameznikov, upravljavec brez nepotrebnega odlašanja v skladu z drugim odstavkom 34. člena Splošne uredbe sporoči posamezniku, na katerega se nanašajo osebni podatki, da je prišlo do kršitve varstva osebnih podatkov.

(2) Obveščanje iz prejšnjega odstavka ni potrebno v primerih iz tretjega odstavka 34. člena Splošne uredbe, razen če Informacijski pooblaščenec v skladu s četrtim odstavkom 34. člena Splošne uredbe določi drugače.

(3) Kadar se kršitev nanaša na obdelave iz 85. člena tega zakona, obveščanje iz prvega odstavka tega člena ni potrebno oziroma se lahko omeji ali zadrži tudi, če tako določa zakon zaradi razlogov iz četrtega odstavka 92. člena tega zakona.

3. poglavje
Ocena učinka in predhodno posvetovanje

37. člen

(ocena učinka in predhodno posvetovanje)

(1) Kadar bi lahko obdelava, zlasti z uporabo novih tehnologij in upoštevaje 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 35. členom Splošne uredbe.

(2) Oceno učinkov je vedno treba opraviti glede:

– 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,

– obdelave posebnih vrst osebnih podatkov ali osebnih podatkov v zvezi s kazenskimi obsodbami in prekrški v velikem obsegu,

– sistematičnega nadzora javno dostopnega območja v velikem obsegu.

(3) Oceno učinkov se opravi tudi v primerih podobnih obdelav s seznama, ki ga v skladu s pogoji iz četrtega in šestega odstavka 35. člena Splošne uredbe določi in v Uradnem listu Republike Slovenije objavi Informacijski pooblaščenec. .

(4) Ocene učinkov ni treba opraviti glede:

– obdelav s seznama, ki ga v skladu s pogoji iz petega in šestega odstavka 35. člena Splošne odredbe določi in v Uradnem listu Republike Slovenije objavi Informacijskih pooblaščenec,

– 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.

(5) Upoštevaje pogoje iz prvega odstavka tega členaupravljavec v primerih nastanka novih tveganj glede obdelave izvede pregled, ali obdelava poteka v skladu z oceno učinkov.

(6) Če upravljavec obdelavo, za katero je treba opraviti oceno učinkov, zaupa obdelovalcu brez predhodne izvedbe ocene učinkov, mora obdelovalec pridobiti oceno od upravljavca preden začne z obdelavo ali zavrniti izvedbo obdelave.

(7) Kadar iz ocene učinka na varstvo osebnih podatkov izhaja, da bi obdelava osebnih podatkov povzročila veliko tveganje za posameznike, če upravljavec ne bi sprejel ukrepov za ublažitev tveganja, se upravljavec pred obdelavo predhodno posvetuje z Informacijskim pooblaščencem. Zahteva za posvetovanje vsebuje sestavine iz tretjega odstavka 36. člena Splošne uredbe.

(8) Kadar Informacijski pooblaščenec v okviru predhodnega posvetovanja ugotovi, da bi obdelava kršila Splošno uredbo oziroma ta zakon, zlasti kadar upravljavec ni ustrezno opredelil ali ublažil tveganja, Informacijski pooblaščenec najpozneje v osmih tednih po prejemu zahteve za posvetovanje pisno svetuje upravljavcu, kadar je ustrezno, pa tudi obdelovalcu. Ta rok se lahko v skladu s pogoji iz drugega odstavka 36. člena Splošne uredbe tudi podaljša.

4. poglavje
Posebne določbe

38. člen

(pošiljanje osebnih podatkov, ki ga izvajajo osebe javnega sektorja ter brezplačnost pošiljanja)

(1) Posredovanje osebnih podatkov, ki ga izvedejo osebe javnega sektorja, v druge osebe javnega sektorja ali tretjim osebam, je dovoljeno, če je potrebno za izvajanje nalog v pristojnosti osebe javnega sektorja, ki posreduje podatke, ali obveznosti ali nalog tretje osebe, ki se ji podatki prenašajo, ali so izpolnjeni pogoji, ki bi dopuščali obdelavo v skladu z 8. ali 9. ali 12. ali 13. členom tega zakona. Oseba javnega sektorja ali tretja oseba, ki se ji podatki posredujejo, sme osebne podatke obdelovati samo za namen, za uresničevanje katerega se ji posredujejo. Obdelava za druge namene je dovoljena le pod pogoji iz šestega in sedmega odstavka 8. člena tega zakona.

(2) Posredovanje osebnih podatkov, ki ga izvedejo osebe javnega sektorja pravnim ali fizičnim osebam zasebnega sektorja, je dovoljeno, če:

– je potrebno za izvajanje nalog v pristojnosti osebe, ki prejema osebne podatke, in so izpolnjeni pogoji, ki dopuščajo obdelavo v skladu s prejšnjim odstavkom;

– 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

– je potrebno za uveljavljanje, izvajanje ali obrambo pravnih zahtevkov in se je tretja oseba do osebe javnega sektorja, ki posreduje podatke, obvezala, da bo podatke obdelovala samo za namen, za uresničevanje katerega se ji prenašajo.

(3) Posredovanje posebnih vrst osebnih podatkov ter osebnih podatkov iz 13. člena tega zakona je dovoljeno, če so izpolnjeni pogoji iz prvega ali drugega odstavka tega člena in je to v skladu z drugim odstavkom 12. člena ali drugim odstavkom 13. člena tega zakona.

(4) Osebe javnega sektorja v skladu s prvim, drugim in tretjim odstavkom tega člena posredujejo osebne podatke drugim osebam javnega sektorja brezplačno.

(5) Upravljavec registra stalnega prebivalstva, matičnega registra in centralnega registra prebivalstva na način, ki je določen za izdajo potrdila, posreduje upravičencu, ki izkaže pravni interes za uveljavljanje pravic pred osebami javnega sektorja, naslednje osebne podatke, kolikor so glede na konkretne okoliščine zadeve potrebni: osebno ime in naslov stalnega ali začasnega prebivališča oziroma stalni ali začasni naslov prebivališča v drugi državi, naslov za vročanje ali datum smrti posameznika, zoper katerega ali v zvezi s katerim uveljavlja svoje pravice.

(6) Upravljavci ali obdelovalci, ki na podlagi zakona za izvajanje svojih pristojnosti ali nalog pridobivajo osebne podatke iz registrov ali evidenc s področja upravnih notranjih zadev, ki so v upravljanju ministrstva, pristojnega za notranje zadeve, na lastne stroške vzpostavijo varnostne mehanizme, ki jih kot ukrepe ali postopke za izvajanje varnosti osebnih podatkov določi minister, pristojen za notranje zadeve.

(7) 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 osebe zasebnega sektorja)

Oseba iz zasebnega sektorja posreduje osebne podatke drugim fizičnim ali pravnim osebam ali osebam javnega sektorja samo na podlagi zahteve iz drugega odstavka 40. člena tega zakona, iz katere izhaja veljavna pravna podlaga za pridobitev podatkov ter utemeljenost zahteve.

40. člen

(postopek posredovanja osebnih podatkov)

(1) Oseba iz 38. ali 39. člena tega zakona proti plačilu stroškov posredovanja, če zakon ne določa drugače, posreduje osebne podatke drugim fizičnim ali pravnim osebam ali osebam javnega sektorja, ki izkažejo pravno podlago za pridobivanje zahtevanih osebnih podatkov.

(2) Zahteva za posredovanje vsebuje:

1. podatke o vlagatelju zahteve (za fizično osebo: osebno ime, naslov opravljanja dejavnosti ali naslov stalnega ali začasnega prebivališča; za samostojnega podjetnika posameznika, posameznika, ki samostojno opravlja dejavnost, ter za pravno osebo: naziv oziroma firmo in naslov oziroma sedež in matično številko) ter podpis pooblaščene osebe;

2. pravno podlago za pridobitev zahtevanih osebnih podatkov;

3. namen obdelave osebnih podatkov oziroma razloge, ki izkazujejo potrebnost in primernost osebnih podatkov za dosego 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 vlagatelju zahteve, če zakon ne določa drugače, zahtevane osebne podatke posreduje najpozneje v 15 dneh od prejema popolne zahteve, ali pa ga v tem roku pisno obvesti o razlogih, zaradi katerih mu zahtevanih osebnih podatkov ne bo posredoval.

(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 v skladu z zakonom, ki ureja upravni spor. V primeru zavrnitve zahteve za posredovanje osebnih podatkov iz zbirk, ki niso uradne evidence ali javne knjige, lahko vlagatelj zahteva sodno varstvo, o katerem odloča sodišče s splošno pristojnostjo v skladu z zakonom, ki ureja nepravdni postopek.

(6) Ta člen se ne uporablja, če fizična ali pravna oseba ali oseba javnega sektorja uveljavlja pravico do pregledovanja in pridobivanja podatkov iz sodnih, upravnih ali drugih spisov v skladu z drugim zakonom.

(7) Upravljavec za vsako posredovanje osebnih podatkov zagotovi možnost poznejše ugotovitve, kateri osebni podatki so bili posredovani, komu, kdaj in na podlagi katere pravne podlage, 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 upravljavec hrani pet let, razen če drug zakon za posredovanje posameznih vrst podatkov ne določa drugačnega roka.

(9) Sedmi in osmi odstavek tega člena veljata tudi za obdelovalce, če so z zakonom ali pogodbo ali drugim dogovorom 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 posameznika, na katerega se nanašajo, z vpogledom v njegovo osebno izkaznico, potni list, vozniško dovoljenje, ki vsebuje tudi njegovo fotografijo. Ta člen ne posega v določbe drugih zakonov, ki urejajo posamezne osebne dokumente glede dopustnosti kopiranja osebnega dokumenta.

42. člen

uporaba povezovalnih znakov in avtomatizirano odločanje)

(1) Pri pridobivanju osebnih podatkov iz zbirk osebnih podatkov s področja zdravstva, policije, obrambe države, sodstva in državnega tožilstva ter iz kazenske evidence in prekrškovnih evidenc ni dovoljeno uporabljati 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 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 se brez odlašanja napravi uradni zaznamek ali drug ustrezen zapis, ki omogoča naknadno preverjanje nujnosti uporabe povezovalnega znaka.

(3) Na področjih varnosti države se povezovalni znak lahko uporablja tako, 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 in osmega odstavka 40. člena tega zakona.

(4) Prvi odstavek tega člena se ne uporablja za povezovanje v skladu s 112. členom tega zakona ter za zemljiško knjigo, sodni register in poslovni register, če tako določa drug zakon.

(5) Odločitve upravljavcev, ki temeljijo izključno na avtomatizirani obdelavi osebnih podatkov, vključno z oblikovanjem profilov, ki imajo negativne pravne posledice za posameznika, na katerega se osebni podatki nanašajo, oziroma lahko v večji meri vplivajo nanj, so prepovedane, razen če to izrecno določa zakon, ki določa tudi ustrezne ukrepe za varstvo človekovih pravic in temeljnih svoboščin ter upravičenih interesov posameznika, zlasti pravico do ugovora. Kadar te odločitve temeljijo na obdelavi posebnih vrst osebnih podatkov, so prepovedane tudi, če bi lahko vodile do diskriminacije posameznika, na katerega se nanašajo osebni podatki, ali njemu bližnjih oseb. Pred uvedbo sistema postopkov avtomatiziranega odločanja je treba izvesti posebno osredotočeno oceno učinka po 37. člena tega zakona, ki mora vsebovati tudi oceno učinka na povezane človekove pravice in temeljne svoboščine, zlasti glede prepovedi diskriminacije.

43. člen

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

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

(2) Upravljavec ob upoštevanju narave obdelovanih podatkov in tveganj občasno in na dokumentiran način preverja, ali je upoštevan prejšnji odstavek.

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

IV. DEL
POOBLAŠČENE OSEBE ZA VARSTVO OSEBNIH PODATKOV, KODEKSI RAVNANJA IN CERTIFICIRANJE

1. poglavje
Pooblaščene osebe za varstvo osebnih podatkov

44. člen

(pooblaščena oseba)

Pooblaščena oseba za varstvo osebnih podatkov (v nadaljnjem besedilu: pooblaščena oseba) je oseba, ki upravljavcu ali obdelovalcu na neodvisen način pomaga pri zagotovitvi skladnosti obdelave s Splošno uredbo, tem zakonom in drugimi zakoni, ki urejajo obdelavo in varstvo osebnih podatkov.

45. člen

(obveznost določitve pooblaščene osebe)

(1) Pooblaščeno osebo določijo:

– upravljavci in obdelovalci v javnem sektorju,

– tisti upravljavci ali obdelovalci v zasebnem sektorju, katerih temeljne dejavnosti ali naloge 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, in

– tisti upravljavci ali obdelovalci v zasebnem sektorju, katerih temeljne dejavnosti ali naloge zajemajo obsežne obdelave posebnih vrst osebnih podatkov ali osebnih podatkov iz 13. člena tega zakona.

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

(3) Vsak upravljavec ali obdelovalec, ki je določil pooblaščeno osebo, lahko imenuje njenega namestnika za čas njene zadržanosti ali odsotnosti.Namestnik mora izpolnjevati pogoje za pooblaščeno osebo v skladu s tem zakonom. Namestnik opravlja naloge pooblaščene osebe in ima vsa pooblastila in upravičenja v skladu s z 39. členom Splošne uredbe in tem zakonom za čas zadržanosti ali odsotnosti pooblaščene osebe.

(4) Upravljavec ali obdelovalec, ki je določil pooblaščeno osebo, v osmih dneh od določitve vpiše njene kontaktne podatke v skladu s 30. členom Splošne uredbe v svojo evidenco dejavnosti obdelav iz 32. člena tega zakona in njen kontakt ter način možnega kontakta javno objavi na primeren način, zlasti na spletni strani. Konkretne kontaktne podatke pooblaščene osebe (osebno ime, telefonska številka, lahko tudi naslov elektronske pošte) sporoči v roku iz prvega stavka tega odstavka Informacijskemu pooblaščencu.

46. člen

(pogoji za določitev pooblaščene osebe)

(1) Za pooblaščeno osebo upravljavca ali obdelovalca v javnem sektorju se lahko določi posameznika, ki izpolnjuje 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,

5. 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 in obsodba še ni bila izbrisana.

(2) Pooblaščena oseba državnega organa mora poleg pogojev iz prejšnjega odstavka izpolnjevati tudi pogoj, da je zaposlena v javnem sektorju.

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

(4) Upravljavci ali obdelovalci iz javnega sektorja, razen državnih organov, lahko za pooblaščeno osebo, če je ni mogoče določiti znotraj osebe javnega sektorja v skladu s tem zakonom ali določiti skupne pooblaščene osebe z drugimi upravljavci ali obdelovalci javnega sektorja, lahko s pogodbo v pisni obliki določijo tudi posameznika ali posameznico iz zasebnega sektorja ali pravno osebo iz zasebnega sektorja v skladu s petim odstavkom tega člena.

(5) Upravljavci ali obdelovalci iz zasebnega sektorja za pooblaščeno osebo določijo osebo, ki je zaposlena pri njih, ali pa s pogodbo v pisni obliki določijo drugega posameznika ali pravno osebo. V pogodbi s pravno osebo se določi vodilni član, ki odgovarja za delo pravne osebe kot pooblaščene osebe in katerega kontaktni podatki se objavijo v skladu s četrtim odstavkom prejšnjega člena.

(6) Pooblaščena oseba, ki je lahko le posameznik ali vodilni član v pravni osebi, mora izpolnjevati pogoje iz prvega odstavka tega člena, razen pogoja državljanstva Republike Slovenije ali države članice Evropske unije ali države članice Evropskega gospodarskega prostora.

(7) Druge osebe, ki pooblaščeni osebi pomagajo pri izvajanju nalog, morajo izpolnjevati pogoje iz prvega odstavka tega člena, razen razen pogoja državljanstva Republike Slovenije ali države članice Evropske unije ali države članice Evropskega gospodarskega prostora. Te osebe so pri svojem delu vezane na navodila pooblaščene osebe.

(8) Za pooblaščeno osebo in osebe, ki ji pomagajo pri izvajanju njenih nalog, se ne smedoločiti oseb, ki so v konfliktu interesov z upravljavcem ali obdelovalcem ali bi bilo njihovo delo kot pooblaščene osebe v konfliktu z njegovimi drugimi nalogami ali s položajem pri upravljavcu ali obdelovalcu.

(9) V javnem sektorju se šteje, da je določena oseba v konfliktu interesov, če ima položaj predstojnika v 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. Če pooblaščena oseba izve za situacijo, ki predstavlja ali bi lahko predstavljala konflikt interesov, o tem takoj pisno obvesti upravljavca oziroma obdelovalca. Upravljavec oziroma obdelovalec v tem primeru odpravi konflikt ali pooblaščeno osebo razreši ob upoštevanju določb tretjega in četrtega odstavka 50. člena tega zakona. Enako velja tudi za osebe, ki pooblaščeni osebi pomagajo pri izvajanju njenih nalog.

(10) Osmi in deveti odstavek se smiselno uporabljata za zasebni sektor.

47. člen

(skupna določitev pooblaščene osebe)

(1) Več upravljavcev oziroma obdelovalcev iz javnega ali več upravljavcev iz zasebnega sektorja lahko ob upoštevanju njihove organizacijske strukture in velikosti ter pod pogoji iz prejšnjega člena, določi skupno pooblaščeno osebo. Pri tem zagotovijo, da je pooblaščena oseba še vedno sposobna opravljati svoje naloge v zvezi z vsemi upravljavci ali obdelovalci, za katere je imenovana.

(2) Občine lahko pod pogoji iz prejšnjega člena določijo skupno pooblaščeno osebo v okviru skupne občinske uprave ali v drugem dogovoru med občinami, vključno z določitvijo skupne pooblaščene osebe v okviru združenja občin, ki jih opredeljuje zakon, ki ureja lokalno samoupravo..

(3) Javni zavodi lahko v dogovoru z občinami ustanoviteljicami določijo skupno pooblaščeno osebo za te javne zavode v skladu s prejšnjim odstavkom ali določijo, da bo naloge pooblaščene osebe za javni zavod opravljala pooblaščena oseba občine ustanoviteljice.

(4) Kadar obveznosti določitve pooblaščene osebe veljajo tudi za odvetnike, lahko odvetniki samostojno določijo z dogovorom z Odvetniško zbornico Slovenije skupno pooblaščeno osebo, ki je zaposlena na Odvetniški zbornici Slovenije.

48. člen

(naloge pooblaščene osebe)

(1) Pooblaščena oseba opravlja naloge iz 39. člena Splošne uredbe ter zlasti svetuje in pomaga pri ocenjevanju tveganj glede varnosti osebnih podatkov v zvezi obdelavami osebnih podatkov v zbirkah., in sicer v zvezi z vsemi obdelavami osebnih podatkov, ki jih izvaja upravljavec oziroma obdelovalec, pri katerem je določena.

(2) Pooblaščena oseba sodišča ali državnega tožilstva ne sme opravljati navedenih nalog v zvezi z obdelavami osebnih podatkov, izvršenimi 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 jih opredleujejo zakon, ki ureja sodišča, in zakon, ki ureja državna tožilstva in zakoni, ki urejajo sodne postopke. Pooblaščena oseba lahko opravlja te naloge iz prejšnjega odstavka samo glede zadev sodne uprave in državnotožilske uprave, kar vključuje tudi zagotavljanje varnosti osebnih podatkov.

(3) Pooblaščena oseba Ustavnega sodišča Republike Slovenije ne sme opravljati nalog iz prvega odstavka tega člena v zvezi z obdelavami osebnih podatkov, izvršenimi v okviru neodvisnega sodniškega odločanja Ustavnega sodišča Republike Slovenije, kot jih opredeljuje zakon, ki ureja ustavno sodišče, ali drugi zakoni. Pooblaščena oseba lahko opravlja naloge iz prvega odstavka tega člena samo glede zadev sodne uprave Ustavnega sodišča ter glede izvajanja varnosti osebnih podatkov.

(4) Pooblaščena oseba Varuha oziroma Varuhinje človekovih pravic (v nadaljnjem besedilu: Varuh človekovih pravic) ne sme opravljati nalog iz prvega odstavka tega člena v zvezi z obdelavami osebnih podatkov, izvršenimi v okviru delovanja Varuha človekovih pravic, kot jih opredeljujejo zakoni, ki določajo njegove pristojnosti ali pooblastila. Pooblaščena oseba lahko opravlja naloge iz prvega odstavka tega člena samo glede zadev obdelav osebnih podatkov s področja zagovorništva 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 pooblaščeno osebo, ki opravlja naloge v skladu s tretjim odstavkom prejšnjega člena.

(2) Vrhovno sodišče Republike Slovenije (v nadaljnjem besedilu: Vrhovno sodišče) določi pooblaščeno osebo, ki opravlja naloge v skladu z drugim odstavkom prejšnjega člena za vsa sodišča s splošno pristojnostjo in specializirana sodišča v Republiki Sloveniji.

(3) Vrhovno državno tožilstvo Republike Slovenije določi pooblaščeno osebo, ki opravlja naloge v skladu z drugim odstavkom prejšnjega člena za vsa državna tožilstva v Republiki Sloveniji.

(4) Varuh človekovih pravic določi pooblaščeno osebo, ki opravlja naloge v skladu s četrtim odstavkom prejšnjega člena.

(5) Vsak minister ali ministrica določi pooblaščeno osebo, ki je zaposlena na njegovem ali njenem ministrstvu. Če je v okviru ministrstva ustanovljen organ v sestavi, lahko minister ali ministrica za pooblaščeno osebo organa v sestavi določita javnega uslužbenca, ki je zaposlen v organu v sestavi.

(6) Na področjih izvajanja obveščevalnih in protiobveščevalnih nalog države predstojnik organizacije s tega področja določi pooblaščeno osebo in njenega namestnika znotraj organizacije s tega področja, ki opravlja tiste naloge iz 39. člena Splošne uredbe, za katere tako določi predstojnik, med njih pa so obvezno vključene naloge glede zagotavljanja varnosti osebnih podatkov, posredovanja osebnih podatkov Vladi Republike Slovenije, Predsedniku Republike Slovenije, policiji, državnim tožilstvom, sodiščem in pristojnemu delovnemu telesu Državnega zbora Republike Slovenije (v nadaljnjem besedilu: državni zbor) ter glede čezmejnih obdelav in prenosov osebnih podatkov.

(7) Pooblaščene osebe za upravne enote lahko določi ministrstvo, pristojno za javno upravo. Več upravnih enot ima lahko skupno pooblaščeno osebo, ki pa mora biti zaposlena v javnem sektorju.

50. člen

(položaj pooblaščene osebe)

(1) Upravljavec ali obdelovalec pooblaščeni osebi zagotovita pogoje za učinkovito in neodvisno opravljanje njenih nalog v skladu z 48. členom tega zakona, zlasti da:

1. je ustrezno in pravočasno vključena v vsa vprašanja in postopke, povezane z varstvom osebnih podatkov, in ima možnost podati ustrezni nasvet, mnenje, predlog ali opozorilo,

2. ima dostop do osebnih podatkov ter dejavnosti 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 stopijo v stik in se posvetujejo glede vseh vprašanj, povezanih z obdelavo njihovih osebnih podatkov in uresničevanjem njihovih pravic iz Splošne uredbe, ter

5. ima neposreden dostop do vodstva upravljavca ali obdelovalca, če oceni, da je to zaradi pomembnosti določene obdelave osebnih podatkov nujno, zlasti kadar gre za tvegane obdelave, obdelave posebnih vrst osebnih podatkov ali osebnih podatkov iz 13. člena tega zakona, množične obdelave in vpliv na človekove pravice, temeljne svoboščine ali interese posameznikov, na katere se nanašajo osebni podatki, ali za očitno neustreznost ukrepov in postopkov varnosti osebnih podatkov. Neposredni dostop vključuje možnost predstavitve stališč ali ocen o neustreznosti varstva osebnih podatkov.

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

(3) Pooblaščena oseba mora podati privolitev za njeno določitev.

(4) Pooblaščena oseba lahko kadarkoli zahteva njeno razrešitev z navedbo razlogov.

(5) Upravljavec oziroma obdelovalec pooblaščene osebe zaradi izvajanja njenih nalog ne sme razrešiti, je kaznovati ali je zapostavljati.

(6) Pooblaščeni osebi se delovno razmerje ne sme odpovedati za čas njene določitve in še eno leto po prenehanju določitve, če ravna v skladu z zakonom, kolektivno pogodbo in pogodbo o zaposlitvi, razen če v primeru poslovnega razloga odkloni ponujeno ustrezno zaposlitev pri delodajalcu ali če gre za odpoved pogodbe o zaposlitvi v postopku prenehanja delodajalca.

