REPUBLIKA SLOVENIJA
MINISTRSTVO ZA PRAVOSODJE
Župančičeva 3, 1000 Ljubljana

T: (01) 369 5342
F: (01) 369 5783
E: gp.mp@gov.si
www.mp.gov.si

Številka: 007-87/2019
Ljubljana, dne 13.12.2021
EVA 2018-2030-0045

GENERALNI SEKRETARIAT VLADE REPUBLIKE SLOVENIJE
gp.gs@gov.si

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

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, 65/14 in 55/17) je Vlada Republike Slovenije na .....seji.....sprejela naslednji:

SKLEP

Vlada Republike Slovenije je določila besedilo Predloga Zakona o varstvu osebnih podatkov (EVA 2018-2030-0045) in ga pošlje Državnemu zboru v obravnavo.

Mag. Janja Garvas Hočevar
vršilka dolžnosti generalnega sekretarja

Prejmejo:
- Državni zbor Republike Slovenije,
- Vsa ministrstva,
- Informacijski pooblaščenec.

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

/

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

- Marjan DIKAUČIČ, minister za pravosodje,
- Zlatko Ratej, državni sekretar, Ministrstvo za pravosodje,
- mag. Nina Koželj, generalna direktorica Direktorata za kaznovalno pravo in človekove pravice,

Ministrstvo za pravosodje,
- Peter Pavlin, višji sekretar v Direktoratu za kaznovalno pravo in človekove pravice, Ministrstvo za pravosodje,
- Matjaž Mešnjak, podsekretar v Direktoratu za kaznovalno pravo in človekove pravice, Ministrstvo za pravosodje.

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:

- Marjan DIKAUČIČ, minister za pravosodje,
- Zlatko Ratej, državni sekretar, Ministrstvo za pravosodje,
- mag. Nina Koželj, generalna direktorica Direktorata za kaznovalno pravo in človekove pravice, Ministrstvo za pravosodje,
- Peter Pavlin, višji sekretar v Direktoratu za kaznovalno pravo in človekove pravice, Ministrstvo za pravosodje,
- Matjaž Mešnjak, podsekretar v Direktoratu za kaznovalno pravo in človekove pravice, Ministrstvo za pravosodje.

5. Kratek povzetek gradiva:

Predlog Zakona o varstvu osebnih podatkov (ZVOP-2) je pripravljen z namenom zagotovitve izvrševanja 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). Predlog ZVOP-2 določa nadzorni organ za varstvo osebnih podatkov, ki je Informacijski pooblaščenec, kot je bil že do sedaj.

Predlog ZVOP-2 v mejah pooblastilnih klavzul iz Splošne uredbe ureja tudi nacionalne posebnosti varstva osebnih podatkov, ter s tem ohranja dosedanjo visoko raven varstva osebnih podatkov v Republiki Sloveniji ter uresničevanje osebne človekove pravice do varstva osebnih podatkov, predvsem pa upošteva tudi informacijsko - komunikacijski ter tehnološki razvoj na področju obdelav osebnih podatkov. Gre za področja obdelav osebnih podatkov zaradi izvajanja nalog v javnem interesu oziroma javnih oblasti, obdelave nekaterih posebnih vrst osebnih podatkov (obdelava osebnih podatkov o odločitvah o kazenskih obsodbah ter o kaznovanjih za prekrške), osebnih podatkov umrlih oseb, pri videonadzoru, biometriji, obdelave v znanstveno in zgodovinsko raziskovalne ter arhivske namene itd.

Zakon se bo uporabljal za posameznike in posameznice, na katere se nanašajo osebni podatki, ko bodo v zvezi z njimi obdelovani. Posamezniku, na katerega se nanašajo osebni podatki, so dane na razpolago različne možnosti za obrambo ali uresničevanje njunih pravic s področja varstva osebnih podatkov napram upravljavcem, za katere meni, da morda nezakonito ali nepravilno obdelujejo njegove osebne podatke (predlagana ureditev je podobna, kot to velja na področju varstva osebnih podatkov pri obravnavanju kaznivih dejanj)**.**

Zakon velja tako za javni kot zasebni sektor, z nekaterimi posebnostmi za javni sektor. Delno velja tudi za sodstvo, vendar ne za del, ki se nanaša na neodvisno sodno odločanje – sojenje, odločanje o pravnih sredstvih itd.

Posebno poglavje je namenjeno posredovanju osebnih podatkov znotraj javnega sektorja in osebam zasebnega sektorja in ureditvi postopka.

Pooblaščene osebe za varstvo osebnih podatkov, ki že vse od uveljavitve Splošne uredbe o varstvu

podatkov opravljajo svoje naloge neposredno na podlagi omenjene uredbe, na podlagi prehodnih in končnih določb tega zakona nadaljujejo z opravljanjem dela pooblaščene osebe po tem zakonu, tako da ni potrebno ponovno imenovanje. Zakon pa ureja določene posebnosti za pooblaščeno osebo državnega organa, ki mora biti med drugim zaposlena v javnem sektorju, določa tudi možnosti skupne določitve pooblaščene osebe več upravljavcev itd.

Predlog ZVOP-2 določa tudi, 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 predloga zakona (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). V zvezi s prekrški iz Splošne uredbe je v Predlogu ZVOP-2 določena tudi kaznivost odgovornih oseb za prekrške, saj te odgovornosti Splošna uredba ne predpisuje, je pa lahko odgovornost teh gospodarskih subjektov le akcesorna odgovornosti odgovorne osebe.

6. Presoja posledic za:

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

7.a Predstavitev ocene finančnih posledic nad 40.000 EUR:

Za vzpostavitev akreditacijske sheme bo potrebno Slovenski akreditaciji zagotoviti finančna sredstva za vzpostavitev sistema in eno zaposlitev v višini 60.000 EUR v letu 2023 in 40.000 EUR v letu 2024.

Sredstva bodo zagotovljena s prerazporeditvijo s proračunske postavke Ministrstva za pravosodje PP 124110 na proračunsko postavko Ministrstva za gospodarski razvoj in tehnologijo PP 127710 Slovenska akreditacija (ukrep 2111-11-0009 Prost pretok blaga in storitev).

Predlog zakona ne bo imel drugih posledic za Proračun Republike Slovenije, saj je bilo precej predlaganih zakonskih rešitev že do sedaj del pravnega reda Republike Slovenije in jih sedanji predlog zakona le nekoliko nadgrajuje. Dodatna finančna sredstva niso potrebna za okrepitev oziroma dodatno zagotovitev učinkovitega in neoviranega delovanja neodvisnega nadzornega mehanizma (Informacijski pooblaščenec), namreč glede dodatnih kadrov in prostorov, ki zagotavljajo učinkoviti nadzor spoštovanja določb novih pravnih aktov Evropske unije glede varstva osebnih podatkov. Za to potrebne pravice porabe so bile pri Informacijskem pooblaščencu zaradi izvajanja Splošne uredbe o varstvu podatkov zagotovljene že z letoma 2018 in 2019 (dodatne zaposlitve in prostori), tako da ta predlog zakona tudi iz tega vidika nima finančnih posledic za državni proračun.

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	0,00	0,00	0,00	0,00
Predvideno povečanje (+) ali zmanjšanje (–) prihodkov občinskih proračunov	0,00	0,00	0,00	0,00
Predvideno povečanje (+) ali zmanjšanje (–) odhodkov državnega proračuna	0,00	**60.000**	**40.000**	**40.000**
Predvideno povečanje (+) ali zmanjšanje (–) odhodkov občinskih proračunov	0,00	0,00	0,00	0,00
Predvideno povečanje (+) ali zmanjšanje (–) obveznosti za druga javnofinančna sredstva	0,00	0,00	0,00	0,00

I. Finančne posledice za državni proračun

I.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
SKUPAJ			**0,00**	

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
Ministrstvo za pravosodje	**Postopki akreditacije**	**PP 124110**	**0 EUR**	**60.000 EUR**
SKUPAJ				

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

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

OBRAZLOŽITEV:
Ocena finančnih posledic, ki niso načrtovane v sprejetem proračunu
/
Finančne posledice za državni proračun
/

II.a Pravice porabe za izvedbo predlaganih rešitev so zagotovljene:
/
II.b Manjkajoče pravice porabe bodo zagotovljene s prerazporeditvijo:
/
II.c Načrtovana nadomestitev zmanjšanih prihodkov in povečanih odhodkov proračuna:
/

7.b Predstavitev ocene finančnih posledic pod 40.000 EUR:

/

8. Predstavitev sodelovanja z združenji občin:

Predlog ZVOP-2 je bil posredovan v usklajevanje Skupnosti občin Slovenije, Združenju občin Slovenije ter Združenju mestnih občin Slovenije. Pripombe in predlogi so bili prejeti s strani Združenja občin Slovenije ter Združenja mestnih občin Slovenije.

Pripombe **Združenja mestnih občin Slovenije** so se nanašale predvsem na videonadzor na javnih površinah. S tem v zvezi predlagatelj pojasnjuje, da je videonadzor na javnih površinah z namenom varovanja premoženja dopusten. Poleg tega je bil v 79. člen, ki ureja videonadzor na javnih površinah, vključen osmi odstavek, ki posebej ureja videonadzor cestnega prometa, ki ga upravljavec lahko izvaja le v naprej določenih cestnih odsekih, da se ne izvaja sistemsko nadzorovanje gibanja posameznikov in poseganje v zasebnost posameznikov. Upoštevana je tudi pripomba glede terminologije o pouku do pravnega sredstva in glede roka hrambe osebnih podatkov v javnem in zasebnem sektorju (42. člen predloga ZVOP-2).

V zvezi s predlogom Združenja mestnih občin glede uporabe EMŠO kot povezovalnega znaka predlagatelj opozarja na določbo prvega odstavka 41. člena predloga zakona, ki določa uporabo vsaj dveh povezovalnih znakov (npr. EMŠO in osebno ime).

Predloga Združenja mestnih občin Slovenije glede poenostavljenega postopka za odločanje o pravicah posameznikov na podlagi Splošne uredbe, kot je predviden za odločanje o zahtevah za dostop do informacij javnega značaja po Zakonu o dostopu do informacij javnega značaja, predlagatelj ni mogel upoštevati, saj ugotavlja, da državni organi in organi samoupravnih lokalnih skupnosti izpolnjujejo vse pogoje za odločanje po bolj formaliziranem postopku (pooblaščene osebe za vodenje upravnih postopkov), hkrati pa pravic dostopa do informacij javnega značaja ni mogoče primerjati s človekovo pravico do varstva osebnih podatkov, katerih kršitve imajo lahko za posameznika pomembne posledice.

Pripombe Združenja občin Slovenije se med drugim nanašajo na 6. člen predloga ZVOP-2, na t.i. pravne podlage za obdelavo osebnih podatkov. Po oceni predlagatelja je predlagana ureditev v tem delu ustrezna in dovolj določna.

Pripombe k 9. členu, ki ureja posebno varstvo osebnih podatkov umrlih posameznikov so upoštevane, v delu, ki se nanaša na smiselno uporabo določb Splošne uredbe.

Niso bile upoštevane pripombe, ki se nanašajo med drugim na črtanje določb glede obravnave zahtevkov, stroškov seznanitve z osebnimi podatki, češ da vsebino v celoti ureja Splošna uredba in potrebe po dodatni nacionalni ureditvi. Predlagatelj meni, da so določbe potrebne zaradi jasnosti predpisov in njihove uporabe.

Pripomba k 21. členu glede roka hrambe, da se namesto »od zaključka koledarskega leta« doda »od nastanka dogodka« ni bila upoštevana, saj je predlagatelj upošteval tudi pripombe drugih deležnikov, ki so zaradi narave njihovega dela predlagali, da se rok veže na zaključek koledarskega leta, čemur je

predlagatelj sledil. Združenje občin Slovenije predlaga tudi črtanje določb 22. člena, ki se nanaša na varnost osebnih podatkov na področju posebnih obdelav, ker meni, da je v nasprotju s Splošno uredbo. Pripomba je bila deloma upoštevana, besedilo je bilo deloma spremenjeno. Predlagatelj ni sledil pripombi k 29. členu predloga zakona, saj meni, da je posamezniku potrebno dati možnost, da se obrne neposredno na nadzorni organ in zahteva nadzor zakonitosti obdelave njegovih osebnih podatkov.	
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: **DA** Predlogi in pripombe združenj, ki so oziroma niso bili upoštevani so podrobneje navedeni zgoraj.	
9. Predstavitev sodelovanja javnosti:	
Gradivo je bilo predhodno objavljeno na spletni strani e-Demokracija.	**DA**
Datum objave: 30. 4. 2021 Javna razprava je potekala že v letu 2019, bilo je več krogov strokovnega in medresorskega usklajevanja, zadnji maja 2021. Predlog ZVOP-2 (EVA 2018-2030-0045) je bil poslan v strokovno in medresorsko usklajevanje 30. 4. 2021, prav tako je bil 30. 4. 2021 objavljen na spletnem portalu e-Demokracija. Rok za podajo pripomb je bil 31. 5. 2021. K podaji pripomb so bili pozvani: – Informacijski pooblaščenec, – Varuh človekovih pravic, – Vrhovno sodišče RS, – Upravno sodišče RS, – Vrhovno državno tožilstvo RS, – Državnotožilski svet, – Sodni svet, – Ekonomsko-socialni svet, – Odvetniška zbornica, – Notarska zbornica, – Banka Slovenije, – Združenje bank Slovenije, – Računsko sodišče RS, – Zagovornik načela enakosti, – Arhiv RS,	

– Slovenska akademija znanosti in umetnosti, – Center za informiranje sodelovanje in razvoj nevladnih organizacij – CNVOS, – Slovenska akreditacija, – SI-CERT, – Skupnost občin Slovenije, – Združenje občin Slovenije, – Združenje Mestnih občin Slovenija, – Univerza v Ljubljani, – Univerza v Mariboru, – Univerza v Novi Gorici, – Pravna fakulteta Univerze v Ljubljani, – Pravna fakulteta Univerze v Mariboru, – Evropska pravna fakulteta v Novi Gorici, – Fakulteta za varnostne vede Univerze v Mariboru, – Inštitut za kriminologijo pri Pravni fakulteti Univerze v Ljubljani, – Gospodarska zbornica Slovenije, – Obrtna zbornica Slovenije, – Trgovinska zbornica Slovenije, – Detektivska zbornica Slovenije, – Zdravniška zbornica Slovenije, – Zbornica za razvoj zasebnega varovanja Slovenije, – Ameriška gospodarska zbornica, – Združenje delodajalcev Slovenije, – Združenje Manager, – Sekcija operaterjev elektronskih komunikacij. Svoje pripombe so v sklopu strokovnega usklajevanja podali naslednji subjekti: zainteresirani državljani prek eDemokracije, Okrožno sodišče v Ljubljani, Varuh človekovih pravic, Notarska zbornica, Zavod za zdravstveno zavarovanje, Banka Slovenije, AJPES, Združenje mestnih občin Slovenije, Združenje delodajalcev obrti in podjetnikov Slovenije GIZ, Vrhovno sodišče RS, Združenje bank Slovenije GIZ, Slovenska akreditacija, GDPR PLUS, d.o.o., Inštitut za kriminologijo pri Pravni fakulteti v Ljubljani, Zagovornik načela enakosti, ARNES, Infocenter, Sodni svet RS, Univerza v Ljubljani, Detektivska zbornica Slovenije, Združenje delodajalcev Slovenije, Odvetniška zbornica Slovenije, Združenje družb za upravljanje investicijskih skladov GIZ, Slovensko zavarovalno združenje, Informacijski pooblaščenec, Zdravniška zbornica Slovenije, AmCham Slovenija, Upravno sodišče, Obrtno-podjetniška zbornica Slovenije, Združenje občin Slovenije, Vrhovno državno tožilstvo, Statistični urad RS, Univerza v Mariboru, Društvo revmatikov Slovenije, Trgovinska zbornica Slovenije, Gospodarska zbornica Slovenije, Microsoft Slovenija d.o.o., Piratska stranka Slovenije, CNVOS, Slovensko združenje za elektronsko identifikacijo in elektronske storitve zaupanja – EIDES, GEN-I, d.o.o., Konfederacija Sindikatov Slovenije PERGAM, SETCCE tehnološki park. Podrobnejši povzetek usklajevanja z navedenimi deležniki je predstavljen v točki 7. vladnega gradiva – prikaz sodelovanja javnosti pri pripravi predloga zakona.	
10. Pri pripravi gradiva so bile upoštevane zahteve iz Resolucije o normativni dejavnosti:	**DA**

11. Gradivo je uvrščeno v delovni program vlade:	DA
Marjan Dikaučič **minister**	

Priloge:

- predlog sklepa Vlade RS,
- predlog zakona.

Datum:
Številka:

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, 65/14 in 55/17) je Vlada Republike Slovenije na .....seji.....sprejela naslednji

SKLEP

Vlada Republike Slovenije je določila besedilo Predloga Zakona o varstvu osebnih podatkov (EVA 2018-2030-0045) in ga pošlje Državnemu zboru v obravnavo.

Mag. Janja Garvas Hočevar
vršilka dolžnosti generalnega sekretarja

Prejmejo:

- Državni zbor Republike Slovenije,
- Vsa ministrstva,
- Informacijski pooblaščenec.

PRILOGA 3

PREDLOG
EVA: 2018-2030-0045

PREDLOG ZAKONA O VARSTVU OSEBNIH PODATKOV (ZVOP-2)

I. UVOD

1. OCENA STANJA IN RAZLOGI ZA SPREJEM PREDLOGA ZAKONA

Predlog zakona 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 do sedaj že tretji slovenski Zakon o varstvu osebnih podatkov (ZVOP-1)[1], je namreč zaradi izjemnega razvoja informacijsko-komunikacijske tehnologije (IKT) prišlo do bistvenega povečanja v količini in tudi kakovosti obdelave osebnih podatkov, prav tako pa do znatnega razvoja sodne prakse in nadzorov glede varstva osebnih podatkov, povečala se je pa tudi splošna občutljivost javnosti glede informacijske zasebnosti. Osebni podatki so tako postali vedno bolj dostopni najprej državi in njenim organom, nato pa tudi zasebnemu sektorju, javnosti, ter posameznikom in posameznicam. Obdelava osebnih podatkov je postala del velike večine poslovnih procesov. Izvajati so se začele vedno bolj sistemske povezave med zbirkami osebnih podatkov. S tem so se tveganja zlorabe osebnih podatkov, kot so nepooblaščeni dostopi, množična razkritja, ter nedovoljeno profiliranje posameznikov, močno povečala.

V odziv na te nove trende sta se najprej začela razvijati dodatna in okrepljena sodna praksa Sodišča Evropske unije in Evropskega sodišča za človekove pravice glede varstva osebnih podatkov, pri nas pa praksa Ustavnega sodišča Republike Slovenije, sčasoma pa je začelo prihajati tudi do sprememb na zakonodajnem področju. Tako je leta 2012 Evropska komisija predlagala sprejetje dveh novih pravnih aktov Evropske unije kot del t. i. »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, znana tudi po angleški kratici »GDPR«)«[2], ki naj bi moderniziral pravno ureditev obdelave osebnih podatkov na splošno, 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], ki naj bi isto storil še za t. i. policijske oziroma kazensko pravosodne in podobne obdelave.

[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).

Zakonodajni pristop Evropske komisije je izhajal zlasti iz naslednjega sistemskega vidika: »Hiter tehnološki razvoj in globalizacija sta prinesla nove izzive za varstvo osebnih podatkov. Obseg zbiranja in izmenjave osebnih podatkov se je bistveno povečal. Tehnologija zasebnim podjetjem in javnim organom omogoča, da osebne podatke uporabljajo za dosego svojih ciljev v obsegu, kakršnega še ni bilo. Posamezniki vedno bolj dajejo osebne podatke na razpolago tako javno kot globalno. Tehnologija je spremenila tako gospodarstvo kot družbeno življenje ter bi morala še naprej omogočati lažje izvajanje prostega pretoka osebnih podatkov v Uniji ter prenosa v tretje države in mednarodne organizacije, pri čemer je treba zagotoviti visoko raven varstva osebnih podatkov.« (iz uvodne navedbe št. 6 Splošne uredbe o varstvu podatkov).

Istočasno se je na ravni Sveta Evrope začela pripravljati reforma prava osebnih podatkov Sveta Evrope, tj. Konvencije o varstvu posameznikov glede na avtomatsko obdelavo osebnih podatkov (Konvencija št. 108, spremenjena s Protokolom CETS št. 223)[4]. Določbe Konvencije so primerljive z določbami Splošne uredbe o varstvu podatkov, pri čemer pa so bolj splošne, posebej poudarjajo načelo zakonitosti, nekoliko drugače urejajo prenose osebnih podatkov v tretje države, za nadzor vzpostavljajo posebni konvencijski odbor, ipd. Priprava Protokola h konvenciji (CETS št. 223) se je začela leta 2011 in je trajala do maja 2018. Republika Slovenija je Protokol podpisala 16. maja 2019, tako da so njegove novosti že vključene v besedilu tega predloga.

1.1 Ocena stanja

V času vložitve predlogov navedenih pravnih aktov na ravni Evropske unije je imela Republika Slovenija sistem varstva osebnih podatkov urejen v skladu z določbami 38. člena Ustave Republike Slovenije[5] iz leta 1991, Direktive 95/46/ES[6] iz leta 1995, Okvirnega sklepa 2008/977/PNZ[7] iz leta 2008 in Konvencije o varstvu posameznikov glede na avtomatsko obdelavo osebnih podatkov[8] (Sveta Evrope) iz leta 1981.

Republika Slovenija je v obdobju od leta 2012 do začetka leta 2016 glede predlagane Splošne uredbe o varstvu podatkov in povezane Direktive iz načelnih sistemskih razlogov navedenima predlogoma pravnih aktov Evropske unije pretežno ali v celoti nasprotovala[9], ob tem pa navedla tudi vrsto posebej obrazloženih pridržkov. Razlogi nasprotovanja oz. kritike so bili opozarjanje na poslabšano pravno varnost, možnost znižanja dosežene visoke ravni varstva osebnih podatkov, pretirane obveznosti za upravljavce osebnih podatkov in obdelovalce – tudi finančne, očitno pretirane globe za upravne kršitve določb Splošne uredbe o varstvu podatkov, nato pretirana pooblastila Evropski komisiji glede izdaje izvedbenih in delegiranih aktov, določeni ustavnopravni vidiki, izbira vrste pravnega akta v primeru predloga Splošne uredbe, ustreznost takratnega Okvirnega sklepa 2008/977/PNZ in torej nepotrebnost sprejetja predlagane Direktive ipd.

Glede takratnega Predloga Splošne uredbe o varstvu podatkov je bil bistveni zaključek iz stališča Republike Slovenije – poleg prej navedene 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

[4] Zakon o ratifikaciji konvencije o varstvu posameznikov glede na avtomatsko obdelavo osebnih podatkov (Uradni list RS – Mednarodne pogodbe, št. 3/94 in Uradni list RS, št. 86/04 – ZVOP-1).

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

[6] 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.

[7] 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.

[8] 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.

[9] 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.

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 ob začetku njenega zakonodajnega obravnavanja pojavili ustavnopravni pomisleki tudi v Zvezni republiki Nemčiji, tako je leta 2012 nemški zvezni ustavni sodnik Johannes Masing objavil članek[10], 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)«[11] – 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«[12] – v nadaljnjem besedilu: Direktiva.

Z vidika končnega rezultata je možno oceniti, da določbe v Splošni uredbi o obdelavi osebnih podatkov na podlagi zakonitih interesov, naknadni obdelavi osebnih podatkov v druge namene ter o pooblaščenih osebah, zlasti s ciljem unifikacije režimov varstva osebnih podatkov v posameznih državah članicah, morda pomenijo določeno stopnjo znižanja dosežene ravni varstva osebnih podatkov. Da bi se ta trend neutemeljenega zniževanja standardov varstva osebnih podatkov v čim večji meri ublažilo, se je predlagatelj odločil v najvišji možni meri nasloniti na t. i. pooblastilne klavzule (»*opening clauses*«) – zlasti v uvodnih navedbah, ki državam članicam Evropske unije glede določenih vprašanj omogočajo ohranitev njihove nacionalne ureditve (npr. glede pogojev obdelave osebnih podatkov zaradi izvajanja nalog v javnem interesu oziroma javnih oblasti, obdelave nekaterih posebnih vrst osebnih podatkov oziroma njim podobnih osebnih podatkov, osebnih podatkov umrlih oseb, ali obdelav v znanstvenoraziskovalne, zgodovinskoraziskovalne, statistične oz. arhivske namene in druge). Te klavzule dajejo Splošni uredbi o varstvu osebnih podatkov v določenem delu značaj t. i. »direktivnega akta«[13], kot da bi bila direktiva Evropske unije, zlasti z vidika možnosti nacionalnega zakonodajnega (področnega) urejanja. Kar pomeni, da je možno nekatere določbe Splošne uredbe implementirati v slovenskih zakonih, z ozirom na konkretne okoliščine stanja ali razvoja varstva osebnih podatkov v Sloveniji.

---

[10] 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.

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

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

[13] 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.

1.2 Razlogi za sprejem zakona

Zaradi Splošne uredbe oz. prenovljene Konvencije Sveta Evrope so potrebne spremembe zakonodaje Republike Slovenije, torej zlasti sprejetje novega Zakona o varstvu osebnih podatkov kot sistemskega zakona Republike Slovenije za področje varstva osebnih podatkov. Drugi del reforme varstva osebnih podatkov, namreč zakonodajna izvedba Direktive, je že bil izveden v Zakonu o varstvu osebnih podatkov na področju obravnavanja kaznivih dejanj (ZVOPOKD)[14], ki je začel veljati dne 31. 12. 2020.

Po sprejetju predloga Zakona o varstvu osebnih podatkov (ZVOP-2), bo področje varstva osebnih podatkov v Republiki Sloveniji sistemsko urejeno na način, da bo imelo tri centralne predpise: ZVOP-2, Splošno uredbo (določbe, ki se neposredno uporabljajo) in ZVOPOKD. Poleg njih bodo tudi področni zakoni urejali konkretne obdelave osebnih podatkov in načine njihovega varstva.

Razmejitev med Predlogom ZVOP-2 in ZVOPOKD je naslednja:

ZVOPOKD je t. i. Direktivni zakon, ki se ukvarja z obdelavami osebnih podatkov v zvezi s kaznivimi dejanji, Splošna uredba, kateri je namenjen ZVOP-2 kot pretežno izvedbeni zakon, pa drugimi obdelavami osebnih podatkov v zasebnem in javnem sektorju. ZVOP-2 je ob tem tudi sistemski zakon, ki ureja določena vprašanja za vse sisteme obdelav osebnih podatkov v Republiki Sloveniji, razen če ZVOPOKD to ureja drugače oz. samostojno ureja.

Ob upoštevanju določb Splošne uredbe je bilo pripravljeno besedilo predloga novega Zakona o varstvu osebnih podatkov, ki 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[15], ob upoštevanju obstoječe ustavnosodne presoje Ustavnega sodišča Republike Slovenije glede človekove pravice do varstva osebnih podatkov od leta 1992[16] dalje ter tudi določb še veljavne Konvencije o varstvu posameznikov glede na avtomatsko obdelavo osebnih podatkov – Konvencija št. 108.

Koncept zakona je v obdobju 2017-2018 ter v prvem krogu medresorskega in strokovnega usklajevanja v letu 2019 vključeval širšo vsebino, vseboval je namreč precej povezovalnih ali dopolnjevalnih določb v zvezi s Splošno uredbo.

Glede na pripombe iz prvega kroga medresorskega in strokovnega usklajevanja v letu 2019 je koncept zakona sedaj spremenjen na način, da se v njem urejajo vprašanja, ki so potrebna zaradi izvrševanja Splošne uredbe, nato postopkovna in druga vprašanja, ki jih je treba urediti na podlagi zahtev iz Splošne uredbe, določene povezovalne določbe s Splošno uredbo ter nacionalne posebnosti ipd.

Predlog zakona še vedno sledi pristopu, da naj bo čim več rešitev na enem mestu, nima pa sistematika predloga zakona več značaja t. i. »zakonika«, saj upošteva neposredno uporabnost Splošne uredbe ter njene razlage, kot so se že razvile v praksi od leta 2018 dalje.

2. CILJI, NAČELA IN POGLAVITNE REŠITVE PREDLOGA ZAKONA

2.1 Cilji

Cilji predloga zakona so:

[14] Uradni list RS, št. 177/20.

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

[16] 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.

- zagotoviti izvrševanje določb Splošne uredbe, tako da se v mejah pooblastitvenih klavzul iz Splošne uredbe določi nacionalne posebnosti ureditve varstva osebnih podatkov, ter s tem v čim večji meri ohrani dosedanja visoka raven varstva osebnih podatkov v Republiki Sloveniji ter uresničevanje osebne človekove pravice do varstva osebnih podatkov (38. člen Ustave Republike Slovenije)[17];
- zagotoviti zakonitost obdelave osebnih podatkov na sistemski ravni (38., 87. in 120. člen Ustave Republike Slovenije);
- zagotoviti učinkoviti nadzor glede varstva osebnih podatkov (38. člen Ustave Republike Slovenije);
- zagotoviti učinkovito prekrškovno kaznovanje glede kršitev varstva osebnih podatkov;
- zagotoviti nadaljnji razvoj področnih ureditev obdelave osebnih podatkov v sistemskem zakonu (npr. videonadzor na javnih površinah, prenovljeni sistemski pristop glede biometrije…).

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

Pri zakonodajni izvedbi določb Splošne uredbe se izhaja predvsem iz upoštevanja pooblastitvenih klavzul Splošne uredbe (tako določb členov kot tudi uvodnih navedb), ki določajo možnosti nacionalnih zakonskih urejanj v razmerju do sicer enotne uredbene ureditve varstva osebnih podatkov. Splošna uredba tako npr. v uvodni navedbi 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.«, v drugem odstavku člena 6 Splošne uredbe pa 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«. Še dalje pa posamezni členi Splošne uredbe določajo področja, kjer države članice niso uspele dogovoriti ali pa ne morejo vzpostaviti enotnih ali skupnih pravil varstva osebnih podatkov, in so zato ureditev teh področij prepustile nacionalni zakonodaji:

- pogoji za obdelavo osebnih podatkov v okviru dejavnosti zunaj področja uporabe prava Evropske unije ter obdelavo osebnih podatkov s strani Republike Slovenije, kadar deluje na področjih skupne varnostne in obrambne politike ter obveščevalno-varnostne dejavnosti (drugi odstavek člena 2 Splošne uredbe);
- pogoji za zagotovitev zakonitosti obdelave, ko gre za obdelave zaradi izpolnitve zakonske obveznosti oziroma izvajanja nalog v javnem interesu ali izvajanja javne oblasti, podeljene upravljavcu (drugi odstavek člena 6 Splošne uredbe);

[17] Gre za načelen in sistemski pristop Republike Slovenije, ki v obdobju zadnjih približno 9 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 in 2015 v postopku pred Sodiščem Evropske unije 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.: https://www.theguardian.com/technology/2016/jul/08/privacy-shield-data-transfer-us-european-union) ter tudi glede garantistične in podrobnejše vsebine določenih bilateralnih mednarodnih pogodb Republike Slovenije (npr. s področja policijskega in pravosodnega sodelovanja).

- pogoji za preverjanje privolitve mladoletnih oseb v rabo storitev informacijske družbe (prvi odstavek člena 8 Splošne uredbe);

- pogoji za obdelavo osebnih podatkov umrlih oseb (uvodna navedba št. 27 k Splošni uredbi);

- pogoji za obdelave genskih podatkov, biometričnih ter zdravstvenih osebnih podatkov (drugi odstavek člena 9. Splošne uredbe);

- pogoji za obdelavo osebnih podatkov v kazenskih in prekrškovnih evidencah (člen 10 Splošne uredbe);

- obveznost izbrisa osebnih podatkov po poteku določenega roka (točka e) prvega odstavka člena 17 Splošne uredbe) oziroma obveznost hrambe osebnih podatkov za določen rok (točki b) in e) tretjega odstavka člena 17 Splošne uredbe);

- obveznost priprave ocene učinkov oziroma izvedbe predhodnega usklajevanja z državnim nadzornim organom pri pripravi zakonodajnih predlogov (peti odstavek člena 36 Splošne uredbe);

- pogoji za obvezno imenovanje pooblaščene osebe za varstvo osebnih podatkov, ter nalog pooblaščenih oseb (četrti odstavek člena 37 Splošne uredbe ter prvi odstavek člena 39 Splošne uredbe);

- pooblastila državnega nadzornega organa za varstvo osebnih podatkov (prvi in šesti odstavek člena 58 Splošne uredbe);

- določitev ter postopek za izrekanje prekrškov zaradi kršitev določb Splošne uredbe (prvi odstavek člena 84 Splošne uredbe).

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

Predlog ZVOP-2 ureja tudi nekatera vprašanja, ki jih Splošna uredba prepušča nacionalni zakonodaji (obdelava osebnih podatkov umrlih oseb, obdelava osebnih podatkov v okviru dejavnosti zunaj področja uporabe prava Evropske unije, obdelava osebnih podatkov, s strani Republike Slovenije, kadar deluje na področjih skupne varnostne in obrambne politike ter obveščevalno-varnostne dejavnosti). Ker je imela Republika Slovenije že od leta 1990 sicer celovit (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 sistemskih posegov v tajnost osebnih podatkov 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 ipd.

Glede na pretekle pobude predstavnikov gospodarstva ter združenja pooblaščenih oseb za varstvo osebnih podatkov, se upošteva tudi dejstvo, da se Splošna uredba neposredno uporablja že več kot tri leta, ter da zato načeloma ni potrebno popolno podrobno urejanje institucije pooblaščenih oseb in da morajo biti odstopanja od Splošne uredbe omejena zgolj na področja, kjer je to resnično potrebno za ohranitev visoke ravni varstva osebnih podatkov.

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 edina možnost, da se pripravi nov Zakon o varstvu osebnih podatkov, ki bi omogočal povezan in čimbolj koherenten pristop glede vseh teh vsebin in njihovih zahtev. Teh vsebin in zahtev ne bi bilo možno doseči le z novelo veljavnega ZVOP-1.

2.3. O zakonodajni tehniki predloga zakona

Uporabljena je kombinacija več zakonodajnih tehnik:

1. tehnika indikacije (sklica), npr. na pravne podlage iz Splošne uredbe;
2. tehnika določanja posebnosti – pri pooblastilnih klavzulah;
3. tehnika razčlenitve – npr. postopka z zahtevki posameznika;
4. tehnika uporabe določb drugega predpisa – npr. določb glede dnevnika obdelave iz Direktive.

Navedena kombinacija je bila izbrana s ciljem, da se zagotovi spoštovanje pravne varnosti zaradi učinkovitega uresničevanja osebne človekove pravice do varstva osebnih podatkov.

2.4. Načela predloga zakona

Načelo spoštovanja osebnosti in pravic človeka

Prvo vodilno načelo novega predloga zakona 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 v varstvo osebnih podatkov na človeka kot subjekta ter opraviti oceno z vidika spoštovanja strogega načela sorazmernosti.

Načelo zakonitosti

Načelo zakonitosti v predlogu zakona 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 uvodne navedbe št. 39 Splošne uredbe, a) točke prvega odstavka 5. člena Splošne uredbe, prvega, drugega in tretjega odstavka 6. člena Splošne uredbe, a) točke prvega odstavka 4. člena Direktive, 8. člena Direktive in a. točke 5. člena Konvencije. Ob tem je pomembno, da drugi stavek uvodne navedbe št. 45 Splošne uredbe navaja (ne pa prepoveduje) da »Ta uredba ne zahteva posebnega zakona za vsako posamezno obdelavo.« To pomeni da lahko države članice Evropske unije glede na svojo nacionalno (zlasti ustavno) ureditev vseeno določijo vsaj splošne pravne podlage za določene vrste obdelav konkretnih osebnih podatkov v sistemskem ali v področnih zakonih, ne pomeni pa za Republiko Slovenijo, da se lahko konkretne obdelave konkretnih osebnih podatkov določa v podzakonskih predpisih (kar je nedopustno po ustaljeni ustavnosodni presoji Ustavnega sodišča Republike Slovenije od leta 1992 dalje[18]). Temu pristopu sledi tudi 6. člen predloga. Za delovanje

[18] Odločba US, št. U-I-115/92, 24. 12. 1992; objava: Uradni list RS, št. 3/93 in OdlUS I, 105. Sedaj je relevantna tudi odločba Ustavnega sodišča RS iz leta 2019 o načelu upravne zakonitosti (drugi odstavek 120. člena Ustave Republike Slovenije: »Upravni organi opravljajo svoje delo samostojno v okviru in na podlagi ustave in zakonov.«), št. U-I-26/17,

(odločanje, poseganje v pravice, določanje obveznosti) s strani javnega sektorja (javne oblasti) velja načelo zakonitosti, za zasebni sektor pa je to načelo nekoliko omiljeno v smislu, da lahko splošne določbe Splošne uredbe ter predloga zakona 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 6. člena Splošne uredbe.

Načelo sorazmernosti

Pri izvajanju posegov v pravico do varstva osebnih podatkov oziroma odločanja za obdelavo osebnih podatkov je treba izhajati iz načela sorazmernosti iz b) in c) točke prvega odstavka 5. člena Splošne uredbe ter 2. člena v zvezi s tretjim odstavkom 15. člena Ustave Republike Slovenije, izvedbeno pa je treba nato izhajati iz ustavnosodne presoje Ustavnega sodišča Republike Slovenije - z uporabo strogega testa sorazmernosti (predvsem odločba US, št. U-I-60/03, 4. 12. 2003[19], zlasti 30. točka v zvezi s 17. točko odločbe).

Načelo namenske obdelave osebnih podatkov

Določbe predloga zakona o namenski obdelavi osebnih podatkov (6. člena Predloga ZVOP-2) 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 ali Splošni uredbi 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 zakona (7. člen Predloga ZVOP-2) delno omejen (relativiziran) saj morajo glede na določbe četrtega odstavka 6. člena Splošne uredbe biti omogočene tudi obdelave osebnih podatkov v druge namene. Tovrsten pristop omogočajo tudi določbe tretjega odstavka 15. člena Ustave Republike Slovenije o omejitvah človekovih pravic s pravicami drugih oseb. Vendar pa je ta odstop dosledno uveljavljen le na področju, kjer je Splošna uredba primarna, torej glede obdelav za zasebne namene – in še tam ima ta rešitev zakonsko podlago (6. člen Splošne uredbe), medtem ko je za obdelave zaradi izvrševanja javnega interesa in javne oblasti - izrecno določilo, da lahko to določa le (področni) zakon.

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

Za morebitne represivne posege države v človekove pravice ali temeljne svoboščine in interese še vedno velja načelo »prepovedano je vse, kar ni izrecno dovoljeno«[20], torej – da mora država za vsak poseg imeti izrecno dovoljenje (pooblastilo) v zakonu. Za posege s strani zasebnega sektorja pa navedeno načelo velja le omejeno v skladu z določbami predloga zakona (npr. prepovedi prodaje osebnih podatkov v določenih primerih) in točkami (a), (b) (d) in (f) prvega odstavka 6. člena Splošne uredbe.

2.5. Poglavitne rešitve

U-I-87/16, U-I-105/16, 24. 10. 2019; objava: Uradni list RS, št. 67/19, kjer je navedeno: »50. Po drugi strani splošnih aktov za izvrševanje javnih pooblastil (kot je tudi Metodologija), ki dopolnjujejo in podrobneje izpeljujejo zakonsko določbo, ni mogoče razumeti kot dejavnik, ki bi omogočal do zakonodajalca blažje razumevanje zahtev načela jasnosti in pomenske določljivosti zakonov. Nasprotno stališče bi ogrozilo zagotavljanje jamstev drugega odstavka 120. člena Ustave. Ni ustavno sprejemljivo, da bi se nerazumljivost in nejasnost zakonov (glede materije, ki mora po Ustavi biti zakonsko urejena) odpravljalo z jasnimi in razumljivimi podzakonskimi akti.«

[19] Objava: Uradni list RS, št. 131/03 in OdlUS XII, 93.

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

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 zakona 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. členu v zvezi s tretjim odstavkom 15. člena Ustave Republike Slovenije. Glede načela poštenosti (v zvezi z načelom preglednosti) pa predlog zakona sledi dosedanjim dosežkom pravne ureditve Republike Slovenije (obligacijsko pravo, pravo dostopa do informacij javnega značaja), ustavnosodne presoje (sicer s področja prikritih preiskovalnih ukrepov po Zakonu o kazenskem postopku) in sodne prakse (zlasti civilnopravne).

Na novo so razdelane obdelave v zvezi s posebnimi vrstami osebnih podatkov (do sedaj: 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 s področja posebnih vrst osebnih podatkov uporabljajo tudi za njih.

Določena je nova ureditev glede drugih (do sedaj: 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 (zakonitosti, poštenosti, sorazmernosti) sta kot obveznost za upravljavce in obdelovalce poleg izvedbe ocene učinka določena tudi ukrepa t. i. notranje sledljivosti posredovanj osebnih podatkov (21. člen Predloga ZVOP-2) ter ukrepa t. i. zunanje sledljivosti obdelav osebnih podatkov (šesti odstavek 40. člena Predloga ZVOP-2), kar je delno podobno ureditvi iz dosedanjega tretjega odstavka 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 nov reguliran poklic, ampak se ureja določitev oseb, ki naj znotraj organizacije upravljavca ali obdelovalca na neodvisni način preprečijo tveganja ali kršitve varstva osebnih podatkov. Glede pooblaščenih oseb za varstvo osebnih podatkov predlagana ureditev zahteva znanja in delovne izkušnje s področja varstva osebnih podatkov, omogoča lažjo izbiro javnemu sektorju (razen državnih organov), enako 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 možnostjo določitve namestnika pooblaščene osebe. Določena je tudi možnost, da imajo lahko organi v sestavi lastno pooblaščeno osebo.

Podrobneje je urejen tudi postopek uveljavljanja pravic posameznikov, na katere se nanašajo osebni podatki, tudi z delno uporabo določb Zakona o splošnem upravnem postopku, kadar gre za državne organe.

Posameznik, na katerega se nanašajo osebni podatki in ki meni, da so njegove pravice varstva osebnih podatkov kršene, ima po Predlogu ZVOP-2 tudi možnost vložitve neposredne zahteve pri Informacijskemu pooblaščencu (poimenovana kot prijava) in je v tem postopku vlagatelj zahteve (poimenovan kot prijavitelj s posebnim položajem) in nastopa kot stranka, s subsidiarno uporabo določb zlasti Zakona o splošnem upravnem postopku ter določb tega zakona (nadzorna pooblastila in nadzorni ukrepi). Posameznik v tem primeru pravice uresničuje posredno.

Informacijski pooblaščenec lahko vodi nadzorne postopke tudi v javnem interesu (po uradni dolžnosti), ki jih uvede ali na lastno pobudo, na podlagi prijave katerekoli fizične ali pravne osebe

ali na pobudo drugih organov, kar je klasični postopek inšpekcijskega nadzora po določbah Zakona o inšpekcijskem nadzoru. Prijavitelj je torej lahko kdorkoli; če je prijavitelj posameznik, na katerega se nanašajo osebni podatki, izvršuje svoje pravice posredno (zadoščeno mu bo preko ukrepanja nadzornega organa v javnem interesu, ne pa osebno).

Posameznik lahko vloži tudi samostojno tožbo (brez predhodne uporabe drugih pravnih sredstev) na Upravno sodišče Republike Slovenije glede obdelave osebnih podatkov pri upravljavcu, in sicer glede sedanjih ali preteklih kršitev njegovih pravic s področja varstva osebnih podatkov (samostojno sodno varstvo), tožena stranka je upravljavec, odločanje poteka s smiselno uporabo določb Zakona o upravnem sporu glede postopka v zvezi s kršitvami človekovih pravic in temeljnih svoboščin, v tožbenem zahtevku je možno zahtevati tudi povrnitev škode, v postopku odloča Upravno sodišče Republike Slovenije, nadzorni organ pa lahko pošlje svoje stališče Upravnemu sodišču. Posameznik izvršuje svoje pravice posredno.

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

Posebej je v predlogu zakona 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.

Enotni oziroma skupni nadzorni organ za varstvo osebnih podatkov Republike Slovenije po določbah predloga zakona ostaja Informacijski pooblaščenec, kot je bil do sedaj po določbah ZVOP-1 in po določbah Zakona o informacijskem pooblaščencu in po določbah ZVOPOKD. Ostaja pristojen za nadzor glede varstva osebnih podatkov za vse obdelave osebnih podatkov v Republiki Sloveniji, razen tistih, kjer to preprečujejo ustavne določbe ali določbe Splošne uredbe ali primerljivi položaji – npr. neodvisno odločanje sodstva ali Ustavnega sodišča Republike Slovenije. Delno podobno je urejeno tudi za področje obveščevalno-varnostne dejavnosti – z izjemo, da se nadzori s strani Informacijskega pooblaščenca izvajajo na način da ne pride do zapisa identitete tajnih delavcev in tajnih sodelavcev obveščevalno-varnostnih služb.

V področnih ureditvah obdelav osebnih podatkov (II. del predloga zakona) so npr. delno prenovljeno razdelane določbe o videonadzoru (npr. uvedba videonadzora na javnih površinah) ter o biometriji.

Kazenske določbe (III. del predloga zakona) 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 predloga zakona (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). Prav tako je za kršitve, katere določa Splošna uredba, v Predlogu ZVOP-2 določeno, da so zaradi zagotavljanja zakonitosti na področju prekrškov t. i. »undertaking« naslednji gospodarski subjekti: pravne osebe, samostojni podjetniki posamezniki in posamezniki, ki samostojno opravljajo dejavnost. V zvezi s prekrški iz Splošne uredbe je v Predlogu ZVOP-2 določena tudi kaznivost odgovornih oseb za prekrške, saj te odgovornosti Splošna uredba ne predpisuje, je pa lahko odgovornost teh gospodarskih subjektov le akcesorna odgovornosti odgovorne osebe.

Glede na drugačne definicije iz Splošne uredbe so izvedene tudi znatne spremembe dosedanjega tradicionalnega izrazoslovja s področja varstva osebnih podatkov (ustaljeno od leta 1984[21]).

Tako so sedanji novi temeljni izrazi varstva osebnih podatkov zlasti:

– zbirka (do sedaj zbirka osebnih podatkov);

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

– varnost osebnih podatkov (do sedaj zavarovanje osebnih podatkov);

– upravljavec (do sedaj upravljavec osebnih podatkov);

– obdelovalec (do sedaj pogodbeni obdelovalec);

– posebne vrste osebnih podatkov (do sedaj občutljivi osebni podatki);

– prenos osebnih podatkov (do sedaj iznos osebnih podatkov v tretje države);

– čezmejna obdelava osebnih podatkov (pomeni izmenjave in obdelave osebnih podatkom med državami članicami Evropske unije);

– posredovanje osebnih podatkov pomeni izmenjavo osebnih podatkov med upravljavcem in uporabnikom ali upravljavcem in upravljavcem ali upravljalcem in obdelovalcem.

Z vidika administrativnih razbremenitev ali poenostavitev, vključno za gospodarstvo, predlog zakona določa večje število rešitev, zlasti:

– ukinitev Registra zbirk osebnih podatkov in dolžnosti notifikacije zbirk Informacijskemu pooblaščencu, kar je nadomeščeno z evidenco dejanj obdelav za upravljalce in obdelovalce osebnih podatkov;

– določen je olajšan sistem izbire pooblaščene osebe za varstvo osebnih podatkov (pomembno za gospodarstvo, samoupravne lokalne skupnosti, pa tudi za državne organe - to so osebe, ki svetujejo znotraj upravljavcev osebnih podatkov glede skladnosti obdelave osebnih podatkov), tudi del javnega sektorja lahko izbere osebo iz zasebnega sektorja, Iz prehodne določbe pa izhaja, da upravljavcem in obdelovalcem, ki so pred začetkom uveljavitve tega zakona posredovali podatke nadzornemu organu o pooblaščenih osebah na podlagi Splošne uredbe, ni treba ponovno posredovati informacij, če podatki o pooblaščenih osebah niso spremenjeni;

– določena je definicija povezovanja zbirk osebnih podatkov – samo veliki sistemi s tveganimi obdelavami osebnih podatkov bodo potrebovali ureditev v področnem zakonu (sodni register, E-Sociala …) ter Informacijski pooblaščenec ne bo izdajal odločb o povezovanju.

2.6. Sprejetje zakona

Zakon bi moral biti uveljavljen že 6. 5. 2018, ko je potekel rok za zakonodajno izvedbo Direktive (EU) 2016/680 oziroma 25. 5. 2018 ko bi moral biti slovenski Zakon o varstvu osebnih podatkov usklajen s Splošno uredbo o varstvu podatkov.

Zato bi zakon moral biti čimprej sprejet in objavljen v Uradnem listu Republike Slovenije.

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, razen na področju akreditacije.

Slovenska akreditacija ocenjuje, da bo potrebno zagotoviti finančna sredstva za vzpostavitev akreditiranja na področju akreditacijske sheme GDPR za enega zaposlenega, kar znese 60.000 EUR v letu 2023 in 40.000 EUR v letu 2024.

Sredstva bodo zagotovljena s prerazporeditvijo s proračunske postavke Ministrstva za pravosodje PP 124110 na proračunsko postavko Ministrstva za gospodarski razvoj in tehnologijo PP 127710 Slovenska akreditacija (ukrep 2111-11-0009 Prost pretok blaga in storitev).

Predlog zakona ne bo imel drugih posledic za Proračun Republike Slovenije, saj je bilo precej predlaganih zakonskih rešitev že do sedaj del pravnega reda Republike Slovenije in jih sedanji predlog zakona le nekoliko nadgrajuje. Dodatna finančna sredstva niso potrebna za okrepitev oziroma dodatno zagotovitev učinkovitega in neoviranega delovanja neodvisnega nadzornega mehanizma (Informacijski pooblaščenec), namreč glede dodatnih kadrov in prostorov, ki zagotavljajo učinkoviti nadzor spoštovanja določb novih pravnih aktov Evropske unije glede varstva osebnih podatkov. Za to potrebne pravice porabe so bile pri Informacijskem pooblaščencu zaradi izvajanja Splošne uredbe o varstvu podatkov zagotovljene že z letoma 2018 in 2019 (dodatne zaposlitve in prostori), tako da ta predlog zakona tudi iz tega vidika nima finančnih posledic za državni proračun.

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 namenjati 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 (DPO, »*data protection officers*«), kolikor v nekaterih primerih še niso vzpostavljene po določbah Splošne uredbe. 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 oziroma nastanka konflikta interesov iz predloga zakona) ali pa dodatno uporabiti (nameniti) že obstoječa finančna sredstva glede zunanjih storitev – npr. pravno svetovanje – za uvedbo zunanjih pooblaščenih oseb (relevantno npr. za samoupravne lokalne skupnosti) ali pa organizirati pooblaščene osebe v okviru medobčinskega sodelovanja – skupne občinske uprave (kot npr. medobčinska redarstva ipd.).

Prav tako so relevantna dodatna sredstva za okrepitev oziroma 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. Ta sredstva so sicer že bila vnaprej zagotovljena v letu 2017 za leti 2018 in 2019 (o tem spodaj).

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 za leto 2023 in 2024 bodo sredstva zagotovljena s prerazporeditvijo s proračunske postavke Ministrstva za pravosodje PP 124110 na proračunsko postavko Ministrstva za gospodarski razvoj in tehnologijo PP 127710 Slovenska akreditacija (ukrep 2111-11-0009 Prost pretok blaga in storitev).

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 bila zagotovljena dodatna sredstva v državnem proračunu.

Dodatna sredstva so bila načrtno zagotovljena že v letu 2017 in sicer za postopno izvedbo v obdobju let 2018 in 2019 – za delovanje neodvisnega nadzornega in samostojnega organa (Informacijski pooblaščenec).

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

Za proračunsko leto 2019 so bila zagotovljena naslednja finančna sredstva oziroma 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 bila tako zagotovljena finančna sredstva skupaj v višini 359.600,00 EUR.

Glede na zgoraj navedeno so dodatna finančna sredstva predvidena le za vzpostavitev sistema akreditacije, kot navedeno zgoraj.

5. PRIKAZ UREDITVE V DRUGIH PRAVNIH SISTEMIH IN PRILAGOJENOSTI PREDLAGANE UREDITVE V PRAVU EVROPSKE UNIJE

5. 1. Uvodno o primerjalnopravni ureditvi

Pred uveljavitvijo Splošne uredbe so bili sprejeti le štirje izvedbeni zakoni držav članic Evropske unije – v Zvezni republiki Nemčiji, v Republiki Avstriji, v Slovaški republiki ter v Kraljevini Belgiji. Večina preostalih držav članic Evropske unije je šele po mesecu maju 2018 sprejela izvedbene zakone.