51. člen

(dolžnost varstva tajnosti osebnih podatkov)

(1) Pooblaščena oseba in osebe, ki izvajajo pomoč pri opravljanju njenih nalog, so pri opravljanju nalog zavezane k varstvu tajnosti obdelovanih osebnih podatkov. Informacije, ki so jim bile dane na razpolago, smejo uporabljati izključno za opravljanje nalog in so tudi po zaključku dejavnosti zavezane k varstvu tajnosti osebnih podatkov.

(2) Dolžnost iz prejšnjega odstavka velja zlasti v zvezi z identiteto posameznika, na katerega se nanašajo osebni podatki, ki se je obrnil na pooblaščeno osebo za varstvo podatkov.

(3) Če ima pooblaščena oseba pri svoji dejavnosti glede seznanjenosti z dejanji obdelave osebnih podatkov, v zvezi s katerimi ima oseba, ki je nadrejena pooblaščeni osebi, pravico do molka, ta pravica velja za postopek po prekršku tudi za pooblaščeno osebo in osebe, ki izvajajo pomoč pri opravljanju njenih nalog, in sicer do mere, v kateri je nadrejena 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, ki jih na prostovoljni podlagi razvijajo in pripravljajo združenja ali drugi predstavniki upravljavcev ali obdelovalcev na določenem področju, tudi ob upoštevanju posebnosti mikro, majhnih in srednjih gospodarskih družb, potrjujejo pa Informacijski pooblaščenec, Odbor oziroma Evropska komisija.

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

(3) Informacijski pooblaščenec po prejemu osnutka izvede ugotovitveni postopek, v okviru katerega ugotovi, ali je predloženi osnutek kodeksa skladen s Splošno uredbo.

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

(5) Kodeksi ravnanja, ki jih potrdi Informacijski pooblaščenec, so za upravljavce in obdelovalce, na katere se nanašajo, obvezni. Enako velja za kodekse ravnanja, ki jih v okviru postopka pregleda v skladu z devetim odstavkom 43. člena v zvezi z drugim odstavkom 93. člena Splošne uredbe z izvedbenim aktom dodatno potrdi in objavi Evropska komisija.

(6) Če Informacijski pooblaščenec v ugotovitvenem postopku iz tretjega odstavka tega člena 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. Če 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, in objavi v Uradnem listu Republike Slovenije. Če ugotovi, da se osnutek nanaša na takšno obdelavo, pa v skladu s sedmim odstavkom 40. člena Splošne uredbe postopek prekine in osnutek kodeksa s sklepom predloži v mnenje Odboru iz 68. člena Splošne uredbe. Če Odbor osnutka kodeksa v svojem mnenju 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 in objavi v Uradnem listu Republike Slovenije.

(7) Spremljanje skladnost obdelav z odobrenim kodeksom ravnanja izvaja Informacijski pooblaščenec.

(8) Informacijski pooblaščenec za spremljanje skladnosti obdelav z odobrenim kodeksom 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) Za certificiranje se uporabljajo merila, ki jih v skladu s petim odstavkom 42. člena Splošne uredbe odobri Informacijski pooblaščenec ali Odbor.

(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 dejanj obdelave osebnih podatkov s Splošno uredbo, tem zakonom in drugimi zakoni in ne posega v nadzorne pristojnosti Informacijskega pooblaščenca v skladu z določbami tega zakona ali Splošne uredbe.

(4) Informacijski pooblaščenec upravlja seznam odobrenih certifikacijskih mehanizmov in 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 (Slovenska akreditacija), v skladu z b) točko prvega odstavka 43. člena Splošne uredbe in zakonom, ki ureja akreditacijo. Dodatne zahteve v skladu z b) točko prvega odstavka in tretjim odstavkom 43. člena Splošne uredbe določi Informacijski pooblaščenec.

(2) Slovenska akreditacija izda akreditacijsko listino certifikacijskemu telesu in o tem obvesti Informacijskega pooblaščenca. Zoper to odločbo je dovoljena pritožba v skladu z zakonom, ki ureja akreditacijo, zoper odločitev o pritožbi pa je dopusten upravni spor.

(3) Če Odbor ali Informacijski pooblaščenec spremenita merila iz drugega odstavka prejšnjega člena ali Informacijski pooblaščenec spremeni dodatne zahteve iz prvega odstavka tega člena, Informacijski pooblaščenec o tem obvesti Slovensko akreditacijo.

V. DEL
PRENOS OSEBNIH PODATKOV V TRETJE DRŽAVE ALI MEDNARODNE ORGANIZACIJE

55. člen
(splošno načelo za prenose)

Vsak prenos osebnih podatkov, ki se obdelujejo ali so namenjeni obdelavi po prenosu v tretjo državo ali mednarodno organizacijo, se ob upoštevanju določb Splošne uredbe oziroma tega zakona lahko izvede le, če upravljavec in obdelovalec ravnata v skladu s pogoji iz V. poglavja Splošne uredbe oziroma tega dela zakona, kar velja tudi za nadaljnje prenose osebnih podatkov iz tretje države ali mednarodne organizacije v drugo tretjo državo ali drugo mednarodno organizacijo. Vsi ti pogoji se uporabljajo za zagotovitev, da ni ogrožena raven varstva osebnih podatkov posameznikov, ki jo zagotavlja Splošna uredba.

56. člen
(prenosi na podlagi sklepa o ustreznosti)

(1) Prenos osebnih podatkov v tretjo državo ali mednarodno organizacijo se lahko izvede, če je Evropska komisija s sklepom predhodno ugotovila, da zadevna tretja država, ozemlje, eden ali več določenih sektorjev v tej tretji državi ali mednarodna organizacija zagotavljajo ustrezno raven varstva podatkov.

(2) Za tak prenos ni potrebno posebno dovoljenje Informacijskega pooblaščenca.

57. člen
(prenosi, za katere se uporabljajo ustrezni zaščitni ukrepi)

(1) Prenos osebnih podatkov v tretjo državo ali mednarodno organizacijo, za katero ne obstaja sklep o ustreznosti iz prejšnjega člena, se lahko izvede le, če upravljavec ali obdelovalec, ki želi prenesti osebne podatke, zagotovi ustrezne zaščitne ukrepe za zagotovitev ustrezne ravni varstva osebnih podatkov po njihovem prenosu, in pod pogojem, da tretja država oziroma mednarodna organizacija posameznikom zagotavljata izvševanje njihovih pravic v skladu s Splošno uredbo oziroma učinovita pravna sredstva zoper morebitne kršitve Splošne uredbe.

(2) Zaščitni ukrepi v skladu s prejšnjim odstavkom se lahko zagotovijo z naslednjimi delovanji, pri čemer za zaščitne ukrepe in prenos ni potrebno posebno dovoljenje Informacijskega pooblaščenca:

a) zavezujočo in izvršljivo mednarodno pogodbo med Republiko Slovenijo ter javnim organom ali telesom tretje države;

b) zavezujočimi poslovnimi pravili, ki jih je odobril Informacijski pooblaščenec;

c) standardnimi določbami o varstvu podatkov, ki jih je v skladu s postopkom pregleda iz drugega odstavka 93. člena Splošne uredbe sprejela Evropska komisija;

č) standardnimi določbami o varstvu osebnih podatkov, ki jih sprejme Informacijski pooblaščenec in odobri Komisija v skladu s postopkom pregleda iz drugega odstavka 93. člena Splošne uredbe;

d) kodeksom ravnanja v skladu z 52. členom tega zakona, pri čemer se morata upravljavec ali obdelovalec v tretji državi izvršljivo zavezati, da bosta izvajala v kodeksu določene zaščitne ukrepe, vključno z ukrepi za zagotavljanje pravic posameznikov, na katere se nanašajo osebni podatki, ali

e) odobrenim mehanizmom certificiranja v skladu s 53. členom tega zakona.

(3) Zaščitni ukrepi v skladu s prvim odstavkom tega člena se lahko zagotovijo tudi z določbami v mednarodni pogodbi, ki obvezuje Republiko Slovenijo, ki vključujejo izvršljive in učinkovite pravice za posameznike, na katere se nanašajo podatki.

58. člen

(odstopanja v posebnih primerih)

(1) Prenos osebnih podatkov v tretjo državo ali mednarodno organizacijo, za katero ne obstaja sklep o ustreznosti iz 56. člena tega zakona oziroma zanj niso bili sprejeti ustrezni zaščitni ukrepi v skladu s prejšnjim členom, se lahko izvede le:

a) če je posameznik, na katerega se nanašajo osebni podatki, izrecno privolil v predlagani prenos, potem ko je bil obveščen o morebitnih tveganjih, ki jih zaradi nesprejetja sklepa o ustreznosti in ustreznih zaščitnih ukrepov takšni prenosi pomenijo zanj;

b) če je prenos potreben za izvajanje pogodbe med posameznikom, na katerega se nanašajo osebni podatki, in upravljavcem ali za izvajanje predpogodbenih ukrepov, sprejetih na zahtevo posameznika, na katerega se nanašajo osebni podatki;

c) če je prenos potreben za sklenitev ali izvajanje pogodbe med upravljavcem in drugo fizično ali pravno osebo, ki je v interesu posameznika, na katerega se nanašajo osebni podatki;

č) če je prenos potreben zaradi pomembnih razlogov javnega interesa, določenih z zakonom;

d) če je prenos potreben za uveljavljanje, izvajanje ali obrambo pravnih zahtevkov;

e) če je prenos potreben za zaščito življenjskih interesov posameznika, na katerega se nanašajo osebni podatki, ali drugih oseb, kadar posameznik, na katerega se nanašajo osebni podatki, fizično ali pravno ni sposoben dati privolitve; ali

f) če se prenos opravi iz uradne evidence, javne knjige ali drugega registra, ki je namenjen zagotavljanju informacij javnosti in je na voljo za vpogled bodisi javnosti na splošno bodisi katerikoli osebi, ki lahko izkaže zakonit interes, vendar le, če so v posameznem primeru izpolnjeni pogoji za tak vpogled, določeni s pravom Evropske unije.

(2) Upravljavec ali obdelovalec dokumentira ustrezne zaščitne ukrepe v evidenci iz 32. člena tega zakona.

59. člen

(postopek pridobitve odobritve Informacijskega pooblaščenca)

(1) Upravljavec ali obdelovalec, ki namerava prenesti osebne podatke v tretjo državo ali mednarodno organizacijo na podlagi zavezujočih poslovnih pravil ali pogodbenih določb, mora pred začetkom prenosa pridobiti dovoljenje Informacijskega pooblaščenca.

(2) V vlogi za pridobitev dovoljenja se navedejo podatki o upravljavcu ali obdelovalcu, h kateremu naj bi se podatke iznašalo, vrste teh podatkov, trajanje iznosa, vsebino zaščitnih ukrepov ter posebej način, kako bodo v tretji državi oziroma pred mednarodno organizacijo zagotovljene pravice posameznikov oziroma pravno varstvo.

(3) Informacijsjki pooblaščenec izda odločbo v dveh mesecih od prejema popolnih informacij iz prejšnjega odstavka.

(4) Zoper odločbo pritožba ni dovoljena, dopusten pa je upravni spor.

VI. DEL

NADZORNI ORGAN ZA VARSTVO OSEBNIH PODATKOV REPUBLIKE SLOVENIJE

1. poglavje

Položaj, 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 v Republiki Sloveniji v skladu s Splošno uredbo in tem zakonom je Informacijski pooblaščenec, kot ga določa zakon, ki ureja Informacijskega pooblaščenca.

(2) Pri Informacijskem pooblaščencu delujejo državne nadzornice oziroma državni nadzorniki za varstvo osebnih podatkov (v nadaljnjem besedilu: nadzornik), ki imajo pristojnosti inšpekcijskega nadzora in druge naloge glede varstva osebnih podatkov v skladu s Splošno uredbo, tem zakonom in drugimi zakoni ali predpisi.

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

61. člen

(temeljne pristojnosti Informacijskega pooblaščenca)

(1) Informacijski pooblaščenec samostojno in neodvisno izvaja inšpekcijski nadzor nad izvajanjem 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 5. členom tega zakona.

(4) Informacijski pooblaščenec je prav tako pristojen za izvajanje inšpekcijskih nadzorov nad obdelavo osebnih podatkov, ki se izvajajo v okviru dejavnosti upravljavca z glavnim ali edinim sedežem v drugi državi članici, če se obdelave nanaša zgolj na sedež v njegovi državi članici ali znatno vpliva zgolj na posameznike v Republiki Sloveniji, pri čemer mora o začetku nadzora takoj obvestiti vodilni nadzorni organ zadevne druge države članice.

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

62. člen

(izjeme glede pristojnosti Informacijskega pooblaščenca)

(1) Ne glede na tretji in četrti odstavka prejšnjega člena Informacijski pooblaščenec ni pristojen za inšpekcijski in prekrškovni nadzor glede:

1. obdelav osebnih podatkov, izvršenih v okviru izvajanja neodvisnega sodniškega odločanja, 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 postopkov kazenskega pregona ali uporabe pravnih sredstev v skladu z zakonom, ki ureja državno tožilstvo,

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

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

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

6. obdelav osebnih podatkov na področju zaščitenih prič v skladu z zakonom, ki ureja zaščito prič, v delu, v katerem bi bila lahko razkrita identiteta teh posameznikov,

7. obdelav osebnih podatkov varnostno preverjanih oseb v skladu z zakonom, ki ureja tajne podatke, iz katerih bi lahko bila razkrita identiteta virov ugotavljanja oziroma preverjanja prejetih osebnih podatkov, ki jih organom, pristojnim za varnostno preverjanje, posredujejo pristojni organi v skladu z zakonom, ki ureja obrambo, ali zakonom, ki ureja Slovensko obveščevalno-varnostno agencijo,

8. obdelav osebnih podatkov iz tretjega odstavka 5. člena tega zakona.

63. (2) Informacijski pooblaščenec je ne glede na prejšnji odstavek pristojen za opravljanje inšpekcijskega nadzora na vseh ostalih delovnih področjih državnih organov ali odločanj ali delovanj funkcionarjev, ki niso določena v prejšnjem odstavku, zlasti 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, razen kadar gre za posredovanje osebnih podatkov med sodišči za potrebe odločanja v sodnih postopkih za potrebe sodnega odločanja ali med državnimi tožilstvi za potrebe državnotožilskega odločanja. V zvezi z 8. točko prejšnjega odstavka Informacijski pooblaščenec glede ustreznega spoštovanja pravil iz tretjega odstavka 5. člena tega zakona sodeluje z nadzornim organom druge države članice, če ga ta nadzorni organ pri

njegovem opravljanju nadzora pozove k sodelovanju glede ustreznega spoštovanja teh pravil.člen

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

(1) Vlada, ministrstva, državni zbor, državni svet, organi samoupravnih lokalnih skupnosti, drugi državni organi ter nosilci javnih pooblastil v postopku priprave predlogov zakonov, podzakonskih predpisov ter drugih splošnih aktov (v nadaljnjem besedilu: pravni akt) pridobijo predhodno mnenje Informacijskega pooblaščenca o skladnosti teh pravnih aktov s tem zakonom, Splošno uredbo, drugimi zakoni in drugimi predpisi, ki urejajo osebne podatke. Kadar predlagani pravni akt predvideva tudi obdelave, glede katerih je treba v skladu s 37. členom tega zakona opraviti oceno učinka na varstvo osebnih podatkov, predlagatelj pravnega akta Informacijskemu pooblaščencu predloži tudi oceno učinka.

(2) Kadar zakon določa, da Informacijski pooblaščenec da soglasje k predlogu podzakonskega predpisa ter drugega splošnega akta, se smiselno uporabljajo določbe prejšnjega odstavka.

(3) 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.

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

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 v skladu z 62. členom Splošne uredbe.

(3) V okviru delovanja iz prejšnjega odstavka člani ali osebje nadzornega organa druge države članice izvajajo nadzor tako, da nadzor vodi Informacijski pooblaščenec, če se nadzor izvaja na ozemlju Republike Slovenije ali v okviru pristojnosti Informacijskega pooblaščenca v skladu s tem zakonom, pri čemer lahko uporabljajo le preiskovalna pooblastila iz tega zakona ali Splošne uredbe, če jih je za to pooblasti Informacijski pooblaščenec. Člani ali osebje drugega nadzornega organa krijejo svoje stroške.

(4) Kadar Informacijski pooblaščenec izvaja nadzor v skladu z drugim odstavkom tega člena 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 v skladu s tem zakonom in Splošno uredbo se uporabljajo določbe Splošne uredbe in tega zakona ter določbe zakona, ki ureja inšpekcijski nadzor, in določbe zakona, ki ureja splošni upravni postopek, če Splošna uredba ali ta zakon ne določata drugače.

66. člen

(obseg inšpekcijskega nadzora)

V okviru inšpekcijskega nadzora Informacijski pooblaščenec:

1. nadzoruje skladnost obdelave osebnih podatkov s Splošno uredbo, tem zakonom in drugimi predpisi, 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 njihovemu prenosu uporabnikom v tretji državi ali mednarodni organizaciji ter čezmejno obdelavo osebnih podatkov.

67. člen

(neposredno opravljanje inšpekcijskega nadzora)

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

(2) Nadzornik, informacijski pooblaščenec in namestnik informacijskega pooblaščenca izkazujejo pooblastilo za opravljanje nalog inšpekcijskega nadzora s službeno izkaznico, ki vsebuje fotografijo nadzornika, informacijskega pooblaščenca oziroma namestnika informacijskega pooblaščenca, njegovo osebno ime, strokovni ali znanstveni naslov, navedbo organa in pooblaščenost za izvajanje inšpekcijskega nadzora. Obliko in vsebino službene izkaznice podrobneje določi Informacijski pooblaščenec.

68. člen

(preiskovalna pooblastila)

(1) Nadzornik, namestniki informacijskega pooblaščenca in informacijski pooblaščenec lahko pri opravljanju inšpekcijskega nadzora poleg uporabe preiskovalnih pooblastil iz prvega odstavka 58. člena Splošne uredbe, tudi:

1. pregledujejo vsebino zbirk ne glede na njihovo tajnost ali drugo vrsto zaupnosti;

2. pregledujejo 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 opravijo pregled vsebine in preverijo način delovanja zavezančevih spletnih strani in drugih javno elektronsko dostopnih storitev, če je to nujno zaradi varovanja človekovih pravic, temeljnih svoboščin ali interesov posameznikov, na katere se nanašajo osebni podatki ali je to potrebno zaradi nujnosti zavarovanja dokazov;

4. preverjajo postopke in ukrepe ter pregledujejo dokumentacijo in akte, ki se nanašajo na varnost osebnih podatkov oziroma na njeno izvajanje;

5. pregledujejo prostore, v katerih se obdelujejo osebni podatki, elektronske naprave, stvari in drugo opremo ter tehnično dokumentacijo;

6. izvajajo druga pooblastila, določena z zakonom, ki ureja inšpekcijski nadzor, zakonom, ki ureja splošni upravni postopek, ali drugim zakonom.

(2) Kadar se izvaja ukrep iz 2. oziroma 5. točke prejšnjega odstavka in upravljavec ali obdelovalec iz zasebnega sektorja za verjetno izkažeta, da obstaja očitna možnost, da bi lahko prišlo do posega v pravice do komunikacijske zasebnosti ali prostorske zasebnosti ali v odvetniško zaupnost, ter ne podata privolitve za izvedbo katerega od teh ukrepov, preiskovalni sodnik krajevno pristojnega sodišča, pristojen po prebivališču oziroma sedežu zavezanca za kazenske zadeve, odloči, da 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, elektronskih naprav, dokumentacije, druge opreme in stvari v njem našli dokazi, ki so pomembni za odločanje v postopku inšpekcijskega nadzora ali v prekrškovnem postopku.

(3) Odločbo iz prejšnjega odstavka izda preiskovalni sodnik najpozneje v 24 urah od vložitve predloga Informacijskega pooblaščenca. Odločba vsebuje:

– opredelitev prostorov oziroma elektronskih naprav oziroma dokumentacije oziroma druge opreme oziroma stvari, ki jih je treba pregledati,

– opredelitev razlogov za preiskavo,

– opredelitev dokazov oziroma vsebine podatkov, ki se iščejo, in

– navedbo okoliščin, ki utemeljujejo uporabo preiskovalnega pooblastila in način njegove izvršitve.

(4) Pregled elektronskih naprav v skladu z drugim in tretjim odstavkom tega člena se opravi v skladu z odredbo preiskovalnega sodnika in 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 upravljavca ali obdelovalca ali njunega predstavnika. Če določeno elektronsko napravo iz prostora zavezanca uporablja oseba, ki upravičeno pričakuje zasebnost na njej, ima tudi ona pravico biti navzoča ob pregledu njene vsebine.

(5) O opravljenem inšpekcijskem ogledu v skladu s tem členom se sestavi zapisnik, ki se lahko ne glede na določbe zakonov, ki urejata splošni upravni in inšpekcijski postopek, v primeru, ko ne gre za nujne in neodložljive ukrepe, sestavi v 15 dneh od dneva opravljenega nadzora ter se vroči upravljavcu ali obdelovalcu ali osebi iz tretjega stavka prejšnjega odstavka. Zapisnik vsebuje ugotovljeno dejansko stanje, ki vključuje dejstva in okoliščine, pomembne za odločbo, vključno s posnetki in izpisi podatkov s spletnih strani ter drugimi pridobljenimi podatki. Upravljavec ali obdelovalec lahko na zapisnik data pripombe ter se o ugotovljenih dejstvih in okoliščinah pisno ali ustno izjavita v roku, ki ga določi nadzornik in ne sme biti krajši od dveh delovnih dni po vročitvi zapisnika, o čemer se ju v zapisniku izrecno pouči.

69. člen

(popravljalna pooblastila in ukrepi ter njihove omejitve)

(1) Nadzornik, informacijski pooblaščenec ali namestnik informacijskega pooblaščenca, ki pri opravljanju inšpekcijskega nadzora ugotovijo kršitev določb Splošne uredbe, tega zakona ali drugega zakona ali predpisa, ki ureja varstvo osebnih podatkov, lahko poleg uporabe popravljalnih pooblastil iz drugega odstavka 58. člena Splošne uredbe, takoj:

1. odredijo, da se nepravilnosti ali pomanjkljivosti, ki jih ugotovijo, odpravijo na način in v roku, ki ga sami določijo;

2. odredijo 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. odredijo prepoved obdelave osebnih podatkov ter anonimiziranje, omejitev obdelave, psevdonimizacijo, brisanje ali uničenje osebnih podatkov, kadar ugotovijo, da se osebni podatki obdelujejo v nasprotju s Splošno uredbo, tem zakonom ali drugimi zakononi;

4. odredijo prepoved prenosa osebnih podatkov v tretjo državo ali v mednarodno organizacijo ali njihovega prenosa uporabnikom osebnih podatkov v tretji državi, če se prenašajo v nasprotju s Splošno uredbo ali zakonom;

5. odredijo druge ukrepe, določene z zakonom, ki ureja inšpekcijski nadzor, zakonom, ki ureja splošni upravni postopek, ali drugim zakonom.

(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;

– 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;

– 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.

(3) Prejšnji odstavek ne vključuje zahteve, da bi se ponudniki morali seznaniti z vsebino podatkov, če to prepoveduje drug zakon.

70. člen

(odločitev, da se postopek ne uvede)

Kadar iz podatkov iz prijave ali iz drugih podatkov ni mogoče sklepati na kršitev varstva osebnih podatkov po Splošni uredbi, tem zakonu ali drugem zakonu oziroma predpisu, ki ureja obdelavo in varstvo osebnih podatkov, nadzornik, namestnik informacijskega pooblaščenca ali informacijski pooblaščenec s sklepom odločijo, da se inšpekcijski postopek ne uvede. V obrazložitvi sklepa se navedejo razlogi za neuvedbo postopka.

71. člen

(pravice prijavitelja)

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

(2) Prijavitelj, ki meni, da obstaja kršitev varstva osebnih podatkov, ki se nanaša nanj, lahko v skladu s prvim odstavkom 80. člena 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 pooblaščencu.

72. člen

(pravno sredstvo zoper odločitve Informacijskega pooblaščenca)

(1) Zoper odločbo ali sklep Informacijskega pooblaščenca ni dovoljena pritožba, dopusten pa je upravni spor zoper odločbo ali sklep o ustavitvi postopka ali sklep o neuvedbi postopka.

(2) V skladu s prvim odstavkom 80. člena 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 v skladu s prejšnjim odstavkom.

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 v skladu z zakonom, ki ureja prekrške, v skladu s Splošno uredbo in v skladu s tem zakonom.

(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) Postopka po prvem odstavku tega člena ni mogoče izvajati zoper ponudnike iz drugega odstavka 69. člena tega zakona.

(4) Če gre za posebej hudo kršitev tega zakona in je za izvedbo prekrškovnega postopka nujno potrebno pridobiti podatke o uporabniku storitev ponudnikov iz drugega odstavka 69. člena tega zakona, 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, pristojno za prekrške, na obrazložen predlog nadzornika, namestnika informacijskega pooblaščenca ali informacijskega pooblaščenca odredi ponudniku iz drugega odstavka 69. člena tega zakona, da nadzorniku, namestniku informacijskega pooblaščenca ali informacijskemu pooblaščencu 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 osmih dneh 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 tudi po prenehanju delovnega razmerja ali funkcije.

(2) Dolžnost iz prejšnjega odstavka velja tudi za vse javne uslužbence ali druge osebe pri Informacijskem pooblaščencu, ki sodelujejo pri postopkih v skladu s tem zakonom.

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 objavlja mnenja iz 63. 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 mogoče 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 v skladu s tem zakonom;

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 nalog 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. To poročilo je del skupnega letnega poročila v skladu z zakonom, ki ureja Informacijskega pooblaščenca.

(2) Poročilo iz prejšnjega odstavka se posreduje tudi Evropski komisiji in 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)

(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 za nadzor obveščevalnih in varnostnih služb lahko sodeluje z Informacijskim pooblaščencem, na lasten predlog ali na pobudo Informacijskega pooblaščenca glede sprememb zakonov ali drugih predpisov ali pa je potrebna zaupna izmenjava informacij o ugotovitvah nadzornih postopkov..

VII. DEL

POSEBNA PRAVILA GLEDE OBDELAVE OSEBNIH PODATKOV ZA ZNANSTVENORAZISKOVALNE, ZGODOVINSKORAZISKOVALNE, STATISTIČNE IN ARHIVSKE NAMENE

79. člen

(obdelava osebnih podatkov v znanstvenoraziskovalne, zgodovinskoraziskovalne in statistične namene)

(1) Ne glede na prvotni namen obdelave lahko upravljavec osebne podatke nadalje obdeluje za znanstvenoraziskovalne, zgodovinskoraziskovalne 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,
– jih pridobi in nadalje obdeluje v anonimizirani obliki ali
– 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, 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 podatke posreduje v psevdonimizirani obliki, razen če s psevdonimizranimi podatki ni mogoče doseči namena raziskave ali bi bila v tem primeru izvedba raziskave povezana z nesorazmernim naporom ali stroški.

(4) Uporabniku iz drugega odstavka tega člena 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.

(5) Predstavitveni elaborat iz drugega odstavka tega člena zaradi varstva osebnih podatkov, ki bodo obdelovani v skladu s tem delom zakona, vsebuje podatke o:

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

(6) Elaboratu iz prejšnjega odstavka se priloži oceno učinkov v zvezi z varstvom osebnih podatkov iz 37. člena tega zakona.

(7) Osebni podatki, ki jih je uporabnik pridobil v skladu s prvo in tretjo alinejo prvega odstavka tega člena ter drugim in tretjim 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 upravljavca, ki mu je posredoval osebne podatke, ob zaključku raziskave pisno obvesti, ali, kdaj in na kakšen način jih je uničil.

(8) 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 ali partner iz zunajzakonske skupnosti ali partner z njima z zakonom izenačene 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.

(9) Posameznik, na katerega se nanašajo osebni podatki, lahko pravico do popravka v skladu s 16. členom Splošne uredbe uveljavlja le, če je upravljavec podatke od njega pridobil neposredno in le do trenutka začetka obdelave za statistične namene. Kadar se osebni podatki obdelujejo za statistične namene, se posameznik, na katerega se nanašajo osebni podatki, nima pravice do seznanitve z lastnimi osebnimi podatki v skladu s 15. členom Splošne uredbe in do omejitve obdelave v skladu z 18. členom Splošne uredbe, vendar le, če bi dajanje informacij ali kopij posameznikovih osebnih podatkov zahtevalo očitno nesorazmeren napor ali kadar upravljavec izkaže, da ne more identificirati posameznika, na katerega se nanašajo osebni podatki v skladu z 11. členom Splošne uredbe.

(10) Ta člen se ne uporablja za obdelave osebnih podatkov v skladu z zakonom, ki ureja varstvo dokumentarnega in arhivskega gradiva ter arhive.

80. člen

(obdelava naslovov za kontaktiranje posameznikov v znanstvenoraziskovalne, zgodovinskoraziskovalne in statistične namene)

(1) V okviru obdelave osebnih podatkov za znanstvenoraziskovalne, zgodovinskoraziskovalne ali statistične namene upravljavec izjemoma lahko tudi obdeluje osebne podatke ciljne skupine posameznikov zaradi pridobitve privolitev 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 privolitev za potrebe drugega uporabnika in za izvrševanje namenov iz prejšnjega odstavka, ki:

– za obdelavo osebnih podatkov nima podlage v zakonu ali privolitvi in

– z elaboratom iz drugega odstavka prejšnjega člena izkaže, da bo osebne podatke po pridobitvi privolitve obdeloval na znanstvenoraziskovalnem, zgodovinskoraziskovalnem 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 v skladu s tem členom se lahko obdelajo izključno za namen raziskave in jih je treba izbrisati takoj, ko niso več potrebni.

(5) Ta člen se ne uporablja za obdelavo osebnih podatkov v skladu z določbami 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. Upravljavec v skladu z zakonom določi 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 v skladu s 15. členom Splošne uredbe, če bi dajanje informacij ali kopij njegovih osebnih podatkov zahtevalo očitno nesorazmeren napor. Posameznik, na katerega se nanašajo osebni podatki, nima pravice zahtevati:

– popravka osebnih podatkov zaradi netočnosti ali neposodobljenosti v skladu s 16. členom Splošne uredbe,
– izbrisa v skladu s 17. členom Splošne uredbe,
– omejitve obdelave v skladu z 18. členom Splošne uredbe,
– prenosljivosti osebnih podatkov v skladu z 20. členom Splošne uredbe ter
– izvršitve pravice do ugovora v skladu z 21. členom Splošne uredbe.

(3) Če posameznik, na katerega se nanašajo osebni podatki, navaja netočnost ali neposodobljenost svojih osebnih podatkov, se mu ne glede na drugi stavek prejšnjega odstavka da na razpolago možnost za nasprotni prikaz dejstev. Pristojni arhiv v primeru utemeljenosti nasprotni prikaz dejstev priložii arhivskemu gradivu ali ustrezno označi na njem, kje se ta prikaz nahaja.

(4) Ta člen se ne uporabljajo, če zakon, ki ureja varstvo dokumentarnega in arhivskega gradiva ter arhive, določa drugače.

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) V razmerju do pravic varstva osebnih podatkov je 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.

(2) Svoboda izražanja v razmerju do varstva osebnih podatkov za namene obveščanja javnosti s strani medijev, književnega, umetniškega ali znanstvenega ustvarjanja, 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, če:

1. je posameznik za uporabo, objavo ali razkritje osebnih podatkov podal privolitev,

2. je posameznik osebne podatke že javno objavil ali dal na razpolago javnosti,

3. so osebni podatki na zakonit način že bili dostopni javnosti,

4. 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. gre za zakonito objavo mnenja ali vrednostne ocene, kjer je objava osebnih podatkov v njima nujna za utemeljitev tega mnenja ali vrednostne ocene,

6. so bili osebni podatki pridobljeni na drug zakonit način,

7. javni interes po obveščanju javnosti, pravica do obveščenosti ter svoboda izražanja prevladajo nad upravičenimi interesi varstva zasebnosti in drugih osebnostnih pravic posameznika ali

8. tako določa drug zakon.

(3) Uveljavljanje pravic posameznika, na katerega se nanašajo osebni podatki, v zvezi s tem členom 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 v skladu z zakonom, ki ureja dostop do informacij javnega značaja.

(2) Zaradi uresničevanja javnega interesa na področju sodelovanja javnosti, zagotavljanja transparentnosti dela ali spremljanja njihove prakse, vključno s sodno prakso sodišč Republike Slovenije, zavezanci iz prejšnjega odstavka po postopku iz zakona, ki ureja dostop do informacij javnega značaja, na zahtevo posredujejo ali proaktivno javno objavijo tudi dokumente z osebnimi podatki, ki niso zajeti v prejšnjem odstavku, če ne veljajo izjeme iz zakona, ki ureja dostop do informacij javnega značaja, , na način delnega dostopa in praviloma v anonimizirani obliki. Kadar uresničevanje navedenih namenov na ta način ni mogoče ali pa bi bilo nesorazmerno, pa jih lahko posredujejo ali javno objavijo v psevdonimizirani ali anonimizirani obliki v skladu s Splošno uredbo.

84. člen

(izjema glede obveščanja posameznika)

Če so osebni podatki javni na podlagi zakona, posameznika, na katerega se nanašajo osebni podatki. ni treba obveščati v skladu z 12. do 14. členom Splošne uredbe in zakonom, 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) Ta del zakona se uporablja za primere, ko osebne podatke obdelujejo pristojni državni organi za namene preprečevanja, preiskovanja, odkrivanja ali pregona kaznivih dejanj, vključno s področji preprečevanja pranja denarja ali financiranja terorizma, izvrševanja nalog in pooblastil policije, varnosti

države, obrambe države ter izvrševanja kazenskih sankcij ter s tem povezanih kazenskih sodnih postopkov.

(2) Če 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.

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

86. člen

(uporaba splošne ureditve varstva osebnih podatkov)

Osebni podatki iz tega dela zakona se obdelujejo v skladu z določbami iz I. do IV. dela tega zakona, kolikor ni v tem delu zakona določeno drugače.

87. člen

(razvrščanje osebnih podatkov po vrstah ter kakovost osebnih podatkov)

(1) Če je to glede na dejanske okoliščine posamezne zadeve mogoče in v skladu z zakonom, se pri obdelavi osebnih podatkov razlikuje zlasti med različnimi položaji posameznikov, katerih osebni podatki se obdelujejo, v določenem postopku, tudi z vidika, ali gre za dejstvo ali le za vrednostno oceno. Razlikuje se zlasti med naslednjimi položaji:

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 ali pravnomočno obsojeni storilci kaznivih dejanj;

4. žrtve kaznivega dejanja ali osebe, pri katerih določena dejstva upravičujejo domnevo, da so ali bi lahko bile 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 tega odstavka;

6. osumljenci storitve prekrška;

7. osebe, zoper katere na podlagi določenih dejstev obstaja sum, da bodo predvidoma kmalu storile prekršek;

8. kaznovani ali obsojeni ali pravnomočno 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 tega odstavka; in

10. osebe, ki prestajajo nadomestni zapor za storjeni prekršek.

(2) Osebne podatke, ki temeljijo zlasti na vrednostni oceni, se ustrezno označi ter, če je to možno in dopustno, utemelji na način, ki omogoča naknadno preverjanje te ocene. To preverjanje izvaja upravljavec.

(3) Osebni podatki, ki so netočni, nepopolni, neposodobljeni ali nezanesljivi ali jih je treba izbrisati, se ne smejo prenašati ali pripraviti za avtomatiziran priklic iz zbirk. Upravljavci v ta namen pred prenosom v skladu z razpoložljivimi možnostmi ustrezno preverijo kakovost podatkov. Glede osebnih podatkov, ki so že na razpolago za avtomatiziran priklic, se stalno izvajajo ustrezna prizadevanja za zagotavljanje njihove točnosti in posodobljenosti.

(4) Pri vsakem posredovanju, čezmejni obdelavi ali prenosu osebnih podatkov se, če je to glede na dejanske okoliščine posamezne zadeve mogoče, priloži informacije, na podlagi katerih lahko uporabnik oceni njihovo točnost, posodobljenost, popolnost in zanesljivost.

(5) Če uporabnik, Informacijski pooblaščenec ali pooblaščena oseba na podlagi prijave, sporočila ali pritožbe posameznika, na katerega se nanašajo osebni podatki, ugotovi, da so bili posredovani osebni podatki, ki ne ustrezajo zahtevam iz tretjega odstavka tega člena, pošiljatelj to nemudoma sporoči vsem uporabnikom. Uporabniki nemudoma izvedejo izbris nezakonito posredovanih podatkov, popravek netočnih, neposodobljenih ali nezanesljivih 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 neposodobljeni in da jih je treba popraviti, omejiti njihovo obdelavo ali jih izbrisati, se nemudoma izvede medsebojno obveščanje. Pošiljatelj nemudoma sprejme ustrezne ukrepe popravka, omejitve obdelave ali izbrisa, če so dejstva o netočnosti ali neposodobljenosti osebnih podatkih potrjena. Uporabnik je na to odločitev vezan, mora pa označiti morebitno nestrinjanje v svoji zbirki.

88. člen

(zakonitost obdelave osebnih podatkov)

(1) Obdelava osebnih podatkov v skladu s tem delom zakona je zakonita le, če je določena z zakonom za namene iz 85. člena tega zakona.

(2) V skladu s prejšnjim odstavkom je obdelava posebnih vrst osebnih podatkov zakonita le v primerih iz c), d), i), j), k) točk drugega odstavka 12. člena tega zakona in le, če je to nujno potrebno in je zagotovljena ustrezno varstvo človekovih pravic ali temeljnih svoboščin posameznika.

(3) Če posameznik javno objavi svoje osebne podatke, brez očitnega ali izrecnega namena, da omeji namen njihove obdelave, je njihova obdelava zakonita, če je v skladu z nameni iz 85. člena tega zakona.

89. člen

(posebne določbe o obdelavi osebnih podatkov za druge namene)

Obdelava osebnih podatkov v skladu s tem delom zakona s strani istega ali drugega upravljavca za drug namen obdelave od tistega, za katerega so bili podatki pridobljeni, je dovoljena le, če ta drug namen obdelave spada med namene iz 85. člena tega zakona ter izpolnjuje pogoje iz 86. člena tega zakona in če tako določa drug zakon.

90. člen

(posebne določbe o prenosih osebnih podatkov)

(1) Prenos, posredovanje ali čezmejna obdelava osebnih podatkov, obdelanih v skladu s tem delom zakona, za namen, ki ni naveden v 85. členu tega zakona, so dovoljeni le, če je to izrecno določeno v zakonu, če je to nujno potrebno in če je uporabnik zakonito pooblaščen za obdelavo teh osebnih podatkov za ta drug namen.

(2) Če za obdelavo osebnih podatkov veljajo posebni pogoji, pošiljatelj uporabnika obvesti o teh pogojih in o tem, da jih je treba upoštevati. Pri prenosu osebnih 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.

2. poglavje

Pravice posameznika, na katerega se nanašajo osebni podatki

91. člen

(splošna pravila)

(1) Upravljavec posamezniku, na katerega se nanašajo osebni podatki, v skladu z 92. do 94. členom tega zakona posreduje informacije in sporočila, ki se nanašajo na obdelavo njegovih osebnih podatkov. Informacije in sporočila poda v čimbolj točni, razumljivi in lahko dostopni obliki ter v jasnem in preprostem jeziku. Informacije in sporočila se posredujejo v posamezniku ustrezni obliki.

(2) Upravljavec posamezniku, na katerega se nanašajo osebni podatki, olajša uveljavljanje njegovih pravic iz 92. do 94. člena tega zakona, zlasti z določitvijo kontaktnih točk in objavljanjem splošnih informacij.

(3) Upravljavec posamezniku, na katerega se nanašajo osebni podatki, informacije o ukrepih, ki so bili na podlagi zahtevka sprejeti, zagotovi 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 posameznika, na katerega se nanašajo osebni podatki, v enem mesecu od vložitve zahtevka obvesti o podaljšanju roka in navede razloge za zamudo. Če posameznik, na katerega se osebni podatki nanašajo, zahtevo predloži elektronsko, se ga obvesti elektronsko, če ne navede drugega kontaktnega naslova. Ta odstavek se ne uporablja, če se izvede ukrep začasne omejitve obveščanja v skladu s četrtim in petim odstavkom 92. člena tega zakona.

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

(5) Informacije iz 92. člena tega zakona 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 osebni podatki nanašajo, zlasti če se zahteve pogosto ponavljajo, lahko upravljavec s posebno obrazložitvijo odkloni ukrepanje na podlagi zahtevka. Obrazložitev vsebuje vsaj povzetek razlogov glede očitne neutemeljenosti ali pretirane narave zahtevka. Upravljavec lahko namesto odklonitve ukrepanja zaračuna razumno pristojbino v skladu s 26. členom tega zakona.

(6) Upravljavec lahko zaradi potrditve identitete posameznika, na katerega se nanašajo osebni podatki, ki je v skladu s 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.

(7) V primerih iz četrtega odstavka 92. člena, tretjega odstavka 93. člena in četrtega odstavka 94. člena tega zakona lahko posameznik, na katerega se nanašajo osebni podatki, s prijavo Informacijskemu pooblaščencu zahteva, da preveri omejitve njegovih pravic s strani upravljavca. Upravljavec posameznika, na katerega se nanašajo osebni podatki, izrecno pouči o tej pravici.

(8) Če se uveljavlja pravica iz prejšnjega odstavka, Informacijski pooblaščenec posameznika, na katerega se osebni podatki nanašajo, obvesti vsaj o uvedbi ali neuvedbi inšpekcijskega postopka, v nadaljevanju pa ga obvešča v skladu z zakonom, ki ureja inšpekcijski nadzor. Informacijski pooblaščenec posameznika, na katerega se nanašajo osebni podatki, obvesti tudi o njegovi pravici do uporabe sodnega varstva v skladu z 28. členom tega zakona.

92. člen

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

(1) Upravljavec posamezniku, na katerega se nanašajo osebni podatki, na njegovo zahtevo ali v primeru objave splošne informacije o obdelavi zagotovi najmanj naslednje informacije:

1. naziv in kontaktne podatke upravljavca;

2. kontaktne podatke pooblaščene osebe, če je določena;

3. navedbo namenov obdelave osebnih podatkov;

4. obstoj pravice do vložitve prijave pri Informacijskem pooblaščencu 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 iz prejšnjega odstavka upravljavec posamezniku, na katerega se nanašajo osebni podatki, na njegovo zahtevo ali v primeru objave splošne informacije o obdelavi, v posameznih primerih, kadar je to glede na konkretne okoliščine zadeve ali obdelave potrebno zaradi zagotovitve poštenosti obdelave, zagotovi naslednje dodatne informacije, da s tem omogoči učinkovitejše uresničevanje njegovih pravic:

1. pravno podlago obdelave;

2. rok hrambe osebnih podatkov ali, če to izjemoma ni mogoče, merila za določitev tega roka v skladu s 43. členom tega zakona;

3. po potrebi 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) Informacije iz prvega in drugega odstavka tega člena se ne dajo, če so bili osebni podatki pridobljeni s prenosom podatkov z 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, v skladu z drugim odstavkom tega člena se lahko 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 postopkov za namene iz prvega odstavka 85. člena tega zakona, vključno s pridobivanjem ali prenosi osebnih podatkov za še nedokončane uradne postopke za namene iz prvega odstavka 85. člena tega zakona;

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.

(5) Začasna omejitev obveščanja v skladu s prejšnjim odstavkom lahko vključuje tudi začasno izjavo upravljavca, 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) Posameznik, na katerega se nanašajo osebni podatki, ima pravico od upravljavca na njegovo zahtevo prejeti potrdilo o tem, ali so v obdelavi osebni podatki, ki se nanašajo nanj. Če so v obdelavi osebni podatki, ki se nanašajo nanj, ima pravico pridobiti 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, v primerih omejitev iz četrtega odstavka tega člena pa se lahko navede le okvirni opis uporabnikov;

4. če je mogoče, predvidenem roku hrambe osebnih podatkov ali, če to izjemoma ni mogoče, o merilih za določitev tega roka v skladu s 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 pooblaščencu 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 prejšnjega odstavka veljajo roki iz četrtega odstavka 91. člena tega zakona. Omejitve pravice do pridobitve informacij so dovoljene le pod pogoji iz četrtega odstavka prejšnjega člena.

(3) V primeru nerazkritja informacij iz prejšnjega odstavka upravljavec posameznika, na katerega se nanašajo podatki, brez nepotrebnega odlašanja, najpozneje pa v treh delovnih dneh, pisno obvesti o zavrnitvi ali omejitvi informacij in razlogih za takšno odločitev. Ta odstavek se ne uporablja, če je zagotovitev teh informacij v nasprotju z enim od namenov iz četrtega odstavka prejšnjega člena. Upravljavec posameznika, na katerega se nanašajo osebni podatki, obvesti o možnosti vložitve prijave Informacijskemu pooblaščencu.

(4) Upravljavec dokumentira razloge za odločitev o nerazkritju informacij iz drugega odstavka tega člena ter Informacijskemu pooblaščencu in pooblaščeni osebi omogočiti dostop do njih.

(5) V obsegu, v katerem ima posameznik, na katerega se nanašajo osebni podatki, v drugem zakonu določeno zakonsko pravico do vpogleda v svoje 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) Posameznik, na katerega se nanašajo osebni podatki, ima pravico od upravljavca zahtevati 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 mora dokazati točnost ali posodobljenost osebnih podatkov, če osebni podatki niso bili pridobljeni izključno na podlagi navedb posameznika, na katerega se podatki nanašajo.

(2) Upravljavec osebne podatke nemudoma izbriše na lastno pobudo ali na podlagi zahtevka posameznika, na katerega se podatki nanašajo, če:

1. obdelava določenih osebnih podatkov ni več potrebna 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) Upravljavec namesto izbrisa osebnih podatkov njihovo obdelavo omeji, če:

1. posameznik, na katerega se osebni 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 preklicem omejitve, ali

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

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

(5) Upravljavec popravek nepravilnih osebnih podatkov sporoči pristojnemu organu, od katerega so mu bili preneseni ali drugače poslani ti osebni podatki.

(6) V primerih popravka, izbrisa podatkov ali omejitve obdelave v skladu s prvim do tretjim odstavkom tega člena upravljavec o tem obvesti vse uporabnike osebnih podatkov. Uporabniki osebne podatke, ki jih v okviru svojih pristojnosti obdelujejo, nemudoma popravijo, izbrišejo, ustrezno označijo ali omejijo njihovo obdelavo.

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

3. poglavje

Prenos osebnih podatkov tretjim državam ali mednarodnim organizacijam ter čezmejne obdelave osebnih podatkov

95. člen

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

(1) To poglavje se uporablja za primere, ko osebne podatke obdelujejo pristojni državni organi za namene preprečevanja, preiskovanja, odkrivanja ali pregona kaznivih dejanj, vključno s področji preprečevanja pranja denarja ali financiranja terorizma, izvrševanja nalog in pooblastil policije, varnosti

države, obrambe države ter izvrševanja kazenskih sankcij ter s tem povezanih kazenskih sodnih postopkov.

(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, prenesti le, če so upoštevane določbe tega dela zakona in:

1. je prenos potreben za namene iz prvega odstavka 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 prvega odstavka 85. člena tega zakona;

3. je pristojna država članica v primerih, ko se osebni podatki posredujejo iz druge države članice ali tej dajo na razpolago, prenos vnaprej odobrila;

4. je Evropska komisija sprejela sklep o ustreznosti ravni varstva osebnih podatkov ali, če tak sklep ne obstaja, obstajajo ustrezni ukrepi v skladu s 97. členom tega zakona, ali je, če ne obstaja sklep o ustreznosti in ne obstajajo ustrezni ukrepi in niso predložena ustrezna zagotovila, možno v skladu z 98. 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 tehtnih meril, vključno z naravo ali težo kaznivega dejanja, namenom prvotnega prenosa osebnih podatkov in stopnjo varstva osebnih podatkov v tretji državi ali mednarodni organizaciji, ki se ji posredujejo osebni podatki oziroma jih namerava posredovati tretji državi ali drugi mednarodni organizaciji.

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

(4) Osebne podatke, za katere ni mogoče podati ustrezne ocene, ali so točni, se sme avtomatizirano prenašati ali čezmejno posredovati pod pogojem, da so ustrezno ali nedvoumno označeni glede stopnje točnosti.

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

96. 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 36. člena 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 odobritve v skladu s 3. točko drugega odstavka prejšnjega člena.