»Modeli« oziroma »smeri« zakonodajnega urejanja iz navedenih zakonov so si precej različne, načeloma je vsaka država razvila zakonsko izvedbeno ureditev v njej lastno smer[22].

Zgolj primeroma, Francoska republika je leta 2016[23] sprejela delni izvedbeni zakon ter naknadno glede njega ocenila, da bo treba zaradi vsebinske nepopolnosti oziroma 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 bil nato izdan leta 2018[24]. 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.

V nadaljevanju so predstavljeni nemški, avstrijski, slovaški in belgijski zakon.

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)[25]. Sistemski pristop zakona je, da upošteva obstoječo nacionalno pravno ureditev (ustavnopravno), ustaljene rešitve iz področnih zakonov Nemčije ter tradicionalno prakso varstva osebnih podatkov v Nemčiji.

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

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

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[26] 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

[22] 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.

[23] Zakon št. 2016-1321 z dne 7. oktobra 2016 za digitalno republiko.

[24] Predlog Zakona o varstvu osebnih podatkov Francoske republike – nujni zakonodajni postopek, z dne 14. 2. 2018.

[25] Zakon z dne 30. junija 2017, Bundesgesetzblatt Teil I, 2097.

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

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 tistim, 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.

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[27], češ da ni dovolj v skladu z določbami Splošne uredbe – da naj bi bile občasno njegove določbe prestroge ali preširoke. Domnevati je, da je Nemčija glede teh vprašanj (vidik 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)[28].

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 (uradni) pravni pomen ustavne norme, ni bil spremenjen zaradi neobstoja zahtevane dvotretjinske večine vseh poslancev in poslank Državnega zbora Republike Avstrije za ustavno revizijo, kar pomeni, da je Avstrija zadržala dosedanjo širšo opredelitev varstva osebnih podatkov kot temeljne pravice – kot nadrejeno glede vseh obdelav osebnih podatkov (tudi obdelav v druge namene). Prav tako je Avstrija zadržala dosedanjo tradicionalno ureditev (po sodni praksi od leta 1951 dalje) glede obravnavanja tudi (dela) podatkov o pravnih osebah, ki se tako varujejo kot (da so) osebni podatki. Za obdelavo osebnih podatkov otrok v zvezi storitvami informacijske družbe je določila 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 (ni jasno uveljavila) rešitev glede kritiziranih (spornih) visokih glob po Splošni uredbi, glede katerih se v Avstriji zatrjuje kršitev človekovih pravic oz. 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. Poleg tega je naknadno glede navedenega kaznovanja z globami dne 20. aprila 2018 sprejela novelo navedenega zakona (sprememba Zakona o varstvu osebnih podatkov z zakonskim nazivom: Zakon o deregulaciji varstva osebnih podatkov – Datenschutz-Deregulierungs-Gesetz 2018, BGBl. I Nr. 24/2018) in v njej določila, da se v primeru predpisanih glob za kršitve po Splošni uredbi najprej izrekajo opozorilne sankcije, šele v primeru ponovljenih kršitev pa globe po Splošni uredbi (spremembe 11. člena), prav tako pa je v isti noveli določila, da nosilci javnih pooblastil niso odgovorni za prekrške po Splošni uredbi (spremembe 35. člena).

Glede razmerja varstvo osebnih podatkov – znanstveno raziskovanje je Avstrija določila le splošne določbe, obdelave pa bodo potekale po obstoječih področnih zakonih. V sprejetem

[27] 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/

[28] Bundesgesetzblatt I Nr. 120/2017, Teil I.

zakonu tudi 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 bilo v predlogu zakona 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 v Avstriji tako kot do sedaj 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 v razmerju do končno sprejetega zakona leta 2017 in njegove novele iz leta 2018) pokazal, da ne gre niti za unificiran pristop niti ne za (dovolj) harmoniziran pristop, ampak ob upoštevanju nespremenjenih določenih sistemskih rešitev ter novih rešitev in rešitev iz področne zakonodaje dejansko za t. i. fragmentacijo pravne ureditve.

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[29]. 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.[30] 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 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

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

[30] Zunanje neodvisne analize tudi navajajo, da »Novi Zakon o varstvu osebnih podatkov precej podvaja določbe Splošne uredbe, ki je kot uredba neposredno uporabna v Slovaški republiki…« (glejte npr. : http://www.konecna-zacha.com/en/new-slovak-data-protection-act-exceptions-to-the-gdpr/).

Predlog Zakona o varstvu fizičnih oseb glede obdelave osebnih podatkov Kraljevine Belgije je bil objavljen 16. marca 2018 in vsebuje 287 členov. Zakonodajno smer takratnega predloga je mogoče oceniti kot 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 zakon 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 predlog 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 – sedaj peti odstavek 63. člena)[31]. Področja iz Direktive 2016/680/EU so urejena v II. delu predloga zakona, delno pa tudi v III. delu predloga zakona. Področja arhiviranja, znanstvenega in zgodovinskega raziskovanja ter statističnega delovanja so urejena v IV. delu predloga 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.

Zakon o varstvu fizičnih oseb glede obdelave osebnih podatkov Kraljevine Belgije je bil nato sprejet 30. julija 2018 in objavljen v Uradnem listu Kraljevine Belgije dne 5. septembra 2018 in začel veljati istega dne. Končno sprejeto besedilo zakona ima 285 členov.

Pred navedenim zakonom je bil v Kraljevini Belgiji dne 3. decembra 2017 sprejet (objavljen dne 10. januarja 2018) Zakon o organu za varstvo osebnih podatkov, ki je začel veljati dne 25. maja 2018, spremenjen pa že 28. maja 2018. Zakon ureja vzpostavitev prenovljenega nadzornega organa za varstvo osebnih podatkov Kraljevine Belgije, njegovo pravno osebnost, razmerje do Predstavniškega doma Kraljevine Belgije, njegove nadzorne pristojnosti in naloge, pristojnosti inšpektorjev, načine odločanja, notranjo organizacijo in notranje načine delovanja, neodvisnost organa, postopek imenovanja in razrešitve vodilnih članov organa ipd.

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. Za postopke seznanitve z lastnimi osebnimi podatki se bodo uporabljale določbe Zakona o splošnem upravnem postopku, kolikor gre za državne organe, ki odločajo (delujejo) po pravilih

[31] Navedena uredba je v mesecu juliju 2019 še vedno v pripravi, po njeni izdaji se bo morala določitev pooblaščenih oseb prilagoditi novi pravni ureditvi.

splošnega upravnega postopka. V drugih primerih se bo uporabljal poenostavljen (neformalni) postopek po tem zakonu.

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 (glejte tudi obrazložitev zakonskih rešitev spodaj o določenih poenostavitvah za zasebni sektor oz. gospodarstvo).

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 pristojno ministrstvo (Ministrstvo za pravosodje) bo predstavilo zakon širši javnosti z objavo na spletu, ožji javnosti pa na predavanjih, srečanjih, posvetih v okviru izobraževalnih dejavnosti ipd. Prav tako lahko Informacijski pooblaščenec po svoji samostojni presoji predstavi zakon v okviru njegovih izobraževalnih, posvetovalnih in drugih podobnih nalog.

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

Zunanji strokovnjaki niso sodelovali pri pripravi predloga zakona.

Druge tovrstne okoliščine niso podane.

7. PRIKAZ SODELOVANJA JAVNOSTI PRI PRIPRAVI PREDLOGA ZAKONA:

Javna razprava (prvi krog) glede prvotnega predloga zakona je bila izvedena od 3. 10. 2017 do 13. 11. 2017 ter ponovno (drugi krog) od 23. 1. 2018 do 2. 2. 2018. Takratni predlog besedila zakona (v nadaljevanju: predlog ZVOP-2) je izhajal iz koncepta enotnosti urejanja varstva osebnih podatkov za obe pravni področji, to je Splošne uredbe o varstvu podatkov (v nadaljevanju: Splošna uredba) ter ti. policijsko pravosodne direktive (Direktiva (EU) 2016/680) in je imel torej nekoliko naravo zakonika. Precej takratnih pripomb deležnikov je bilo upoštevanih, zlasti glede neposrednega trženja, pooblaščenih oseb, privolitve, obdelave v druge namene. Nato je bila glede prenovljenega predloga zakona izvedena nova Javna razprava od 7. 3. 2019 do 25. 3. 2019 in v naslednjem obdobju je glede na konceptualne spremembe v predlogu zakona bil nov drugi krog strokovnega in medresorskega usklajevanja – do 16. 8. 2019.

Konec leta 2019 je bila sprejeta odločitev, da se vsebina takratnega predloga ZVOP-2 razdeli na dva zakona, na enega, ki bo izvrševal določbe Direktive (EU) 2016/680 in na drugega, ki bo določal potrebne izvedbene določbe za Splošno uredbo ter povezane nacionalne določbe glede obdelav osebnih podatkov. Tako je bil najprej novembra 2020 sprejet ZVOPOKD[32], ki ureja obdelave osebnih podatkov v zvezi z obravnavanjem kaznivih dejanj.

Sedanji predlog zakona je konceptualno delno podoben predlogu zakona iz druge polovice leta 2019 in izhaja iz pristopa, da se v njem urejajo vsebine, ki omogočajo izvrševanje Splošne uredbe ter nacionalne posebnosti, nima pa več narave zakonika. Predlog je bil ponovno posredovan v medresorsko usklajevanje 30. 4. 2021, v strokovno usklajevanje 3. 5. 2021, na spletnih straneh e-Demokracije pa je bil objavljen 30. 4. 2021.

Predlog je bil v strokovno usklajevanje posredovan naslednjim deležnikom: Informacijski pooblaščenec, Varuh človekovih pravic, Vrhovno sodišče RS, Upravno sodišče RS, Vrhovno državno tožilstvo RS, Državnotožilski svet, Sodni svet, Ekonomsko-socialni svet, Odvetniška zbornica, Notarska zbornica, Banka Slovenije, Združenje bank Slovenije, Računsko sodišče RS, Zagovornik načela enakosti, Arhiv RS, Slovenska akademija znanosti in umetnosti, Center za informiranje sodelovanje in razvoj nevladnih organizacij – CNVOS, Slovenska akreditacija, SI-CERT, Skupnost občin Slovenije, Združenje občin Slovenije, Združenje Mestnih občin Slovenija, Univerza v Ljubljani, Univerza v Mariboru, Univerza v Novi Gorici, Pravna fakulteta Univerze v Ljubljani, Pravna fakulteta Univerze v Mariboru, Evropska pravna fakulteta v Novi Gorici, Fakulteta za varnostne vede Univerze v Mariboru, Inštitut za kriminologijo pri Pravni fakulteti Univerze v Ljubljani, Gospodarska zbornica Slovenije, Obrtna zbornica Slovenije, Trgovinska zbornica Slovenije, Detektivska zbornica Slovenije, Zdravniška zbornica Slovenije, Zbornica za razvoj zasebnega varovanja Slovenije, Ameriška gospodarska zbornica, Združenje delodajalcev Slovenije, Združenje Manager, Sekcija operaterjev elektronskih komunikacij.

Svoje pripombe so v sklopu strokovnega usklajevanja podali naslednji subjekti: zainteresirani državljani prek eDemokracije, Okrožno sodišče v Ljubljani, Varuh človekovih pravic, Notarska zbornica, Zavod za zdravstveno zavarovanje, Banka Slovenije, AJPES, Združenje mestnih občin Slovenije, Združenje delodajalcev obrti in podjetnikov Slovenije GIZ, Vrhovno sodišče RS, Združenje bank Slovenije GIZ, Slovenska akreditacija, GDPR PLUS, d.o.o., Inštitut za kriminologijo pri Pravni fakulteti v Ljubljani, Zagovornik načela enakosti, ARNES, Infocenter, Sodni svet RS, Univerza v Ljubljani, Detektivska zbornica Slovenije, Združenje delodajalcev Slovenije, Odvetniška zbornica Slovenije, Združenje družb za upravljanje investicijskih skladov GIZ, Slovensko zavarovalno združenje, Informacijski pooblaščenec, Zdravniška zbornica Slovenije, AmCham Slovenija, Upravno sodišče, Obrtno-podjetniška zbornica Slovenije, Združenje občin Slovenije, Vrhovno državno tožilstvo, Statistični urad RS, Univerza v Mariboru, Društvo revmatikov Slovenije, Trgovinska zbornica Slovenije, Gospodarska zbornica Slovenije, Microsoft Slovenija d.o.o., Piratska stranka Slovenije, CNVOS, Slovensko združenje za elektronsko identifikacijo in elektronske storitve zaupanja – EIDES, GEN-I, d.o.o., Konfederacija Sindikatov Slovenije PERGAM, SETCCE tehnološki park.

Kljub nekaterim pripombam strokovne javnosti po skrajšanju besedila zakona z vidika neposredne uporabe Splošne uredbe smo se na posameznih mestih odločili slediti izhodišču »vse na enem mestu« saj se po naši oceni s tem ohranja dosedanja visoka raven varstva osebnih podatkov v Republiki Sloveniji, poleg tega pa smo bili dolžni upoštevati tudi precej nasprotujoče pripombe in predloge deležnikov, ki so zahtevali po svoji vsebini več zakonodajnega urejanja, zlasti z vidika zagotavljanja pravne varnosti. Uveljavljanje pravic posameznikov pred državnimi organi in širšim javnim ter zasebnim sektorjem je urejeno na poseben način, da se subjektov ne obremenjuje s formalnimi postopki, kadar ne gre za državne organe (našteti v predlogu).

Zakon velja tako za javni kot zasebni sektor, z nekaterimi razlikami med obema sektorjema, ob upoštevanju posebnosti. Za javni sektor smo pri izvajanju oblasti in opravljanju zakonskih nalog

[32] Uradni list RS, št. 177/20.

na primer predvideli strogo načelo zakonitosti glede obdelav osebnih podatkov posameznikov, kar pomeni, da morajo biti obdelave določene v zakonu, medtem ko lahko subjekti zasebnega sektorja obdelave izvajajo neposredno na podlagi določb Splošne uredbe (prvi odstavek člena 6 Splošne uredbe). Poleg tega tudi slovenska ustavnosodna presoja že od leta 1992 in še posebej od 2019 zahteva popolno regulacijo delovanj z osebnimi podatki v zakonih (kadar se mora obdelave osebnih podatkov urejati v zakonih). Podobna ureditev je bila tudi v slovenskih zakonih o varstvu osebnih podatkov iz 1990, 1999 in 2004 – kar pomeni, da mora veljavna zakonodaja te kriterije že upoštevati. Poleg tega se je tudi na področju upravne zakonitosti okrepila ustavna presoja Ustavnega sodišča Republike Slovenije – delovanja države morajo biti nujno urejena v zakonih (odločba US U-I-79/20, 13. 5. 2021, glejte točke 69-72).

Glede postopkovnih določb smo prejeli večje število pripomb različnih subjektov. Predlogi so bili deloma nasprotujoči, nekateri subjekti so predlagali večjo formalizacijo postopka v skladu z ZUP, medtem ko so drugi predlagali povsem neformalni postopek, podoben tistemu v ZDIJZ. Predlagatelj je pripombe deloma upošteval in postopek uredil tako, da je postopek pred državnimi organi in organi lokalne samouprave formaliziran (ti organi tudi v drugih postopkih odločajo na podlagi ZUP, zato za te organe ta način postopanja ni novost), za preostale subjekte javnega sektorja in za zasebni sektor pa je postopek nekoliko poenostavljen in manj formaliziran. Kljub temu je postopek pred vsemi upravljavci in obdelovalci treba izpeljati na način, ki omogoča naknadni nadzor Informacijskega pooblaščenca ali sodišča.

Pripombe, ki so se nanašale na nepotrebno urejanje podlag za obdelave osebnih podatkov v tem zakonu v povezavi s členom 6 Splošne uredbe, niso bile upoštevane, ker želimo ohraniti visoko stopnjo varstva osebnih podatkov, ki izhaja že iz drugega odstavka 38. člena Ustave Republike Slovenije. V javnem in zasebnem sektorju se lahko osebni podatki obdelujejo na podlagah iz prvega odstavka člena 6 Splošne uredbe, vključno s pogodbo, privolitvijo ali zakonitim interesom, kadar pa je podlaga za obdelavo izvajanje oblastnih nalog ali zakonskih obveznosti, pa morajo te biti določene v zakonu.

Glede pravnih podlag za obdelave osebnih podatkov je Zagovornik načela enakosti izpostavil priporočila iz prejšnjih let, skladno s katerimi bi bilo treba zgotoviti podlago za zbiranje statističnih podatkov o narodnostni pripadnosti, ki so potrebni za preprečevanje diskriminacije. Pripombe so bile upoštevane in peti odstavek 6. člena predloga zakona je dopolnjen, tako da omogoča zbiranje navedenih podatkov ob predpostavki, da to določa zakon in da je podana ali privolitev posameznika ali pa da se posameznik sam opredeli glede narodnosti in to za bodoče zakonsko določene primere (npr. ko je podatek o narodni ali etnični pripadnosti bistven za odločanje o storitvi, opomoči, ukrepanju na področju antidiskriminacije).

Pripombe v zvezi s privolitvijo mladoletne osebe za uporabo storitev informacijske družbe so se nanašale tako na starost mladoletne osebe, kot na njeno privolitev oziroma na odobritev s strani staršev oziroma skrbnikov ali drugih zakonsko določenih oseb. V skladu z veljavno zakonodajo je starost 15 let tista, ki že omogoča delno poslovno sposobnost, zato smo temu sledili tudi v predlogu ZVOP-2.

Glede pripomb v zvezi s sodnim varstvom pravic posameznika, na katerega se nanašajo osebni podatki, ki so se nanašale na številna pravna sredstva, ki jih imajo posamezniki in na možnost hkratnega uveljavljanja pravic v različnih postopkih pred nadzornim organom in sodišči, pojasnjujemo, da taka ureditev velja že od uveljavitve veljavnega ZVOP-1 leta 2004 in se je izkazala kot učinkovita, saj omogoča posameznikom, da se sami odločijo na kakšen način bodo uveljavljali svoje pravice. Podobna ureditev pa je tudi vsebovana v že sprejetem Zakonu o varstvu osebnih podatkov na področju obravnavanja kaznivih dejanj (12. člen).

Pripombe v zvezi z postopki pred upravljavcem in obdelovalcem so v delu med seboj nasprotujoče. Pripombe, ki so se nanašale na nepotrebno normiranje v zakonu glede na neposredno uporabnost določb Splošne uredbe so bile v največji možni meri upoštevane, tako da se predlog zakona zaradi preglednosti postopkov zgolj sklicuje na uporabo določb Splošne

uredbe, razen v delu, kjer ureja postopek pred državnimi organi in organi lokalne samouprave, ki v teh postopkih uporabljajo ZUP in v postopku izdajo odločbo.

Pripombe, ki so se nanašale na poglavje varnosti osebnih podatkov in oceno učinka so bile v glavnem upoštevane. Spremenjen je bil predmet določb (posebna obdelava namesto posebna zbirka), prav tako pa je bil upoštevan predlog, naj se pri varnosti posebnih obdelav izhaja iz ocene učinka tveganj na varnost osebnih podatkov. Pripomb, katerih cilj je bil črtanje določb iz razloga, da posebnih obdelav Splošna uredba ne pozna, predlagatelj ni upošteval, saj gre za obdelave, ki se nanašajo na najbolj občutljive zbirke osebnih podatkov v državi (tudi z vidika količine podatkov), Splošna uredba pa dopušča zakonsko urejanje obdelav osebnih podatkov v skladu z zakoni držav članic (drugi in tretji odstavek člena 6 Splošne uredbe).

Ocena učinka je skladno s pripombami zamejena na situacije, ko to predpisuje Splošna uredba, črtana pa so bila tudi posebna izobraževanja za pooblaščene osebe v subjektih, ki izvajajo posebne obdelave. V tem delu so bile pripombe deležnikov upoštevane.

Pripombe glede roka hrambe dnevnikov obdelave so bile upoštevane, tako da je mogoče z oceno učinka zakonsko predpisani rok hrambe podatkov v dnevnikih podaljšati, po tem pa je podatke mogoče hraniti, če za to obstaja druga pravna podlaga (npr. tista iz člena 6 Splošne uredbe).

Pri vprašanjih možnosti posameznika na katerega se nanašajo osebni podatki za obrambo ali uresničevanje njegovih pravic s področja varstva osebnih podatkov napram upravljavcem, za katere meni, da morda nezakonito ali nepravilno obdelujejo njegove osebne podatke smo se odločili slediti že sprejeti ureditvi na področju varstva osebnih podatkov pri obravnavanju kaznivih dejanj (ZVOPOKD). Po oceni predlagatelja so v predlogu ZVOP-2 sedaj dovolj jasno razmejeni postopki pred upravljavcem, nadzornim organom in sodišči. V nadaljevanju so prikazani postopki uresničevanja pravic posameznika:

1. Posameznik se obrne z zahtevo na upravljavca in zahteva dostop do osebnih podatkov ali njihove spremembe (npr. popravek, izbris). Če mu ni ugodeno ali meni, da mu ni ugodeno, se obrne s pritožbo na nadzorni organ (Informacijski pooblaščenec). Postopek se pred državnim organom oziroma pred organom lokalne samouprave vodi na podlagi klasičnega upravnega postopka z določenimi prilagoditvami obravnavanim zadevam (npr. omejitev vpogleda v spis, zavarovanje osebnih podatkov, ki so predmet nadzornega postopka, izključitev stranske udeležbe) oziroma na podlagi določb Splošne uredbe in tega zakona (neformalni postopek). Pravice uresničuje neposredno, ko gre za obravnavanje zahteve pri upravljavcu, preko nadzornega organa (pritožbeni postopek) pa posredno.

2. Posameznik, ki meni, da so njegove pravice kršene, ima po predlaganem zakonu tudi možnost vložitve neposredne zahteve po določbah Zakona o splošnem upravnem postopku pri Informacijskemu pooblaščencu (poimenovana kot prijava) in je v tem postopku vlagatelj zahteve (prijavitelj s posebnim položajem) in nastopa kot stranka, s subsidiarno uporabo določb zlasti Zakona o splošnem upravnem postopku ter določb tega zakona (nadzorna pooblastila in nadzorni ukrepi). Posameznik pravice uresničuje posredno.

3. Informacijski pooblaščenec lahko vodi nadzorne postopke tudi v javnem interesu (po uradni dolžnosti), ki jih uvede ali na lastno pobudo, na podlagi prijave katerekoli fizične ali pravne osebe ali na pobudo drugih državnih organov, nadzornih agencij RS ali nadzornega organa za varstvo osebnih podatkov države članice Evropske unije ali Sveta Evrope, kar je klasični postopek inšpekcijskega nadzora po določbah Zakona o inšpekcijskem nadzoru. Prijavitelj je torej lahko kdorkoli; če je prijavitelj posameznik, na katerega se nanašajo osebni podatki, izvršuje svoje pravice posredno (zadoščeno mu bo preko ukrepanja nadzornega organa v javnem interesu, ne pa osebno).

4. Posameznik lahko vloži tudi samostojno tožbo na sodišče glede obdelave osebnih podatkov pri upravljavcu, in sicer glede sedanjih ali preteklih kršitev njegovih pravic s področja varstva osebnih podatkov (samostojno sodno varstvo), tožena stranka je upravljavec, odločanje poteka s smiselno uporabo določb Zakona o upravnem sporu glede postopka v zvezi s kršitvami

človekovih pravic in temeljnih svoboščin, v tožbenem zahtevku je možno zahtevati tudi povrnitev škode, v postopku odloča Upravno sodišče Republike Slovenije. Posameznik izvršuje svoje pravice posredno.

Pripombe Informacijskega pooblaščenca so se nanašale na zahtevo po enovitem postopku, čemur pa predlagatelj ni sledil, meni namreč, da morajo posamezniki imeti možnost, da se sami odločijo, na kakšen način bodo uveljavljali svojo pravico. Prav tako smo sledili enotnosti ureditve v ZVOP-2 in že uveljavljenem ZVOPOKD.

Delno so bile upoštevane pripombe Varuha človekovih pravic z vidika njegove nadzorne vloge v sistemu varstva človekovih pravic, predvsem v delu, glede določanja izjem inšpekcijskega nadzora. Varuh je v svojih pripombah obširno obrazložil svoj predlog za izvzetje iz inšpekcijskega nadzora glede obdelav osebnih podatkov, v okviru zakonskih pristojnosti Varuha, čemur je predlagatelj v določeni meri sledil.

Posebno poglavje je namenjeno posredovanju osebnih podatkov znotraj javnega sektorja in osebam zasebnega sektorja in ureditvi postopka. Glede teh vprašanj smo prejeli pripombe glede plačljivosti posredovanja podatkov in ostali pri dosedanjih usmeritvah, po katerih se podatki posredujejo brezplačno (tako znotraj javnega sektorja, s strani zasebnega sektorja javnemu sektorju pa zaradi spoštovanja bistvenega javnega interesa pravne države).

Glede pooblaščenih oseb za varstvo osebnih podatkov predlagatelj pojasnjuje, da obveznost imenovanja pooblaščene osebe ni nova, zavezanci so jih imenovali neposredno po določbah Splošne uredbe ob njeni uveljavitvi. Predlagatelj ni želel bistveno posegati v vzpostavljene in delujoče mehanizme, zato predlog ZVOP-2 določa le minimalne standarde za imenovanje in delovanje pooblaščene osebe. Predlagatelj je prejel nekaj predlogov deležnikov za vzpostavitev možnosti za imenovanje namestnika pooblaščene osebe, čemur je v predlogu zakona tudi sledil (kot neobvezna možnost).

Glede pripomb GZS o nepotrebnem urejanju podrobnosti določanja pooblaščenih oseb, skupnega določanja pooblaščenih oseb več upravljavcev itd. predlagatelj pojasnjuje, da so bili glede teh vprašanj podani tudi številni predlogi različnih subjektov za zakonsko določitev posebnosti na tem področju.

Predlagatelj zakona je pri vprašanjih urejanja pooblaščenih oseb v izogib nalaganju dodatnih obveznosti (ponovno preverjanje izpolnjevanja pogojev itd.) sledil cilju, da že imenovane pooblaščene osebe nadaljujejo s svojim delom. Temu je namenjena tudi prehodna določba.