(2) Sklep Evropske komisije, sprejet v skladu s petim odstavkom 36. člena Direktive o razveljavitvi, spremembi ali začasni odložitvi izvajanja sklepa iz tretjega odstavka 36. člena Direktive ne vpliva na že izvedene prenose osebnih podatkov tretji državi, regiji oziroma enemu ali več specifičnim sektorjem v tretji državi oziroma mednarodni organizaciji, niti na prenose v skladu z 98. in 99. členom tega zakona.

97. člen

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

(1) Če ne obstaja sklep v skladu s tretjim odstavkom 36. člena Direktive, je prenos osebnih podatkov v tretjo državo ali mednarodno organizacijo dopusten, če:

1. so v zakonu 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 prejšnjega odstavka obstajajo ustrezni ukrepi za določene vrste prenosov, upravljavec o njih obvesti Informacijskega pooblaščenca, ki lahko ne glede na omejitve iz 62. člena tega zakona odredi prepoved prenosa osebnih podatkov, če ugotovi neskladnosti s tem delom zakona

(3) Prenose v skladu z 2. točko prvega odstavka tega člena se dokumentira. Dokumentacija vsebuje datum in čas prenosa, informacije o pristojnemu organu ali uporabniku, pravno podlago, razloge prenosa in opis prenešenih osebnih podatkov.

98. člen

(Izjeme za posamezne primere)

(1) Če ne obstajata ne sklep o ustreznosti v skladu s tretjim odstavkom 36. člena Direktive in tudi ne ustrezen ukrep v skladu s prejšnjim členom, 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 podatk in je to določeno v zakonu države članice, ki se ji prenaša osebne podatke ali v enakovrednem predpisu mednarodne organizacije;

3. za odvrnitev neposredne in resne nevarnosti za javno varnost države članice 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 prejšnjega odstavka je prenos dovoljen le, če človekove pravice in temeljne svoboščine posameznika, na katerega se nanašajo osebni podatki, ne prevladajo nad javnim interesom. V primerih iz 4. in 5. točke prejšnjega odstavka lahko Informacijski pooblaščenec ne glede na omejitve iz 62. člena tega zakona odredi prepoved prenosa osebnih podatkov, če ugotovi neskladnosti s tem delom zakona.

(3) Za prenose v skladu s prvim odstavkom tega člena se uporablja tretji odstavek prejšnjega člena.

99. člen

(posebni prenosi določenim uporabnikom v tretjih državah)

(1) Ne glede na 2. točko drugega odstavka 95. člena tega zakona smejo smejo pristojni organi iz 1. točke drugega odstavka 6. člena tega zakona, , ki so upravljavci ali uporabniki, izvesti prenos osebnih podatkov v tretjo državo v posebnem posameznem primeru, tako da jih prenesejo neposredno upravljavcu ali uporabniku javnega ali zasebnega sektorja v tretji državi ali mednarodni organizaciji, če je prenos nujno potreben za opravljanje konkretnih zakonskih nalog 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 primeru pristojni organ ugotovi, da človekove pravice in temeljne svoboščine posameznika, na katerega se nanašajo osebni podatki, ne prevladujejo nad javnim interesom za prenos,

3. bi bil prenos v nskladu z drugimi določbami 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 te namene in v obsegu, v katerem je obdelava za te namene potrebna.

(2) Za prenose v skladu s prejšnjim odstavkom se uporabljata drugi in tretji odstavek 97. člena tega zakona.

(3) Ne glede na prvi in drugi odstavek tega člena se prenosi osebnih 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.

X. DEL

PODROČNE UREDITVE OBDELAV OSEBNIH PODATKOV

1. poglavje

Neposredno trženje

100. člen

(pravice in dolžnosti upravljavca na področju neposrednega trženja)

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

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

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

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

- identiteto in kontaktne podatke upravljavca;

- ali je upravljavec podatke zbral iz javno dostopnih virov, ali v okviru zakonitega opravljanja dejavnosti; in

- na kakšen način lahko posameznik uveljavlja pravico iz 16. člena in drugega odstavka 21. člena Splošne uredbe ter iz 101. člena tega zakona.

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

(6) Obdelava osebnih podatkov s področja neposrednega trženja je prepovedana za druge namene trženja, zlasti za politično trženje, kar vključuje kontaktiranje ali prepričevanje morebitnih volivcev ali njihovo profiliranje.

101. člen

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

(1) Posameznik, na katerega se nanašajo osebni podatki, 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 v primeru iz prejšnjega stavka najpozneje v 15 dneh preneha obdelovati osebne podatke za namen neposrednega trženja ter o tem v nadaljnjih petih dneh pisno ali na drug dogovorjen način obvesti posameznika, ki je vložil to zahtevo.

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

2. poglavje

Videonadzor

102. člen

(splošne določbe o videonadzoru in varstvu osebnih podatkov)

(1) Odločitev o uvedbi videonadzora sprejme pristojni funkcionar, predstojnik, direktor ali drug pristojen 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.

(2) Oseba javnega ali zasebnega sektorja, ki izvaja videonadzor, o tem objavi obvestilo. Obvestilo se vidno in razločno objavi na način, ki omogoča posamezniku, da se seznani z izvajanjem videonadzora najpozneje, ko se nad njim začne izvajati videonadzor.

(3) Obvestilo iz prejšnjega odstavka vsebuje 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.

(4) Šteje se, da je z obvestilom iz prejšnjega odstavka posameznik obveščen o obdelavi osebnih podatkov.

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

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

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

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

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

103. člen

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

(1) V javnem in zasebnem sektorju se lahko izvaja 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 te namene, če drug zakon ne določa drugače.

(2) Videonadzor se lahko izvaja le na takšen način, da se ne izvaja snemanja notranjosti stanovanjskih stavb, ki nimajo vpliva na dostop do prostorov iz prvega odstavka, in snemanja vhodov v stanovanja.

(3) O izvajanju videonadzora se pisno obvesti 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.

104. člen

(videonadzor in večstanovanjske stavbe)

(1) Videonadzor se lahko v večstanovanjski stavbi uvede le zaradi varnosti ljudi in premoženja. Vpogled, uporaba in posredovanje posnetkov so dopustni le za ta namen, če drug zakon ne določa drugače.

(2) Videonadzor v večstanovanjskih stavbah se uvede, če za to obstaja strinjanje lastnikov, ki imajo v lasti več kot 70 odstotkov solastniških deležev na skupnih delih.

(3) Strinjanje iz prejšnjega odstavka mora biti pisno, pri čemer se na listini izrecno navede, kateri lastniki so se strinjali z uvedbo 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) Prepovedano je omogočiti ali izvajati sprotno ali naknadno pregledovanje dogajanja v območju izvajanja videonadzora preko interne kabelske televizije, javne kabelske televizije, svetovnega spleta ali s pomočjo drugega elektronskega komunikacijskega sredstva, ki lahko prenaša te posnetke.

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

(7) Združevanje videonadzornega sistema z napravami, ki jih uporabljajo lastniki za potrebe vstopa v večstanovanjsko stavbo, kot sta na primer domofon ali video domofon, je dovoljeno le, če te naprave ne omogočajo snemanja ali spremljanja dogajanja v območju izvajanja videonadzora na posamezni napravi. Spremljanje dogajanja v območju izvajanja videonadzora onemogoči upravljavec videonadzora.

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

105. člen

(delovni prostori)

(1) Izvajanje videonadzora znotraj delovnih prostorov se lahko izvaja le v primerih, kadar je to nujno potrebno za varnost ljudi ali premoženja ali preprečevanja ali odkrivanja kršitev na področju iger na srečo ali za varovanje tajnih podatkov ali za varovanje poslovnih skrivnosti, teh namenov pa ni možno doseči z milejšimi sredstvi. Vpogled, uporaba ali posredovanje posnetkov je dopustno le za te namene, če drug zakon ne določa drugače.

(2) Videonadzor se lahko izvaja le glede tistih delov prostorov in v obsegu, kjer je treba 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 pooblaščeno varnostno osebje ali drugo posebej pooblaščeno in usposobljeno osebje upravljavca.

(4) Zaposleni se pred začetkom izvajanja videonadzora po tem členu vnaprej pisno obvesti 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 oziroma delavskim zaupnikom, če obstajajo. Posvetovanje se izvede v roku 30 dni oziroma v drugem daljšem roku, ki ga določi delodajalec. Po prejetju morebitnega mnenja delodajalec dokončno odloči o uvedbi ali neuvedbi videonadzora.

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

106. člen

(videonadzor na javnih površinah)

(1) Videonadzor na javnih površinah je dovoljen le, kadar je to nujno potrebno zaradi obstoja resne in utemeljene nevarnosti za življenje ali zdravje ljudi, varnost premoženja ali varovanje tajnih podatkov in tega namena ni mogoče doseči z milejšimi sredstvi, ali za potrebe varovanja oseb, objektov in okolišev objektov, ki jih varuje policija, oziroma varovanja drugih prostorov, zgradb ali območij, ki jih je treba varovati na podlagi zakona, in sicer samo v obsegu in trajanju, ki je za dosego namena nujno potreben. Vpogled, uporaba ali posredovanje posnetkov je dopustno le za te namene, če drug zakon ne določa drugače.

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

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

3. poglavje

Obdelava osebnih podatkov z uporabo biometrije

107. člen

(biometrični ukrepi v javnem sektorju)

(1) Biometrične ukrepe v javnem sektorju se lahko 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 ali varovanja poslovne skrivnosti, teh namenov 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.

(3) Ne glede na določbe prvega in drugega odstavka tega člena se v javnem sektorju lahko uvedejo biometrični ukrepi v zvezi z vstopom v stavbo ali dele stavbe, ki se izvedejo ob smiselni uporabi četrtega, petega in šestega odstavka 108. člena tega zakona.

108. člen

(biometrični ukrepi v zasebnem sektorju)

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

(2) Biometrične ukrepe lahko oseba zasebnega sektorja pod pogoji iz prejšnjega odstavka izvaja le v svojih prostorih nad svojimi zaposlenimi in nad zaposlenimi pri njenih pogodbenih partnerjih, ki so bili o tem predhodno pisno obveščeni.

(3) Oseba zasebnega sektorja lahko izvaja biometrične ukrepe tudi nad svojimi strankami podpogojem, da to za namene varovanja interesov iz prvega odstavka tega člena določa drug zakon in so stranke podale pisno privolitev ter se na ta način preprečuje nastanek hude škode.

(4) Oseba zasebnega sektorja, ki namerava izvajati biometrične ukrepe, pred uvedbo ukrepov posreduje Informacijskemu pooblaščencu opis nameravanih ukrepov in razloge za njihovo uvedbo.

(5) Informacijski pooblaščenec po prejemu posredovanih informacij iz prejšnjega odstavka v dveh mesecih odloči, ali je nameravana uvedba biometričnih ukrepov v skladu s tem zakonom. Rok se ob upoštevanju zapletenosti predvidene obdelave lahko podaljša za največ dva meseca.

(6) Oseba zasebnega sektorja lahko začne 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) Osebi zasebnega sektorja ni treba pridobiti odločbe iz petega odstavka tega člena, če se biometrični ukrepi izvajajo na način, da so biometrične značilnosti ali matematične pretvorbe biometričnih značilnosti vedno pod nadzorom posameznika, na katerega se nanašajo osebni podatki in je posameznik za izvedbo teh ukrepov podal privolitev..

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

109. člen

(prepoved pridobivanja biometričnih osebnih podatkov v zvezi s trženjem)

V okviru trženja ali temu podobne druge poslovne dejavnosti se ne sme 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

110. 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 navedbo vseh ali nekaterih osebnih podatkov 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 obdelujejo 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 treba pridobiti podatke z vidika koristi mladoletnika ali za izvrševanje pristojnosti policije ali obveščevalno-varnostne dejavnosti.

(4) Osebni podatki iz evidence iz drugega odstavka tega člena se lahko hranijo največ tri leta od vnosa osebnih podatkov v zbirko, nato se zbrišejo ali na drug način uničijo, če drug zakon ne določa drugače.

5. poglavje

Javne knjige in varstvo osebnih podatkov

111. člen

(zakoniti namen javne knjige)

Osebni 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

112. člen

(povezovanje uradnih evidenc in javnih knjig)

(1) Uradne evidence in javne knjige, v katerih se obdelujejo posebne vrste osebnih podatkov, osebni podatki v zvezi s kazenskimi obsodbami in prekrški, 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 centralni kreditni register, in uradne evidence v skladu z zakonom, ki ureja naloge in pooblastila policije, in zakonom, ki ureja preprečevanje pranja denarja in financiranja terorizma, se lahko povezuje med seboj ali z drugimi zbirkami samo, če takšno povezovanja izrecno določa zakon.

(2) Uradne evidence in javne knjige, ki ne vsebujejo podatkov iz prejšnjega ostavka, 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 v skladu s prvim in drugim odstavkom tega člena pomeni elektronsko povezovanje dveh ali več uradnih evidenc, javnih knjig ali drugih zbirk, ki se upravljajo pri različnih upravljavcih ali pri istem upravljavcu na podlagi različnih pravnih podlag, in ki se, neodvisno od tehnične izvedbe, izvaja v obsegu oziroma na način, ki predstavljata ali bi lahko predstavljala bistveno večje tveganje za človekove pravice ali temeljne svoboščine posameznikov kot obdelava osebnih podatkov le v okviru ene same uradne evidence, javne knjige ali zbirke. Povezovanje zbirk pomeni tudi obdelavo dveh ali več zbirk istega ali različnih upravljavcev pri istem obdelovalcu, če ni z organizacijskimi in tehničnimi ukrepi in postopki zagotovljena popolna ločitev obdelav osebnih podatkov iz teh zbirk.

(4) Najpozneje 30 dni pred začetkom povezovanja zbirk iz prvega odstavka tega člena mora upravljavec oziroma obdelovalec poslati obvestilo Informacijskemu pooblaščencu, v katerem navededa namerava izvesti povezovanje v skladu s tem členom.

7. poglavje

Strokovni nadzor

113. 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.

114. 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 dosego namena strokovnega nadzora.

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

115. 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.

116. 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
Javni kontaktni podatki in podatki za organiziranje uradnih dogodkov

117. člen

(javni kontaktni podatki)

Osebe javnega ali zasebnega sektorja lahko javnosti posredujejo in javno objavijo osebno ime, naziv ali funkcijo, službeno telefonsko številko in naslov službene elektronske pošte vodilnih oseb in tistih zaposlenih, katerih delo je pomembno zaradi poslovanja s strankami oziroma uporabniki storitev, če drug zakon ne določa drugače.

118. člen

(podatki za organiziranje uradnih dogodkov)

(1) Oseba iz javnega sektorja lahko uporablja kontaktne podatke posameznikov, ki jih je zbrala iz javno dostopnih virov ali v okviru izvrševanja svojih javnih nalog ali so ji jih posamezniki, na katere se nanašajo, prostovoljno razkrili ali podali za to privolitev, za namene organiziranja uradnih srečanj in dogodkov, dajanje izjav za javnost oziroma druge aktivnost obveščanja zainteresirane javnosti o svojem delovanju. Zbirke osebnih podatkov, ki nastanejo na tej podlagi, morajo biti ločene od drugih zbirk osebnih podatkov, ki nastanejo pri izvrševanju zakonitih pristojnosti, nalog ali obveznosti.

(2) Za namene iz prejšnjega odstavka lahko oseba javnega sektorja uporablja le naslednje osebne podatke: osebno ime, naslov stalnega ali začasnega prebivališča, telefonsko številko, naslov elektronske pošte ali drugo komunikacijsko številko oziroma oznako, podatke o delodajalcu ali organizaciji ter podatke o področju dela ali položaju ali funkciji ali članstvu v klubu ali hobiju posameznika, na katerega se nanašajo osebni podatki. Na podlagi privolitve posameznika lahko oseba javnega sektorja za iste namene obdeluje tudi druge osebne podatke, posebne vrste osebnih podatkov pa le izjemoma in če ima za to izrecno privolitev posameznika.

(3) Če namerava oseba javnega sektorja posredovati, prenašati ali čezmejno obdelovati osebne podatke iz drugega odstavka tega člena za iste ali podobne namene, o tem obvesti posameznika in pred izvedbo teh dejanj obdelave pridobi njegovo privolitev. Obvestilo posamezniku o predvidenih dejanjih obdelave vsebuje informacijo, katere podatke namerava posredovati, komu in za kakšen namen. Stroške obvestila krije oseba javnega sektorja.

(4) Posameznik lahko kadarkoli pisno ali na drug dogovorjen način brezplačno zahteva, da oseba javnega sektorja trajno ali začasno preneha uporabljati ali drugače obdelovati njegove osebne podatke po tem členu. Oseba javnega sektorja najpozneje v 15 dneh preneha obdelovati osebne podatke za namene iz prvega odstavka tega člena ter o tem v nadaljnjih petih dneh pisno ali na drug dogovorjen način obvesti posameznika, ki je to zahteval.

(5) Stroške vseh delovanj v zvezi z zahtevo iz prejšnjega odstavka krije oseba javnega sektorja.

XI. DEL

KAZENSKE DOLOČBE

119. člen

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

(1) Informacijski pooblaščenec odloča o predpisanih kršitvah in upravnih globah iz 83. člena Splošne uredbe kot o prekrških v okviru pristojnosti prekrškovnega organa po določbah zakona, ki ureja prekrške

(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 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 odvračanje teh kršitev imela višine globe.

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

(4) 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.

120. člen

(kršitve iz četrtega odstavka 83. člena Splošne uredbe)

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

1. če krši obveznosti upravljavca in obdelovalca, kot so določene v 8. 11. ter 25. do 39. členu ter v 42. in 43. členu Splošne uredbe;

2. če krši obveznosti organa za potrjevanje, kot je določeno v 42. in 43. členu Splošne uredbe;

3. če krši obveznosti organa za spremljanje v skladu s četrtim odstavkom 41. člena Splošne uredbe.

(2) Z globo od 800 do 1.200 eurov se kaznuje za prekršek iz prejšnjega odstavka 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 iz prvega odstavka tega člena odgovorna oseba državnega organa ali organa samoupravne lokalne skupnosti. (4) Z globo od 200 do 800 eurov se kaznuje za prekršek iz prvega odstavka tega člena posameznik.

121. člen

(kršitve iz petega odstavka 83. člena Splošne uredbe)

(1) Z globo od 4.000 do 20.000.000 eurov ali v primeru gospodarske družbe v znesku od 4.000 eurov do 4 odstotke skupnega svetovnega letnega prometa v preteklem koledarskem letu, odvisno, kateri znesek 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 privolitev, kot so določena v 5., 6., 7. in 9. členu Splošne uredbe;

2. če krši pravice posameznika, na katerega se nanašajo podatki, kot so določene 12. do 22. členu Splošne uredbe;

3. če krši določbe v zvezi s prenosi osebnih podatkov uporabniku v tretji državi ali mednarodni organizaciji, kot so določene v 44. do 49. členu 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 58. člena Splošne uredbe, ali če ne zagotovi dostopa, s čimer se krši prvi odstavek 58. člena Splošne uredbe.

(2) Z globo od 800 do 1.200 eurov se kaznuje za prekršek iz prejšnjega odstavka 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 iz prvega odstavka tega členaodgovorna oseba državnega organa ali organa samoupravne lokalne skupnosti.

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

122. člen

(kršitve določb o uporabi povezovalnega znaka in avtomatiziranem odločanju)

(1) Z globo od 1.000 do 8.000 eurov se kaznuje za prekršek odgovorna oseba državnega organa, organa samoupravne lokalne skupnosti ali nosilca javnih pooblastil:

1. če uporablja povezovalni znak v nasprotju s prvim ali drugim ali tretjim odstavkom 42. člena,

2. če izvaja avtomatizirano odločanje v nasprotju s prepovedmi iz petega odstavka 42. člena.

(2) Z globo od 1.000 do 6.000 eurov se kaznuje za prekršek iz prejšnjega odstavka odgovorna oseba pravne osebe, samostojnega podjetnika posameznika ali posameznika, ki samostojno opravlja dejavnost.

(3) Z globo od 200 do 2.000 eurov se kaznuje za prekršek iz prvega odstavka tega člena posameznik.

123. 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, organa samoupravne lokalne skupnosti ali nosilca javnih pooblastil:

1. če obdeluje osebne podatke za namen iz prvega odstavka 85. člena tega zakona, brez da bi za to imela podlago v zakonu (88. člen), pa ne gre za primer, ko je obdelava nujno potrebna za varovanje življenja in telesa;

2. če obdeluje osebne podatke, ki so bili pridobljeni za namen iz prvega odstavka 85. člena tega zakona, za drug namen iz prvega odstavka 85. člena, pa pri tem krši splošna pravila o varstvu osebnih podatkov (86. člen) oziroma za takšno obdelavo za dodatni namen nima podlage v drugem zakonu (prvi odstavek 89. člena);

3. če prenese, posreduje ali pošlje v čezmejno obdelavo osebne podatke, ki so bili pridobljeni za namen iz prvega odstavka 85. člena tega zakona, brez da bi bilo to izrecno določeno v zakonu, nujno potrebno za dosego namena prenosa, posredovanja ali čezmejne obdelave, ali če uporabnik prejetih, posredovanih ali poslanih osebnih podatkov ni bil zakonito pooblaščen za obdelavo teh podatkov (drugi in tretji odstavek 89. člena);

4. če avtomatizirano obdeluje osebne podatke v nasprotju s 90. členom tega zakona;

5. če krši pravice posameznika, na katerega se nanašajo osebni podatki, kot so določene v 91. do 94. členu tega zakona;

6. če dostopa do vsebine osebnih podatkov v nasprotju s sedmim odstavkom 40. člena tega zakona.

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

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

124. 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 100.. ali 101.. členom tega zakona.

(2) Z globo od 400 do 1.200 eurov se kaznuje za prekršek iz prejšnjega odstavka 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 iz prvega odstavka tega člena posameznik.

125. 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 se izvaja videonadzor brez pisne odločitve po prvem odstavku 102. člena tega zakona;

2. če ne objavi obvestila na način iz drugega odstavka 102. člena tega zakona;

3. če obvestilo ne vsebuje informacij iz tretjega odstavka 102. člena tega zakona;

4. če ne zavaruje videonadzornega sistema, s katerim izvaja videonadzor, na način iz petega odstavka 102. člena tega zakona.

(2) Z globo od 800 do 1.200 eurov se kaznuje za prekršek iz prejšnjega odstavka 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 iz prvega odstavka tega člena odgovorna oseba državnega organa ali organa samoupravne lokalne skupnosti.

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

(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 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 iz petega odstavka tega člena odgovorna oseba državnega organa ali organa samoupravne lokalne skupnosti.

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

126. 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 ali obdeluje posnetke v neskladju z namenom iz prvega odstavka 103. 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 103. člena tega zakona);

3. če pisno ne obvesti zaposlenih (tretji odstavek 103. člena tega zakona).

(2) Z globo od 800 do 1.200 eurov se kaznuje za prekršek iz prejšnjega odstavka 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 iz prvega odstavka tega člena odgovorna oseba državnega organa ali organa samoupravne lokalne skupnosti.

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

127. 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 ali obdeluje posnetke v neskladju z namenom iz 104. člena tega zakona.

(2) Z globo od 400 do 1.200 eurov se kaznuje za prekršek iz prejšnjega odstavka 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 iz prvega odstavka tega člena odgovorna oseba državnega organa ali organa samoupravne lokalne skupnosti.

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

128. 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 ali obdeluje posnetke v neskladju z namenom iz 105. člena tega zakona.

(2) Z globo od 1.200 do 2.000 eurov se kaznuje za prekršek iz prejšnjega odstavka 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 iz prvega odstavka tega člena odgovorna oseba državnega organa ali organa samoupravne lokalne skupnosti.

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

129. 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 s 106. členom tega zakona.

(2) Z globo od 1.200 do 2.000 eurov se kaznuje za prekršek iz prejšnjega odstavka 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 iz prvega odstavka tega člena odgovorna oseba državnega organa ali organa samoupravne lokalne skupnosti.

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

130. člen

(kršitev določb o biometriji v javnem sektorju)

(1) Z globo od 1.200 do 2.000 eurov se kaznuje za prekršek odgovorna oseba pravne osebe javnega sektorja, ki izvaja biometrične ukrepe v nasprotju s 107. členom tega zakona.

(2) Z globo od 1.200 do 2.000 eurov se kaznuje za prekršek iz prejšnjega odstavka tega člena odgovorna oseba državnega organa ali organa samoupravne lokalne skupnosti.

131. 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 108. členom tega zakona.

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

132. člen

(kršitev določb o prepovedi pridobivanja biometričnih osebnih podatkov v zvezi s trženjem)

(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 109. členom tega zakona.

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

133. 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 110. člena tega zakona;

2. ki ravna v nasprotju s četrtim odstavkom 110. člena tega zakona.

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

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

134. 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 111. člena tega zakona.

(2) Z globo od 400 do 1.200 eurov se kaznuje za prekršek iz prejšnjega odstavka 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 iz prvega odstavka tega člena odgovorna oseba državnega organa ali organa samoupravne lokalne skupnosti.

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

135. 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 v nasprotju s prvim odstavkom 112. člena tega zakona ali jih povezuje ali poveže brez odločbe Informacijskega pooblaščenca, v nasprotju s četrtim odstavkom 112. člena tega zakona.

(2) Z globo od 400 do 4.000 eurov se kaznuje za prekršek iz prejšnjega odstavka odgovorna oseba pravne osebe, samostojnega podjetnika posameznika ali posameznika, ki samostojno opravlja dejavnost.

(2) Z globo od 400 do 6.000 eurov se kaznuje za prekršek iz prejšnjega odstavka odgovorna oseba državnega organa ali organa samoupravne lokalne skupnosti.

136. 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 114. člena tega zakona;
2. če ne naredi uradnega zaznamka ali drugega uradnega zapisa iz 114. člena tega zakona.

(2) Z globo od 800 do 1.200 eurov se kaznuje za prekršek iz prejšnjega odstavka odgovorna oseba pravne osebe.

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

XII. DEL

PREHODNE IN KONČNE DOLOČBE

137. člen

(prehodne določbe glede prilagoditev dejanj obdelave)

(1) Upravljavci in obdelovalci v enem letu od začetka veljavnosti tega zakona izvedejo ustrezne ukrepe prilagoditve z določbami tega zakona glede obdelave privolitev 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. 86/04, 113/05 – ZInfP, 51/07 – ZUstS-A, 67/07 in 94/07 – uradno prečiščeno besedilo). Če upravljavec in obdelovalec v obdobju iz prejšnjega stavka izvajata ustrezne ukrepe prilagoditve glede obdelave privolitev iz prejšnjega stavka, to preprečuje nastanek kaznivosti za prekršek za obdobje enega leta od začetka veljavnosti tega zakona.

(2) Dejanja obdelave osebnih podatkov pri upravljavcih 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) najdlje 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 priprav na uskladitev dejanj obdelav z določbami Splošne uredbe in tega zakona, da gre za ustrezni prilagoditveni ukrep, ki preprečuje nastanek kaznivosti za prekršek za obdobje šest mesecev od začetka veljavnosti tega zakona.

138. člen

(prehodne določbe glede pooblaščenih oseb)

(1) Upravljavci in obdelovalci v devetih mesecev od uveljavitve tega zakona izvedejo ustrezne ukrepe prilagoditve glede določitve pooblaščene osebe po določbah tega zakona. Za obdobje iz prejšnjega stavka se šteje, da če obdelovalec in upravljavec izvajata ustrezne ukrepe glede določitve pooblaščene osebe in zagotavljata v tem obdobju skladnost dejanj obdelave po tem zakonu na drug način, da gre za ustrezni prilagoditveni ukrep, ki preprečuje nastanek kaznivosti za prekršek za obdobje devetih mesecev od uveljavitve tega zakona.

(2) Ne glede na določbe prejšnjega odstavka so občine in javni vzgojno-izobraževalni zavodi v dveh letih od uveljavitve tega zakona določijo pooblaščene osebe. 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.

(3) Ne glede na pogoja izobrazbe iz 3. točke in vsebine in trajanja delovnih izkušenj iz 4. točke prvega odstavka 46. člena tega zakona se do 25. maja 2020 za pooblaščeno osebo lahko določi osebo, ki ima najmanj eno leto delovnih izkušenj s primerljivih področij informacijske varnosti, varstva poslovne skrivnosti po zakonu, ki ureja gospodarske družbe, ali varstva zaupnih podatkov po zakonu, ki ureja bančništvo.

139. člen

(prehodne določbe glede delovanja Informacijskega pooblaščenca)

(1) Vsi postopki razen prekrškovnih in sodnih postopkov, ki so se pred začetkom uveljavitve tega zakona začeli pri Informacijskem pooblaščencuh, se nadaljujejo in končajo po določbah tega zakona.

(2) Dosedanje odločitve Informacijskega pooblaščenca o ustreznosti varstva osebnih podatkov v tretjih državah in prenosov osebnih podatkov ostanejo v veljavi, dokler niso spremenjene v skladu s Splošno uredbo ali tem zakonom.

(3) Seznam tretjih držav iz 66. člena Zakona o varstvu osebnih podatkov (Uradni list RS, št. 101/15, 11/17 in 16/17) velja v skladu z določbo prejšnjega odstavka.

(4) Z dnem uveljavitve tega zakona preneha delovati Register zbirk osebnih podatkov pri Informacijskem pooblaščencu, Informacijski pooblaščenec njegovo vsebino arhivira in preda v roku enega leta Arhivu Republike Slovenije, ki vsebino Registra hrani kot trajno arhivsko gradivo.

140. člen

(prehodne določbe glede pridobivanja podatkov iz uradnih evidence in registrov ter povezovanja)

(1) Za izvrševanje petega odstavka 38. člena tega zakona so upravljavci ali obdelovalci, ki za izvajanje svojega delovanja pridobivajo osebne podatke iz registrov ali evidenc s področja upravnih notranjih zadev, v dveh letih od uveljavitve tega zakona vzpostavijo ustrezne varnostne mehanizme.

(2) Povezovanja uradnih evidenc in javnih knjig se uskladijo s 112. členom tega zakona v štirih letih od uveljavitve tega zakona.

141. člen

(prehodne določbe glede certificiranja)

Slovenska akreditacija začne izvajati postopke akreditacije 1. januarja 2021.

142. člen

(razveljavitev in uporaba podzakonskih predpisov)

(1) Z dnem uveljavitve tega zakona prenehajo veljati:

– Pravilnik o metodologiji vodenja registra zbirk osebnih podatkov (Uradni list RS, št. 28/05 in 30/11) preneha veljati na dan uveljavitve tega zakona;

– Pravilnik o pridobivanju potrebnih informacij za odločanje o iznosu osebnih podatkov v tretje države (Uradni list RS, št. 79/05) preneha veljati na dan uveljavitve tega zakona;

– Pravilnik o službeni izkaznici državnega nadzornika za varstvo osebnih podatkov (Uradni list RS, št. 35/13)in.

– Pravilnik o zaračunavanju stroškov pri izvrševanju pravice posameznika do seznanitve z lastnimi osebnimi podatki (Uradni list RS, št. 85/07 in 5/12).

(2) Predpis iz tretje alineje prejšnjega odstavka se uporablja do uveljavitve predpisa iz drugega odstavka 67. člena tega zakona, kolikor ni v nasprotju s tem zakonom, predpis iz četrte alineje prejšnjega odstavka pa se uporablja do uveljavitve predpisa iz tretjega odstavka 26. člena tega zakona, kolikor ni v nasprotju s tem zakonom.

143. člen

(izdaja aktov)

Informacijski pooblaščenec izda akte iz tretjega odstavka 26. člena in drugega odstavka 67. člena v roku treh mesecev od uveljavitve tega zakona.

144. 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).

145. člen

(končna določba)

Ta zakon začne veljati 25. maja 2018.

III. Obrazložitev členov

Besedilo Predloga ZVOP-2 še ne upošteva načrtovanih sprememb (popravkov) v besedilu določb slovenskih inačic Splošne uredbe in Direktive, ker le-te še niso objavljene v Uradnem listu Evropske unije ter tako tudi še niso mogle biti upoštevane v obrazložitvi členov, razen izjemoma – privolitev in varnost osebnih podatkov. Kot je že navedeno v uvodni obrazložitvi, utegne biti vpliv na določbe Predloga ZVOP-2 še nekoliko širši, saj utegneta biti delno spremenjeni tudi inačici 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 s tem zakonom v pravnem redu Republike Slovenije 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 ter 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. Določbe navedene Direktive se izvršuje z zakonom, delno podobno velja glede določb Splošne uredbe, ki se lahko izvršijo ali morajo izvršiti z zakonom Republike Slovenije, 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 razdela, 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 določa bistvo človekove pravice do varstva osebnih podatkov. Pravico oziroma skupek pravic s področja podatkovne zasebnosti (varstvo 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 in 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 posameznicam 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). Izraz podatkovna zasebnost ni nov, gre samo za določeno posodobljenje izraza »informacijska zasebnost«[34].

V primeru omenjene podatkovne samoodločbe[35] (ki dodatno kaže, da gre za človekovo posebej poudarjeno osebno pravico razpolaganja svojimi osebnimi podatki) gre za to, da je (in ima) vsak posameznik »oblast« nad svojimi osebnimi podatki, da torej primarno sam odloča ali želi ali ne želi, da se njegove osebne podatke obdela, posreduje (npr. za izpolnitev pogodbe), izjeme pa so dopustne (ob spoštovanju strogega testa sorazmernosti), da se namreč določene podatke obdeluje proti njegovi volji – npr. če to določi zakon, ki prestane navedene pogoje presoje. Torej tudi ne gre za lastninski koncept zasebnosti, ampak za strogo osebni koncept zasebnosti.

Druge pravice na katere nakazuje predlagana določba, so npr. pravice s področja seznanitve z lastnimi osebnimi podatki (tretji odstavek 38. člena Ustave Republike Slovenije).

Ddoločeno je tudi, 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. Podlaga za del določbe o tajnosti osebnih podatkov je v drugem odstavku 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)[36]. 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 dosedanjo širšo 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 dosedanji 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 z 2. 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 3. 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 zakonika[37] ter prvi odstavek 1. člena Zakona o varstvu pred diskriminacijo[38]) 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.

[34] Odločba US, št. U-I-92/01, 28. 2. 2002, 27. točka odločbe; objava: Uradni list RS, št. 22/02 in OdlUS XI, 25.
[35] Odločba US, št. U-I-98/11, 26. 9. 2012, opomba št. 2; objava: Uradni list RS, št. 79/12.
[36] Objava: Bundesgeetzblatt I Nr. 120/2017, Teil I.
[37] Uradni list RS, št. 50/12 – uradno prečiščeno besedilo, 6/16 – popr., 54/15, 38/16 in 27/17.
[38] Uradni list RS, št. 33/16.

Predlagani člen pomeni, da se nikogar ne sme diskriminirati glede varstva osebnih podatkov, kar med drugim vključuje tudi prebivališče (vpliv glede 5. 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 podatkov[39] (Sveta Evrope), ki se v tem delu v okviru še nedokončane reforme varstva osebnih podatkov v okviru Sveta Evrope ne spreminja.

K 4. členu:

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 (ti. ročne ozir. papirnate 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 pazljiv 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 dnevov 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 pripravljalna delovanja za njo, kot so npr. ukrepi trženja ali trgovanje z osebnimi podatki za to, da se dobi storitev.«[40]

V tretjem odstavku je določeno, da če IX. del tega zakona ne določa 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, drugiin tretji odstavek), njenega nadzornega organa (Informacijski pooblaščenec) ter posredno tudi (jurisdikcije) 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

[39] Uradni list RS, št. 11/94 – Mednarodne pogodbe, št. 3/94 in 86/04 – ZVOP-1.
[40] 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.

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 uredbe[41] 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 Splošna uredba oziroma tak zakon, oziroma da bi upravljavec oziroma obdelovalec to varstvo zaobšla[42] 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 ne[43].

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 unije[44] 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 ustanovitev[45], oziroma ki na ozemlju Republike Slovenije opravljajo dejansko in resnično, čeprav majhno, dejavnost, v okviru katere se izvaja ta obdelava[46].

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 uporablja[47] , upoštevaje okoliščino, 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.

[41] Npr. drugi stavek prvega ostavka 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).
[42] 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)*.
[43] Uvodna navedba št. 22 Splošne uredbe.
[44] Sodba Sodišča EU v zadevi C-131/12, tč. 52, 56 in 67.
[45] Uvodna navedba št. 22 Splošne uredbe.
[46] 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*.
[47] http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2010/wp179_en.pdf

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 unije[48] (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 Evropske unije). Pri tem pa sama dostopnost spletne strani upravljavca, obdelovalca ali njunega 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, še zlasti tako, da pri tem uporablja slovenski jezik[49] 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 vedenja[50]. V takšnih primerih bo Informacijski pooblaščenec pristojen za nadzor skladnosti obdelave tujega upravljavca ozir. obdelovalca s tem zakonom, ter za obravnavo pritožb posameznikov v zvezi s tem.

Posamezne ureditve iz 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[51] (zlasti (c) točka prvega odstavka člena 6 v zvezi s tretjim odstavkom ter področnimi ureditvami zlasti iz členov 85-91 Splošne uredbe). To ti. »načelo dodatne 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. Vsi primeri uporabe tega načela so v tem odstavku posebej našteti. Po njih bo državni nadzorni organ za varstvo osebnih podatkov Republike Slovenije (Informacijski pooblaščenec) pristojen sprejeti prijave 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.

Primera možnih uporab tretjega odstavka:

Primer št. 1: italijanski zdravnik obdeluje zdravstvene podatke prebivalca Slovenije. Prebivalec Slovenije se pritoži pri italijanskem ali nadzornem organu za varstvo osebnih podatkov Republike Slovenije - Informacijski pooblaščenec se mora vključiti v postopek in zahtevati uporabo slovenskega ZVOP-2.

[48] Navedba št. 23 Splošne uredbe.
[49] Navedba št. 23 Splošne uredbe.
[50] Navedba št. 24 Splošne uredbe.
[51] Tako je v Predlogu Zakona o varstvu osebnih podatkov Francoske republike – nujni zakonodajni postopek, z dne 14. 2. 2018 v drugem odstavku 8. člena (ki dodaja nov člen 5-1 v zakon iz leta 1978) določeno, da spada pod ti. »načelo dodatne rezidenčnosti« tudi obdelava osebnih podatkov v okviru svobode izražanja – velja torej pravo Francoske republike.

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 dobesedni 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. Zelo pomembno za izvajanje ZVOP-2 pa je, da je izjemoma že popravljeno besedilo definicije privolitve, ne glede na besedilo veljavne slovenske inačice Splošne uredbe, saj bi zadržanje uradne inačice pomenilo drugačno pravno razumevanje privolitve kot 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«[52]. 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. Privolitev, kot je sedaj določena v Splošni uredbi, je nekoliko drugačna[53] od prejšnje privolitve po Direktivi 95/46/ES in je nekoliko bližja nekdanji privolitvi za obdelavo občutljivih osebnih podatkov, torej izrecnosti privolitve. Domnevana privolitev ni dopustna, niti vnaprej »potrjene« opt-in oznake, privolitev mora biti tudi opcijsko osredotočena (»granular«) – da se pač pri privolitvi lahko da različne opcije za obdelavo, npr. za manjši krog osebnih podatkov, za manj posegajočo obdelavo ipd.

Prav tako je v 12. točki glede na očitne napake v slovenski inačici definicije iz 12. točke člena 4 Splošne uredbe drugače določena kršitev varnosti osebnih podatkov, ki po predlagani ureditvi pomeni: »kršitev varnosti, ki povzroči nenamerno ali nezakonito uničenje, izgubo, spremembo, nepooblaščeno razkritje ali dostop do osebnih podatkov, ki so poslani, shranjeni ali kako drugače obdelani«.

Zapisi temeljnih definicij s področja varstva osebnih podatkov (npr. osebni podatki, obdelava...) – kolikor se nanašajo na definicije iz Splošne uredbe, so v četrtem odstavku pojasnjeni z navedbo, da gre (samo) za »spoštovanje obveznosti iz drugega odstavka 1. člena [ZVOP-2]«. To pomeni, da je

[52] 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«.
[53] Glejte: Carey, Peter et. al., *Data Protection : A Practical Guide to UK and EU Law*, Oxford University Press, Oxford, 5th Edition, 2018, str. 50-53.

navedeni zapis (prepis), kolikor se nanaša na definicijske določbe iz Splošne uredbe, le informativne ozir. povezovalne narave v korist pravne varnosti in ne pomeni in ne sme pomeniti pravnega urejanja izven dometa Splošne uredbe (tudi glede na uvodno navedbo št. 8 Splošne uredbe), torej namen zakona ni prenos določb Splošne uredbe, ampak zgolj ustvarjanje pogojev za njeno izvrševanje (npr. s tehniko sklica, povezovanja ipd.).

V delu, ko se isti zapisi temeljnih definicij nanašajo na Direktivo in so spet enaki določbam Splošne uredbe, pa tudi relevanten zaključni zapis v četrtem odstavku 6. člena.

Dodatno pa je upoštevana tudi mednarodna obveznost s področja Sveta Evrope - to pomeni da ta člen pomeni tudi izvajanje določb 2. in 5. člena Konvencije o varstvu posameznikov glede na avtomatsko obdelavo osebnih podatkov (Sveta Evrope)[54]. In 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 - s tega vidika pa je tudi logično, da Slovenija ne izbere drugačnih definicij s področja varstva osebnih podatkov, kot so določene v členu 4 Splošne uredbe.

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 interpretativnih zamejitev (glede uporabe Splošne uredbe), kot je predlagano na koncu besedila 6. člena ZVOP-2 (četrti odstavek).

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.

Od dodatnih definicij v tretjem odstavku 6. člena ZVOP-2 so npr. pomembne definicije izbrisa, skupnih upravljavcev, zakona, varnosti države in sorazmernosti.

Izbris osebnih podatkov (5. točka tretjega odstavka) 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 drugim 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), kar pomeni tudi, da ni posega v dokumentarno gradivo javnih organov, ki ga arhivska služba s strokovnim navodilom določi kot arhivsko gradivo – če zakon za javnopravno področje ne določa izbrisa ali pa določa ti. »zamejeni izbris« (arhiviranje v ti. neaktivno« arhivsko zbirko).

Skupni upravljavci pa 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 upravljavskega tipa), skupni upravljavci pa so nekoliko podrobneje urejeni v 33. členu ZVOP-2.

Po 9. točki tretjega odstavka 6. člena ZVOP-2 pojem »zakon« pomeni glede na člen 6 Splošne uredbe, člen 4 Direktive ter za izvrševanje a) in b) točke 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

[54] Uradni list RS, št. 11/94 – Mednarodne pogodbe, št. 3/94 in 86/04 – ZVOP-1.

pravne akte ali odločitve Evropske unije, katerih določbe so enakovredne zakonom in neposredno uporabljive ali neposredno učinkovite (glede na določbe tretjega 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 – glede na tam navedeno določbo o »zakonu« ter z njim povezano ustaljeno ustavnosodno presojo Ustavnega sodišča Republike Slovenije od leta 1992 dalje[55] ter glede na določbe 87. in 153. člena Ustave Republike Slovenije).

Definicija varnosti države iz 10. točke tretjega odstavka 6. člena ZVOP-2 je pomembna za uporabo določb o varnosti države v ZVOP-2 ter določb podorčnih zakonov glede varnosti države, kadar določajo obdelavo osebnih podatkov: 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, šesti odstavek 38. člena, tretji odstavek 42. člena, šesti odstavek 49. člena, prvi odstavek 85. člena ipd. ZVOP-2).

V 11. točki tretjega odstavka je z vidika lažje povezave in uporabe določb zakona dodano na kratko opredeljeno temeljno načelo sorazmernosti obdelave osebnih podatkov, katero je sicer vsebovano v c) točki, v delni povezavi z b) in d) točko prvega odstavka 7. člena 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) in č) urejajo omejitev 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 skladnost 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, da morata izvajati dokumentiranje 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 ((e) točka drugega odstavka 34. člena ZVOP-2) in zunanjo sledljivostjo obdelav osebnih podatkov (sedmi odstavek 40. člena ZVOP-2) po določbah tega zakona.

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, tretjem šestem in sedmem odstavku.

[55] 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 šestim 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) – vsebinsko 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 tretjega 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 6. člena ZVOP-2 delujejo tudi na podlagi privolitve[56], 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 zakonskih (dejansko: oblastvenih[57]) 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 določenemu subjektu javnega prava ozir. le temu subjektu javnega prava. To prostovoljno razkritje zahteva, da se poda privolitev in je podobno določbi d) točke drugega odstavka predlaganega 12. člena ZVOP-2 – prostovoljno razkritje posebne vrste osebnih podatkov.

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. Primer je npr. 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

[56] 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).«

[57] 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 […].«

zvezi s 87. členom Ustave Republike Slovenije)[58]. Gre za nadgradnjo vsebine dosedanjega četrtega odstavka 9. člena ZVOP-1.

Predlagani tretji odstavek določa, da se v javnem sektorju lahko izjemoma (!) obdelujejo tudi osebni podatki, ki so nujni za izvrševanje zakonitih pristojnosti, nalog ali obveznosti javnega sektorja, če se s to obdelavo ne poseže v upravičen interes posameznika, na katerega se nanašajo osebni podatki. Predlagana določba temelji na (c) in (e) točki prvega pododstavka prvega odstavka člena 6 Splošne uredbe in je primerljiva dosedanji določbi četrtega odstavka 9. člena ZVOP-1, katere uporabo sicer sodna praksa slovenskih sodišč nekoliko omejuje[59].

Predlagani četrti 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 peti 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 – sicer 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 šesti odstavek določa obdelavo osebnih podatkov v druge namene[60] 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 sedmi 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 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 2016/679*[61]« 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

[58] 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.

[59] Glejte: sodba Vrhovnega sodišča RS, opr. št. I Up 307/2016, 21. 6. 2017.

[60] 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.

[61] »Guidelines on Consent under Regulation 2016/679«, 17/EN, WP259, Adopted on 28 November 2017, str. 12.

namen, ni pa možna obdelava v druge namene – in nato je za obdelavo v drug namen potrebno pridobiti dodatno privolitev – skladno s členom 6, četrtim 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 zasebnemu 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 upravičenih ter istočasno zakonitih (v skladu z določbami tega zakona ali Splošne uredbe ali področnega zakona) 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 obdela na tej podlagi osebne podatke, ki jih zakonito ima, za potrebe pravdnega postopka, ne gre pa morda za obdelavo osebnih podatkov za namene neposrednega trženja, saj je to posebno (področno) urejeno v 1. poglavju X. Dela 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, 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 četrtim 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 namen[62], 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, četrtim odstavkom Splošne uredbe ter členom 5, (b) točko prvega odstavka iste uredbe ter glede na uvodno navedbo št. 32 uredbe[63].

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 **o**sebni 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 pooblaščeni 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, dedičem ali drugim osebam, če izkažejo pravni interes.

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, enciklopedijh itd, se pa ne nanaša na klasične članke v medijih (za te primere načeloma velja svoboda izražanja po 82. členu predloga zakona).

---

[62] 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.

[63] 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.

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 torej 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 zakonika[64]: »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.

Dodatne določbe v drugem in tretjem odstavku (glede na besedilo iz Splošne uredbe) pomenijo zakonsko razdelavo, s katero se za konkretne obdelave zagotovi učinkovitejše izvajanje zakona ((c) točka prvega odstavka člena 6 v zvezi s tretjim odstavkom člena 6 Splošne uredbe). V Francoski republiki je tako v Predlogu Zakona o varstvu osebnih podatkov Francoske republike – nujni zakonodajni postopek, z dne 14. 2. 2018, v 14 A členu (ki dodaja člen 7 – 1 v Zakon št. 78-17 o informacijski tehnologiji, zbirkah osebnih podatkov in državljanskih svoboščinah iz leta 1978) določeno, da je starost za mladoletnika za podajo privolitve za uporabo storitev informacijske družbe 15 let, dodano pa je v okviru prostega polja zakonodajne presoje določeno, da kadar gre za mladoletnika pod starostjo 15 let, je privolitev zakonita le, če jo skupaj podata mladoletnik in oseba, ki ima starševsko odgovornost za mladoletnika. Poleg tega je kot zakonska specifičnost predpisano tudi, da mora upravljavec s področja storitev informacijske družbe pogoje poslovanja in druge komunikacije (tudi posredovanje informacij) z mladoletnikom izvajati na jasen in preprost način, tako da mladoletnik to vsebino razume na enostaven način. Določena razdelava glede storitev informacijske družbe in mladoletnikov je narejena tudi v amandmiranem Predlogu Zakona o varstvu osebnih podatkov 2018 Irske (z dne 15. 2. 2018) v drugem odstavku 30. člena, da namreč storitve informacijske družbe ne vključujejo storitev preventivne ali svetovalne narave – namreč ne vključujejo pomoči mladoletnikom. Za take primere ni zahtevana privolitev mladoletnika.

[64] Uradni list RS, št. 15/17.