Predlagatelj zakona je skladno s prejetimi pripombami spremenil izraz »certificiranje« v »potrjevanje«, da je skladen s terminologijo iz Splošne uredbe.

Pripombe Slovenske akreditacije glede potrebnih finančnih sredstev za vzpostavitev sistema certificiranja ozir. akreditacije so bile upoštevane in je gradivo prilagojeno na način, da je določen daljši zakonski rok za vzpostavitev sistema certificiranja, ki omogoča postopno prilagoditev finančnih sredstev v okviru finančnih načrtov neposrednih finančnih porabnikov.

Glede poglavja, ki ureja pristojnosti nadzornega organa je bistveno navesti, da je Informacijski pooblaščenec še vedno sistemski nadzorni organ za varstvo osebnih podatkov v Republiki Sloveniji, kot je bil po dosedanji ureditvi. Omejitve glede varstva neodvisnosti sodstva oziroma tajnih delavcev in sodelavcev (obdelav osebnih podatkov o njihovi identiteti) so le manjše izjeme, načeloma je Informacijski pooblaščenec pristojen za vsa področja dejanj obdelave po določbah Splošne uredbe.

Posebej izpostavljamo strokovno usklajevanje določb predloga ZVOP-2 glede poglavja, ki ureja posebna pravila obdelave osebnih podatkov na področju znanstvenega, zgodovinskega in statističnega raziskovanja ter za arhivske namene. V tem delu je predlagatelj prejel obsežne pripombe številnih deležnikov, ki vse zasledujejo cilj zagotavljanja razvoja znanstvenoraziskovalnega dela ob hkratni sorazmerni in razumni zaščiti posameznikov, na katere se osebni podatki nanašajo. Skrb deležnikov je bila predvsem v tem, da predlagano besedilo

postavlja previsoke zahteve za upravljavce osebnih podatkov, kar bi lahko privedlo celo do onemogočanja znanstvenoraziskovalne dejavnosti. Predlagatelj zakona je pripombam v največji možni meri sledil in določbe v tem poglavju preoblikoval na način, da je zagotovil večjo dostopnost podatkov za te namene ob hkratnem visokem varstvu varnosti podatkov.

Predlagatelj je sledil tudi pripombam Statističnega urada in uporabo zakona izključil za namene obdelovanja osebnih podatkov za državno statistiko, ker so ta vprašanja že ustrezno urejena s področno zakonodajo.

Glede na pripombe deležnikov iz gospodarstva k določbam o videonadzoru je predlagatelj podaljšal najdaljši dopustni rok hrambe posnetkov na eno leto. Dodatno je opredelil možnost uporabe telesnih kamer za prenos premoženja večje vrednosti (npr. za varnostne službe, ki prevažajo denar).

Dodatno je predlagatelj uredil tudi videonadzor v prevoznih sredstvih, namenjenih javnemu potniškemu prometu in videonadzor cestnih odsekov.

V okviru strokovnega usklajevanja je predlagatelj prejel tudi večje število pripomb v zvezi z obdelavo biometričnih osebnih podatkov, predvsem v zasebnem sektorju. Glede izpostavljenega vprašanja ugotavlja, da so bile posamezne pripombe med seboj v nasprotju, zato je iskal kompromisno rešitev med omogočanjem tovrstnih obdelav in hkratnim zagotavljanjem visokega varstva biometričnih osebnih podatkov. Predlagatelj je po skrbni preučitvi vseh prejetih pripomb predvidel dodatne varovalke oziroma ustrezne mehanizme, ki zagotavljajo varnost osebnih podatkov, tudi v obliki potrjevanja dejanj obdelave, ki je po predlogu ZVOP-2 v zasebnem sektorju pogoj za obdelovanje biometričnih osebnih podatkov.

Pripomb deležnikov glede kazenskih določb predlagatelj ni mogel upoštevati. Globe za upravljavce in obdelovalce predpisuje že Splošna uredba, ki se uporablja neposredno. Predlagatelj je v predlogu ZVOP-2 le uredil podlago za njihovo izrekanje, ki trenutno še ni ustrezno urejena v Zakonu o prekrških ter podlago za prekrškovno sankcioniranje odgovornih oseb, ki je Splošna uredba ne ureja, je pa z vidika slovenskega pristopa k prekrškovnemu sankcioniranju pravnih oseb nujna (odgovornost pravnih oseb je akcesorna).

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

- Marjan Dikaučič, minister za pravosodje,
- Zlatko Ratej, državni sekretar na Ministrstvu za pravosodje,
- mag. Nina Koželj, generalna direktorica Direktorata za kaznovalno pravo in človekove pravice,
- Peter Pavlin, višji sekretar,
- Matjaž Mešnjak, podsekretar.

II. BESEDILO ČLENOV

I. DEL
TEMELJNE DOLOČBE

1. poglavje
Splošne določbe

1. člen
(vsebina)

(1) Ta zakon ureja uresničevanje človekove pravice do varstva osebnih podatkov, obveznosti, načela, upravičenja, postopke in ukrepe, s katerimi se zagotavlja ustavna skladnost, zakonitost in upravičenost posegov v zasebnost, dostojanstvo, tajnost osebnih podatkov, podatkovna samoodločba oziroma druge temeljne pravice posameznika pri obdelavi osebnih podatkov ter pravila o prostem pretoku osebnih podatkov za izvajanje 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) (UL L št. 119 z dne 4. 5. 2016, str. 1), zadnjič popravljene s Popravkom (UL L št. 127 z dne 23. 5. 2018, str. 2; v nadaljnjem besedilu: Splošna uredba) ter druga vprašanja obdelave in varstva osebnih podatkov.

(2) Za vprašanja varstva in obdelave osebnih podatkov, ki jih ne ureja zakon, ki ureja varstvo osebnih podatkov na področju obravnavanja kaznivih dejanj, se uporabljajo določbe tega zakona.

2. člen
(prepoved diskriminacije glede obdelave osebnih podatkov)

Obdelava osebnih podatkov je prepovedana, če se izvaja na način ali ima za posledico nedopustno diskriminacijo 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, invalidnost, državljanstvo, kraj oziroma vrsto prebivališča, zdravstveno stanje, genske predispozicije ali katero koli drugo osebno okoliščino posameznice in posameznika (v nadaljnjem besedilu posameznik).

3. člen
(področje uporabe)

(1) Določbe tega zakona veljajo za obdelave osebnih podatkov na področjih, ki jih ureja Splošna uredba, ali jih posebej ureja ta zakon in se izvajajo v celoti ali delno z avtomatiziranimi sredstvi, in za obdelave osebnih podatkov, ki so del zbirke ali so namenjeni oblikovanju dela zbirke, ki se ne izvaja z avtomatiziranimi sredstvi.

(2) Določbe tega zakona ne veljajo za obdelave osebnih podatkov, ki jih izvajajo posamezniki med potekom popolnoma osebne ali domače dejavnosti.

(3) Za obdelave osebnih podatkov, ki jih Splošna uredba ne ureja, se subsidiarno uporabljajo določbe tega zakona.

4. člen

(veljavnost zakona)

(1) Ta zakon velja za obdelavo osebnih podatkov, ki se izvaja v okviru javnega sektorja Republike Slovenije, ter za zasebni sektor, kadar gre za obdelavo osebnih podatkov, ki se izvaja v okviru dejavnosti ustanovitve upravljavca ali obdelovalca, registrirane v Republiki Sloveniji, četudi obdelava osebnih podatkov ne poteka v Republiki Sloveniji.

(2) Ta zakon velja tudi za obdelavo osebnih podatkov, ki se izvaja v okviru dejavnosti ustanovitve upravljavca ali obdelovalca, ki je registrirana zunaj Evropske unije, če so dejavnosti obdelave povezane z nudenjem blaga ali storitev posameznikom v Republiki Sloveniji, ne glede na to, ali je zanje potrebno plačilo, ali če so povezane s spremljanjem delovanja ali vedenja posameznikov, če to poteka v Republiki Sloveniji.

5. člen

(pomen izrazov)

(1) Izrazi, uporabljeni v tem zakonu, pomenijo enako kot izrazi, opredeljeni v 4. členu Splošne uredbe.

(2) Drugi izrazi, uporabljeni v tem zakonu, pomenijo:

1. »nadzorni organ« je Informacijski pooblaščenec, določen z zakonom, ki ureja Informacijskega pooblaščenca;
2. »nadzorne osebe« so informacijski pooblaščenec in nadzorniki za varstvo osebnih podatkov, kot jih določa zakon, ki ureja Informacijskega pooblaščenca, kadar izvajajo nadzor po določbah tega zakona;
3. »javni sektor« so državni organi, organi samoupravnih lokalnih skupnosti, nosilci javnih pooblastil v delu, kjer izvršujejo javna pooblastila, javne agencije, javni skladi, javni zavodi, univerze, samostojni visokošolski zavodi, zasebni vrtci in zasebne osnovne ter srednje šole, ki izvajajo javno veljavne vzgojno-izobraževalne programe, samoupravne narodne skupnosti, Svet romske skupnosti Republike Slovenije in druge osebe javnega prava, ustanovljene z zakonom;
4. »zasebni sektor« vključuje 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 samoupravne lokalne skupnosti ali samoupravne narodne skupnosti ali dejstvo, da so nosilci javnega pooblastila;
5. »povezovalni znak« je osebna identifikacijska številka in druge z zakonom opredeljene enolične identifikacijske številke posameznika, z uporabo katerih je mogoče zbrati oziroma priklicati osebne podatke iz zbirk osebnih podatkov, v katerih so enolične identifikacijske številke obdelovane ter druge podobne znake, ki se redno ali sistematično uporabljajo za povezovanje zbirk med različnimi upravljavci ali dveh ali več zbirk znotraj enega upravljavca;
6. »zadeva sodišča« je izvajanje sodne oblasti, kar vključuje sojenje in obravnavanje pravnih sredstev v sodnih zadevah iz pristojnosti sodišč s splošno pristojnostjo in specializiranih sodišč, kot jo določa zakon, ki ureja sodišča ali specializirana sodišča, ter o kateri odločajo sodišča v skladu z zakoni, ki urejajo sodne postopke, razen v kazenskih zadevah sodišč, kot jih določa zakon, ki ureja varstvo osebnih podatkov na področju obravnavanja kaznivih dejanj;

7. »zakon« je ta zakon, drugi zakoni, obvezujoče mednarodne pogodbe, ki zavezujejo Republiko Slovenijo, ter pravni akti ali odločitve Evropske unije, katerih določbe so enakovredne zakonom in neposredno uporabljive ali neposredno učinkovite;

8. »varnost države« je izvajanje nalog ali pooblastil v skladu z zakoni, ki urejajo izvajanje obveščevalnih in protiobveščevalnih dejavnosti ter obrambe države;

9. »kazenske evidence« so evidence, ki so določene v zakonu, ki ureja izvrševanje kazenskih sankcij;

10. »prekrškovne evidence« so evidence o pravnomočnih odločbah o prekrških, pravnomočnih sodb oziroma sklepov o prekrških in kazenskih točk, ki so določene v zakonu, ki ureja prekrške;

11. »storitev informacijske družbe« je katerakoli storitev, ki se običajno opravi odplačno, na daljavo (storitev se opravi, ne da bi bile stranke sočasno navzoče), elektronsko (storitev se pošlje na začetnem kraju in sprejme na cilju z elektronsko opremo za obdelavo in shranjevanje podatkov ter se v celoti prenaša, pošilja in sprejema po žici, radijsko, z optičnimi ali drugimi elektromagnetnimi sredstvi) in na posamezno zahtevo prejemnika storitev (storitev opravi s prenosom podatkov na posamezno zahtevo).

6. člen

(pravne podlage za obdelavo osebnih podatkov)

(1) Osebni podatki se lahko obdelujejo le in v obsegu, kadar je to v skladu s pravnimi podlagami za obdelavo osebnih podatkov iz prvega odstavka 6. in 9. člena Splošne uredbe.

(2) Obdelava osebnih podatkov v javnem sektorju in v zasebnem sektorju je zaradi izvajanja zakonske obveznosti, javnega interesa ali izvajanja javne oblasti v primerih iz točk c) in e) prvega odstavka ter drugega in tretjega odstavka 6. člena Splošne uredbe zakonita le, če obdelavo osebnih podatkov, vrste osebnih podatkov, ki naj se obdelujejo, kategorije posameznikov, na katere se ti osebni podatki nanašajo, namen njihove obdelave in rok hrambe osebnih podatkov ali rok za redni pregled potrebe po hrambi določa zakon. Če je mogoče, se v zakonu določi tudi uporabnike osebnih podatkov, posamezna dejanja obdelave in postopke obdelave ter druge ukrepe za zagotovitev zakonite, poštene in pregledne obdelave.

(3) V javnem sektorju se lahko v skladu s prvim odstavkom tega člena obdelujejo osebni podatki posameznika, ki je podal privolitev za obdelavo svojih osebnih podatkov za enega ali več določenih namenov, če takšno možnost določa zakon, sicer pa na podlagi privolitve, če ne gre za izvrševanje zakonskih pristojnosti, nalog ali oblastnih obveznosti javnega sektorja.

(4) Ne glede na določbe drugega odstavka tega člena se za izvrševanje točke e) prvega odstavka 6. člena Splošne uredbe lahko v javnemu sektorju izjemoma obdelujejo tisti osebni podatki, ki so potrebni za izvrševanje zakonitih pristojnosti, nalog ali obveznosti javnega sektorja, če se s to obdelavo ne poseže v upravičen interes posameznika, na katerega se osebni podatki nanašajo.

(5) Ne glede na določbo prvega odstavka tega člena je obdelava osebnega podatka o narodni ali etnični pripadnosti posameznika, na katerega se nanašajo osebni podatki, v javnem sektorju izjemoma dopustna, če to določa zakon, ki določa tudi privolitev posameznika, na katerega se nanašajo osebni podatki, ali če zakon določa obdelavo teh podatkov, glede katerih se posameznik svobodno opredeli. Z zakonom se obdelavo iz prejšnjega stavka določi za primere, ko je to nujno za odločitev o osebnem stanju, pravicah, spodbudah in ugodnostih za posameznika, na katerega se nanašajo osebni podatki ali za zagotavljanje in spodbujanje enakega obravnavanja, enakih možnosti ter zajamčenih posebnih pravic pripadnikov narodne ali etnične skupnosti v Republiki Sloveniji.

7. člen

(obdelava osebnih podatkov v druge namene)

Obdelava osebnih podatkov za drug namen kot za tistega, za katerega so bili zbrani (v nadaljnjem besedilu: nadaljnja obdelava), je v javnem sektorju in v zasebnem sektorju dopustna, če je to v skladu z določbami iz četrtega odstavka 6. člena Splošne uredbe. Kadar gre za nadaljnjo obdelavo, ki jo izvajajo upravljavci zaradi zakonske obveznosti ali v okviru svojih nalog v javnem interesu ali zaradi izvajanja javne oblasti, mora takšno obdelavo določati zakon v skladu z drugim odstavkom prejšnjega člena.

8. člen

(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 je 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, njen skrbnik, rejnik, oseba, ki ji je podeljena starševska skrb ali predstavnik zavoda, v katerega je nameščena mladoletna oseba. V primerih, ko pogoji poslovanja izvajalca storitev informacijske družbe predpisujejo višjo starost mladoletne osebe za uporabo storitev informacijske družbe, se upošteva starost iz navedenih pogojev poslovanja izvajalca storitev.

(2) Privolitev mladoletne osebe iz prvega odstavka tega člena ne sme biti pogojena s pretiranimi pogoji s strani upravljavca, tako da bi mladoletna oseba morala posredovati več osebnih podatkov, kot je potrebno za namen opravljanja takšne dejavnosti.

9. člen

(posebno varstvo osebnih podatkov umrlih posameznikov)

(1) Osebni podatki umrlih posameznikov se obdelujejo v skladu z zakonom.

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

(3) Ne glede na določbe prejšnjega odstavka upravljavec osebne podatke o umrlem posamezniku na njihovo zahtevo posreduje zakoncu, zunajzakonskemu partnerju ter partnerju v z njima izenačeni skupnosti, otrokom, staršem ali dedičem, če umrli posameznik ni pisno prepovedal upravljavcu posredovanja njegovih osebnih podatkov ali če drug zakon ne določa drugače.

(4) Če zakon ne določa drugače, lahko upravljavec podatke o umrlem posamezniku posreduje tudi drugi osebi, ki izkaže, da namerava te podatke uporabljati za namene znanstvenega raziskovanja, zgodovinskega raziskovanja, izobraževalne, statistične ali arhivske namene.

(5) Za obdelavo za namene iz prejšnjega odstavka ali v okviru izvajanja svobode izražanja se lahko obdelujejo zakonito pridobljeni osebni podatki umrlih posameznikov, če tako določa zakon, če je privolitev pred smrtjo dal posameznik sam ali če je za takšno obdelavo v času po smrti posameznika podana pisna privolitev naslednjih oseb v izključujočem vrstnem redu: zakonec ali partner iz zunajzakonske skupnosti ali partner v z njima z zakonom izenačeni skupnosti, otroci ali starši umrlega posameznika. Ne glede na določbe prejšnjega stavka se lahko za objavo ali drugo obdelavo v zgodovinskih in drugih izobraževalnih publikacijah obdelujejo zakonito pridobljeni osebni podatki umrlih posameznikov, če so bili umrli posamezniki javne osebe in če tega ne prepoveduje drug zakon.

(6) Določbe tega člena se uporabljajo za osebne podatke umrlih posameznikov 20 let po njihovi smrti, če drug zakon ne določa drugače.

10. člen

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

(1) Podatki o vpisu ali izbrisu v ali iz kazenskih evidenc in prekrškovnih evidenc ter prenosi teh podatkov se obravnavajo kot posebne vrste osebnih podatkov v skladu s prvim in drugim odstavkom 9. člena Splošne uredbe.

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

(3) Kazenske evidence in prekrškovne evidence se lahko samodejno povezujejo s Centralnim registrom prebivalstva. Povezovanje po tem odstavku se izvaja zaradi zagotavljanja točnosti in posodobljenosti osebnih podatkov v kazenskih evidencah in prekrškovnih evidencah, pri čemer mora biti zlasti zagotovljeno, da se osebni podatki iz evidenc in registra ne obdelujejo nepooblaščeno ali drugače nezakonito razkrivajo ali obdelujejo.

(4) Za izvedbo povezovanja iz prejšnjega odstavka se za državljana Republike Slovenije ali osebo s prebivališčem v Republiki Sloveniji kot identifikacijski znak uporabi enotna matična številka občana iz kazenske ali prekrškovne evidence.

(5) Povezovanje iz tretjega odstavka tega člena se izvede tako, da se osebni podatki določenega ali določljivega posameznika v kazenskih evidencah in prekrškovnih evidencah ob vsaki spremembi usklajujejo s podatki iz Centralnega registra prebivalstva oziroma tako, da se pri neusklajenih podatkih pojavi opozorilo, da je pri njegovih podatkih v drugi zbirki osebnih podatkov prišlo do spremembe ali da več ne obstajajo.

11. člen

(splošno sodno varstvo pravic posameznika)

(1) Posameznik, ki meni, da upravljavec ali obdelovalec iz javnega ali zasebnega sektorja krši njegove pravice, določene s Splošno uredbo ali z zakoni, ki urejajo obdelavo ali varstvo osebnih podatkov, lahko zahteva sodno varstvo svojih pravic ves čas, dokler kršitev traja, brez predhodnega uveljavljanja pravic po drugih določbah tega zakona ali uporabe drugih pravnih sredstev.

(2) Posameznik lahko s sodnim varstvom po določbah tega člena zahteva poleg prenehanja kršitve in vzpostavitve zakonitega stanja tudi povrnitev škode.

(3) Če je kršitev iz prvega odstavka tega člena prenehala, lahko posameznik s tožbo zahteva ugotovitev, da je kršitev obstajala.

(4) V postopku po prvem, drugem in tretjem odstavku tega člena odloča upravno sodišče po postopku, ki ga zakon, ki ureja upravni spor, določa za tožbo zaradi kršitve človekovih pravic in temeljnih svoboščin, posameznik pa lahko v tožbo vključi tudi odškodninski zahtevek.

(5) V postopku pred upravnim sodiščem je zaradi varstva podatkovne zasebnosti posameznika ali njegovega osebnega dostojanstva javnost izključena, če sodišče na predlog posameznika, na katerega se nanašajo osebni podatki, iz utemeljenih razlogov ne odloči drugače.

(6) Ta člen se ne uporablja za postopke proti upravljalcem ali obdelovalcem osebnih podatkov glede obdelav osebnih podatkov s področja varnosti države.

2. poglavje

Postopek pred upravljavcem in obdelovalcem

12. člen

(splošna določba)

V postopkih uveljavljanja pravic ali zahtev iz 15. do 22. člena Splošne uredbe pred upravljavcem in pred obdelovalcem, kadar deluje po desetem odstavku 28. člena Splošne uredbe, se uporabljajo določbe Splošne uredbe in tega poglavja.

13. člen

(postopkovne določbe za državne organe in organe samoupravnih lokalnih skupnosti)

(1) Upravljavci, ki so državni organi ali organi samoupravnih lokalnih skupnosti o pravici ali zahtevi posameznika iz 15. do 22. člena Splošne uredbe, tega ali drugega zakona odločajo s smiselno uporabo zakona, ki ureja splošni upravni postopek, če zakon ne določa drugače, v roku, določenem s Splošno uredbo. Odločba poleg sestavin, ki jih določa zakon, ki ureja splošni upravni postopek, vsebuje tudi sestavine, ki jih določa ta zakon, kadar upravljavec odloči, da se posamezniku posredujejo osebni podatki, ki se nanašajo nanj, mu jih pošlje skupaj z odločbo.

(2) Kadar pravici ali zahtevi posameznika ni ugodeno, mora biti v odločbi v pravnem pouku navedena pravica do pritožbe pri nadzornem organu v roku 15 dni od seznanitve z odločitvijo v zadevi, po določbah točke f) prvega odstavka 57. in 77. člena Splošne uredbe.

14. člen

(obravnavanje zahtevkov posameznika v javnem in zasebnem sektorju)

Kadar upravljavec, ki ni državni organ ali organ samoupravne lokalne skupnosti, obravnava zahtevke posameznika iz 15. do 22. člena Splošne uredbe in tega ali drugega zakona, posameznika seznani z odločitvijo in če je to predmet zahteve, z osebnimi podatki, ki se nanašajo nanj, v roku, določenem s Splošno uredbo. Če posameznik to zahteva, ga lahko z osebnimi podatki seznani tudi ustno. Odločitev mora vsebovati razloge, informacijo o pravici do pritožbe pri nadzornem organu v roku 15 dni od seznanitve z odločitvijo, po določbah točke f) prvega odstavka 57. in 77. člena Splošne uredbe. Odločitev ima lahko obliko uradnega zaznamka, ki se ga pošlje posamezniku na način, ki omogoča dokazovanje prejema.

15. člen

(sestavine odločbe)

(1) Če je to potrebno zaradi omejitev iz 17. člena tega zakona, odločba iz 13. člena tega zakona vsebuje tudi obseg dovoljenega pregleda spisa, zbirke ali drugače obdelanih lastnih osebnih podatkov.

(2) Ne glede na določbe 13. člena tega zakona odločba ne obsega konkretnih razlogov za zavrnitev ali omejitev dostopa, če bi to ogrozilo izvrševanje namena zavrnitve ali omejitve dostopa iz prvega odstavka 17. člena tega zakona.

(3) Odločba iz prejšnjega odstavka tudi ne obsega navedb, s katerimi bi se potrdilo ali zanikalo izvajanje ali neizvajanje prikritih preiskovalnih ukrepov iz zakona, ki ureja Slovensko obveščevalno-varnostno agencijo ali zakona, ki ureja obrambo.

(4) Konkretne razloge iz drugega odstavka upravljavec navede ločeno v prilogi k odločbi. Priloga, opremljena s številko zadeve, datumom in podpisom pristojne uradne osebe, je dostopna samo nadzornemu organu in pristojnemu sodišču. Priloga, opremljena s številko zadeve, datumom in podpisom pristojne uradne osebe, se ne vroča prijavitelju s posebnim položajem iz 29. člena tega zakona.

16. člen

(stroški seznanitve z osebnimi podatki)

(1) Informacije, sporočila, odgovori in ukrepanja upravljavca iz 15. do 22. člena Splošne uredbe ter glede izvajanja pravic iz tega ali drugega zakona se zagotavljajo brezplačno.

(2) Kadar so zahteve posameznika, na katerega se nanašajo osebni podatki, očitno neutemeljene ali pretirane, zlasti ker se ponavljajo, lahko upravljavec, kljub temu zahtevi ugodi, če je po vsebini utemeljena, in posamezniku zaračuna razumne stroške, pri čemer upošteva samo materialne stroške posredovanja informacij, sporočil, odgovorov oziroma izvajanja zahtevanega ukrepanja.

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

(4) Višino stroškov iz 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 minister, pristojen za pravosodje v soglasju z ministrom, pristojnim za zdravje, po predhodnem mnenju nadzornega organa.

(5) Če upravljavec ugotovi, da bodo nastali stroški v skladu z določbami tega člena, posameznika o tem vnaprej obvesti.

(6) Stroške ugotavljanja tehnične izvedljivosti prenosljivosti osebnih podatkov po 20. členu Splošne uredbe in stroške priprave podatkov ter njihovega neposrednega prenosa nosi upravljavec.

17. člen

(omejitev pravic in obveznosti)

(1) Z zakonom se lahko v skladu z razlogi in pogoji iz 23. člena Splošne uredbe izjemoma določijo omejitve pravic posameznika iz III. Poglavja in 34. člena Splošne uredbe, 1. poglavja tega zakona ali drugega zakona.

(2) Obveznosti in naloge upravljavcev ali obdelovalcev iz Splošne uredbe, tega ali drugega zakona, ki se nanašajo na varstvo ali obdelavo osebnih podatkov, se lahko omejijo v skladu z določbami prejšnjega odstavka.

18. člen

(posebna pravila glede načina uveljavljanja pravic ali zahtevkov na določenih področjih)

(1) Pravice ali drugi zahtevki posameznikov, na katere se nanašajo osebni podatki, se na področjih iz 72. do 74. člena tega zakona ne izvajajo v postopkih pred nadzornim organom po določbah tega zakona ali po določbah Splošne uredbe.