Glede merila »razumna prizadevanja« predlagani člen sicer načeloma izhaja (enako tudi določbe člena 8 Splošne uredbe) iz COPPA Združenih držav Amerike, ki ne vsebuje podrobnejših meril, 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).

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, biometrijskih 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 dosedanji 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 i) 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 varnosti osebnih podatkov iz 34. 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 34. 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 zbiranja in obdelave osebnih podatkov o narodni pripadnosti za statistične ali raziskovalne ali poročevalske namene ima Republika Slovenija glede dela posebnih vrst osebnih podatkov že ustavnopravno dokaj strogo ureditev 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) – spoštovan mora biti torej strogi test (v zvezi načelom) sorazmernosti, kar praktično skoraj onemogoča da bi se ta podatek, glede katerega je ustavna opredelitev še posebej poudarja njegovo »svobodno«[65] opredeljevanje, sploh lahko zbiral in nato nadalje obdeloval. Torej zbiranja in nadaljnje obdelave (ali celo obdelave v druge namene) osebnih podatkov o narodni pripadnosti 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), ali poročanja mednarodnim organizacijam[66], če ni ustavnopravno opravičen (utemeljen) že primarni namen za zbiranje podatka o narodni in etnični pripadnosti za potrebe določenega postopka ali odločanja (npr. izjemoma prosilci za mednarodno zaščito – preganjanje zaradi narodne pripadnosti[67] - na podlagi druge ustavne vrednote – npr. 48. člen Ustave Republike Slovenije). Prav tako, če se odmisli prej navedeni primarni namen zbiranja (za potrebe postopka ozir. odločanja), bi bilo pa zbiranje in obdelava podatkov o pripadnosti na podlagi izrecne 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 o narodni pripadnosti iz 61. člena Ustave) in realno ne bi kaj bistvenega moglo pomeniti z vidika ocene delovanj ali odločanj o ljudeh v raznih uradnih (zakonsko določenih) postopkih.

Še bolj zamejen (strožji) pristop velja glede zbiranja in obdelave osebnih podatkov o verski pripadnosti[68] – po 41. členu Ustave Republike Slovenije, po katerem je izpovedovanje vere svobodno (prvi odstavek) in kjer je tudi določeno, da se nihče ni dolžan opredeliti glede verskega ali drugega (npr. svetovnonazorskega) prepričanja (drugi odstavek).

Seveda pa pravni red Republike Slovenije ne preprečuje, da nevladne organizacije ali raziskovalne organizacije ne raziskujejo same, na podlagi uporabe arhivskega gradiva ali drugače dostopnega gradiva (npr. z uporabo Zakona o dostopu do informacij javnega značaja), če ta gradiva o tem vsebujejo vsaj posredne informacije o narodni ali verski pripadnosti (npr. kazniva dejanja s področja

[65] Glejte tudi prvi odstavek 3. člena Okvirne konvencije za varstvo narodnih manjšin (Sveta Evrope), Uradni list RS, št. 20/98 – Mednarodne pogodbe, št. 4/98, ki določa: »Vsak pripadnik narodne manjšine ima pravico do proste izbire, da je ali ni obravnavan kot pripadnik narodne manjšine, in iz te njegove izbire ali uresničevanja pravic, ki so z njo povezane, ne izhajajo nobene neugodne posledice.« ter Obrazložitveno poročilo k prvemu odsatavku 3. člena Konvencije:
»Prvi odstavek
34. Prvi odstavek najprej jamči vsaki osebi, ki pripada narodni manjšini, da ima svobodo, da izbere, da se jo obravnava ali ne obravnava kot tako. Ta določba prepušča vsaki taki osebi, da odloči, ali se želi ali ne vključiti pod zaščito, ki izhaja iz načel Okvirne konvencije.«

[66] Glede spreminjanja stališča s strani mednarodnih organizacij (v smeri delnega ukinjanja oziroma odsvetovanja zbiranja in obdelave osebnih podatkov o narodni pripadnosti) glejte: »*Statement by the OSCE Mission to Bosnia and Herzegovina about the conclusions of the High Judicial and Prosecutorial Council BiH*«, Sarajevo, 27. 10. 2017, kjer je med drugim navedeno: »Sklepi Visokega sodnega in tožilskega sveta, ki med drugim zahtevajo od vseh sodišč v Bosni in Hercegovini, naj zagotovijo podatke o etnični pripadnosti obtožencev v tekočih in zaključenih sodnih postopkih vojnih hudodelstev […], ne odražajo pomena in namena neodvisnosti sodstva kot [dela] vrhovnosti načela vladavine prava.«

[67] 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).

[68] Glejte: odločba US, št. U-I-92/01, 28. 2. 2002; objava: Uradni list RS, št. 22/02 in OdlUS XI, 25, zlasti 34. in 21. točka.

131. (Kršitev enakopravnosti) ali 297. člena Kazenskega zakonika (Javno spodbujanje sovraštva, nasilja ali nestrpnosti)), kakšna so določena razmerja/vpliv glede narodne ali verske pripadnosti v zvezi z uradnimi (zlasti sodnimi) postopki, storitvami ipd. v Republiki 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 – npr. 27. člen Ustave Republike Slovenije). V prvem odstavku je tako določeno, da za podatke o vpisu ali izbrisu v ali iz kazenske evidence ali evidenc (posebej urejene zbirke osebnih podatkov – uradne evidence), 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 (vrst) 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 pooblaščenca[69].

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 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 pooblaščencem oziroma pred sodišči.

[69] Glede na določbe Zakona o dostopu o informacijah javnega značaja in praksi Informacijskega pooblaščenca ti osebni podatki niso dostopni javnosti, glejte: odločba IP, št. 021-65/2008/4, 30. 6. 2008 in odločba IP, št. 090-111/2010/2, 5. 8. 2010.

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 varstvu 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 pooblaščeno 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:

Predlagani 15. ter sledeči členi 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.

K 16. členu:

Predlagani 16. 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. Drugi odstavek določa možnost potrditve prejema zahteve po določenimi pogoji in v roku sedmih delovnih dni.

Člen določa tudi v tretjem odstavku, da se za obravnavo zahteve v določenih primerih uporabljajo določbe Zakona o splošnem upravnem postopku.

K 17. členu:

Predlagani 17. člen ureja načine preverjanja istovetnosti posameznika, na katerega se nanašajo osebni podatki, kadar uporablja pravice po 14.-21. členu ZVOP-2. Med drugim se v javnem ali zasebnem sektorju to preveri preko elektronskega podpisa, ki je izenačen z lastnoročnim poddpisom in velja v skladu z Uredbo (EU) št. 910/2014, s potrditvijo zahteve 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.

K 18. členu:

Predlagani 18. člen določa, da mora upravljavec odgovor zagotoviti brez nepotrebnega odlašanja, vendar v vsakem primeru v enem mesecu 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 upravljavca.

Predlagani tretji odstavek določa, da stranke in stranski udeleženci do prejema odločitve upravljavca nimajo pravice do pregledovanja dokumentacije v zvezi z osebnimi podatki, ki so bili zahtevani, ali drugih sporočil ali informacij.

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 upravljavca glede posredovanja osebnih podatkov. Predlagano je, da 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 Informacijskem pooblaščencu) pri upravljavcu vloži obrazložen ugovor v roku osmih dni. Upravljavec mora o ugovoru odločiti kot o novi zahtevi v 5 delovnih dneh, če gre za zadeve z direktivnega področja (85. člen Predloga ZVOP-2) pa v 15 delovnih dneh, saj gre za lahko tudi za izmenjavo informacij med različnimi subjekti, ki so lahko tudi v tujini (druge države Evropske unije, tretje države, mednarodne organizacije) in gre tudi za vprašanje odzivnosti (tuji policijski organi, tuja kazenska sodišča…) in je lahko ustrezni predpisani rok za izvedbo odločitve le 15 delovnih dni.

K 21. členu:

V 21. členu je določeno, da če upravljavec ne odloči o zahtevi posameznika v roku iz 18. člena ZVOP-2, lahko posameznik pri Informacijskem pooblaščencu vloži pritožbo zaradi molka. Če upravljavec zahtevo zavrne, lahko posameznik pri upravljavcu, če gre za javni sektor oziroma pri Informacijskem pooblaščencu, če gre za zasebni sektor vloži obrazloženo pritožbo v roku 15 dni od prejema obvestila ali odločbe upravljavca. 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., sicer v skladu z omejitvami posegov v pravice s področij komunikacijske in prostorske zasebnosti iz drugega do četrtega odstavka 68. člena tega zakona. 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.

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 Slovenije[70].

K 25. členu:

25. člen določa, da je za izvedbe upravne izvršbe v zvezi z odločbami, izdanimi v pritožbenem postopku, 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 četrti odstavek 41. člena Zakona o pacientovih pravicah[71].

K 27. členu:

Predlagani 27. člen ZVOP-2 določa omejitve pravic posameznikov. Po prvem odstavku je pravice posameznika iz tega dela zakona mogoče z zakonom izjemoma omejiti iz razlogov navedenih v prvem odstavku člena 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 mora 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.

[70] 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.
[71] Uradni list RS, št. 15/08 in 55/17.

K 28. členu:

V 28. členu je posebej urejeno sodno varstvo posameznika. V prvem odstavku je določeno, da ima posameznik, ki ugotovi, da so kršene njegove pravice, določene s tem zakonom, lahko zahteva sodno varstvo po določbah Obligacijskega zakonika (osebnostne pravice, odškodnine) in to po določbah Zakona o pravdnem postopku – torej pred pravdnim oddelkom pristojnega sodišča. 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 je zadevnem sodnem postopku praviloma javnost izključena.

Po četrtem 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 interesu[72], da v njegovem imenu uveljavlja sodno varstvo po določbah tega člena. Sodni postopek je po predlaganem petem odstavku je nujen in prednosten (kot je bilo dosedaj enako določeno tudi v petem odstavku 34. člena ZVOP-2).

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 ozir. 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, upoštevaje tveganost obdelave), popis sredstev obdelave, popis dostopnih pravic zaposlenih, pogodbenih partnerjev in drugih uporabnikov, ter rezultate rednih revizij skladnosti obdelave podatkov. Upravljavec lahko za pripravo in hrambo te dokumentacijo pooblasti tudi pooblaščeno osebo 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 upravljavec.

K 30. členu:

[72] Navedene organizacije bodo priznane oziroma jim bo podeljen zahtevani status v skladu z določbami bodočega Zakona o nevladnih organizacijah, ki je bil sprejet dne 20. 3. 2018 (EPA 2300-VII).

Upravljavec 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 upravljavec 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 upravljavec 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.

Upravljavec 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 upravljavec 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 pooblaščencem 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 7 točk namesto prejšnjih 13 (prvi odstavek člena 30 Splošne uredbe), 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 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 (15. člen ZVOP-2).

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) v skladu s petim odstavkom člena 30 Splošne uredbe določene tri alternativne in seveda obvezujoče izjeme[73] 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,

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

- 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.

K 34. členu:

Predlagani člen nadomešča dosedanji pojem oziroma institut "zavarovanje osebnih podatkov" (24. člen ZVOP-1) s pojmom "varnost osebnih podatkov". Sprememba seveda ni samo izrazoslovna, ampak je vezana zlasti na spremenjene tehnološke realnost, 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, 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 dnevniških sledi o dejanjih obdelave osebnih podatkov.

Konkretneje 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,

[73] 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«.

- 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 (e) točki drugega odstavka in 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 2003[74]). 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 pooblaščencu, 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") – realno najpozneje 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 ukrepa za zagotovitev varnosti osebnih podatkov, kot tudi v tem, da v primeru najresnejših kršitev skupaj z upravljavcem oziroma obdelovalcem, pri katerem je prišlo do incidenta, premisli, ali je potrebno o njem obvestiti tudi končne uporabnike, zato da lahko izvedejo ustrezne ukrepa za zaščito njihovih osebnih podatkov.

Obveščati je zatorej 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.

[74] Glejte: Database Breach NotificationSecurity Act (“SB 1386”) iz leta 2003 (zadnjič spremenjen leta 2015).

Posamezne vidike notifikacijske dolžnosti je že obravnavala Delovna skupina po členu 29 Direktive 95/46/ES, in o tem izdala svoje mnenje[75].

K 36. členu:

V primerih suma hujših incidentov, tj. ko je med preiskavo incidenta verjetno, da če da so ozir. bodo nastala velika tveganja za človekove pravice in temeljne svoboščine posameznikov, mora upravljavec o incidentu obvestiti tudi svoje uporabnike (posameznike), zato da lahko izvedejo 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. Takšen dokument je v praksi poimenovan kot »Ocena učinkov v zvezi z varstvom osebnih podatkov« (»*Data Protection Impact Assessment – DPIA*«). Gre za ukrep, ki se močno povezuje z obveznostjo vgrajenega varstva osebnih podatkov (30. člen ZVOP-2), 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 pooblaščeno 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 ter k obdelavi osebnih podtakov v skladu z načelom sorazmernosti.

Podrobnosti za izvedbo ocene razlaga Informacijski pooblaščenec v svojih smernicah iz novembra 2017[76].

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, državnih tožilstev in sodišč za posredovanje podatkov, relevantnih za odločanje ali delovanje v konkretni zadevi. Pomembna zakonska rešitev je v prvem odstavku 38. člena, kateri določa, da se pri tem posredovanju preverja tudi ali gre za zaščito življenjskih interesov posameznika po petem odstavku 38. člena in tretjem odatavku 39. člena ZVOP-2.

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. Šele na podlagi takšnega dopisa pa je potem mogoče pripraviti zaprošene podatke in jih tudi posredovati.

Prtedlagani 39. člen je neke vrste »zrcalna slika« 38. člena – zasebni sektor posreduje določene podatke uporabnikom iz javnega sektorja ali celo iz zasebnega sektorja, če gre za nalogo javnega sektorja po drugem odstavku 38. člena.

[75] Glejte: WP250 z dne 3.10.2017, Guidelines on Personal data breach notification under Regulation 2016/679.
[76] Glejte: https://www.ip-rs.si/fileadmin/user_upload/Smernice_o_ocenah_ucinka__DPIA__nov2017.pdf

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 40. člena izvedbeno zahteva tudi vodenje revizijskih sledi o posredovanjih – za dobo petih let.

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: mora[77]) 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 ali vozniško dovoljenje 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 glede povezovalnih znakov (EMŠO, davčna številka, ZZZS številka) ohranja obstoječe sistemske omejitve iz 20. člena ZVOP-1 pri povezovanju z nekaterimi zbirkami osebnih podatkov (evidence), 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. Prepovedi iz prvega odstavka 42. člena so bile vsebovane že v četrtem odstavku 8. člena Zakona o varstvu osebnih podatkov iz leta 1999 ter v veljavnem prvem odstavku 20. člena ZVOP-1, vključene pa so bile v zakon kot povezava s sprejemanjem Zakona o centralnem registru prebivalstva[78] leta 1998, namreč kot varovalkav povezavi s takratnimi idejami, da bi bilo treba (v Zakonu o centralnem registru prebivalstva) ukiniti enotno matično številko občana, ker naj bi le-ta omogočala preveliko moč državi in preveč ogrožala zasebnost ljudi.

V petem odstavku se ureja avtomatizirano odločanje, ki velja tako za javni kot za zasebni sektor kot tudi za IX. del zakona. Določeno je, da so odločitve upravljavcev, 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 osebni podatki nanašajo, oziroma lahko v večji meri vplivajo nanj, prepovedane, razen če to možnost tovrstnega

[77] 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).
[78] Izvirno: Uradni list RS, št. 1/99.

avtomatiziranega odločanja izrecno določa zakon (torej drug zakon, obvezujoča mednarodna pogodba ali pravni akt ali odločitev Evropske unije, ki sta enakovredna zakonu in se v Republiki Sloveniji uporabljata neposredno), ki določa tudi ustrezne ukrepe za varstvo človekovih pravic in temeljnih svoboščin ter upravičenih interesov posameznika, zlasti posebno pravico do ugovora. Kadar pa tovrstne odločitve po drugem zakonu temeljijo na obdelavi posebnih vrst osebnih podatkov, so prepovedane tudi, če bi lahko vodile do diskriminacije posameznika (kršitev vsaj 14., 22. in 23. člena Ustave Republike Slovenije in 1. člena Protokola št. 12 k Evropski konvenciji o človekovih pravicah), na katerega se nanašajo osebni podatki, ali njemu bližnjih oseb. V povezavi z navedenim je v zadnjem stavku petega odstavka določeno, da je pred uvedbo sistema postopkov avtomatiziranega odločanja treba izvesti posebno osredotočeno oceno učinka po 37. člena ZVOP-2. Osredotočenost ocene učinka pomeni, da mora ta ocena vsebovati tudi oceno učinka na povezane človekove pravice in temeljne svoboščine, zlasti glede prepovedi diskriminacije, lahko pa tudi glede svobode gibanja, splošne zasebnosti, dostojanstva, komunikacijske zasebnosti ipd.

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, ni pa predlagan splošen (zakonsko določen) rok hrambe za primere, ko področni zakoni, pogodbe ipd. tega ne določajo[79], saj je to odvisno od konkretnih situacij in zakonsko prepdisani rok bi bil prenevaren (verjetno predolg za določene »rutinske« obdelave). 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:

V 1. poglavju IV. delu Predloga ZVOP-2 se urejajo novi subjekti na področju varstva osebnih podatkov - pooblaščene osebe za varstvo podatkov (»*data protection officers*«) ter certificiranje obdelav osebnih podatkov. Obveznost imenovanja pooblaščene 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 zahtevke posameznikov v zvezi z obdelavami njihovih podatkov, ter vzdrževati določeno pojasnjevalno komunikacijo z državnim nadzornim organom za varstvo osebnih podatkov (Informacijskim pooblaščencem) – 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 pooblaščene osebe so individualne osebe, delajo neodvisno, lahko jim

[79] Glede rezervnega pravila za določitev roka hrambe 5 let (ki je lahko predolg za »rutinske« obdelave) glejte npr.: »VARSTVO OSEBNIH PODATKOV V DELOVNIH RAZMERJIH : Smernice Informacijskega pooblaščenca«, 20. 12. 2016, razdelka 7.1 in 7.2 (str. 33), dostopno na: https://www.ip-rs.si/fileadmin/user_upload/Pdf/smernice/Smernice_-_Varstvo_OP_v_delovnih_razmerjih.pdf

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 pooblaščeno 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 pooblaščene 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 uredbe) imenovanje pooblaščene 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 strožje), 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. Pooblaščena oseba za varstvo podatkov je tako le oseba, 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.

V 44. členu je tako podana opredelitev pooblaščene 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 pooblaščene osebe.

K 45. členu:

45. člen ZVOP-2 določa v prvem odstavku, da morajo pooblaščeno osebo za varstvo podatkov določiti 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 in del upravljavcev v javnem 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, po 3. točki pa enako, kadar gre za posebne vrste osebnih podatkov ali osebne podatke iz 13. člena ZVOP-2. Vsi ti subjekti so dolžni ddoločiti pooblaščeno osebo, če so izpolnjeni predpisani pogoji, kar pa tudi pomeni, da je treba posebej opraviti presojo, ali gre za takšne obdelave, in treba jo je upraviti posebej pri upravljavcu in pri obdelovalcu, ki sta v rzamerju (pogodbene) obdelave. Tako je možno, da bosta k imenovanju pooblaščene 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 pooblaščene 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/ES[80] na to temo.

[80] Glejte: WP 243 rev.01, 5. 4. 2017, dostopne na: http://ec.europa.eu/newsroom/document.cfm?doc_id=44100

Velika večina upravljavcev in obdelovalcev bo torej prosta te obveznosti. Bodo pa še vedno lahko pooblaščeno 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 drugem odstavku lahko tudi ostali upravljavci ali obdelovalci prostovoljno imenujejo pooblaščeno osebo in na ta način izkažejo kakovost njihovih obdelav osebnih podatkov.

Tretji odstavek določa možnost imenovanja namestnika pooblaščene osebe za čas zadržanosti ali odsotnosti pooblaščene osebe.

Po četrtem odstavku morata upravljavec ali obdelovalec, ki sta imenovala pooblaščeno 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 pooblaščencu, 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 pooblaščene osebe za varstvo podatkov – v skladu z usmeritvamiiz petega odstavka člena 37 in drugega stavka šestega odstavka člena 38 Splošne uredbe.

Po prvem odstavku je za javni sektor določeno, da je za pooblaščeno osebo za varstvo osebnih podatkov lahko imenovan posameznik, ki poleg pogojev iz prvega odstavka izpolnjuje še naslednje pogoje, da je namreč:

1. državljan Republike Slovenije ali državljan 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 (po področni zakonodaji je to: izobrazba, pridobljena po študijskem programu druge stopnje, oziroma izobrazba, 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 izobrazba, pridobljena po študijskem programu druge stopnje, oziroma izobrazba, 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 (glejte začasne izjeme glede sorodnih področij v tretjem odstavku 140. člena ZVOP-2),

5. 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 del javnega sektorja nato drugi odstavek 46. člena določa še nekatere dodatne pogoje za imenovanje pooblaščene osebe.

V tretjem odstavku je določena razumna področna ureditev za področje vzgoje in izobraževanja, po kateri se v primeru, če se za pooblaščeno 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 obdobja in konkretnih 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 pooblaščeno osebo izjemoma s pogodbo v pisni obliki imenuje tudi posameznika ali posameznico iz zasebnega sektorja, ali pravno osebo

zasebnega sektorjalzjema od te izjeme je določena v petem odstavku 49. člena Predloga ZVOP-2 – za ministrstva.

Po petem odstavku lahko zasebni sektor za pooblaščeno 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, ob tem je tudi določeno, da je pooblaščena oseba lahko le individualno določena, kar pomeni, da ne more biti kolektiovnega subjekta/organa, v primeru pravne osebe pa, da mora določena fizična osebe iz te pravne osebe imeti položaj vodilnega člana Šesti odstavek nekoliko prilagodi pogoje glede državljanstva za pooblaščene osebe. Pooblaščeni osebi namreč pri opravljanju njenih nalog pomagajo tudi druge osebe, ki so pri tem vezane na njena navodila. Te osebe morajo izpolnjevati pogoje za imenovanje za pooblaščeno osebo. To pomeni, da je pooblaščena oseba funkcionalno in 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 pooblaščene osebe (kolegijski subjekt ali kolegijski »organ«). Ta vodilna oseba je hierarhično nadrejena ostalim članom skupine in odgovorna za delo.

Po sedmem odstavku je obveznost, da morajo v primerih, kadar se v skladu s tem členom določi pravno osebo, vsi zaposleni in drugi sodelavci in pravne osebe, kateri bodo opravljali naloge pooblaščene osebe, izpolnjevati pogoje za imenovanje v pooblaščeno osebo, razen pogoja državčjanstva.

V osmem odstavku je določena sistemska prepoved, po kateri za pooblaščeno osebo in osebe, ki ji pomagajo pri opravljanju njenih nalog ne smejo biti imenovana osebe, ki imajo konflikt interesov z upravljavcem ali obdelovalcem. Npr. to ne more biti oseba iz kadrovske službe določenega upravljavca, lahko pa je, če je posebej izkazano, da ni konflikta interesov – oseba iz službe za informacijsko podporo, ipd.

V devetem odstavku je prepoved iz osmega 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 pooblaščena 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 pooblaščeno osebo razrešiti ob upoštevanju določb tretjega in četrtega odstavka 50. člena ZVOP-2. Enako ravna v primeru, če se na drug način seznani z obstojem ali verjetnostjo obstoja konflikta interesov. Vse navedeno velja tudi za osebe, ki pooblaščeni osebi pomagajo pri opravljanju njenih nalog.

Po predlaganem desetem odstavku veljajo določbe osmega in devetega odstavka o razrešitvi konflikta interesov smiselno tudi za zasebni sektor.

K 47. členu:

V 47. členu je določena možnost imenovanja skupne pooblaščene osebe za varstvo podatkov. Več upravljavcev iz javnega sektorja ali več upravljavcev iz zasebnega sektorju lahko, upoštevaje njihovo delovno področje, organizacijsko strukturo in velikost, imenuje tudi skupno pooblaščeno osebo (ne more pa del javnega sektorja skupaj z delom zasebnega sektorja imenovati skupne pooblaščene osebe). Pri tem morajo zagotoviti, da je pooblaščena 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 pooblaščene osebe obstaja skrb, da bodo morale pooblaščeno 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 pooblaščeno 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 družb, društva ipd. določijo eno pooblaščeno osebo, ki skrbi za notranje varstvo osebnih podatkov v več subjektih.