(2) Pravice in drugi zahtevki iz Splošne uredbe ter pravice zasebnosti v zvezi s področji iz 72. do 74. člena tega zakona se izvajajo v skladu z zakoni, ki urejajo ta področja, ter določbami tega zakona.

(3) Ne glede na določbe prvega in drugega odstavka tega člena nadzor nad zakonitostjo posredovanja, razkritja ali omogočanja nepooblaščenega dostopa do osebnih podatkov iz zbirke za namene iz četrtega odstavka 72. člena izvaja nadzorni organ.

(4) Če drug zakon v zadevi sodišča določa uresničevanje pravic s področja varstva osebnih podatkov iz Splošne uredbe, posameznik, na katerega se nanašajo osebni podatki, uresničuje te pravice le v obsegu in na način, kot je določeno z drugim zakonom.

(5) V postopku z zahtevo in pritožbo po 41., 42., in 45. členu zakona, ki ureja pacientove pravice, se uporabljajo določbe zakona, ki ureja pacientove pravice ter se smiselno uporabljajo določbe Splošne uredbe in tega zakona.

19. člen

(izjema glede uveljavljanja zahtevka posameznika preko zakonitega zastopnika)

Upravljavec lahko izjemoma zavrne zahtevo posameznika iz 15. do 22. člena Splošne uredbe ali dostop do osebnih podatkov iz posameznikove zdravstvene dokumentacije, ki je vložen 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. V tem primeru so razlogi za zavrnitev dostopni nadzornemu organu, Varuhu človekovih pravic, kolizijskemu skrbniku, kadar gre za osebne podatke iz zdravstvene dokumentacije, pa zastopniku pacientovih pravic po zakonu, ki ureja pacientove pravice.

20. člen

(zavarovanje osebnih podatkov, ki so predmet postopka)

(1) Upravljavec ali obdelovalec od prejema zahteve po tem zakonu ne sme izbrisati, odsvojiti ali spremeniti zahtevanih osebnih podatkov, ki so predmet postopka, dnevnikov obdelav in drugih povezanih informacij, ne glede na potek predpisanih ali interno določenih rokov hrambe, dokler o zadevi ni pravnomočno odločeno, po pravnomočnosti pa skladno s pravnomočno odločitvijo v zadevi.

(2) Ob upoštevanju okoliščin konkretnega postopka lahko nadzorni organ zaradi učinkovitega izvajanja poslovanja, nalog ali pooblastil upravljavca ali obdelovalca odredi izdelavo kopije osebnih podatkov ali kopije postopkov obdelave ali na drug način, ki ne otežuje poslovanja oziroma izvajanja nalog ali pooblastil upravljavca ali obdelovalca, zavaruje osebne podatke, ki so predmet postopka.

3. poglavje

Varnost osebnih podatkov in ocena učinka

21. člen

(vodenje dnevnikov obdelav)

(1) Zaradi učinkovitejšega izvajanja 2. in 3. oddelka IV. poglavja Splošne uredbe upravljavci po tem zakonu vodijo dnevnik obdelave, kadar se v avtomatiziranih sistemih obdelave osebnih podatkov izvajajo obsežne obdelave posebnih vrst osebnih podatkov, ali kadar gre za redno in sistematično spremljanje posameznikov, ali kadar je z oceno učinka ugotovljeno tveganje, ki ga je mogoče učinkovito upravljati z vodenjem dnevnika obdelave, ali če tako določa zakon, o naslednjih dejanjih obdelave osebnih podatkov:

1. zbiranje;
2. spreminjanje;
3. vpogled;
4. razkritje, vključno s prenosi;
5. povezovanje;
6. izbris,
7. druga dejanja obdelave, ki jih določa zakon.

(2) Dnevnik obdelave iz prejšnjega odstavka mora za dejanja vpogleda in razkritja osebnih podatkov vsebovati vrsto dejanja obdelave, datum in čas obdelave, identifikacijo osebe, ki je izvedla dejanje obdelave, ter identifikacijo uporabnikov osebnih podatkov, da je mogoče naknadno ugotoviti točno identiteto teh oseb. Dodatne vsebine dnevnika obdelave lahko določi upravljavec ob upoštevanju ocene učinka.

(3) Dnevnik obdelave se uporablja le za izkazovanje zakonitosti obdelave ter izvajanje notranjega nadzora, izvajanje nadzorov ali drugih zakonsko določenih preverjanj s strani nadzornega organa ali drugih pristojnih organov, zagotavljanje celovitosti in varnosti osebnih podatkov ter za odpravljanje napak v delovanju informacijskega sistema ali obdelavi podatkov.

(4) Upravljavec in obdelovalec nadzornemu organu ali drugemu zakonsko določenemu pristojnemu organu na njegovo zahtevo omogočita dostop do dnevnika obdelave.

(5) Vsebina dnevnika obdelave se hrani dve leti od zaključka koledarskega leta, v katerem so bila zabeležena dejanja obdelave, če drug zakon ne določa drugače. Kadar je z oceno učinka ali analize upoštevnih tveganj ugotovljeno tveganje, ki ga je mogoče učinkovito upravljati s podaljšanjem roka hrambe, se sme dnevnik obdelave hraniti največ pet let od zaključka koledarskega leta, v katerem so bila zabeležena dejanja obdelave. Kadar so za seznanitev s podatki iz dnevnika določene omejitve iz 17. člena tega zakona, se vsebina dnevnika obdelave hrani dve leti po prenehanju omejitev, če drug zakon ne določa drugače.

22. člen

(varnost osebnih podatkov na področju posebnih obdelav)

(1) Za obdelave osebnih podatkov:

1. določenih v zakonih, ki urejajo področja upravnih notranjih zadev, finančne uprave, državljanstva, Slovenske obveščevalno-varnostne agencije, obrambe, zdravstvenega varstva, obveznega zdravstvenega zavarovanja, uveljavljanja pravic iz javnih sredstev ter kazenskih in prekrškovnih evidenc, ali

2. kadar se na podlagi zakonov v zbirki osebnih podatkov obdelujejo osebni podatki več kot 100.000 posameznikov, ali
3. kadar upravljavec ali obdelovalec v zbirki osebnih podatkov obdeluje predvsem posebne vrste osebnih podatkov, ali
4. kadar se v zbirki osebnih podatkov obdeluje posebne vrste osebnih podatkov več kot 10.000 posameznikov, ali
5. v zasebnem sektorju, kadar se v zbirki osebnih podatkov obdelujejo osebni podatki več kot 200.000 posameznikov,

veljajo posebni ukrepi iz tega člena, s katerimi se dodatno zagotavlja varnost in tajnost osebnih podatkov ter človekove pravice in temeljne svoboščine posameznikov, na katere se podatki nanašajo.

(2) Obdelave iz prejšnjega odstavka se izvaja tako, da se sistemsko onemogoča razkritje osebnih podatkov ali obdelav nepooblaščenim osebam ali drugim subjektom, ki za njihov dostop nimajo pravne podlage in s tem stalno preprečuje škodo varnosti ter interesom Republike Slovenije.

(3) Za obdelave iz 1. do 4. točke prvega odstavka tega člena, ki jih izvajajo državni organi in organi samoupravnih lokalnih skupnosti, javne agencije in javni zavodi in ki vsebujejo biometrične osebne podatke ali zdravstvene osebne podatke ali podatke iz kazenskih in prekrškovnih evidenc, je prepovedana hramba v zasebnem računalniškem oblaku, kjer fizična lokacija hrambe teh podatkov ni znana v vseh fazah hrambe ter obdelave.

23. člen

(ocena učinka glede obdelav osebnih podatkov)

(1) Ocena učinka glede varstva osebnih podatkov in predhodno posvetovanje z nadzornim organom se izvajata skladno s 35. in v zvezi s 36. členom Splošne uredbe ter objavljenim seznamom nadzornega organa glede vrst dejanj obdelave, za katere velja zahteva po oceni učinka.

(2) Ocena učinka glede varstva osebnih podatkov in predhodno posvetovanje z nadzornim organom se izvajata tudi pred obdelavo osebnih podatkov iz prvega odstavka prejšnjega člena. Ocena učinka mora upoštevati okoliščine, določene v tretjem odstavku tega člena in možne škodljive posledice za varnost države, vključno z njenimi političnimi ali gospodarskimi koristmi, če bi bili obdelovani podatki razkriti nepooblaščenim osebam ali subjektom.

(3) Pred začetkom obdelave se oceno učinkov ponovno izdela tudi v naslednjih primerih:

1. kadar je bila spremenjena pravna podlaga za obdelavo iz 6. člena tega zakona;
2. kadar se uvajajo nova sredstva obdelave;
3. kadar se uvajajo nova dejanja obdelave, ki lahko pomenijo večje tveganje za varnost osebnih podatkov ali
4. kadar se spremeni narava, obseg, okoliščine oziroma namen obdelave osebnih podatkov večjega števila posameznikov, na katere se nanašajo osebni podatki, kar bi lahko povzročilo tveganje za človekove pravice in temeljne svoboščine posameznikov.

(4) Za izdelavo ocene učinka in za izvedbo ukrepov za obravnavanje tveganj je odgovoren predstojnik ali vodstveni organ upravljavca.

(5) Kadar se z zakonom določa obdelava osebnih podatkov, za katero je treba izdelati oceno učinka, predlagatelj predlogu zakona priloži oceno učinka v skladu s 35. členom Splošne uredbe. Na podlagi ocene učinka nadzorni organ izda mnenje glede obdelave osebnih podatkov, glede katerega se mora predlagatelj zakona opredeliti.

(6) Za obdelave osebnih podatkov na področju varnosti države, pristojni organ s področja varnosti države pripravi oceno učinka s smiselno uporabo določb tega člena. Ocena učinka je za potrebe nadzorov dostopna nadzornemu organu, Varuhu človekovih pravic in komisiji iz drugega odstavka 63. člena tega zakona.

4. poglavje

Postopki pred nadzornim organom

1. oddelek

Posebnosti postopka

24. člen

(uporaba določb zakona, ki ureja splošni upravni postopek)

V postopkih pred nadzornim organom po tem zakonu se uporabljajo določbe zakona, ki ureja splošni upravni postopek, če ta zakon ne določa drugače.

25. člen

(izvajanje postopkovnih dejanj brez prisotnosti)

(1) V postopkih pred nadzornim organom lahko nadzorni organ opravlja razgovore z osebami pri upravljavcu ali obdelovalcu in s pričami brez prisotnosti posameznika, na katerega se nanašajo osebni podatki, v celoti ali deloma, če bi takšna prisotnost škodovala izvedbi uradnih postopkov, varstvu ali uresničevanju človekovih pravic in temeljnih svoboščin tretjih oseb, o čemer nadzorni organ odloči s sklepom in o tem obvesti posameznika. V tem primeru nadzorni organ tudi ne dovoli prisotnosti pri drugih dejanjih v postopku in posameznika ne seznanja z vsebino dejanj.

(2) Nadzorni organ v zadevah s področja varnosti države opravlja razgovore z osebami pri upravljavcu ali obdelovalcu brez prisotnosti posameznika, na katerega se nanašajo osebni podatki, ter ne dovoli njegove prisotnosti pri drugih dejanjih v postopku in ga ne seznanja z vsebino dejanj.

(3) Proti sklepu iz prvega odstavka tega člena, s katerim se omeji prisotnost posameznika, na katerega se nanašajo osebni podatki, pri postopkovnih dejanjih po tem členu, ni pritožbe, sklep pa se sme izpodbijati skupaj z odločitvijo o glavni zadevi.

26. člen

(izključitev stranske udeležbe)

V postopkih pred nadzornim organom ni dopustna stranska udeležba, kot jo določa zakon, ki ureja splošni upravni postopek.

27. člen

(nadzorna pooblastila)

(1) Nadzorna pooblastila nadzornega organa so:

1. pregled dokumentacije upravljavca ali obdelovalca, ki se nanaša na obdelavo osebnih podatkov, ne glede na njeno zaupnost ali tajnost, ter prenos osebnih podatkov v tretjo državo in posredovanje osebnih podatkov tujim uporabnikom;

2. pregled poslovnih knjig, pogodb, listin, poslovnih evidenc in drugih podatkov, ki se nanašajo na obdelavo osebnih podatkov s strani upravljavca ali obdelovalca ali druge pravne ali fizične osebe po njunem pooblastilu oziroma na prenos osebnih podatkov v tretjo državo ali posredovanje uporabnikom osebnih podatkov iz tretjih držav s strani upravljavca ali obdelovalca oziroma druge pravne ali fizične osebe po njunem pooblastilu (v nadaljnjem besedilu: poslovne knjige in druga dokumentacija), ne glede na njihovo tajnost ali drugo vrsto zaupnosti ter ne glede na vrsto nosilca, na katerem so zapisani ali shranjeni;

3. vstop in pregled prostora, zemljišča, prevoznih sredstev (v nadaljnjem besedilu: prostori) ter opreme in sredstev za obdelavo osebnih podatkov (v nadaljnjem besedilu: oprema), v oziroma s katerimi upravljavec ali obdelovalec (v nadaljnjem besedilu: nadzorovani subjekt) sam ali drug poslovni subjekt ali posameznik po njihovem pooblastilu opravlja obdelavo osebnih podatkov, za katero izhaja verjetnost kršitve določb zakona, podzakonskih predpisov ali splošnih aktov za izvrševanje javnih pooblastil s področja varstva osebnih podatkov iz tega zakona;

4. zavarovanje in pregled poslovne korespondence, elektronskih in z njimi povezanih naprav ter nosilcev elektronskih podatkov, vključno s preko omrežja dosegljivimi informacijskimi sistemi, na katerih so shranjeni podatki (v nadaljnjem besedilu: elektronska naprava), za katere je verjetno, da so na njih podatki, glede katerih izhaja verjetnost kršitve določb zakona, podzakonskih predpisov ali drugih splošnih aktov za izvrševanje javnih pooblastil s področja varstva osebnih podatkov iz tega zakona;

5. odvzem ali pridobitev ustrezne kopije na stroške nadzorovanega subjekta, forenzične kopije ali izvlečka iz poslovnih knjig in druge dokumentacije v kakršni koli obliki z uporabo fotokopirnih sredstev ali računalniške opreme upravljavca ali obdelovalca oziroma nadzornega organa. Če zaradi tehničnih ali časovnih razlogov ni mogoče narediti kopij na kraju samem, se lahko poslovne knjige in druga dokumentacija odnesejo za čas, potreben, da se naredijo kopije, o čemer se naredi uradni zaznamek, če so osebni podatki označeni s stopnjo tajnosti, pa se naredijo le ustrezne kopije;

6. zapečatenje ustreznega dela prostorov in opreme, poslovnih knjig in druge dokumentacije ter elektronskih naprav za največ pet delovnih dni, v najmanjšem možnem obsegu, potrebnem za izvedbo nadzora, o čemer se naredi uradni zaznamek;

7. zaseg predmetov ter poslovnih knjig in druge dokumentacije za največ deset delovnih dni, če je to potrebno za izvedbo postopka, o čemer se izda potrdilo o zasegu, ki vsebuje navedbo zaseženih predmetov in njihov opis, navedbo kraja, kjer so bili najdeni, ter navedbo razloga za zaseg.

(2) Nadzorna oseba lahko odredi začasno zapečatenje oziroma blokiranje ustrezne opreme ali elektronske naprave le, če je to nujno, da se ohranijo možni dokazi, in če zapečatenje ali blokiranje opreme ali elektronske naprave ne onemogoča izvajanja rednega poslovanja, zakonskih nalog ali pristojnosti nadzorovanega upravljavca ali obdelovalca, vendar le za čas, dokler ni izdana sodna odredba iz prvega stavka tretjega odstavka tega člena oziroma do poteka roka za njeno izdajo iz drugega stavka tretjega odstavka tega člena.

(3) Nadzorna oseba izvaja nadzorna pooblastila iz 3. in 4. točke prvega odstavka tega člena pri pregledu poslovne korespondence, opreme ali elektronske naprave, ki bi posegel v upravičeno pričakovano zasebnost posameznika, le z njegovim soglasjem ali na podlagi predhodne pisne odredbe sodišča. O predlogu nadzorne osebe za izdajo odredbe iz prejšnjega stavka

preiskovalna sodnica ali preiskovalni sodnik (v nadaljnjem besedilu: preiskovalni sodnik) pri Okrožnem sodišču v Ljubljani odloči najpozneje v 48 urah od prejema predloga. Nadzorna oseba predlogu za izdajo odredbe priloži stališče nadzorovanega subjekta, do katerega se lahko tudi opredeli. Stališče nadzorovani subjekt poda najpozneje v 48 urah po pozivu nadzornega organa.

(4) Preiskovalni sodnik z odredbo odloči, da se pregled iz prejšnjega odstavka izvede, če obstajajo utemeljeni razlogi za sum, da je nadzorovani subjekt kršil ali krši določbe zakona, podzakonskih predpisov ali drugih splošnih aktov za izvrševanje javnih pooblastil s področja varstva osebnih podatkov iz tega zakona, in je verjetno, da se bodo pri pregledu opreme oziroma elektronskih naprav iz prejšnjega odstavka našli dokazi, pomembni za odločanje v postopku nadzora ali s tem postopkom povezanem prekrškovnem postopku. Odredba vsebuje:

1. opredelitev poslovne korespondence, opreme oziroma elektronskih naprav, ki jih je treba zavarovati in pregledati;
2. opredelitev razlogov za pregled;
3. opredelitev dokazov oziroma vsebine podatkov, ki se iščejo;
4. navedbo razlogov, ki utemeljujejo uporabo nadzornega pooblastila in način njegove izvršitve.

(5) Pregled poslovne korespondence, prostora ali elektronske naprave se opravi na način, s katerim se v najmanjši možni meri posega v pravice oseb, zoper katere ni uveden nadzor, in varuje tajnost oziroma zaupnost podatkov ter ne povzroča nesorazmerna škoda, kadar je izdana odredba preiskovalnega sodnika glede opreme ali elektronske naprave, pa tudi v skladu z njo. Za zavarovanje podatkov na elektronskih napravah se smiselno uporabljajo določbe zakona, ki ureja kazenski postopek glede zavarovanja podatkov v elektronski obliki. Predstavnik nadzorovanega subjekta ima pravico biti navzoč pri zavarovanju in pregledu poslovne korespondence, elektronske naprave ter pri pregledu prostora, pri pregledu poslovne korespondence, prostorov, elektronske naprave odvetnika ter prostorov, ki jih uporablja odvetnik, pa ima pravico biti navzoč tudi predstavnik Odvetniške zbornice Slovenije. Če določeno elektronsko napravo uporablja oseba, ki upravičeno pričakuje zasebnost na njej, ima pravico biti navzoča ob zavarovanju ali pregledu elektronske naprave sama ali po pooblaščencu. Če prostor uporablja druga oseba, ki upravičeno pričakuje zasebnost na njem, ima pravico biti navzoča ob zavarovanju ali pregledu sama ali po pooblaščencu, nadzorni organ pa pri pregledu zagotovi tudi prisotnost dveh polnoletnih prič.

(6) O opravljenem nadzoru se sestavi zapisnik, ki se lahko ne glede na določbe zakona, ki ureja splošni upravni postopek, kadar gre za nujne in neodložljive ukrepe, sestavi takoj, v drugih primerih pa najpozneje v treh dneh od dneva opravljenega nadzora ter se vroči nadzorovanemu subjektu ali njegovemu predstavniku ali vodstvu. Nadzorovani subjekt lahko na zapisnik poda pripombe v roku, ki ga določi nadzorna oseba in ne sme biti krajši od dveh delovnih dni po vročitvi zapisnika, o čemer se ga v zapisniku izrecno pouči. Določbe prejšnjega stavka ne veljajo za zapisnike, ki vsebujejo vsebine glede nujnih in neodložljivih ukrepov, nadzorovani subjekt pa lahko na tak zapisnik takoj ustno poda pripombe.

(7) Zoper odredbo preiskovalnega sodnika ni dovoljena pritožba, sme pa se izpodbijati v upravnem sporu zoper končno odločitev nadzornega organa.

(8) Kadar pri izvajanju pooblastil iz prvega do šestega odstavka tega člena nadzorna oseba obdeluje tudi tajne podatke ali poslovno skrivnost, upošteva tudi predpise, ki urejajo tajne podatke ali poslovno skrivnost.

(9) Pooblastila iz 58. člena Splošne uredbe se izvajajo v skladu z določbami tega člena.

(10) Nadzorna oseba lahko nadzorna pooblastila iz tega člena uporabi v postopkih obravnave prijave prijavitelja s posebnim položajem in v postopku inšpekcijskega nadzora po 3. oddelku tega poglavja.

28. člen

(nadzorni ukrepi)

(1) Kadar se pri opravljanju nadzora ugotovi kršitev določb zakona, podzakonskih predpisov ali splošnih aktov za izvrševanje javnih pooblastil glede na določbe 3. člena tega zakona v delih, ki urejajo varstvo osebnih podatkov, nadzorni organ lahko:

1. odredi, da se nepravilnosti ali pomanjkljivosti, ki jih ugotovi, odpravijo na način in v roku, ki ga sam določi;
2. odredi omejitve obdelave, kot so anonimiziranje, blokiranje ali arhiviranje;
3. odredi prepoved prenosa osebnih podatkov v tretjo državo ali njihovega posredovanja tujim uporabnikom osebnih podatkov, če se iznašajo ali posredujejo v nasprotju z določbami zakona;
4. odredi brisanje ali uničenje osebnih podatkov ali druge ukrepe, ki pomenijo prepoved obdelave osebnih podatkov, če ne gre za arhivsko gradivo, ki ga določa drug zakon;
5. odredi druge ukrepe skladno s tem zakonom, zakonom, ki ureja splošni upravni postopek ali zakonom, ki ureja varstvo podatkov na področju obravnavanja kaznivih dejanj;
6. izvaja preventivne ukrepe in izreka opozorila v skladu z zakonom, ki ureja inšpekcijski nadzor;
7. poda kazensko ovadbo oziroma izvede postopke v skladu z zakonom, ki ureja prekrške, če pri nadzoru ugotovi, da obstaja sum storitve kaznivega dejanja ali prekrška.

(2) Nadzorni organ pri opravljanju nadzora upošteva, da:

1. ponudnik izključnega prenosa (če se storitev informacijske družbe, ki jo opravlja, nanaša na prenos podatkov, ki jih zagotovi prejemnik storitve, v komunikacijskem omrežju ali na zagotovitev dostopa do komunikacijskega omrežja), ni odgovoren za poslane podatke, če ponudnik ne sproži prenosa, ne izbere prejemnika prenosa in ne izbere ali spremeni podatkov, ki so predmet prenosa;
2. ponudnik shranjevanja podatkov v predpomnilniku (če se storitev informacijske družbe, ki jo opravlja, nanaša na prenos podatkov v komunikacijskem omrežju, ki jih zagotovi prejemnik storitve), ni odgovoren za samodejno, vmesno in začasno shranjevanje teh podatkov, ki je namenjeno zgolj učinkovitejšemu posredovanju podatka drugim prejemnikom storitve na njihovo zahtevo, pod pogojem, da ponudnik ne spremeni podatkov in ponudnik hitro ukrepa in odstrani ali onemogoči dostop do podatka, ki ga je hranil, takoj ko je obveščen, da je bil podatek na začetnem izhodnem mestu prenosa odstranjen iz omrežja ali da je bil dostop do njega onemogočen;
3. ponudnik gostovanja (če se storitev informacijske družbe nanaša na shranjevanje podatkov, ki jih zagotovi prejemnik storitve) ni odgovoren za podatek, ki ga je shranil na zahtevo prejemnika storitve, pod pogojem, da prejemnik storitve ne ukrepa v okviru pooblastil ali pod nadzorom ponudnika, da ponudnik dejansko ne ve za nezakonito dejavnost ali podatek in mu glede podanih zahtevkov niso znana dejstva ali okoliščine iz katerih je očitno, da gre za nezakonito dejavnost ali podatek, ali da ponudnik, takoj ko za to izve ali se tega zave, nemudoma ukrepa in odstrani ali onemogoči dostop do podatka.

(3) V obsegu v katerem ponudnik iz prejšnjega odstavka ni odgovoren za podatke in njihovo shranjevanje in posredovanje, zoper njega ni mogoče odrediti ukrepov iz prvega odstavka tega člena.

(4) S pooblastili in ukrepi iz prejšnjega in tega člena nadzorni organ ne sme posegati v zadeve sodišč in zadeve Ustavnega sodišča Republike Slovenije, kadar Ustavno sodišče obravnava zadeve sodišč.

(5) Nadzorna oseba lahko nadzorne ukrepe iz tega člena uporabi v postopkih obravnave prijave prijavitelja s posebnim položajem po 2. oddelku tega poglavja in v postopku inšpekcijskega nadzora po 3. oddelku tega poglavja.

2. oddelek

Položaj prijavitelja s posebnim položajem

29. člen

(prijava in prijavitelj s posebnim položajem)

(1) Posameznik, ki meni, da obdelava njegovih osebnih podatkov s strani upravljavca ali obdelovalca krši določbe Splošne uredbe, tega zakona ali drugih zakonov, ki urejajo obdelavo ali varstvo osebnih podatkov, ali krši določbe s temi zakoni povezanih podzakonskih predpisov ali splošnih aktov za izvrševanje javnih pooblastil (v nadaljnjem besedilu: prijavitelj s posebnim položajem), lahko pri nadzornem organu vloži zahtevo v skladu z zakonom, ki ureja splošni upravni postopek, s katero zahteva nadzor zakonitosti obdelave svojih osebnih podatkov (v nadaljnjem besedilu: prijava), lahko pa v njej predlaga tudi potrebno ukrepanje v skladu z 28. členom tega zakona v primeru ugotovljenih kršitev, tako da se doseže vzpostavitev zakonitega stanja.

(2) V postopku po tem oddelku vsaka stranka krije svoje stroške postopka.

30. člen

(obravnavanje prijave)

(1) V primeru prijave prijavitelja s posebnim položajem nadzorni organ uvede postopek nadzora, ko prijava vsebuje sestavine, kot jih za vlogo določa zakon, ki ureja splošni upravni postopek, ter navedbo upravljavca ali obdelovalca in navedbo kršitev pri obdelavi ali varnosti njegovih osebnih podatkov, iz katerih izhaja kršitev predpisov iz prejšnjega člena.

(2) Nadzorni organ o prijavi odloči z odločbo najpozneje v roku treh mesecev po prejemu prijave. Rok lahko nadzorni organ zaradi zahtevnosti obravnavanja zadeve s sklepom podaljša za največ en mesec.

31. člen

(pravice prijavitelja s posebnim položajem)

(1) Nadzorni organ prijavitelja s posebnim položajem na njegovo zahtevo obvešča o bistvenih dejanjih v postopku in stanju zadeve, razen ko se prijava nanaša na obdelave osebnih podatkov s področja varnosti države.

(2) Nadzorni organ pred izdajo odločbe prijavitelju vroči zapis ugotovitev, bistvenih za odločitev v tem postopku, in ga pozove, naj se v določenem roku, ki ne sme biti krajši od dveh delovnih dni, pisno ali ustno o njih izjavi, o čemer se nadzorni organ opredeli v odločbi. Zapis ugotovitev ne

vsebuje razlogov in navedb, ko so izpolnjeni pogoji iz drugega odstavka 15. člena tega zakona. Če se prijavitelj v določenem roku ne izjavi, to ni ovira za izdajo odločbe.

32. člen

(položaj nadzorovanega upravljavca ali obdelovalca)

(1) Pri izvajanju nadzora po določbah tega oddelka ima nadzorovani upravljavec ali obdelovalec položaj stranke in ima pravico biti neposredno prisoten pri vseh postopkovnih dejanjih.

(2) Nadzorni organ pred izdajo odločbe nadzorovanemu upravljavcu ali obdelovalcu vroči zapis ugotovitev, bistvenih za odločitev v tem postopku, in ga pozove, naj se v določenem roku, ki ne sme biti krajši od dveh delovnih dni, pisno ali ustno o njih izjavi, o čemer se nadzorni organ opredeli v odločbi. Če se upravljalec ali obdelovalec v določenem roku ne izjavi, to ni ovira za izdajo odločbe.

33. člen

(odločba)

(1) Odločba v postopku nadzora po določbah tega oddelka poleg sestavin, ki jih določa zakon, ki ureja splošni upravni postopek, vsebuje:

1. ugotovitev o obstoju ali neobstoju zatrjevane kršitve obdelave osebnih podatkov prijavitelja s posebnim položajem v trenutku vložitve prijave;
2. ukrepe, odrejene upravljavcu ali obdelovalcu glede obdelave osebnih podatkov, ki se nanašajo na prijavitelja s posebnim položajem, in rok za njihovo izvedbo;
3. dovoljen obseg pregleda spisa zadeve za prijavitelja s posebnim položajem.

(2) Ne glede na prejšnji odstavek v primerih iz 15. člena tega zakona odločba ne obsega konkretnih razlogov za zavrnitev ali omejitev dostopa, če bi to ogrozilo izvrševanje namena zavrnitve ali omejitve dostopa iz 23. člena Splošne uredbe, ki ga določa zakon. Odločba tudi ne obsega navedb, s katerimi bi se potrdilo ali zanikalo izvajanje ali neizvajanje prikritih preiskovalnih ukrepov iz zakona, ki ureja Slovensko obveščevalno varnostno agencijo ali zakona, ki ureja obrambo.

(3) Konkretne razloge iz prvega stavka prejšnjega odstavka nadzorni organ navede ločeno v prilogi k odločbi. Priloga, opremljena s številko zadeve, datumom in podpisom pristojne uradne osebe, se ne vroča prijavitelju s posebnim položajem.

34. člen

(ukrepanje glede obdelav osebnih podatkov drugih posameznikov)

Kadar nadzorni organ v postopku nadzora zazna sum kršitve varstva pravic glede osebnih podatkov po določbah tega oddelka, ki bi lahko vplivale na pravice drugih posameznikov, na katere se nanašajo osebni podatki, uvede tudi postopek nadzora po določbah naslednjega oddelka.

3. oddelek

Inšpekcijski nadzor glede varstva osebnih podatkov

35. člen

(uporaba zakona, ki ureja inšpekcijski nadzor)

V postopku inšpekcijskega nadzora po tem oddelku se uporabljajo določbe 17. člena, določbe 25. do 28. člena ter 33. člena tega zakona. Za vprašanja inšpekcijskega nadzora, ki niso urejena z določbami 17. člena in 25. do 28. člena tega zakona, se uporabljajo določbe zakona, ki ureja inšpekcijski nadzor.

36. člen

(uvedba inšpekcijskega nadzora)

(1) Nadzorni organ uvede inšpekcijski nadzor v skladu z določbami zakona, ki ureja inšpekcijski nadzor.

(2) Nadzorni organ uvede inšpekcijski nadzor tudi na pobudo, ki jo prejme od drugega državnega organa, nadzornih javnih agencij Republike Slovenije ali nadzornega organa za varstvo osebnih podatkov države članice Evropske unije ali Sveta Evrope.

37. člen

(letni načrt nadzorov in poročanje)

(1) Nadzorni organ v letnem načrtu nadzorov posebej opredeli nadzore na področju posebnih obdelav iz 22. člena tega zakona.

(2) O izvedbi nadzorov iz prejšnjega odstavka nadzorni organ letno poroča v letnem poročilu Informacijskega pooblaščenca, po zakonu, ki ureja informacijskega pooblaščenca.

5. poglavje

Posebne določbe

38. člen

(posredovanje osebnih podatkov, ki ga izvedejo osebe javnega sektorja)

(1) Osebe javnega sektorja posredujejo osebne podatke drugim osebam javnega sektorja ali drugim fizičnim ali pravnim osebam, če je za posredovanje podana pravna podlaga v skladu s 6. členom tega zakona. Prejemnik podatkov sme osebne podatke obdelovati samo za namen, za uresničevanje katerega se ji posredujejo.

(2) Posredovanje posebnih vrst osebnih podatkov ter osebnih podatkov iz 10. člena tega zakona je dovoljeno, če so izpolnjeni pogoji iz prvega odstavka tega člena in je to v skladu z drugim odstavkom 9. člena Splošne uredbe ali drugim odstavkom 10. člena tega zakona.

(3) Osebe javnega sektorja v skladu s prvim in drugim odstavkom tega člena posredujejo osebne podatke brezplačno, če zakon ne določa drugače.

(4) Ne glede na določbe prejšnjih odstavkov tega člena upravljavci registra stalnega prebivalstva, matičnega registra, registra registriranih vozil in centralnega registra prebivalstva na način, ki je določen za izdajo potrdila, posredujejo upravičencu, ki izkaže zakoniti 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.

(5) Upravljavci ali obdelovalci, katerim se na podlagi zakona za izvajanje svojih pristojnosti ali nalog posredujejo osebni podatki 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.

(6) Ne glede na določbe prvega do četrtega odstavka tega člena se posredovanje osebnih podatkov s področja varnosti države ureja v zakonih, ki urejajo izvajanje obveščevalnih in protiobveščevalnih nalog.

39. člen

(posredovanje podatkov, ki ga izvajajo osebe zasebnega sektorja)

(1) Osebe zasebnega sektorja posredujejo osebne podatke drugim fizičnim ali pravnim osebam ali osebam javnega sektorja samo na podlagi zahteve iz prvega odstavka 40. člena tega zakona, iz katere izhaja veljavna pravna podlaga za pridobitev podatkov ter utemeljenost zahteve, razen če zakon določa drugače.

(2) Osebe zasebnega sektorja posredujejo osebne podatke osebam javnega sektorja brezplačno, razen če zakon določa drugače.

40. člen

(postopek posredovanja osebnih podatkov)

(1) Če zakon ne določa drugače, zahteva za posredovanje osebnih podatkov vsebuje naslednje podatke:

1. podatke o vlagatelju zahteve (za fizično osebo: osebno ime, 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 vlagatelja oziroma 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 ter navedbo organa ali drugega subjekta, ki obravnava zadevo;
5. vrste osebnih podatkov, ki naj se mu posredujejo,
6. obliko in način pridobitve zahtevanih osebnih podatkov.

(2) Upravljavec vlagatelju zahteve, če zakon ne določa drugačnega načina, 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. Upravljavec in vlagatelj zahteve se v roku iz prejšnjega stavka lahko dogovorita za njegovo podaljšanje.

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

(4) 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 nadzorni organ. Kadar ta zavrne zahtevo ali kadar na prvi stopnji odloča nadzorni organ sam, lahko vlagatelj 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.

(5) 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.

(6) Upravljavec za vsako posredovanje osebnih podatkov zagotovi možnost poznejše ugotovitve, kateri osebni podatki so bili posredovani, komu, kdaj in na kateri pravni podlagi, za kateri namen oziroma iz katerih razlogov oziroma za potrebe katerega postopka, razen če zakon za posredovanje posameznih vrst podatkov določa drugače oziroma je to razvidno iz dnevnika obdelave po 21. členu tega zakona.

(7) Informacije iz prejšnjega odstavka upravljavec hrani dve leti, razen če zakon za posredovanje posameznih vrst podatkov določa drugačen rok.

(8) Šesti in sedmi odstavek tega člena veljata tudi za obdelovalce, če so z zakonom, pogodbo ali drugim dogovorom zavezani posredovati določene osebne podatke.

(9) Šesti in sedmi odstavek tega člena ne veljata za osebne podatke, ki jih upravljavec zakonito objavi na svojih spletnih straneh ali na drug ustrezen način in osebne podatke za katere ta ali drug zakon določa, da so javni ali javno dostopni.

41. člen

(uporaba povezovalnih znakov)

(1) Pri pridobivanju osebnih podatkov iz zbirk osebnih podatkov s področja zdravstva, varnosti države, sodstva, kazenskih 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 storilca ali kaznivo dejanje, ki se preganja po uradni dolžnosti ali 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 notranjim aktom o varnosti osebnih podatkov ter ob upoštevanju določb o sledljivosti obdelav osebnih podatkov iz drugega in tretjega odstavka 21. člena tega zakona.

(4) Prvi odstavek tega člena se ne uporablja za povezovanje kazenskih in prekrškovnih evidenc z drugimi zbirkami. Prav tako se prvi odstavek tega člena ne uporablja za povezovanje zemljiške knjige, sodnega registra in poslovnega registra z drugimi zbirkami, če tako določa zakon.

42. člen

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

(1) Rok hrambe osebnih podatkov je 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 se upoštevajo določbe prejšnjega odstavka.

(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, njihovo blokiranje ali njihovo arhiviranje.

6. poglavje

Pooblaščene osebe za varstvo osebnih podatkov

43. člen

(pooblaščena oseba za varstvo osebnih podatkov)

Pooblaščena oseba za varstvo osebnih podatkov (v nadaljnjem besedilu: pooblaščena oseba) je oseba, ki upravljavcu ali obdelovalcu v skladu z 39. členom Splošne uredbe na neodvisen način svetuje pri zagotavljanju skladnosti obdelave s Splošno uredbo in z zakonom.

44. člen

(obveznost določitve pooblaščene osebe)

(1) Pooblaščeno osebo določijo upravljavci in obdelovalci v skladu s prvim odstavkom 37. člena Splošne uredbe in vsi upravljavci in obdelovalci v javnem sektorju ter upravljavci in obdelovalci ki obdelujejo osebne podatke iz 1. do 4. točke prvega odstavka 22. člena tega zakona.

(2) Ne glede na določbe prejšnjega odstavka lahko drugi upravljavci ali obdelovalci 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 opravlja za ta čas naloge pooblaščene osebe in ima vsa pooblastila in upravičenja v skladu z 38. in 39. členom Splošne uredbe in tem zakonom.

(4) Upravljavec ali obdelovalec v osmih dneh od določitve pooblaščene osebe vpiše njene kontaktne podatke v skladu s 30. členom Splošne uredbe v svojo evidenco dejavnosti obdelav in njen kontakt javno objavi na primeren način, zlasti na spletnih straneh. V istem roku kontaktne podatke pooblaščene osebe in njenega morebitnega namestnika (osebno ime, delovno mesto pooblaščene osebe, naziv upravljavca ali obdelovalca, telefonska številka, naslov elektronske pošte pooblaščene osebe) sporoči nadzornemu organu, ki jih vključi v seznam pooblaščenih oseb. Seznam ni dostopen javnosti.

45. člen

(pogoji za določitev pooblaščene osebe)

(1) Za pooblaščeno osebo upravljavca ali obdelovalca in njenega namestnika se lahko določi posameznika, ki izpolnjuje naslednje pogoje:

1. je poslovno sposoben,
2. ima znanja oziroma praktične izkušnje s področja varstva osebnih podatkov,
3. ni bil pravnomočno obsojen na kazen zapora najmanj šestih mesecev oziroma ni bil pravnomočno obsojen za kaznivo dejanje glede zlorabe osebnih podatkov ali prevzema identitete druge osebe.

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

(3) Upravljavci ali obdelovalci iz javnega sektorja, razen državnih organov, lahko določijo drugo pooblaščeno osebo, če je ni mogoče določiti znotraj osebe javnega sektorja. V primeru iz prejšnjega stavka lahko pooblaščeno osebo določijo skupaj z drugimi upravljavci ali obdelovalci javnega sektorja, lahko pa s pogodbo v pisni obliki določijo tudi posameznika ali posameznico iz zasebnega sektorja ali pravno osebo iz zasebnega sektorja v skladu s četrtim odstavkom tega člena.

(4) 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 posameznik, ki odgovarja za delo pravne osebe kot pooblaščene osebe in katerega kontaktni podatki se objavijo v skladu s četrtim odstavkom prejšnjega člena. Posameznik iz prejšnjega stavka mora izpolnjevati pogoje iz prvega odstavka tega člena.

(5) Za pooblaščeno osebo in njenega namestnika v javnem in zasebnem sektorju, se ne sme določiti osebe, ki so v nasprotju interesov z upravljavcem ali obdelovalcem ali bi bilo njihovo delo kot pooblaščene osebe v nasprotju z njegovimi drugimi nalogami ali s položajem pri upravljavcu ali obdelovalcu.

(6) V javnem sektorju se šteje, da je določena oseba v nasprotju interesov, če je določena kot upravljavec informacijskega sistema, skrbnik informacijskega sistema ali vodja informacijske varnosti 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 okoliščine, ki predstavljajo ali bi lahko predstavljale nasprotje interesov, o tem takoj pisno obvesti upravljavca oziroma obdelovalca. Upravljavec oziroma obdelovalec v tem primeru odpravi nasprotje ali pooblaščeno osebo razreši opravljanja določene naloge kot pooblaščene osebe. Enako velja tudi za namestnika pooblaščene osebe. Določbe tega odstavka se smiselno uporabljajo za zasebni sektor.

46. člen

(skupna določitev pooblaščene osebe)

(1) Več upravljavcev oziroma obdelovalcev lahko ob upoštevanju svoje organizacijske strukture in velikosti določi skupno pooblaščeno osebo in njenega namestnika.

(2) Odvetniki in odvetniške družbe lahko v dogovoru z Odvetniško zbornico Slovenije določijo skupno pooblaščeno osebo.

(3) Notarji lahko v dogovoru z Notarsko zbornico Slovenije določijo skupno pooblaščeno osebo.

47. člen

(naloge pooblaščene osebe)

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

(2) Pooblaščena oseba sodišča ali Ustavnega sodišča Republike Slovenije ne sme opravljati nalog iz prejšnjega odstavka v zvezi z obdelavami osebnih podatkov v konkretnih zadevah sodišč ali zadev Ustavnega sodišča, kadar Ustavno sodišče obravnava zadeve sodišč.

48. člen

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

(1) Vrhovno sodišče Republike Slovenije 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.

(2) 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 in Državnotožilski svet.

(3) Vsak minister ali ministrica (v nadaljnjem besedilu: minister) določi pooblaščeno osebo, ki je zaposlena na tem ministrstvu, v primeru ministrstva brez listnice pa na organu ali v službi ministra. Če je v okviru ministrstva ustanovljen organ v sestavi, minister za pooblaščeno osebo organa v sestavi določi javnega uslužbenca, ki je zaposlen v organu v sestavi ali na tem ministrstvu.

(4) Predstojnik organa s področja varnosti države določi pooblaščeno osebo in njenega namestnika znotraj organa. Pooblaščena oseba tega organa opravlja tiste naloge iz 39. člena Splošne uredbe, za katere tako določi predstojnik, obvezno pa opravlja naloge glede zagotavljanja varnosti osebnih podatkov, posredovanja osebnih podatkov Vladi Republike Slovenije, Predsedniku Republike Slovenije, policiji, državnim tožilstvom, sodiščem, pristojnemu delovnemu telesu Državnega zbora Republike Slovenije (v nadaljnjem besedilu: državni zbor) in drugim subjektom ter glede čezmejnih obdelav in prenosov osebnih podatkov.

(5) Pooblaščeno osebo upravne enote ali skupno pooblaščeno osebo več upravnih enot določi ministrstvo, pristojno za javno upravo. Po dogovoru z ministrstvom lahko tudi upravne enote določijo pooblaščene osebe. Pooblaščena oseba upravne enote mora biti zaposlena v ministrstvu, pristojnem za javno upravo ali v upravni enoti.

49. člen

(dolžnost varstva tajnosti osebnih podatkov)

Pooblaščena oseba in namestnik sta pri opravljanju dela in po njegovem zaključku zavezana k varstvu tajnosti obdelovanih osebnih podatkov. Pridobljene informacije smeta uporabljati izključno za opravljanje nalog pooblaščene osebe.

7. poglavje

Kodeksi ravnanja in potrjevanje

50. 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. Kodekse potrjujejo nadzorni organ, Evropski odbor za varstvo podatkov po 68. členu Splošne uredbe (v nadaljnjem besedilu: 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 nadzornemu organu.

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

(4) Če nadzorni organ 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 nadzorni organ, 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) Upravljavec je ob predložitvi osnutka kodeksa nadzornemu organu dolžan izkazati, ali se vsebina kodeksa nanaša na več držav članic Evropske unije. Če nadzorni organ 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 pravnomočnosti odločbe vpiše v seznam potrjenih kodeksov, ki ga upravlja na svojih spletnih straneh, 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. Če Odbor osnutka kodeksa v svojem mnenju ne potrdi, nadzorni organ nadaljuje postopek in z odločbo zavrne osnutek kodeksa. Če Odbor osnutek kodeksa potrdi, nadzorni organ nadaljuje postopek, z odločbo potrdi kodeks in ga po pravnomočnosti odločbe vpiše v seznam potrjenih kodeksov na svojih spletnih straneh in objavi v Uradnem listu Republike Slovenije.

51. člen

(potrjevanje)

(1) Potrjevanje 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 potrjevanja. O ugotovitvi takšne skladnosti se upravljavcu ali obdelovalcu izda certifikat.

(2) Za potrjevanje se uporabljajo merila, ki jih v skladu s petim odstavkom 42. člena Splošne uredbe odobri nadzorni organ 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 nadzornega organa v skladu z določbami tega zakona ali Splošne uredbe.

(4) Nadzorni organ upravlja seznam odobrenih potrjevalnih mehanizmov in ga sproti objavlja na svoji spletni strani.

52. člen

(postopek akreditiranja teles za potrjevanje)

(1) Potrjevanje izvajajo telesa, ki jih na podlagi njihove vloge za to akreditira nacionalni akreditacijski organ (v nadaljnjem besedilu: 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 nadzorni organ, skladno z njimi pa v okviru postopka akreditacije preverja Slovenska akreditacija.

(2) Slovenska akreditacija izda akreditacijsko listino potrjevalnemu telesu in o tem obvesti nadzorni organ. Zoper izdano akreditacijsko listino je dovoljena pritožba v skladu z zakonom, ki ureja akreditacijo, zoper odločitev o pritožbi pa je dopusten upravni spor.

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

8. poglavje

Nadzorni organ za varstvo osebnih podatkov Republike Slovenije

53. člen

(nadzorni organ za varstvo osebnih podatkov)

(1) Nadzor nad izvajanjem določb Splošne uredbe in tega zakona izvaja Informacijski pooblaščenec kot nadzorni organ za varstvo osebnih podatkov Republike Slovenije.

(2) Zoper odločitve nadzornega organa ni dovoljena pritožba, je pa dopusten upravni spor v skladu z zakonom, ki ureja upravni spor.

54. člen

(pristojnosti nadzornega organa)

(1) Nadzorni organ:

1. izvaja nadzore nad izvajanjem določb Splošne uredbe, tega zakona in drugih zakonov, podzakonskih predpisov ali drugih splošnih aktov za izvrševanje javnih pooblastil glede obdelav osebnih podatkov s področij iz 1. člena tega zakona;
2. odloča v pritožbenem postopku, odloča v postopkih prijav prijaviteljev s posebnim položajem in izvaja inšpekcijski nadzor po tem zakonu;
3. daje predhodna mnenja ministrstvom, državnemu zboru, organom samoupravnih lokalnih skupnosti, drugim državnim organom in nosilcem javnih pooblastil o usklajenosti določb predlogov zakonov ter ostalih predpisov z zakoni in drugimi predpisi, ki urejajo osebne podatke s področij iz 1. člena tega zakona; ministrstva in drugi organi posredujejo predloge zakonov in drugih predpisov pravočasno v mnenje nadzornemu organu;
4. izvaja predhodno posvetovanje v skladu s Splošno uredbo in tem zakonom;
5. daje pristojnim organom in posameznikom neobvezna mnenja, pojasnila in stališča o vprašanjih glede varstva osebnih podatkov v zvezi z zakoni in povezanimi predpisi, v skladu s 1. členom tega zakona;
6. spodbuja ozaveščenost in razumevanje javnosti o tveganjih, pravilih, zaščitnih ukrepih in pravicah v zvezi z obdelavo in za ta namen izvaja brezplačna izobraževanja in usposabljanja;
7. spodbuja ozaveščenost upravljavcev in obdelovalcev o njihovih obveznostih na podlagi tega zakona;
8. sodeluje z nadzornimi organi drugih držav ali mednarodnih organizacij;

9. sodeluje z nadzornimi organi drugih držav članic Evropske unije pri izvajanju čezmejnih nadzornih postopkov, postopkih izrekanja sankcij ter v drugih zadevah čezmejne obdelave osebnih podatkov v skladu s VII. poglavjem Splošne uredbe;
10. deluje kot vodilni nadzorni organ pri izvajanju čezmejnih nadzornih postopkov v skladu s Splošno uredbo;
11. sodeluje pri delovanju Evropskega odbora za varstvo osebnih podatkov;
12. pripravi letno poročilo o izvajanju tega zakona;
13. obvesti pristojno sodišče o kršitvah zakona, lahko pa sodišču v sodnem postopku tudi posreduje mnenje o ugotovljenih kršitvah;
14. sodeluje z upravljavci in obdelovalci pri izvajanju nadzorov v skladu z določbami tega zakona;
15. olajša postopek vložitve pritožb in zahtev iz drugega odstavka 13, drugega odstavka 14. in četrtega odstavka 18. člena tega zakona, zahtev iz 29. člena tega zakona in drugih vlog v postopku inšpekcijskega nadzora iz 36. člena tega zakona, in sicer tako, da pripravi obrazce, ki se lahko vložijo tudi v elektronski obliki;
16. je prekrškovni organ, pristojen za nadzor glede izvajanja določb Splošne uredbe v zvezi s prekrški iz 83. člena Splošne uredbe, tega zakona, drugih zakonov ali predpisov, ki urejajo varstvo osebnih podatkov;
17. izvaja druge naloge, določene v 57. členu Splošne uredbe in v tem zakonu.

(2) Nadzorni organ izvaja pristojnosti in naloge iz prejšnjega odstavka brezplačno.

(3) Nadzore po tem zakonu izvajajo nadzorne osebe, pri nadzoru pa lahko sodeluje strokovno osebje nadzornega organa.

55. člen

(javnost dela)

(1) Nadzorni organ lahko poleg nalog iz 57. člena Splošne uredbe:

1. izdaja notranje glasilo ter strokovno literaturo;
2. na spletnih straneh ali na drug primeren način objavlja odločbe ali mnenja;
3. na spletnih straneh oziroma na drug primeren način objavlja odločbe in sklepe Ustavnega sodišča Republike Slovenije o zahtevah ocene ustavnosti, ki jih je vložil nadzorni organ ter odločitve Ustavnega sodišča Republike Slovenije o njih;
4. na spletnih straneh oziroma na drug primeren način objavlja odločbe in sklepe sodišč s splošno pristojnostjo, upravnega sodišča, Vrhovnega sodišča ter dokončne odločbe in sklepe nadzornega organa, 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. na spletnih straneh objavlja psevdonimizirane pomembnejše odločitve v nadzornih in pritožbenih postopkih;
6. na spletnih straneh objavlja podatke o uvedbi in zaključku nadzornih postopkov, uvedenih po uradni dolžnosti;

7. daje mnenja o skladnosti splošnih pogojev poslovanja oziroma njihovih predlogov s predpisi s področja varstva osebnih podatkov;
8. daje neobvezna mnenja, pojasnila in stališča o vprašanjih s področja varstva osebnih podatkov in jih objavlja na spletnih straneh ali na drug primeren način;
9. pripravlja in daje neobvezne smernice in priporočila glede varstva osebnih podatkov na posameznem področju;
10. daje izjave za javnost o nadzoru v posamičnih zadevah v skladu s tem zakonom;
11. izvaja konference za medije v zvezi z delom nadzornega organa ter prepise izjav ali posnetke izjav s konferenc za medije objavi na spletnih straneh;
12. na spletnih straneh objavlja druga pomembna obvestila.

(2) Nadzorni organ lahko za opravljanje nalog iz 7., 8., in 9. točke prejšnjega odstavka povabi k sodelovanju tudi predstavnike društev in drugih nevladnih organizacij s področja človekovih pravic in temeljnih svoboščin in potrošnikov ter strokovnjake določenih strok, povezanih s prej navedenimi področji.

56. člen

(omejitve pri izvajanju nadzorov)

(1) Nadzorne osebe niso pristojne za nadzor in izrekanje sankcij glede 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) Nadzorne osebe niso pristojne za nadzor in izrekanje sankcij glede obdelav osebnih podatkov, izvedenih v okviru neodvisnega sodniškega odločanja Ustavnega sodišča Republike Slovenije v zadevah odločanja iz prejšnjega odstavka.

(3) Nadzorne osebe niso pristojne za nadzor in izrekanje sankcij glede obdelav osebnih podatkov s strani stečajnih upraviteljev, izvršiteljev, sodnih tolmačev, sodnih izvedencev in sodnih cenilcev, v zadevah, v katerih po odredbi sodišča delujejo v postopkih iz prvega odstavka tega člena.