Za odvetnike, ki so kot del pravosodja v širšerm smislu samostojni in neodvisni (svobodni) poklic (prvi odstavek 137. člena Ustave Republike Slovenije) je dodan poseben odstavek, po katerem se lahko lahko individualno dogovorijo z Odvetniško zbornico Slovenije, da jim le-ta določi pooblaščeno osebo. Precejšnje število odvetnikov sicer ne izvaja sistematičnih obdelav osebnih podatkov kot njihove temeljne dejavnosti in tako ne bodo potrebovali pooblaščene osebe, kar pa bodo morali samostojno presoditi glede na njihovo dejansko situacijo.

K 48. členu:

48. člen Predloga ZVOP-2 določa naloge pooblaščene osebe za varstvo podatkov. Po prvem odstavku pooblaščena oseba opravlja naloge iz člena 39 Splošne uredbe, zlasti pa glede ocene tveganj obdelav osebnih podatkov v zbirkah. Po drugem odstavku pooblaščena 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 sodiščih[81] (3. člen) in Zakon o državnem tožilstvu[82] (19. člen). Pooblaščena 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 tretjem odstavku določeno, da pooblaščena 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). Pooblaščena oseba sme opravljati te naloge samo glede zadev sodne uprave Ustavnega sodišča (sodna uprava Ustavnega sodišča ter tudi zadeve s področja odločanja upravne seje Ustavnega sodišča) ter glede izvajanja varnosti osebnih podatkov.

Po četrtem odstavku pooblaščena 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 ravnanju[83]). 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). Pooblaščena oseba za varstvo podatkov Varuha človekovih pravic sme opravljati te naloge samo glede zadev obdelav osebnih podatkov s področja zagovorništva 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:

[81] Uradni list RS, št. 94/07 – uradno prečiščeno besedilo, 45/08, 96/09, 86/10 – ZJNepS, 33/11, 75/12 – ZSPDSLS-A, 63/13, 17/15 in 23/17 – ZSSve.
[82] 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.
[83] Uradni list RS, št. 114/06 – Mednarodne pogodbe, št. 20/06.

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 pooblaščeno osebo, ki opravlja naloge v skladu s četrtim odstavkom 48. člena tega zakona. V drugem odstavku je določeno, da mora Vrhovno sodišče Republike Slovenije določiti (le) eno pooblaščeno 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 pooblaščeno osebo, ki opravlja naloge v skladu z drugim odstavkom 48. člena tega zakona za vsa državna tožilstva v Republiki Sloveniji. V četrtem odstavku je določeno, da Varuh človekovih pravic (kot državni organ) določi eno pooblaščeno osebo, ki opravlja naloge v skladu s četrtim odstavkom 48. člena tega zakona.

V petem odstavku je določeno strogo pravilo, po katerem mora vsak minister ali ministrica določiti svojo pooblaščeno 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 Slovenije[84]). Za organe v sestavi ministrstev je določeno, da se lahko določi posebno pooblaščeno osebo, kar bo v praksi verjetno veljalo le za večje organe v sestavi.

Za področja obveščevalno-varnostne dejavnosti je v šestem odstavku določeno, da predstojnik organizacije (Slovenska obveščevalno-varnostna agencija, Obveščevalno varnostna služba Ministrstva za obrambo) s tega področja določi eno pooblaščeno osebo 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.

V sedmem odstavku je podano posebno pooblastilo glede določitve pooblaščenih oseb za *sui generis* del javnega sektorja, ki opravlja državne upravne naloge – za upravne enote. Pooblaščene osebe za njih lahko določi Ministrstvo za javno upravo, več upravnih enot ima lahko določeno skupno pooblaščeno osebo, ki pa mora biti zaposlena v javnem sektorju.

K 50. členu:

Prvi odstavek določa, da morata upravljavec ali obdelovalec pooblaščeni osebi zagotovita pogoje za učinkovito in neodvisno opravljanje njenih nalog po 48. členu ZVOP-2, zlasti, da je pooblaščena 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

[84] 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.

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, podatke iz 13. člena ZVOP-2, 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 pooblaščena oseba pri izvajanju svojih nalog ne prejema nobenih navodil. Pooblaščena 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 pooblaščene osebe za varstvo podatkov zaradi izvajanja njenih nalog ne sme razrešiti, je kaznovati ali je zapostavljati (kar je del jamstva neodvisnosti iz drugega odstavka).

Po četrtem odstavku je odpoved delovnega razmerja pooblaščeni osebi prepovedana za čas njenega določitve in še eno leto po prenehanju določitve, po vzorcu 112. člena 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 2. člen 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 pooblaščena oseba.

Tretji odstavek predlaganega člena določa, da če ima pooblaščena oseba pri svoji dejavnosti vpogled v osebne podatke, v zvezi s katerimi ima oseba, ki je podvržena nadzoru pooblaščene osebe, pravico do molka (kazenski postopek, prekrškovni postopek), ta pravica kot del privilegija zoper samoobtožbo velja tudi za pooblaščeno osebo in za v njenem imenu delujoče osebe, in sicer do mere, v kateri je oseba, ki ima zakonsko pravico do molka, slednjo uveljavila. Gre za smiselni 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 izdaja ustrezni 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 pojavni 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 pooblaščencu 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 52. 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 ne preprečuje, da ne bi mogel Informacijski pooblaščenec razveljaviti uporabe določenega kodeksa, če oceni, da ni oziroma da ni več ustrezen. Navedeno izhaja iz sodbe Sodišča Evropske unije v *primeru Maximillian Schrems* (ozir. ti. *Facebook primer*)[85], 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 odobri 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 četrtem odstavku Informacijski pooblaščenec pripravlja in upravlja seznam pravnomočnih certifikacijskih mehanizmov, ki jih je odobril in ta seznam sprotno objavlja na svoji spletni strani.

K 54. členu:

[85] Sodba SEU, C-362/14, 6. 10.2015.

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 akreditaciji[86] (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 pooblaščeno 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 ni povezan 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. Gre za tehnično izvedbo določb Splošne uredbe (členi 44. do 49.).

K 55. členu:

V predlaganem 55. členu ZVOP-2 so določena splošna pravila za prenos osebnih podatkov v tretjo državo ali mednarodno organizacijo.

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.

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 o ustreznosti varstva osebnih podatkov.

K 58. členu:

V 58. členu so določene dodatne izjeme glede prenosov osebnih podatkov.

[86] Uradni list RS, št. 59/99.

K 59. členu:

Predlagani 59. člen določa posebna pravila glede prenosov osebnih podatkov na podlagi zavezujočih poslovnih pravil ali pogodbenih določil.

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 pooblaščencu[87]. Informacijski pooblaščenec je (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 drugem odstavku določeno, da pri Informacijskem pooblaščencu 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 tretjem 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.

K 61. členu:

V 61. členu ZVOP-2 so določene temeljne pristojnosti Informacijskega pooblaščenca. V prvem odstavku je določeno, da Informacijski pooblaščenec samostojno in neodvisno[88] 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.

[87] Uradni list RS, št. 113/05 in 51/07 – ZUstS-A.
[88] Glejte: Pirc Musar, Nataša, *Neodvisni nadzor in varstvo osebnih podatkov*, Pravna praksa, št. 35/2016, str. 6-10.

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)[89] ali po določbah drugih zakonov, ki določajo njihovo samostojno delovanje (brez posebne odredbe sodnika[90]), nato obdelav osebnih podatkov, izvršenih v okviru opravljanja samostojne državnotožilske funkcije po Zakonu o državnem tožilstvu (vsebine iz 19. člena v zvezi s 3. členom, vendar omejeno – kot je doloočeno v predlagani zakonski določbi, zlasti odredtoočenje na odločanje o kazenskem pregonu in njegovo uveljavljanje, vključno z nastopanjem na sodiščih), obdelav osebnih podatkov, izvršenih v okviru odločanja Ustavnega sodišča Republike Slovenije, kot jih opredeljujejo Zakon o ustavnem 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 zagovorništva otrok ter glede obdelav osebnih podatkov na področjih predkazenskega postopka ali obveščevalno-varnostne dejavnost, 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 posameznikov[91] 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 ter glede identitet virov pri varnostnem preverjanju po določbah Zakona o tajnih podatkih

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 sistem[92] 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 funkcije[93].

---

[89] 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.

[90] Glejte: drugi in zlasti tretji odstavek 6. člena Zakona o izvršbi in zavarovanju (Uradni list RS, št. 3/07 – uradno prečiščeno besedilo, 93/07, 37/08 – ZST-1, 45/08 – ZArbit, 28/09, 51/10, 26/11, 17/13 – odl. US, 45/14 – odl. US, 53/14, 58/14 – odl. US, 54/15 , 76/15 – odl. US in 11/18).

[91] 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 pooblaščena 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.«

[92] Odločba US, št. U-I-42/12, 7. 2. 2013; objava: Uradni list RS, št. 17/13 in OdlUS XX, 1.

[93] 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. …«

Po drugem odstavku je Informacijski pooblaščenec ne glede na prvi odstavek tega člena pristojen za opravljanje inšpekcijskega nadzora z vsemi ostalimi delovnimi področji organov ali funkcionarjev iz prvega odstavka, zlasti 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 »odločevalna« oziroma »oblastvena« 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 izločena področja sodnega delovanja, ki so izločena po prvem odstavku, predlagan kakšen poseben (*sui generis*) nadomestni nadzorni sistem (mehanizem) glede varstva osebnih podatkov (npr. poseben organ pri Sodnem svetu), 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.

Ne glede na navedeno izbrana izločena področja po prvem odstavku ne ostanejo brez zunanjega nadzora glede posegov v človekove pravice in temeljne svoboščine, pa četudi naknadnega (nadzor sodnega odločanja po 24. členu Zakona o varuhu človekovih pravic[94]). Varuh človekovih pravic je namreč po 159. členu Ustave Republike Slovenije ter po 1. členu Zakona o varuhu človekovih pravic poseben ustavni organ, ki na neoblastven in neformalen način izvaja nadzore na vseh[95] področjih človekovih pravic in temeljnih svoboščin.

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 ministrstvom Vlade Republike Slovenije, Državnemu zboru Republike Slovenije ter Državnemu svetu Republike Slovenije, nato organom samoupravnih lokalnih skupnosti, drugim 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. Kadar se vrste obdelav, ki jih ureja predlagani predpis, nanašajo na situacije iz 41. člena ZVOP-2, mora predlagatelj predpisa v okviru posvetovanja Informacijskemu pooblaščencu predložiti tudi oceno učinka iz sedmega odstavka člena 25. člena Splošne uredbe. V drugem odstavku je določeno, da kadar zakon določa, da Informacijski pooblaščenec poda soglasje k predlogu predpisa, se smiselno uporabljajo določbe drugega odstavka. V tretjem 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 četrtem 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).

K 64. členu:

[94] Uradni list RS, št. 69/17 – uradno prečiščeno besedilo.

[95] Glejte: odločba US, št. U-I-327/94, 16.3.1995; objava: Uradni list RS, št. 20/95 in OdlUS IV, 25. Po vsebini to pomeni, da je institucija Varuha človekovih pravic po prvem odstavku 159. člena Ustave pristojna za vsa področja človekovih pravic in temeljnih svoboščin, posebni varuhi človekovih pravic pa le za določena podorčja, vendar to ne odvzame »obsega« nadzora nad vsemi področji, ki po Ustavi pripada Varuhu človekovih pravic (zlasti 2. točka obrazložitve). Odločbo sicer obširno kritizira dr. Trpin, Gorazd, v: *Komentar Ustave Republike Slovenije*, ur.: prof. dr. Šturm, Lovro, Fakulteta za podiplomske državne in evropske študije, Ljubljana, 2002, str. 1082.

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, predstavniki Informacijskega pooblaščenca pa krijejo svoje stroške skupnega nadzora.

Nato sta 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 njihovemu 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, informacijskega pooblaščenca in namestnikov informacijskega pooblaščenca v mejah pristojnosti Informacijskega pooblaščenca (kot državnega nadzornega organa po tem zakonu, Zakonu o Informacijskem pooblaščencu 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, 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 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 zasebnosti[96] (37. člen Ustave Republike Slovenije), prostorske zasebnosti[97] (36. člen Ustave Republike Slovenije) ali v odvetniško zaupnost[98] 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. Bistveno je namreč, da je nadzor Informacijskega pooblaščenca usmerjen (in specializiran) v odkrivanje kršitev s področja podatkovne zasebnosti

[96] 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.
[97] 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.
[98] 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.

(varstvo osebnih podatkov), pri čemer pa lahko trči v druga varovana polja zasebnosti (prostorska – 36. člen Ustave Republike Slovenije[99] in komunikacijska – 37. člen Ustave Republike Slovenije).

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.

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 poučen[100].

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:

[99] Za prisilne ukrepe države, katerih namen ni poseg v prostorsko zasebnost in sta torej relevantna le prvi odstavek in prvi del drugega odstavka 36. člena Ustave Republike Slovenije glejte: odločba US, št. U-I-64/14, 12. 10. 2017, zlasti 16. točka odločbe; objava: Uradni list RS, št. 66/17.
[100] Glejte: odločba US, št. U-I-252/00, 8. 10. 2003, 15. točka; objava: Uradni list RS, št. 105/03 in OdlUS XII, 80,

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-1[101]. 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.

Predlagana je torej ureditev, ki naj bi preprečevala nastanek zlasti slučajnega vzpostavljanja cenzure ozir. spodbujanja samocenzure (svoboda izražanja in svoboda komuniciranja)[102], 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 trgu[103] – sodno odrejeni »*take down*« sistem ter tudi novejša praksa na ravni Evropske unije na področjih razprav o 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

[101] 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.

[102] 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).

[103] Uradni list RS, št. 96/09 – uradno prečiščeno besedilo in 19/15.

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 (2. člen Predloga ZVOP-2) in zagotavljanja pravne varnosti ter enakega obravnavanja (22. člen Ustave Republike Slovenije[104]), člen pa je povezan tudi z 72. členom Predloga ZVOP-2, ki določa sodno (upravnosodno) varstvo zoper takšno odločanje Informacijskega pooblaščenca.

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 neodvisni državni organ za varstvo osebnih podatkov torej ne sme imeti (nad seboj) drugostopenjskega upravnega organa, torej pritožbenega organa[105].

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 o prekrških in po določbah Splošne uredbe. V drugem odstavku je določeno, da če nadzornik pri izvrševanju svojih pristojnosti ugotovi, da obstaja sum storitve kaznivega 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

[104] 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.
[105] Glejte: odločba US, št. P-5/11, 2. 6. 2011; objava: Uradni list RS, št. 52/11.

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 pooblaščencu 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 pooblaščencu, če le-ta pridobi sodno odredbo, predati določene identifikacijske podatke o teh uporabnikih po vsebinskih določbah drugega zakona (Zakon o elektronskem poslovanju na trgu[106]) 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 2013[107]). Takšna sodna odredba temu primerno tudi ne more biti izdana v inšpekcijskem postopku, ampak le v prekškovnem 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:

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 pooblaščencu 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;

[106] Uradni list RS, št. 96/09 – uradno prečiščeno besedilo in 19/15.
[107] Odločba US, št. U-I-40/12, 11. 4. 2013; objava: Uradni list RS, št. 39/13.

5. daje mnenja o skladnosti kodeksov poklicne etike, splošnih pogojih 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.

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 pooblaščencem, 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 arhivih[108], v Zakonu o državni statistiki[109] (kjer bi morda vseeno bilo potrebno urediti področno povezovanje zbirk) ter v Zakonu o raziskovalni in razvojni dejavnosti[110] (ki pa bi ga bilo treba širše spremeniti ozir. dopolniti z vidika urejanja varstva osebnih podatkov).

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 privolitev (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),

[108] Uradni list RS, št. 30/06 in 51/14.
[109] Uradni list RS, št. 45/95 in 9/01.
[110] Uradni list RS, št. 22/06 – uradno prečiščeno besedilo, 61/06 – ZDru-1, 112/07, 9/11 in 57/12 – ZPOP-1A.

- 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 podatki posredujejo v psevdonimizirani obliki, v četrtem odstavku pa so urejeni načini vpogleda.

Peti 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 šestem in sedmem odstavku se elaboratu priloži ocena učinkov, osebne podatke se 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.

Osmi 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 devetem odstavku so določene razumne omejitve pravic posameznikov glede na namene znanstvenega raziskovanja ipd.

V desetem odstavku je določeno, da določbe 79. člena ZVOP-2 ne posegajo v (področne) določbe Zakona o varstvu dokumentarnega in arhivskega gradiva ter arhivih[111],

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

[111] Uradni list RS, št. 30/06 in 51/14.

- 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 arhivih[112] (podobno kot to velja za določbe 79. 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 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 uredbe[113]. Posameznik, na katerega se nanašajo osebni podatki nima pravice zahtevati izvedbe izbrisa v skladu s pravico do pozabe iz člena 17 Splošne uredbe ipd..

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.

[112] Uradni list RS, št. 30/06 in 51/14.
[113] Glejte: Sklep Višjega sodišča v Ljubljani, opr. št. I Cp 490/2000, 11. 4. 2001.

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 Slovenije[114]. 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 pravicah[115]) področje, ki ga je treba nekoliko bolje 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. 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 medijih[116]. Posredno (posledično) pa pokriva predlagani člen tudi področje svobode komuniciranja[117] 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 ali dal na razpolago javnosti (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),

---

[114] 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....«.

[115] 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.

[116] 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.

[117] 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.

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 ocene[118] (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 tožilstvu[119]).

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 pravdnem 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).

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 značaja[120].

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)[121].

Po drugem odstavku za namene uresničevanja javnega interesa na področju sodelovanja javnosti, zagotavljanja transparentnosti dela ali spremljanja njihove prakse, zavezanci iz prvega odstavka po

[118] 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..

[119] 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.

[120] Uradni list RS, št. 51/06 – uradno prečiščeno besedilo, 117/06 – ZDavP-2, 23/14, 50/14, 19/15 – odl. US in 102/15.

[121] Uradni list RS, št. 113/03 – uradno prečiščeno besedilo, 20/06 – ZNOMCMO, 76/08, 108/09, 80/10 – ZUTD in 31/15.

postopku iz Zakona o dostopu do informacij javnega značaja zakona, lahko proaktivno javno objavijo tudi osebni podatki iz dokumentov, 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. To vključuje tudi osebne podatke iz sodb sodišč Republike Slovenije (tudi prve stopnje), kjer bo v praksi najverjetnej izvedena lahko (najbolj) le psevdonimizacija s strani sodstva.

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 in po določbah Zakona o splošnem upravnem postopku[122] (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 države, obrambe države ter izvrševanja kazenskih sankcij. Zakonodajni pristop, da se področje ureja v posebnem delu sistemskega 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 sistemsko raven) urejanja varstva osebnih podatkov po (nekoliko prilagojenih) določbah iz Splošne uredbe. To je tudi pristop predlagatelja ZVOP-2.

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 sistemsko napotilo (ne sistemska 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. Ob tem veljajo tudi določbe

[122] Uradni list RS, št. 24/06 – uradno prečiščeno besedilo, 105/06 – ZUS-1, 126/07, 65/08, 8/10 in 82/13.

drugih delov tega zakona, razen kadar gre za drugačno urejanje – npr. prenosi osebnih podatkov (55.-59. člen Predloga ZVOP-2). V četrtem odstavku je posebej urejeno za področje varnosti države, da se obdelave osebnih podatkov urejajo v področnih zakonih z navedenega področja.

K 86. členu:

V 86. členu so podarjeno določena temeljna načela obdelave osebnih podatkov za področja (namene) iz 85. člena ZVOP-2, na način sistemskega sklica na I. del ZVOP-2.

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 pooblaščena 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 komunikacijah[123].

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), j) in k) (tako določajo zakoni, ki urejajo izvajanje obveščevalnih in protiobveščevalnih dejavnosti države[124]) iz prvega odstavka 12. člena ZVOP-2. Tretji odstavek določa uporabo javno objavljenih podatkov (če posameznik ni javne objave omejil).

K 89. členu:

V 89. členu ZVOP-2 so določene posebne določbe o obdelavi osebnih podatkov za druge namene ter prenos osebnih podatkovObdelava 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 86. člena ZVOP-2.

K 90. členu:

Predlagani 90. člen na splošno ureja prenos, posredovanje ali čezmejna obdelava osebnih podatkov, obdelanih skladno z določbami tega dela, za namen, ki ni naveden v 85. členu tega zakona, in določa, da je taka obdelava dovoljena 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 drugem 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. Nadaljnje razdelave navedenih določb so v 3. poglavju IX. dela ZVOP-2 (od 95. člena dalje).

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

[123] Uradni list RS, št. 109/12, 110/13, 40/14 – ZIN-B, 54/14 – odl. US, 81/15 in 40/17.
[124] 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).

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 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 četrtem 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 pooblaščencu, navesti kontaktne podatke Informacijskega pooblaščenca ter navesti možnosti za uveljavljanju pravice do pravnega sredstva. Po petem 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 šestem 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 (uporabljena splošna formulacija glede na to, da še niso v celoti sprejete odločitve glede ustrezne izvedbe E-IDAS Uredbe). Po sedmem 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 osmem 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 pooblaščene osebe (glede na konkretne okoliščine zadeve ali zahtevka);

3. navedbo namenov, v katere bodo osebni podatki obdelani;

4. obstoj pravice do vložitve prijave pri Informacijskem pooblaščencu 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 informacije iz prvega in drugega odstavka 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 z drugim 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 pooblaščencu in pooblaščeni 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, zakoni, ki urejajo sodne postopke).

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 nezdružljiva 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 pooblaščencu 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.

3. poglavje ureja prenos osebnih podatkov tretjim državam ali mednarodnim organizacijam ter čezmejno obdelavo osebnih podatkov.

K 95. členu:

95. člen ureja 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, preprečevanja pranja denarja in financiranja terorizma, 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;

4. je Evropska komisija sprejela sklep o ustreznosti ali, če tak sklep ne obstaja, so bili predloženi oziroma obstajajo ustrezni ukrepi v smislu 97. člena tega zakona ali je, če ne obstaja sklep o ustreznosti, možno v skladu z 98. 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 tehtnih 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.

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 96. členu:

V 96. 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 že izvedene prenose osebnih podatkov tretji državi, regiji oziroma enemu ali več specifičnim sektorjem v tretji državi oziroma mednarodni organizaciji v skladu s 97. in 98. členom tega zakona, niti ne vpliva na obveznosti iz področnih mednarodnih pogodb.

K 97. členu:

Po 97. 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 4. točko drugega odstavka 95. 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 pooblaščencu.

K 98. členu:

V 98. členu so določene izjeme (glede na člen 38 Direktive), ki urejajo dodatne možnosti prenosa osebnih podatkov, če ne obstajajo podlage po 96. in 97. 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 97. člena tega zakona (obveznost dokumentiranja).

K 99. členu:

Predlagani 99. 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) in mimo običajnih (v prejšnjih členih, v področnih zakonih, mednarodnih pogodbah določenih) pravnih poti – pač po tem členu, kjer gre v bistvu za ti. »tiktakajoča bomba« situacijo (»*ticking bomb situation*«). 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 97. 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. Določba je pojasnilne narave (»lahko«), kar pomeni, da če če je čas da se podatke pošlje po običajni poti in to (le) centralnemu pristojnemu organu druge države, se to izvede (po običajni predpisani poti).

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 100. členu:

Predlagani 100. člen ZVOP-2 ureja pravice in dolžnosti upravljavca na področju neposrednega trženja, kar je posebna zakonska ureditev (področna obdelava v druge namene v zvezi z upravičenimi interesi upravljavca po sicer nejasni in sporno formulirano oziroma interpretirani določbi (f) točke prvega odstavka člena 6 Splošne uredbe[125]) - glede na možnosti iz zadnjega stavka uvodne navedbe št. 47, ki je načeloma opcijska (»Obdelava osebnih podatkov za neposredno trženje se lahko šteje za opravljeno v upravičenem interesu.«). Drugi odstavek primarno izhaja iz koncepta zakonitega opravljanja dejavnosti (določeni osebni podatki so že bili zakonito pridobljeni v okviru kakšne storitve/pogodbe, po privolitvi) ali javnih virov – ti osebni podatki, natančno določeni, se lahko uporabijo za namene neposrednega trženja. Nato je omogočena pridobitev drugih osebnih podatkov na podlagi privolitve ali po drugih zakonskih podlagah (drug zakon, npr. tudi upravičeni interes upravljavca, če je naveden v področnem zakonu). Glede posebnih vrste osebnih podatkov je določeno, da se lahko za namene neposrednega trženja pridobijo le na podlagi izrecne privolitve, ni pa omogočena obdelava 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 (tako se npr. za obdelavo posebnih vrst osebnih podatkov navaja kot pravna podlaga izrecna privolitev in ne pisna privolitev).

Ureditev v besedilu v skladu z navedenimi pravnimi podlagami določa ti. »*soft opt-in*«, izhaja namreč iz primarnega 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 101. členu ZVOP-2.

[125] Glejte: Carey, Peter et. al., *Data Protection : A Practical Guide to UK and EU Law*, Oxford University Press, Oxford, 5th Edition, 2018, str. 57-58.

V predlaganem šestem odstavku je določena prepoved glede uporabe osebnih podatkov s področja neposrednega trženja za področje političnega trženja (volitve, referendumi), pač izrecno določena neskladnost med poslovnim in političnim namenom obdelave osebnih podatkov. Odločitev za takšno rešitev je nasledek najnovejše »afere Deutsche Post«, katera je bila razkrita dne 31. 3. 2018[126]

K 101. členu:

Predlagani 101. 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 102. členu:

S 102. členom se začne posebno (drugo) poglavje X. dela Predloga ZVOP-2, ki velja za področno ureditev (kot da bi bila poseben zakon). Določbe tega poglavja veljajo za uvedbe videonadzora v Sloveniji, razen če kak področni zakon posebej (podrobno) ureja videonadzor, prav tako pa ta področna ureditev pomeni, da videonadzora ni možno uvesti z uporabo sistemskih pravnih podlag za obdelavo osebnih podatkov (8. in 9. člen ZVOP-2)[127],

V 102. členu 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 103. členu:

Predlagani 103. člen določa uporabo videonadzora glede dostopa v uradne službene oziroma poslovne prostore. Gre za vsebino dosedanjega 95. člena ZVOP-1.

K 104. členu:

V 104. 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 ustrezna

[126] Glejte: http://www.dw.com/en/deutsche-post-defends-voter-microtargeting-data-practice/a-43223747 in https://www.tagesschau.de/inland/post-kundendaten-101.html. Deutsche Post naj bi sicer dvema političnima strankama za uporabo za volilno kampanjo za parlamentarne volitve 2017 prodala načeloma anonimizirane/psevdonimizirane osebne podatke – namreč v smislu, da gre za statistično mikro-ciljanje preko »mikro-celic«, kjer se izvede statistično analizo osebnih podatkov na kriterij na stanovanjsko zgradbo s cca 6.6 stanovanjskimi enotami.

[127] Glejte npr.: sodba Upravnega sodišča RS, opr. št. I U 1843/2015, 15. 6. 2017, 11.-13. točka.

pravna ureditev prostorov za čistilke ali čistilce[128]. 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 105. členu:

V predlaganem 105. členu ZVOP-2 je urejen videonadzor glede delovnih prostorov, gre za nekoliko drugačno ureditev glede vstopov v uradne službene oziroma poslovne prostore v 103. 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 v prvem odstavku sedaj omenjeno tudi področje (namen) preprečevanja ali odkrivanja kršitev na področju iger na srečo. Tretji odstavek dodal, da je spremljanje neposrednega dogajanja pred kamerami pod pogoji iz prvega in drugega odstavka 105. člena ZVOP-2 dopustno le, če ga izvaja pooblaščeno varnostno osebje ali drugo posebej pooblaščeno ter ustrezno usposobljeno osebje upravljavca (npr. glede na specifično delovno področje posebej poblaščeni in usposobljeni uslužbenci Arthiva Republike Slovenije). 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 »jamstveni« prispevek k dodatnemu spoštovanju človeškega dostojanstva z uporabo mehanizmov participacije s področja socialne države (2. člen Ustave Republike Slovenije). To pomeni, da delodajalec pridobiva le mnenje sindikata ali drugega predstavnika delavcev, da ne gre za soglasje. Delodajalec po prejetju mnenja v tem postopku posvetovanja[129] dokončno odloči o uvedbi ali neuvedbi videonadzora v delovnih prostorih, gre torej le za obveznost proučitve morebitnih nasprotnih argumentov, ne pa za vezanost na mnenje (posvetovanje namreč vsebinsko ne pomeni zahteve po soglasju).

V sedmem odstavku je na podoben način kot pri videonadzoru in večstanovanjskih stavbah (drugi odstavek 104. člena) določen tudi način uvedbe videonadzora v poslovnih zgradbah, kjer je lahko več lastnikov.

K 106. členu:

V 106. 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 ter objektov, prostorov in oseb, katere varuje policija 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 106. člena ZVOP-2. V tretjem odstavku je podana še pravnoorganizacijska 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.

[128] 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.
[129] Glejte npr.: sodba Vrhovnega sodišča RS, opr. št. VIII Ips 32/2015, 8. 4. 2015, 14. točka.

K 107. členu:

V 107. 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.

107. 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 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 132. členu ZVOP-2.

K 108. členu:

V predlaganem 108. 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 pooblaščencu 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 133. členu ZVOP-2.

K 109. členu:

Predlagani 109. 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 ustrezni prekršek v 134. 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 110. členu:

V 110. 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 135. členu ZVOP-2.

K 111. členu:

V 111. členu je določeno, da se lahko osebni podatki iz javne knjige, urejene z zakonom (npr. zemljiška knjiga), uporabljajo le v skladu z namenom[130], 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 136. členu ZVOP-2.

K 112. členu:

Predlagani 112. člen o povezovanju uradnih evidenc in javnih knjig predstavlja nadaljevanje in v določeni meri tudi nadgradnjo obstoječe ureditve povezovanja zbirk iz 84. člena ZVOP-1. Glavna poteza ureditve tako ostaja enaka kot dosedaj, in sicer, da se omejuje vsako količinsko ozir. kakovostno znatnejše povezovanje uradnih evidenc med sabo ali z zunanjimi evidencami zgolj na tiste

[130] 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.

primere, ko sta to posebej dovolila zakonodajalec oziroma v (najbolj tveganih) primerih tudi informacijski pooblaščenec.

Pri tem se ureditev najbolj tveganih povezovanj ureja nekoliko strožje (zakonodajalec mora izrecno določiti povezovanje kot način prenosa podatkov iz ene zbirke v drugo, zahteva po dovoljenju Informacijskega pooblaščena pa ostaja), ureditev manj tveganih pa blažje (ni več potrebe po obveščanju ali pridobivanju dovoljenja Informacijskega pooblaščenca).

Razlog za tak sorazmerno restriktivni pristop leži v dejstvu, da se v uradnih evidencah oziroma javnih knjigah hranijo uradni podatki o posamezniku, ki se zatorej tudi štejejo za resnične in torej predstavljajo neposredno podlago za odločanje o pravicah, obveznostih in pravnih koristih posameznika. Združevanje podatkov iz več takšnih zbirk ali omogočanje zunanjega dostopa do njih posledično bistveno povečuje tveganja za posege v nakazane pravice, obveznosti ali pravne koristi posameznika. Takšne tvegane situacije lahko nastanejo zlasti, ko so zbirke osebnih podatkov medsebojno tehnološko tako močno povezane, da lahko uporabnik ene od zbirk v svojem informacijskem okolju z enostavno poizvedbo (npr. z vnosom EMŠA) pridobi podrobne osebne podatke o tem posamezniku iz večjega števila medsebojno povezanih zbirk. Primer takšnega posebej obsežnega povezovanja je informacijski sistem eSociala, ki zaradi odločanja o pravicah iz javnih sredstev pridobiva in združuje podatke iz (v danem trenutku) vsaj 44 različnih uradnih evidenc in drugih zbirk osebnih podatkov. Enostavna dostopnost velikega obsega osebnih podatkov pomeni veliko razgaljenost posameznika in s tem veliko moč odločanja o posamezniku, profiliranje njegovega vedenja, ter zlorabe njegovih podatkov (povišana tveganja za notranjo in zunanjo nenamensko uporabo,. okrepljeni motivi za hekerski ali državni vdor v informacijski sistem, tveganja na nepooblaščeno objavo podatkov, idr.). Vse to očitno terja ustrezno stroge varovalke.

Ekstremni primer, ki ga ta ureditev preprečuje, je t.i. »slučajni« nastanek/omogočanje »totalne nadzorovalne družbe«. Pristop izhaja iz francoske »afere SAFARI« iz leta 1974[131], 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, za povezovanje pa bi se uporabila takratna francoska enotna matična številka občana (INSEE koda). Projekt je bil na koncu preklica zavoljo nasprotovanja javnosti oziroma razumevanja, da uvedba takšne totalne družbe nadzora nikakor ne more biti dopustna v razmerah, ki niso izredno ali vojno stanje, pa še takrat da je lahko dopustna le začasno in v skladu z načelom sorazmernosti.

Posebna zakonska ureditev povezovanja osebnih podatkov je določena v Zakonu št. 2472/1997 o varstvu osebnih podatkov Helenske republike. V f) točki 2. člena je določena definicija povezovanja, po kateri »povezovanje pomeni sredstvo za obdelavo, ki vključuje možnost uskladitve podatkov iz ene zbirke osebnih podatkov do osebnih podatkov iz druge zbirke osebnih podatkov ali zbirk osebnih podatkov, katere upravlja drug upravljavec ali upravljavci za drug namen.» 8. člen določa, da v primerih, ko se povezuje zbirke osebnih podatkov z občutljivimi osebnimi podatki ali se uporablja povezovalni znak, da je potrebna odločitev nadzornega organa za varstvo osebnih podatkov Helenske republike glede ustreznosti povezovanja.

Definicija povezovanja je zdaj urejena v samem členu (tretji odstavek), pri čemer je po novem določena tehnološko nevtralno oz. splošno, tako da lahko pokrije različne tehnične načine izvajanja povezovanja zbirk, ki so se pojavila v zadnjih desetih letih. Definicija se namesto na sam način povezovanja osredotoča zlasti na obseg in pogostost povezovanja, ter tveganja, ki pri tem nastajajo. Bistveno vprašanje pri presoji, ali določeno dostopanje do uradne zbirke šteje za povezovanje je, ali zaradi takšne povezave nastanejo znatno večja tveganja za pravice posameznika. Tako je vseeno, ali se povezovanje izvede samodejno oz. brez zahteve uporabnika (npr. da informacijski sistemi medsebojno čez noč posodabljajo 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).

[131] Afero je razkril in kritiziral francoski časopis: Le Monde, Boucher, Philippe, *SAFARI ou la chasse aux Français*, 21. 3. 1974.

Posledice pa so v praksi iste. Prav tako je vseeno, ali se prejeti podatki združijo šele pri uporabniku ali na kakšnem mestu pred njim (primer rešitve ti. »Pladenj«). Prav tako se kot 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. Smiselno eneko velja tudi v primeru, če isti pogodbeni obdelovalec vodi različne zbirke za različne upravljavce. Če te zbirke niso ustrezno ločene, je tudi treba govoriti o povezovanju.

Tako kot dosedaj pa se za povezovanje ne štejejo primeri, ko se pooblaščeni 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 posebej 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.

Za povezovanje z vsebinsko najbolj tveganimi uradnimi evidencami (zlasti: evidence posebnih vrst osebnih podatkov, evidencami premoženjskih in dohodkovnih podatkov) bo moral upravljavec po novem od zakonodajalca dobiti izrecno odobritev, da sme pridobivati podatke s pomočjo povezovanja (torej, ob premisleku tveganj, ki lahko nastopijo zaradi tega) preko sprejetja določb v področnem zakonu (npr. Zakon o sodnem registru).

Ne bo pa več treba pridobiti dovoljenja Informacijskega pooblaščenca (upravna odločba), zadostovalo bo, da upravljavec, ki bi izvedel povezovanje o tem predhodno (rok 30 dni) obvesti Informaicjskega pooblaščenca, ki lahko v tej predhodni fazi oceni, dda je treba izvesti ti. »tematski« (svetovalni) nadzor.

Za povezovanja z manj tveganimi evidencami pa se ohranja le pogoj, da zakon določi možnost pridobivanja podatkov iz te evidence (na kakršenkoli način že), ne določa pa obveznosti notifikacije informacijskega pooblaščenca oziroma pridobivanja njegovega dovoljenja. Navedeno sledi splošni premisi nove ureditve varstva osebnih podatkov (Splošna uredba o varstvu podatkov), da morajo biti ukrepi in postopki varstva osebnih podatkov primerni naravi obdelovanih osebnih podatkov ter tveganjem, ki pri tem nastajajo.

Predlog ZVOP-2 tako po eni strani predvideva, da bodo številna manj tvegana povezovanja po novem bistveno enostavnejša. Za povezovanje s podatki v matičnih registrih (CRP, davčni register, ipd.) tako kljub rabi uradnih povezovalnih znakov več ne bo potrebno ne dovoljenje ne notifikacija Informacijskega pooblaščenca, le še zakonska določba, da sme upravljavec določene zbirke za te in te namene pridobivati tudi te in te podatke iz matičnega registra.

Po drug strani pa predlog ZVOP-2 predvideva, da bodo najbolj tvegana povezovanja dopustna le, če jih bo zakonodajalec izrecno odobril, z besedilom, ki bo jasno kazalo, da dopušča tudi pridobivanje na način in v obsegu, ki predstavlja povezovanje zbirk. V kolikor te izrecne zakonske avtorizacije ne bo, se povezovanje ne bo smelo začeti, že začeta povezovanja pa bo potrebno ustaviti.

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. Navedeno postroženje bo tako nastopilo le postopoma. V vmesnem času bodo lahko bolj tvegana

povezovanja potekajo na istovrstni zakonski podlagi kot manj tvegana (se pravi, zakon mora določati vsaj možnost pridobivanja podatkov iz zadevnih uradnih evidenc), pri čemer pa se še vedno mora pridobiti dovoljenje Informacijskega pooblaščenca (četrti odstavek člena, za katerega prehodno obdobje ne velja). Pri tem se seveda šteje, da obstoječa, že izdana dovoljenja veljajo še naprej, dokler se okoliščine povezovanja bistveno ne spremenijo oziroma jih Informacijski pooblaščenec v postopku nadzora sam ne prekliče. V roku štirih let pa bo potrebno poskrbeti za prilagoditev zakonske podlage, sicer bo lahko nastopila situacija, da bo Informacijski pooblaščenec povezovanje prepovedal.

Zaradi lažjega razumevanja nove ureditve podajamo nekatere primere pridobivanja podatkov iz različnih uradnih zbirk, pri čemer komentiramo, ali gre za posredovanje ali ne, ter po katerem režimu naj poteka.

- eSociala I/O modul in namenski spletni servisi – JE POVEZOVANJE, velja strožja ureditev po prvem odstavku
- eSociala asinhroni modul (uporabnik na center za socialno delo (CSD) prek ISCSD2 sistema in Pladnja posreduje zahtevo bankam, banke gredo po zahtevek 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, velja strožja ureditev po prvem odstavku;
- pridobivanje podatkov zaradi odločanja o vlogah za dodelitev neprofitnih stanovanj po 11.a členu Stanovanjskega zakona – JE POVEZOVANJE, velja strožja ureditev po prvem odstavku, v prehodnem obdobju je potrebno prilagoditi zadevni člen, da bo izrecno dovoljeval povezovanje kot način pridobivanja podatkov;
- 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; zanj velja milejši režim po drugem odstavku;
- aplikacije e-RISK, e-Poizvedbe, eMRVL - dostop do podatkov v registru MRVL – NI POVEZOVANJE, če pa se posamezne evidence povezujejo preko spletnih servisov, npr. prekrškovna evidenca redarskih služb, pa 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; odvisno od podatkov, ki se pridobivajo, velja strožji ali milejši režim;
- 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 odvisno od podatkov, ki se pridobivajo, velja strožji ali milejši režim.

K 113. členu:

V 113. 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 114. členu:

V 114. 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 138. členu ZVOP-2.

K 115. členu:

V 115. členu je določeno obveščanje posameznika in dodatna obdelava osebnih podatkov, kot je to določeno v 89. členu ZVOP-1.

K 116. členu:

V 116. 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 138. členu ZVOP-2.

K 117. členu:

Predlagani 117. člen določa objavo kontaktnih podatkov za potrebe uradnih postopkov, kot je to določeno že v drugem odstavku 106. člena ZVOP-1.

K 118. členu:

V 118. členu se ureja posebna pravna podlaga za organiziranje uradnih dogodkov, samo za javni sektor – namreč kako pridobiti osebne podatke za udeležbo na državnih proslavah in drugih uradnih dogodkih (tudi medijske konference, izdaje raznih knjig ipd.).

V tem primeru ne gre za izvrševanje oblastvenih[132] nalog ali pristojnosti javnega sektorja v smislu odločanja o človekovih pravicah ali temeljnih svoboščinah ali obveznostih, gre ali za uporabo javno dostopnih podatkov ali za podatke, pridobljene ob opravljanju uradnih nalog javnega sektorja ali pa za delovanje ob upoštevanju posameznikove podatkovne samoodločbe, da pač razkrije svoje osebne podatke določenemu krogu ljudi v določenemu 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-poštnih 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.

[132] 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 […].«

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. Predlagana določba torej pomeni neposredno pravno podlago za obdelavo osebnih podatkov v javnem sektorju. Četrti odstavek določa možnost ugovora glede obdelave teh osebnih podatkov (»opt-out« sistem).

11. K XI. delu Predloga ZVOP-2:

K 119. členu:

Predlagani 119. 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 odvračanje 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 120. členu:

V predlaganem 120. 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 121. členu:

V predlaganem 121. 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 122. členu:

V 122. členu so predpisane kršitve (prekrški) glede določb ZVOP-2 o uporabi povezovalnega znaka ter avtomatiziranem odločanju. Predpisane globe so glede na občutljivost varovanih vrednot nekoliko višje, tudi za posameznike – od 200 do 2000 evrov.

K 123. členu:

V 123. členu so predpisani določeni prekrški s področja IX. dela tega zakona, namreč bistvene kršitve glede nezakonite obdelave osebnih podatkov ter nezakonitega dostopanja do njihove vsebine.

K 124. členu:

V 124. členu so določeni prekrški glede kršitve splošnih določb prve področne ureditve po ZVOP-2, namreč določb o neposrednem trženju.

K 125. členu:

V 125. 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 126. členu:

V predlaganem 126. členu so določeni prekrški glede **k**ršitev določb o videonadzoru glede dostopa v uradne službene oziroma poslovne prostore. Tudi v tem primeru so globe razumno (sorazmerno) predpisane.

K 127. členu:

V 127. členu so določeni prekrški glede nove pravne ureditve glede obdelave osebnih podatkov glede organiziranja uradnih dogodkov.

K 128. členu:

V predlaganem 128. 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 126. in 127. členu ZVOP-2, ker se upošteva pomembnejši zasebnopravni kontekst stanovanjskih razmerij.

K 129. členu:

V 129. 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 127. in 128. členu ZVOP-2, ker se upošteva pomembnejši kontekst varstva delavcev v delovnih prostorih.

K 130. členu:

V 130. 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 ti. totalne nadzorovalne države ozir. družbe je višina glob za prekrške nekoliko višja, vseeno pa primerljiva globam po 126. členu ZVOP-2.

K 131. členu:

V predlaganem 131. 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 132. členu:

V predlaganem 132. členu je določen drugi prekršek s področja področne ureditve biometrije. Globe so razumno (sorazmerno) predpisane za kršitve določb glede biometrije v zasebnem sektorju.

K 133. členu:

Predlagani 133. člen določa poseben prekršek glede kršitev določb o prepovedi trženja biometričnih osebnih podatkov v zasebnem sektorju (109. 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 134. členu:

V predlaganem 134. 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 126. in 127. členu ZVOP-2.

K 135. členu:

V predlaganem 135. 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 136. členu:

V predlaganem 136. 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 112. člena ZVOP-2). Globe so glede na kontekst predpisane v nekoliko večji višini (glede na 134. člen).

12. K XII. delu Predloga ZVOP-2:

Predlagani XII. del ZVOP-2 ureja prehodne in končne določbe.

K 137. členu:

V predlaganem 137. členu se urejajo prehodne določbe ZVOP-2, upoštevajoč zlasti načelo pravne varnosti in njegovo »pod-načelo« zaupanja v pravo.

Prvi in drugi 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 Splošni uredbi in določbam tega zakona – 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)[133] dne 19. 2. 2018[134] podala javno pojasnilo - napoved prehodne nadzorovalne politike - v zvezi 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.

Glede predlaganih določb prvega in drugega odstavka 139. 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 začasnih prilagoditvenih izjem in povezane začasne (!) nekaznivosti na drug način, kot to lahko morda določijo ali delujejo 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

[133] 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.
[134] Glejte: https://www.cnil.fr/fr/rgpd-comment-la-cnil-vous-accompagne-dans-cette-periode-transitoire

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«[135], 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 (145. 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 popravljalne 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 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 uskladitev 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.

K 138. členu:

Predlagani člen ureja začasno ureditev glede pooblaščenih oseb za varstvo osebnih podatkov glede vprašanja delovne dobe, izobrazbe ter izkušenj z določenih delovnih področij, poseben položaj za občine ter za vzgojno-izobraževalne zavode ter možnost začasnega (rok devetih mesecev) uresničevanja te obveznosti na drug način. Gre za nov institut in potrebna je prehodna doba.

K 139. členu:

Predlagani člen določa ureditev glede dosedanjih postopkov ali odločanja Informaicjskega pooblaščenca, vključno glede uporabe seznama tretjih držav iz 66. člena Zakona o varstvu osebnih podatkov[136] ter ukinitev Registra zbirk osebnih podatkov pri Informacijskem pooblaščencu,

K 140. členu:

V prvem odstavku 140. člena je določeno prehodno obdobje za izvrševanje petega odstavka 38. člena tega zakona - upravljavci ali obdelovalci, ki za izvajanje svojega delovanja pridobivajo osebne podatke iz registrov ali evidenc s področja upravnih notranjih zadev, morajo v dveh letih od uveljavitve tega zakona vzpostaviti ustrezne varnostne mehanizme, kot jih določi Ministrstvo za notranje zadeve.

Predlagani člen v drugem odstavku določa prehodne določbe glede pridobivanja podatkov iz uradnih evidenc in javnih knjig ter povezovanja – glede na 112. člen ZVOP-2 (štiriletno prehodno obdobje). To pomeni, da imajo upravljavci na razpolago štiri leta, da si v svojem področnem zakonu glede na kriterije iz prvega odstavka 112. člena ZVOP-2 zagotovijo zakonsko ureditev povezovanja. V vmesnem času ostanejo obstoječa povezovanj zakonita.

Konkretno, za primer povezovanja zbirk po 46., 48. in 77. členu Zakona o finančni upravi[137] Finančna uprava Republike Slovenije ne bo več potrebovala odločb Informacijskega pooblaščenca, ampak bo

[135] Ponovno drugi odstavek 120. člena Ustave Republike Slovenije.
[136] Uradni list RS, št. 101/15, 11/17 in 16/17.

(kot upravljavec) le pošiljala obvestila Informacijskemu pooblaščencu o nameravanem povezovanju. Dosedanja povezovanja pa so ohranjena v prej navedeni štirlietni prehopdni dobi, do takrat se po potrebi spremeni navedeni zakon, če bi bila potrebna ddodatna povezovanja (glede na kriterije iz prvega odstavka 112. člena ZVOP-2).

K 141. členu:

Določene so prehodne določbe za uvedbo certificiranja po ZVOP-2 – šele od 1. 1. 2021, saj se izhaja iz dejstva, da je 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 več kot dvoletni rok za začetek delovanja določb o postopkih akreditacije in temu sledi tudi predlagana prehodna določba.

K 142. členu:

Predlagani 142. člen določa prenehanje veljavnosti podzakonskih predpisov, za določene (npr. službene izkaznice ter zaračunavanje) pa določa njihovo začasno uporabo do uveljavitve novih podzakonskih predpisov (katere izda Informacijski pooblaščenec).

K 143. členu:

Predlagani 146. člen določa, da Informacijski pooblaščenec izda pravilnike iz tretjega odstavka 26. člena in drugega odstavka 67. člena ZVOP-2 v roku treh mesecev od uveljavitve tega zakona. Predlagani člen je povezan tudi s 142. členom.

K 144. členu:

Predlagani 144. člen določa prenehanje veljavnosti dosedanjega ZVOP-1 (iz leta 2004, s spremembami do leta 2007[138]).

K 145. členu:

V končni določbi je v 145. členu predlagano, da novi Zakon o varstvu osebnih podatkov (ZVOP-2) začne veljati dne 25. maja 2018.

[137] Uradni list RS, št. 25/14.
[138] Uradni list RS, št. 86/04, 113/05 – ZInfP, 51/07 – ZUstS-A, 67/07 in 94/07 – uradno prečiščeno besedilo.