(4) Nadzorne osebe pri opravljanju nadzora in izrekanju sankcij ne smejo zabeležiti, kopirati, prepisati ali drugače prevzeti identifikacijskih osebnih podatkov oziroma kopirati nobene dokumentacije glede:

1. obdelav osebnih podatkov na področjih obveščevalno-varnostne dejavnosti v delu, kjer je izvedena identifikacija tajnih delavcev oziroma sodelavcev v skladu z zakonom, ki ureja obrambo, ali zakonom, ki ureja Slovensko obveščevalno-varnostno agencijo,
2. obdelav osebnih podatkov varnostno preverjanih oseb v skladu z zakonom, ki ureja tajne podatke, v delu, kjer je izvedena identifikacija 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,
3. obdelav osebnih podatkov pobudnikov v postopkih na podlagi zakona, ki ureja Varuha človekovih pravic ali drugimi zakoni, ki urejajo njegove pristojnosti, drugih posameznikov, kadar je Varuh človekovih pravic postopek začel na lastno pobudo in posameznikov, za katere je Varuh človekovih pravic vložil ustavno pritožbo, v delu kjer je izvedena njihova identifikacija.

(5) Ne glede na določbe prejšnjega odstavka lahko nadzorne osebe na področjih iz prejšnjega odstavka pri izvajanju nadzora po tem zakonu zabeležijo, kopirajo, prepišejo ali drugače prevzamejo identifikacijske osebne podatke oziroma druge podatke, če je prijavo glede svojih osebnih podatkov podal prijavitelj s posebnim položajem, pri opravljanju nadzora pa ni dopustno razkriti podatkov o delovanju upravljavca iz prejšnjega odstavka v konkretni zadevi.

(6) Ob izvajanju nadzora nad osebnimi podatki, ki se obdelujejo za namene zagotavljanja varnosti države, ki so jih organom Republike Slovenije, pristojnim za področji varnosti države posredovali tuji organi, pristojni za ti področji, ali ki so bili pridobljeni v sodelovanju z njimi, se sme izvesti vpogled, kopiranje, prepis ali drugi prevzem le tistih podatkov, za katere je tuji organ, ki je podatke posredoval ali pridobil, podal predhodno soglasje za vpogled ali drug prevzem.

(7) Nadzorni organ lahko nadzor pri Varuhu človekovih pravic uvede le na podlagi prijave prijavitelja, nadzor iz 36. člena pa le na zahtevo Varuha človekovih pravic. Nadzorne osebe izvajajo nadzor in izrekajo sankcije glede obdelav osebnih podatkov pri Varuhu človekovih pravic na način, da ne posegajo v izvajanje nadzorov glede varovanja človekovih pravic in temeljnih svoboščin in se ne razkrivajo podatki iz zaupnega postopka.

57. člen

(sodelovanje z drugimi organi)

(1) Nadzorni organ 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, nadzornimi organi tretjih držav za varstvo osebnih podatkov, zavodi, združenji, nevladnimi organizacijami s področja varstva osebnih podatkov ali zasebnosti ter drugimi organizacijami in organi glede vprašanj, ki so pomembna za varstvo osebnih podatkov.

(2) Nadzorni organ je pristojen tudi za čezmejno sodelovanje ali izvajanje nadzorov z drugimi nadzornimi organi držav.

(3) V okviru postopkov skupnega ukrepanja po 62. členu Splošne uredbe člani ali osebje nadzornega organa druge države članice Evropske unije izvajajo nadzor tako, da nadzor vodi nadzorni organ, če se nadzor izvaja na ozemlju Republike Slovenije ali v okviru pristojnosti nadzornega organa v skladu s tem zakonom, pri čemer lahko uporabljajo le nadzorna pooblastila iz tega zakona in Splošne uredbe, če jih je za to pooblastil nadzorni organ. Člani ali osebje nadzornega organa druge države članice Evropske unije krijejo svoje stroške.

58. člen

(opravljanje nadzorov)

Nadzorne osebe neposredno opravljajo nadzore po tem zakonu, pri nadzorih pa lahko sodeluje strokovno osebje nadzornega organa.

59. člen

(službena izkaznica)

(1) Nadzorna oseba s službeno izkaznico izkazuje pooblastilo za opravljanje nadzora po tem in drugih zakonih. Službena izkaznica vsebuje fotografijo nadzorne osebe, osebno ime, naziv nadzorne osebe, strokovni ali znanstveni naslov, navedbo organa in pooblastilo za izvajanje nadzora, datum izdaje in podpis predstojnika nadzornega organa.

(2) Obliko službene izkaznice podrobneje določi predstojnik nadzornega organa in jo objavi v Uradnem listu Republike Slovenije.

(3) Službeno izkaznico izda nadzorni organ.

60. člen

(varovanje tajnosti)

(1) Nadzorna oseba je dolžna varovati tajnost osebnih podatkov, s katerimi se seznani pri opravljanju nadzora tudi po prenehanju delovnega razmerja ali funkcije.

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

9. poglavje

Zunanji nadzor delovanja nadzornega organa

61. člen

(letno poročilo nadzornega organa)

(1) Nadzorni organ 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 vsebuje tudi informacije o sodelovanju z drugimi organi pri izvajanju nadzorov po tem zakonu ter o predlaganih in opravljenih nadzorih iz četrtega odstavka 62. člena tega zakona.

(3) Poročilo se posreduje tudi Evropski komisiji in Odboru ter je dostopno javnosti.

62. 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.

(3) Varuh v svojem letnem poročilu poroča državnemu zboru o ugotovitvah, predlogih in priporočilih ter o stanju na področju varstva osebnih podatkov.

(4) Varuh človekovih pravic lahko nadzornemu organu predlaga izvedbo nadzora po 36. členu tega zakona pri kateremkoli upravljavcu ali obdelovalcu. Predlog iz prejšnjega stavka lahko nadzorni organ zavrne z navedbo razlogov, ki jih sporoči varuhu človekovih pravic. V postopku izvajanja nadzora se lahko nadzorni organ in varuh človekovih pravic dogovorita za skupno opravljanje nadzora.

63. člen

(pristojnosti državnega zbora)

(1) Stanje na področju varstva osebnih podatkov in izvrševanje določb tega zakona spremlja državni zbor.

(2) Pristojno delovno telo državnega zbora za nadzor obveščevalnih in varnostnih služb lahko sodeluje z nadzornim organom, na lasten predlog ali na pobudo nadzornega organa sodeluje tudi

glede sprememb zakonov ali drugih predpisov ali pa kadar je v določenih primerih potrebna izmenjava tajnih podatkov ali drugih informacij o poteku ali o ugotovitvah nadzornih postopkov.

10. poglavje
Prenosi določenih osebnih podatkov državam članicam Evropske unije, tretjim državam ali mednarodnim organizacijam

64. člen
(splošne določbe)

(1) Prenosi osebnih podatkov iz Republike Slovenije v tretje države ali mednarodne organizacije se izvajajo le v skladu z določbami V. Poglavja Splošne uredbe.

(2) Nadzorni organ je pristojen za odločanje po določbah tretjega odstavka 46. člena in 47. člena Splošne uredbe.

(3) Nadzorni organ odloča o prenosih osebnih podatkov po zakonu, ki ureja splošni upravni postopek, če ta zakon ali Splošna uredba ne določata drugače.

65. člen
(posebni prenosi)

Osebni podatki zunaj področja uporabe prava Evropske unije, se posredujejo v države članice Evropske unije, tretje države ali mednarodne organizacije le po določbah tega poglavja ali če to določa zakon ob smiselni uporabi določb V. Poglavja Splošne uredbe.

66. člen
(odstopanja v posebnih primerih)

(1) Po določbah tega poglavja se osebni podatki iz prejšnjega člena posredujejo v tretjo državo ali mednarodno organizacijo, za katero ne obstaja sklep o ustreznosti iz 45. člena Splošne uredbe oziroma niso bili sprejeti ustrezni zaščitni ukrepi iz prvega odstavka 49. člena Splošne uredbe.

(2) Določbe a) do c) točke prvega odstavka 49. člena Splošne uredbe ne veljajo za izvrševanje zakonitih pristojnosti, nalog ali obveznosti javnega sektorja.

(3) Upravljavec ali obdelovalec lahko na podlagi dovoljenja nadzornega organa vzpostavita ustrezne zaščitne ukrepe, ki zagotavljajo učinkovito varstvo osebnih podatkov in pomenijo ustrezno pravno podlago za prenos osebnih podatkov. Nadzorni organ izda dovoljenje na podlagi smiselne uporabe določb tretjega odstavka 46. člena Splošne uredbe.

(4) Upravljavec ali obdelovalec dokumentira ustrezne zaščitne ukrepe v evidenci dejavnosti obdelav.

(5) Kadar ne obstaja druga pravna podlaga za posredovanje osebnih podatkov v tretjo državo ali mednarodno organizacijo, se lahko prenos v tretjo državo ali mednarodno organizacijo izjemoma izvede, če prenos ni ponovljiv, zadeva le omejeno število posameznikov, na katere se nanašajo osebni podatki, je potreben zaradi nujnih zakonitih interesov, za katere si prizadeva upravljavec in nad katerimi ne prevladajo človekove pravice ali temeljne svoboščine ali interesi posameznika, na katerega se nanašajo osebni podatki, in pod pogojem, da je upravljavec ocenil vse okoliščine v zvezi s prenosom podatkov in na podlagi te ocene predvidel ustrezne zaščitne ukrepe v zvezi z varstvom osebnih podatkov. Upravljavec o takem prenosu naknadno najpozneje v roku 3 delovnih dni obvesti nadzorni organ. Upravljavec posreduje posamezniku, na katerega se

nanašajo osebni podatki informacije iz 13. in 14. člena Splošne uredbe ter bistvene informacije o izvedenem prenosu in opis nujnih zakonitih interesov iz prejšnjega stavka.

(6) Osebni podatki iz prejšnjega člena, ki jih obdelujejo subjekti javnega sektorja, se smejo posredovati državam članicam Evropske unije, tretjim državam ali mednarodnim organizacijam le če to v javnem interesu določa zakon.

II. DEL
PODROČNE UREDITVE OBDELAVE OSEBNIH PODATKOV

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

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

(1) Obdelava osebnih podatkov za znanstvenoraziskovalne, zgodovinskoraziskovalne in statistične namene (v nadaljnjem besedilu: raziskovanje) je dovoljena organizacijam in posameznikom, ki pri svojem delovanju uporabljajo etična načela in metodologijo s področja raziskovanja ter pravila glede varstva osebnih podatkov iz tega poglavja.

(2) Šteje se, da namen obdelave osebnih podatkov za raziskovanje ni v nasprotju z namenom njihovega zbiranja.

68. člen
(pogoji obdelave osebnih podatkov v raziskovalne namene)

(1) Ne glede na prvotni namen obdelave lahko upravljavec osebne podatke, vključno s posebnimi vrstami osebnih podatkov, nadalje obdeluje za namen raziskovanja če tako obdelavo dovoljuje drug zakon ali če:

1. posameznik, na katerega se ti podatki nanašajo, ni prepovedal obdelave svojih osebnih podatkov za namen raziskovanja ali prepovedal obdelave svojih osebnih podatkov na določenem raziskovalnem področju, ki vključuje tudi namene raziskave ali
2. je posameznik, na katerega se nanašajo osebni podatki, ki pomenijo poklicno skrivnost, za obdelavo podal pisno soglasje.

(2) Raziskovalne organizacije ter raziskovalci, ki so pri raziskovanju vezani na etična načela in metodologijo iz prvega odstavka prejšnjega člena, lahko za namene iz prvega odstavka prejšnjega člena od upravljavca pridobijo osebne podatke, vključno s posebnimi vrstami osebnih podatkov, če predložijo opis raziskave, ki vključuje:

1. naslov raziskave ter navedbo nosilcev raziskave (za fizične osebe osebno ime, naziv in prebivališče, za pravno osebo pa firma, matična številka in sedež);
2. podatke o neposrednih izvajalcih raziskave (osebno ime, naziv, prebivališče, razmerje do nosilca raziskave in morebitna šifra raziskovalca);
3. namene oziroma cilje raziskave;

4. predvidena sredstva in dejanja obdelave osebnih podatkov, vključno z navedbo etičnih načel in metodologije iz prejšnjega člena in ukrepi za varnost osebnih podatkov;
5. vrste osebnih podatkov, ki bi jih želeli pridobiti od upravljavca, ter kategorije posameznikov, na katere se nanašajo ti podatki;
6. obliko, v kateri želijo prejeti osebne podatke (izvorni osebni podatki, psevdonimizirani osebni podatki, osebni podatki v obliki, ki ne zahteva identifikacije, anonimizirani podatki) ter navedbo razloga za določeno obliko podatkov;
7. način objave ali drugačne dostopnosti raziskave.

(3) Opisu raziskave iz prejšnjega odstavka se pod pogoji iz prvega odstavka 35. člena Splošne uredbe priloži oceno učinkov v zvezi z varstvom osebnih podatkov, pod pogoji iz 36. člena Splošne uredbe oziroma kadar gre za osebne podatke, ki jih upravljavec obdeluje na podlagi zakona, ki ureja varstvo osebnih podatkov na področju obravnavanja kaznivih dejanj, pa tudi zaključke posvetovanja z nadzornim organom.

(4) Upravljavec zavrne posredovanje osebnih podatkov:

1. če niso izpolnjeni pogoji iz drugega in tretjega odstavka tega člena,
2. če oceni, da zahtevani osebni podatki niso primerni za izvedbo raziskave,
3. če oceni, da nameni oziroma cilji raziskave ne upravičujejo posega v pravice posameznikov, na katere se nanašajo osebni podatki,
4. če oceni, da ukrepi za varnost osebnih podatkov niso ustrezni ali
5. če gre za tajne podatke v skladu z zakonom o tajnih podatkih.

(5) Upravljavec in izvajalec raziskave posameznikov, na katere se nanašajo podatki, ne obveščata o obdelavah njihovih osebnih podatkov, razen če zakon določa drugače. Upravljavec osebnih podatkov o posredovanju osebnih podatkov izvajalcu raziskave obvesti javnost z objavo na svojih spletnih straneh. Objava obsega navedbo naslova raziskave, namene oziroma cilje raziskave, kategorij posameznikov ter vrst osebnih podatkov, ki so bili posredovani izvajalcu raziskave.

(6) Osebni podatki, ki so bili predmet raziskave, se ob zaključku raziskave uničijo ali nepovratno anonimizirajo, če zakon ne določa drugače, če posameznik ni privolil v nadaljnjo hrambo osebnih podatkov ali če nadaljnja hramba ni pomembna za izvršitev namena raziskave. Izvajalec raziskave upravljavca, ki mu je posredoval osebne podatke, ob zaključku raziskave pisno obvesti, ali, kdaj in na kakšen način jih je uničil.

(7) Rezultati raziskave se objavijo v anonimizirani obliki. Rezultati raziskave se lahko objavijo tudi v psevdonimizirani obliki, če objava podatkov v anonimizirani obliki iz tehničnih razlogov ali zaradi zasledovanja ciljev raziskave ni mogoča. Rezultati raziskave lahko vsebujejo tudi osebne podatke, če ta ali drug zakon to določa ali če je posameznik, na katerega se nanašajo osebni podatki, za objavo osebnih podatkov podal pisno privolitev ali če je za takšno objavo v času po smrti posameznika podana pisna privolitev oseb v izključujočem vrstnem redu iz prvega stavka petega odstavka 9. člena tega zakona. Osebnih podatkov iz raziskave se ne sme objaviti, če je to v nasprotju z interesom varovanja tajnosti ali zaupnosti uradnih postopkov, ali če ti postopki še niso zaključeni.

(8) Posameznik, na katerega se nanašajo osebni podatki, ima v razmerju do izvajalca raziskave pravico dostopa do lastnih osebnih podatkov iz 15. člena Splošne uredbe in pravico do ugovora iz šestega odstavka 21. člena Splošne uredbe.

(9) Upravljavci, ki so subjekti javnega sektorja, za namene raziskovanja po tem poglavju izvajalcu raziskave osebne podatke posredujejo brezplačno.

69. člen

(kontaktiranje posameznikov)

(1) V okviru obdelave osebnih podatkov za raziskovanje upravljavec izjemoma lahko obdeluje tudi osebne podatke ciljne skupine posameznikov zaradi pridobitve privolitev za obdelavo njihovih osebnih podatkov ali zaradi pridobitve dodatnih podatkov ali pojasnil za namene raziskovanja.

(2) Upravljavec lahko na podlagi zbirk, s katerimi razpolaga v okviru zakonitega opravljanja dejavnosti, proti plačilu stroškov obdelave osebnih podatkov kontaktira posameznike z namenom pridobivanja privolitev za izvrševanje namenov iz prejšnjega odstavka.

(3) Za namen kontaktiranja se lahko obdelujejo naslednji osebni podatki: osebno ime, naslov stalnega ali začasnega prebivališča, telefonska številka in naslov elektronske pošte.

70. člen

(obdelava podatkov za namene arhivskega delovanja)

(1) Obdelava osebnih podatkov za namene arhivskega delovanja je dovoljena, če to določa zakon. 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 dostopa do lastnih osebnih podatkov 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:

1. popravka osebnih podatkov zaradi netočnosti ali neposodobljenosti v skladu s 16. členom Splošne uredbe,
2. izbrisa v skladu s 17. členom Splošne uredbe,
3. omejitve obdelave v skladu z 18. členom Splošne uredbe,
4. prenosljivosti osebnih podatkov v skladu z 20. členom Splošne uredbe ter
5. 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, ima možnost podati dopolnilno izjavo z navedbo nasprotnih dejstev. Upravljavec v primeru utemeljenosti dopolnilno izjavo priloži arhivskemu gradivu ali na gradivu ustrezno označi, kje se ta izjava nahaja.

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

71. člen

(obdelava podatkov za namene statističnega raziskovanja)

(1) Obdelava osebnih podatkov za namene izvajanja državne statistike je dovoljena, če je to v javnem interesu, ki ga določa zakon. 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 dostopa do lastnih osebnih podatkov v statističnem gradivu ali v zbirkah statističnih raziskav Statističnega urada Republike Slovenije v skladu s 15. členom Splošne uredbe in pravice do omejitve obdelave v skladu z 18. členom Splošne uredbe, če bi dajanje informacij ali kopij njegovih osebnih podatkov zahtevalo očitno nesorazmeren napor ali kadar upravljavec dokaže, da ne more identificirati posameznika, na katerega se nanašajo osebni podatki v skladu z 11. členom Splošne uredbe. Pravico do popravka v skladu s 16. členom Splošne uredbe lahko posameznik uveljavlja le, če je upravljavec podatke od njega pridobil neposredno in le do trenutka začetka statistične obdelave. Posameznik, na katerega se nanašajo osebni podatki, nima pravice do izbrisa v skladu s 17. členom Splošne uredbe in pravice do ugovora v skladu z 21. členom Splošne uredbe.

(3) Ta člen se ne uporablja, če zakon, ki ureja delovanje državne statistike, določa drugače.

2. poglavje
Varstvo svobode izražanja ter dostopa do informacij javnega značaja v razmerju do varstva osebnih podatkov

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

(1) Obdelava osebnih podatkov v okviru uresničevanja svobode izražanja misli, govora in javnega nastopanja, tiska in drugih oblik javnega obveščanja in izražanja v okvirih pravnega reda Republike Slovenije je dovoljena. Vsakdo lahko svobodno zbira, sprejema in širi vesti in mnenja ter obdeluje v njih vsebovane osebne podatke, ki so potrebni za ta namen.

(2) V okviru svobode izražanja se lahko osebni podatki za namene obveščanja javnosti s strani medijev, književnega, umetniškega ali raziskovalnega ustvarjanja, resne kritike, obrambe kakšne pravice ali varstva upravičene koristi ter izobraževanja, ali izobraževanja preko javno dostopnih objav in publikacij, obdelajo, objavijo ali drugače razkrijejo za namene uresničevanja svobode izražanja, če:

1. je posameznik za obdelavo, 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 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, ki se obdelujejo po tem členu, zagotavljajo sodišča v skladu z določbami drugih zakonov, ki urejajo svobodo izražanja in sodno varstvo.

(4) Upravljavci ali obdelovalci ne smejo za namene izvajanja svobode izražanja nezakonito razkriti, nezakonito posredovati ali omogočiti nepooblaščenega dostopa do osebnih podatkov.

73. 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 sodelovanja z javnostmi, zagotavljanja transparentnosti dela ali spremljanja prakse zavezancev iz prejšnjega odstavka, vključno s sodno prakso sodišč Republike Slovenije, ti zavezanci po postopku iz zakona, ki ureja dostop do informacij javnega značaja, na zahtevo posredujejo ali proaktivno javno objavijo tudi osebne podatke, ki niso zajeti v prejšnjem odstavku, na način delnega dostopa in praviloma v psevdonimizirani obliki.

(3) Kadar zakon določa javnost podatkov ali kadar gre za podatke, ki so informacija javnega značaja, jih upravljavec, ki z njimi razpolaga, lahko javno objavi.

74. 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 s 13. in 14. členom Splošne uredbe ali določbami zakona, ki ureja splošni upravni postopek.

3. poglavje

Videonadzor

75. člen

(splošne določbe o videonadzoru in varstvu osebnih podatkov)

(1) Določbe tega poglavja se uporabljajo za izvajanje videonadzora, če drug zakon ne določa drugače.

(2) Odločitev o uvedbi videonadzora sprejme predstojnik, direktor ali drug pooblaščen posameznik osebe javnega sektorja ali osebe zasebnega sektorja kot upravljavca. V pisni odločitvi morajo biti obrazloženi razlogi za uvedbo videonadzora.

(3) Upravljavec, ki izvaja videonadzor (v nadaljnjem besedilu: upravljavec videonadzornega sistema), o odločitvi iz prejšnjega odstavka objavi obvestilo. Obvestilo se vidno in razločno objavi na način, ki omogoča posamezniku, da se seznani z izvajanjem videonadzora in da se lahko vstopu v nadzorovano območje odpove.

(4) Obvestilo iz prejšnjega odstavka poleg informacij iz prvega odstavka 13. člena Splošne uredbe vsebuje naslednje informacije:

1. pisno ali nedvoumno grafično opisano dejstvo, da se izvaja videonadzor;

2. namene obdelave, navedbo upravljavca videonadzornega sistema, telefonsko številko ali naslov elektronske pošte ali spletni naslov za potrebe uveljavljanja pravic posameznika s področja varstva osebnih podatkov;
3. informacije o posebnih vplivih obdelave, zlasti nadaljnje obdelave;
4. kontaktne podatke pooblaščene osebe (telefonska številka ali naslov e-pošte);
5. neobičajne nadaljnje obdelave, kot so prenosi subjektom v tretje države, spremljanje dogajanja v živo, možnost zvočne intervencije v primeru spremljanja dogajanja v živo.

(5) Namesto objave v obvestilu po tretjem odstavku tega člena se lahko obveščanje posameznika izvede tudi na način, da upravljavec informacije iz prvega odstavka 13. člena Splošne uredbe ter informacije iz 3. do 5. točke prejšnjega odstavka objavi na spletnih straneh. V tem primeru mora na obvestilu iz prejšnjega odstavka objaviti spletni naslov, kjer so te informacije dostopne.

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

(7) Če ni z zakonom drugače določeno, zbirka posnetkov videonadzornega sistema vsebuje posnetek posameznika (slika), datum in čas posnetka, lahko pa tudi zvok.

(8) Videonadzorni sistem, s katerim se izvaja videonadzor, mora biti zavarovan, kot to določata 24. in 32. člen Splošne uredbe.

(9) Posnetki videonadzora se lahko ob upoštevanju načel iz 5. člena Splošne uredbe hranijo največ eno leto od trenutka nastanka posnetka, razen če drug zakon določa drugače.

(10) Videonadzora ni dovoljeno izvajati v dvigalih, sanitarijah, prostorih za preoblačenje, hotelskih sobah in drugih podobnih prostorih, v katerih posameznik utemeljeno pričakuje višjo stopnjo zasebnosti.

(11) Vpogled, uporaba ali posredovanje posnetkov videonadzornega sistema je dopustno samo za namene, ki so zakonito obstajali ali bili navedeni na obvestilu v času zajema posnetka, če drug zakon ne določa drugače.

(12) Upravljavec videonadzornega sistema za vsak vpogled ali uporabo posnetkov zagotovi možnost naknadnega ugotavljanja kateri posnetki so bili obdelani, kdaj in kako so bili uporabljeni ali komu so bili posredovani, kdo je izvedel ta dejanja obdelave, kdaj in s kakšnim namenom ali na kateri pravni podlagi. Te podatke hrani v dnevniku obdelave iz 21. člena tega zakona dve leti po koncu leta, ko so nastali, razen če zakon določa drugače.

76. člen

(videonadzor dostopa v uradne službene oziroma poslovne prostore)

(1) Upravljavci videonadzornega sistema v javnem in zasebnem sektorju lahko izvajajo videonadzor dostopa v uradne službene oziroma poslovne prostore, če je to potrebno za varnost ljudi ali premoženja, zaradi zagotavljanja nadzora vstopa v te prostore ali izstopa iz njih ali če zaradi narave dela obstaja možnost ogrožanja zaposlenih.

(2) Videonadzor se izvaja brez snemanja delov stanovanjskih stavb, ki niso prostori iz prvega odstavka in snemanja vhodov v stanovanja.

(3) O izvajanju videonadzora ter o vsebinah iz četrtega odstavka prejšnjega člena se pisno obvesti vse zaposlene, ki opravljajo delo v nadzorovanem prostoru.

(4) Videonadzor skupnih prostorov je dovoljen, če soglašajo lastniki, ki imajo v lasti več kot 70 odstotni delež skupnih delov.

(5) Zbirka osebnih podatkov po tem členu lahko vsebuje poleg podatkov iz sedmega odstavka prejšnjega člena tudi datum in čas vstopa v uradni službeni prostor in izstopa iz njega, osebno ime posnetega posameznika, naslov njegovega stalnega ali začasnega prebivališča, zaposlitev, številko in podatke o vrsti njegovega osebnega dokumenta ter razlog vstopa, če se navedeni osebni podatki zbirajo skupaj s posnetkom videonadzornega sistema.

77. člen

(videonadzor znotraj delovnih prostorov)

(1) Izvajanje videonadzora znotraj delovnih prostorov se lahko izvaja le 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.

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

(3) Prepovedano je z videonadzorom snemati delovna mesta, kjer delavec običajno dela, razen če je to nujno potrebno v skladu s prvim odstavkom tega člena.

(4) Neposredno spremljanje dogajanja pred kamerami je pod pogoji iz prvega in drugega odstavka tega člena dopustno le, če ga izvaja izrecno pooblaščeno osebje upravljavca.

(5) Zaposlene se pred začetkom izvajanja videonadzora po tem členu vnaprej pisno obvesti o njegovem izvajanju.

(6) 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 ali v drugem daljšem roku, ki ga določi delodajalec. Po prejetju morebitnega mnenja delodajalec dokončno odloči o uvedbi ali neuvedbi videonadzora. Kadar gre za uvedbo videonadzora v skladu s tretjim odstavkom tega člena se posvetovanje izvede v roku 60 dni ali v drugem daljšem roku, ki ga določi delodajalec.

(7) Na področju varnosti države in varovanja tajnih podatkov dveh najvišjih stopenj tajnosti se ne uporablja šesti odstavek tega člena.

(8) Videonadzor skupnih prostorov v poslovnih zgradbah je dovoljen, če soglašajo lastniki, ki imajo v lasti več kot 70 odstotni delež skupnih delov.

(9) Določbe tega člena se smiselno uporabljajo tudi za zagotavljanje nadzora vstopa ali izstopa v ali iz uradnih službenih oziroma poslovnih prostorov, ali če zaradi narave dela obstaja možnost varnostnega ogrožanja zaposlenih.

78. člen

(videonadzor v prevoznih sredstvih, namenjenih javnemu potniškemu prometu)

(1) Videonadzor v prevoznih sredstvih, namenjenih javnemu potniškemu prometu, se sme izvajati le v delih prevoznega sredstva, namenjenih potnikom, za namen varnosti potnikov in premoženja, če tega ni mogoče doseči z drugimi ukrepi, ki manj posegajo v pravice iz prvega odstavka 1. člena tega zakona.

(2) Upravljavec mora uničiti posnetke najpozneje v sedmih dneh po njihovem nastanku. Posnetke se sme uporabljati za uveljavljanje ali obrambo pravnih zahtevkov ali za izvrševanje nalog policije.

79. člen

(videonadzor na javnih površinah)

(1) Videonadzor na javnih površinah, kot jih določa zakon, ki ureja urejanje prostora, je dovoljen le, kadar je to potrebno zaradi obstoja resne in utemeljene nevarnosti za življenje, osebno svobodo, telo ali zdravje ljudi, varnost premoženja upravljavca ali varovanje tajnih podatkov upravljavca ali obdelovalca in tega namena ni mogoče doseči z drugimi sredstvi, ki manj posegajo v pravice iz prvega odstavka 1. člena tega zakona. Videonadzor na javnih površinah je dovoljen tudi za namene varovanja varovanih oseb ter posebnih objektov in okolišev objektov, ki jih varuje policija, Slovenska vojska, pravosodna 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 potreben za dosego namena. 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. Videonadzor smejo za javni sektor izvajati le uradne osebe ali pooblaščeno varnostno osebje, za zasebni sektor pa pooblaščeno varnostno osebje. Osebe ali osebje iz prejšnjega stavka mora biti izrecno pooblaščeno za izvajanje videonadzora.

(4) Videonadzor se lahko izvaja tudi na način, da se ob snemanju izvaja spremljanje dogajanja v živo.

(5) Videonadzor iz prvega odstavka se za namen varovanja oseb, prenosa tajnih podatkov, poslovnih skrivnosti ali premoženja večje vrednosti lahko opravlja tudi z uporabo telesne kamere, če jih uporabljajo za to posebej usposobljene osebe.

(6) Posnetki videonadzora na javnih površinah se lahko ob upoštevanju splošnih načel iz 5. člena Splošne uredbe hranijo največ šest mesecev od trenutka nastanka posnetka, če zakon ne določa drugače.

(7) Upravljavec videonadzornega sistema, ki izvaja videonadzor javnih površin, mora v primeru, ko videonadzorni sistem posname dogodek, ki ogroža zdravje ali življenje posameznika, o tem nemudoma obvestiti policijo ali drug pristojni subjekt.

(8) Na področju videonadzora cestnega prometa sme upravljavec izvajati videonadzor le na vnaprej določenih odsekih cest v njegovem upravljanju, tako da se ne izvaja sistemsko nadzorovanje gibanja posameznikov ali poseganje v zasebnost posameznikov. Upravljavec mora v skladu z zakonom določiti tiste odseke ceste v njegovem upravljanju, kjer z drugimi sredstvi ni mogoče doseči nujnega in učinkovitega varovanja cestnega prometa ali njegovega upravljanja.

(9) Upravljavec videonadzornega sistema iz prejšnjega odstavka mora pred dokončno določitvijo lokacij iz prejšnjega odstavka izdelati oceno učinka, ki vsebuje lokacijo odsekov cest, in jo posredovati v predhodno mnenje nadzornemu organu.

(10) Na javnih površinah je prepovedana uporaba sistemov za avtomatsko prepoznavo registrskih tablic in sistemov, s katerimi se obdelujejo biometrični osebni podatki, razen če zakon izrecno določa drugače.

4. poglavje

Obdelava osebnih podatkov z uporabo biometrije

80. člen

(omejitev biometrije)

(1) Obdelava biometričnih osebnih podatkov v nasprotju z določbami tega poglavja je prepovedana.

(2) Obdelava biometričnih osebnih podatkov se lahko določi le z zakonom, ki poleg vsebin iz drugega ali tretjega odstavka 6. člena tega zakona določi tudi pogoje za njeno uporabo ter morebitne omejitve uporabe.

(3) Prepovedano je povezovati zbirke biometričnih osebnih podatkov z drugimi zbirkami ter omogočati prenosljivost teh podatkov, razen, če to določa zakon ali v to privoli posameznik, na katerega se nanašajo biometrični osebni podatki.

81. člen

(biometrija v javnem sektorju)

(1) Obdelava biometričnih osebnih podatkov v javnem sektorju se lahko določi le z zakonom, če je to nujno potrebno za varnost ljudi, varnost premoženja ali za varovanje tajnih podatkov, za identifikacijo pogrešanih ali umrlih posameznikov ali za varovanje poslovnih skrivnosti, teh namenov pa ni možno doseči z milejšimi sredstvi.

(2) Obdelavo biometričnih osebnih podatkov v javnem sektorju je izjemoma dopustno izvajati tudi pod pogojem, da so dejanja obdelave teh podatkov potrjena na način, ki zagotavlja obdelavo in uporabo teh podatkov posameznika pod njegovim izključnim nadzorom ali izključno oblastjo ter mu omogoča, da izrecno dovoli obdelavo teh podatkov drugim obdelovalcem in upravljavcem za namen dokazovanja točnosti svoje identitete.

(3) Ne glede na prvi odstavek tega člena se obdelave biometričnih osebnih podatkov lahko določi z zakonom, če gre za izpolnjevanje obveznosti iz obvezujoče mednarodne pogodbe ali za identifikacijo posameznikov pri prehajanju državnih meja.

(4) Obdelava biometričnih osebnih podatkov v javnem sektorju se lahko določi z zakonom tudi za namen identifikacije posameznikov pri izdaji sredstev elektronske identifikacije v skladu z zakonom, ki ureja sredstva elektronske identifikacije, in je takšno identifikacijo posameznik zahteval.

(5) Ne glede na določbe prvega odstavka tega člena se v javnem sektorju lahko uvede obdelava biometričnih osebnih podatkov v zvezi z vstopom v stavbo ali dele stavbe, ki se izvedejo ob smiselni uporabi četrtega, petega in šestega odstavka 82. člena tega zakona.

82. člen

(biometrija v zasebnem sektorju)

(1) Obdelava biometričnih osebnih podatkov v zasebnem sektorju se lahko izvaja le v skladu z določbami tega člena, če je to nujno potrebno za opravljanje dejavnosti, za varnost ljudi, varnost premoženja, varovanje tajnih podatkov, varovanje poslovnih skrivnosti ali za varstvo točnosti identitete strank. Dejanja obdelave biometričnih osebnih podatkov morajo biti potrjena v skladu z 51. členom tega zakona.

(2) Oseba zasebnega sektorja lahko obdeluje biometrične osebne podatke tudi glede svojih strank. Takšna obdelava je dopustna, če to za namene varovanja interesov iz prvega odstavka tega člena določa drug zakon, če to posebej določa pogodba ali so stranke podale izrecno privolitev. Kadar se biometrični osebni podatki obdelujejo na podlagi pogodbe s potrošnikom, mora upravljavec posamezniku, na katerega se nanašajo osebni podatki, omogočiti tudi način identifikacije brez obdelave biometričnih osebnih podatkov.

(3) Obdelava biometričnih osebnih podatkov v zasebnem sektorju se sme izvajati tudi pod pogojem, da so dejanja obdelave teh podatkov potrjena na način, ki zagotavlja obdelavo in uporabo teh podatkov stranke pod njenim izključnim nadzorom ali njeno izključno oblastjo ter omogoča stranki, da izrecno dovoli obdelavo teh podatkov drugim obdelovalcem in upravljavcem za namen dokazovanja točnosti svoje identitete.

(4) Pred začetkom obdelave biometričnih osebnih podatkov morajo biti posamezniki o tem pisno obveščeni, kadar gre za zaposlene pa mora upravljavec z zaposlenimi izvesti predhodno posvetovanje o sorazmernosti obdelave.

(5) Oseba zasebnega sektorja, ki namerava obdelovati biometrične osebne podatke, pred začetkom obdelave posreduje nadzornemu organu opis nameravanih obdelav in razloge za njihovo uvedbo.

(6) Nadzorni organ 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.

(7) Oseba zasebnega sektorja lahko začne izvajati biometrične ukrepe po prejemu odločbe iz prejšnjega odstavka, s katero je izvajanje biometričnih ukrepov dovoljeno.

(8) Zoper odločbo nadzornega organa iz šestega odstavka tega člena ni pritožbe, dovoljen pa je upravni spor.

(9) Osebi zasebnega sektorja ni treba pridobiti odločbe iz šestega odstavka tega člena, če se biometrični ukrepi izvajajo na način, določen v tretjem odstavku tega člena.

83. člen

(prepoved pridobivanja biometričnih osebnih podatkov v zvezi s trženjem)

V okviru trženja ali 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.

5. poglavje

Evidentiranje vstopov in izstopov

84. 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 uradni identifikacijski dokument.

(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 uradnega identifikacijskega dokumenta, naslov prebivališča, zaposlitev, vrsta in registrska številka vozila ter datum, ura in razlog vstopa ali izstopa v prostore ali izstopa iz njih.

(3) Osebni podatki iz drugega odstavka tega člena se lahko hranijo največ dve leti od konca koledarskega leta po vnosu osebnih podatkov v zbirko, nato se izbrišejo ali na drug način uničijo, če drug zakon ne določa drugače.

6. poglavje

Javne knjige in varstvo osebnih podatkov

85. 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.

7. poglavje

Povezovanje zbirk osebnih podatkov

86. člen

(povezovanje uradnih evidenc in javnih knjig)

(1) Kadar se 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 obdelujejo v uradnih evidencah ali javnih knjigah, 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 odstavka, se lahko povezuje med seboj ali z drugimi zbirkami samo, če zakon določa pravico upravljavca uradne evidence, javne knjige ali druge zbirke, da pridobi osebne podatke iz uradne evidence, javne knjige ali druge zbirke.

(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 obvestiti nadzorni organ, v obvestilu navede, da namerava izvesti povezovanje v skladu s tem členom ter ga podrobno opiše zlasti z navedbo pravnih podlag, tehničnih rešitev in zaščitnih ukrepov.

8. poglavje

Strokovni nadzor

87. člen

(strokovni nadzor)

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

88. člen

(splošne določbe)

(1) Oseba, ki izvaja strokovni nadzor (v nadaljnjem besedilu: izvajalec strokovnega nadzora), lahko za namen izvedbe strokovnega nadzora obdeluje vse osebne podatke, ki jih obdelujejo upravljavci osebnih podatkov, nad katerimi izvaja 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) Ne glede na določbe prejšnjih dveh odstavkov se pri izvajanju strokovnega nadzora upoštevajo omejitve iz četrtega odstavka 56. člena tega zakona.

(4) Stroške vpogleda, izpisa, prepisovanja ali kopiranja iz prejšnjega odstavka krije upravljavec.

89. člen

(obveščanje posameznika in pridobivanje podatkov)

(1) Izvajalec strokovnega nadzora lahko pri opravljanju strokovnega nadzora, če je to potrebno za uspešen nadzor in tega z drugimi ukrepi ni mogoče doseči, pisno obvesti posameznika, na katerega se nanašajo osebni podatki, da izvaja strokovni nadzor. Obvesti ga, da lahko pisno ali ustno poda svoja stališča in dodatne informacije, pomembne za nadzor, s katerimi razpolaga. Izvajalec strokovnega nadzora lahko s posameznikom, na katerega se nanašajo osebni podatki, opravi razgovor.

(2) Posameznik iz prejšnjega odstavka lahko izvajalcu strokovnega nadzora za namene izvajanja strokovnega nadzora posreduje kontaktne osebne podatke drugega posameznika (osebno ime, zaposlitev, številke ali naslove službenih komunikacijskih sredstev in navedbo povezave z zadevo nadzora), ki bi lahko o zadevi, v kateri se izvaja strokovni nadzor, podal pomembne informacije, s katerimi razpolaga. Če izvajalec strokovnega nadzora ugotovi, da je to potrebno, opravi razgovor tudi z drugim posameznikom.

90. člen

(posebne vrste osebnih podatkov)

Če se pri izvajanju strokovnega nadzora obdelujejo posebne vrste osebnih podatkov ali podatki iz kazenskih ali prekrškovnih evidenc, se o tem naredi uradni zaznamek ali drug uradni zapis v zadevi ali zbirki upravljavca.

9. poglavje

Obdelava kontaktnih podatkov in osebnih dokumentov

91. 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.

92. člen

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

(1) Oseba iz javnega ali zasebnega 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 privolitev, za namene organiziranja uradnih srečanj, izobraževanj, usposabljanj in dogodkov, določanja sestav ali delovanje komisij, svetov, delegacij in drugih podobnih dejavnosti javnega sektorja, dajanja izjav za javnost, razen izvajanja neposrednega trženja. 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, telefonsko številko, naslov elektronske pošte ali drugo komunikacijsko številko oziroma oznako, podatke o delodajalcu ali organizaciji ter podatke o področju dela, položaju, funkciji, 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 naslov stalnega ali začasnega prebivališča in druge osebne podatke, posebne vrste osebnih podatkov pa le izjemoma in če ima za to izrecno privolitev posameznika.

(3) Za namene obveščanja javnosti sme oseba javnega ali zasebnega sektorja obdelovati, vključno z objavo, osebna imena, nazive, fotografije in videoposnetke posameznikov, pridobljene na dogodkih, ki jih v okviru svojih nalog, pristojnosti ali dejavnosti organizira ta oseba.

93. člen

(obdelava osebnih podatkov iz uradnega identifikacijskega dokumenta)

(1) Obdelovalec ali uporabnik, ki izvajata z zakonom predpisano nalogo, smeta za namen identifikacije posameznika vpogledati v njegove uradne identifikacijske dokumente.

(2) Upravljavec, ki izvaja z zakonom predpisano nalogo, sme za namen identifikacije posameznika prepisati, kopirati ali na drug način obdelati podatke iz njegovih uradnih identifikacijskih dokumentov.

(3) Uradni identifikacijski dokument po tem členu je osebna izkaznica, potni list, obmejna prepustnica, vozniško dovoljenje, orožni list in uradni identifikacijski dokumenti drugih držav ali mednarodnih organizacij.

III. DEL

KAZENSKE DOLOČBE

94. člen

(sankcije za kršitve, ki jih predpisuje Splošna uredba)

(1) Sankcije za kršitve, ki jih predpisuje Splošna uredba, se izrekajo pravnim osebam, samostojnim podjetnikom posameznikom in posameznikom, ki samostojno opravljajo dejavnost kot globe za prekrške, v višini in razponih, kot jih določa Splošna uredba.

(2) S tem zakonom se predpisujejo tudi sankcije za kršitve Splošne uredbe, ki so jih storile odgovorne osebe ali posamezniki.

95. člen

(kršitve določb iz četrtega odstavka 83. člena Splošne uredbe)

(1) Z globo od 100 do 5.000 eurov se kaznuje za prekršek odgovorna oseba pravne osebe, samostojnega podjetnika posameznika ali posameznika, ki samostojno opravlja dejavnost:

1. če krši obveznosti upravljavca ali 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 100 do 5.000 eurov se kaznuje za prekršek iz prvega odstavka tega člena odgovorna oseba državnega organa ali organa samoupravne lokalne skupnosti.

96. člen

(kršitve določb iz petega in šestega odstavka 83. člena Splošne uredbe)

(1) Z globo od 100 do 5.000 eurov se kaznuje za prekršek odgovorna oseba pravne osebe, samostojnega podjetnika posameznika ali posameznika, 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 nadzorni organ v skladu z drugim odstavkom 58. člena Splošne uredbe, ali če ne zagotovi dostopa, s čimer se krši prvi odstavek 58. člena Splošne uredbe;
5. če ne upošteva popravljalnih ukrepov, ki jih naloži pristojni nadzorni organ v skladu z drugim odstavkom 58. člena Splošne uredbe.

(2) Z globo od 100 do 5.000 eurov se kaznuje za prekršek iz prvega odstavka tega člena odgovorna oseba državnega organa ali organa samoupravne lokalne skupnosti.

(3) Z globo od 100 do 1.000 eurov se kaznuje za prekršek iz prvega odstavka tega člena posameznik.

97. člen

(kršitve temeljnih določb tega zakona)

(1) Z globo od 4.000 do 12.000 eurov se kaznuje za prekršek pravna oseba, če se pravna oseba po zakonu, ki ureja gospodarske družbe, šteje za srednjo ali veliko gospodarsko družbo, pa z globo od 8.000 do 36.000 eurov:

1. če ne uvede ukrepov za zagotavljanje sledljivosti obdelave osebnih podatkov v skladu z 21. členom tega zakona,
2. če ne imenuje osebe, pristojne za nadzor in usmerjanje varnostnih ukrepov v zvezi z izvajanjem obdelave osebnih podatkov, če obdeluje podatke iz 1. do 4. točke prvega odstavka 22. člena tega zakona (četrti odstavek 22. člena tega zakona);
3. če ne uvede ukrepov sledljivosti posredovanja osebnih podatkov v skladu s šestim odstavkom 40. člena tega zakona.

(2) Z globo od 3.000 do 9.000 eurov se za prekršek iz prejšnjega odstavka kaznuje samostojni podjetnik posameznik ali posameznik, ki samostojno opravlja dejavnost.

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

(4) Z globo od 400 do 4.000 eurov se kaznuje za prekršek iz prvega odstavka odgovorna oseba v državnem organu ali v samoupravni lokalni skupnosti.

(5) Z globo od 400 do 2.000 eurov se kaznuje za prekršek iz prvega odstavka tega člena posameznik.

98. člen

(kršitev določb o posredovanju osebnih podatkov v zvezi s svobodo izražanja)

(1) Z globo od 4.000 do 12.000 eurov se kaznuje za prekršek pravna oseba, če se pravna oseba po zakonu, ki ureja gospodarske družbe, šteje za srednjo ali veliko gospodarsko družbo, pa z globo od 8.000 do 36.000 eurov, če kot upravljavec ali obdelovalec nezakonito razkrije, nezakonito posreduje ali omogoči nepooblaščen dostop do osebnih podatkov iz zbirke za namene iz drugega odstavka 72. člena tega zakona (četrti odstavek 72. člena tega zakona).

(2) Z globo od 3.000 do 9.000 eurov se za prekršek iz prejšnjega odstavka kaznuje samostojni podjetnik posameznik ali posameznik, ki samostojno opravlja dejavnost.

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

(4) Z globo od 400 do 4.000 eurov se kaznuje za prekršek iz prvega odstavka odgovorna oseba v državnem organu ali v samoupravni lokalni skupnosti.

(5) Z globo od 400 do 2.000 eurov se kaznuje za prekršek iz prvega odstavka posameznik.

99. člen

(kršitve določb o uporabi povezovalnega znaka)

(1) Z globo od 1.000 do 8.000 eurov se kaznuje za prekršek pravna oseba, če se pravna oseba po zakonu, ki ureja gospodarske družbe, šteje za srednjo ali veliko gospodarsko družbo, pa z globo od 8.000 do 36.000 eurov:

1. če pri pridobivanju osebnih podatkov iz zbirk osebnih podatkov s področja zdravstva, varnosti države, sodstva ter iz kazenske ali prekrškovnih evidenc uporablja samo en povezovalni znak (prvi odstavek 41. člena tega zakona);
2. če ne napravi uradnega zaznamka ali drugega ustreznega zapisa o nujnosti uporabe izključno enega povezovalnega znaka za predpisane namene (drugi odstavek 41. člena tega zakona);
3. če na področju varnosti države povezovalni znak uporablja v nasprotju z notranjim aktom o varnosti osebnih podatkov (tretji odstavek 41. člena tega zakona).

(2) Z globo od 400 do 2.000 eurov se za prekršek iz prejšnjega odstavka kaznuje samostojni podjetnik posameznik ali posameznik, ki samostojno opravlja dejavnost.

(3) Z globo od 400 do 2.000 eurov se kaznuje za prekršek iz prvega odstavka odgovorna oseba pravne osebe, samostojnega podjetnika posameznika ali posameznika, ki samostojno opravlja dejavnost.

(4) Z globo od 400 do 2.000 eurov se kaznuje za prekršek iz prvega odstavka odgovorna oseba v državnem organu ali v samoupravni lokalni skupnosti.

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

100. člen

(kršitev splošnih določb o videonadzoru)

(1) Z globo od 4.000 do 10.000 eurov se kaznuje za prekršek pravna oseba, če se pravna oseba po zakonu, ki ureja gospodarske družbe, šteje za srednjo ali veliko gospodarsko družbo, pa z globo od 8.000 do 20.000 eurov:

1. če se izvaja videonadzor brez pisne odločitve iz drugega odstavka 75. člena tega zakona;
2. če ne objavi obvestila na način iz tretjega odstavka 75. člena tega zakona;
3. če obvestilo ne vsebuje informacij iz četrtega odstavka 75. člena tega zakona;
4. če ne zavaruje videonadzornega sistema, s katerim izvaja videonadzor, na način iz osmega odstavka 75. člena tega zakona.

(2) Z globo od 1.000 do 2.000 eurov se za prekršek iz prejšnjega odstavka kaznuje samostojni podjetnik posameznik ali posameznik, ki samostojno opravlja dejavnost.

(3) Z globo od 500 do 2.000 eurov se kaznuje za prekršek iz prvega odstavka odgovorna oseba pravne osebe, samostojnega podjetnika posameznika ali posameznika, ki samostojno opravlja dejavnost.

(4) Z globo od 500 do 2.000 eurov se kaznuje za prekršek iz prvega odstavka odgovorna oseba v državnem organu ali v samoupravni lokalni skupnosti.

(5) Z globo od 100 do 1.000 eurov se kaznuje za prekršek iz prvega odstavka posameznik.

101. člen

(težje kršitve določb o videonadzoru)

(1) Z globo od 8.000 do 20.000 eurov se kaznuje za prekršek pravna oseba, če se pravna oseba po zakonu, ki ureja gospodarske družbe, šteje za srednjo ali veliko gospodarsko družbo, pa z globo od 16.000 do 40.000 eurov:

1. če se posnetki videonadzora hranijo več kot šest mesecev od trenutka nastanka posnetka, razen če drug zakon določa drugače (deveti odstavek 75. člena tega zakona);
2. če se izvaja videonadzor izvaja v dvigalih, sanitarijah, prostorih za preoblačenje, hotelskih sobah in drugih podobnih prostorih, v katerih lahko posameznik utemeljeno pričakuje višjo stopnjo zasebnosti (deseti odstavek 75. člena tega zakona).

(2) Z globo od 4.000 do 10.000 eurov se za prekršek iz prejšnjega odstavka kaznuje samostojni podjetnik posameznik ali posameznik, ki samostojno opravlja dejavnost.

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

(4) Z globo od 1.000 do 4.000 euro se kaznuje za prekršek iz prvega odstavka odgovorna oseba v državnem organu ali v samoupravni lokalni skupnosti.

(5) Z globo od 400 do 3.000 eurov se kaznuje za prekršek iz prvega odstavka posameznik.

102. člen

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

(1) Z globo od 2.000 do 5.000 eurov se kaznuje za prekršek pravna oseba, če se pravna oseba po zakonu, ki ureja gospodarske družbe, šteje za srednjo ali veliko gospodarsko družbo, pa z globo od 2.000 do 8.000 eurov:

1. če izvaja videonadzor brez pravne podlage ali obdeluje posnetke v nasprotju z namenom iz prvega odstavka 76. člena tega zakona;
2. če izvaja videonadzor dostopa v uradne službene oziroma poslovne prostore v notranjosti stanovanjskih stavb, ki nimajo vpliva na dostop do teh prostorov ali snema vhode v stanovanja (drugi odstavek 76. člena);
3. če pisno ne obvesti zaposlenih, ki opravljajo delo v nadzorovanem prostoru ali v obvestilu ne navede vseh vsebin iz četrtega odstavka 76. člena (tretji odstavek 76. člena).

(2) Z globo od 2.000 do 5.000 eurov se kaznuje za prekršek iz prejšnjega odstavka samostojni podjetnik posameznik ali posameznik, ki samostojno opravlja dejavnost

(3) Z globo od 500 do 2.000 eurov se kaznuje za prekršek iz prvega odstavka odgovorna oseba pravne osebe, samostojnega podjetnika posameznika ali posameznika, ki samostojno opravlja dejavnost.

(4) Z globo od 500 do 2.000 eurov se kaznuje za prekršek iz prvega odstavka tega člena odgovorna oseba državnega organa ali organa samoupravne lokalne skupnosti.

(5) Z globo od 100 do 500 eurov se kaznuje za prekršek iz prvega odstavka tega člena posameznik.

103. člen

(kršitev določb o videonadzoru znotraj delovnih prostorov)

(1) Z globo od 4.000 do 10.000 eurov se kaznuje za prekršek pravna oseba, če se pravna oseba po zakonu, ki ureja gospodarske družbe, šteje za srednjo ali veliko gospodarsko družbo, pa z globo od 8.000 do 20.000 eurov:

1. če izvaja videonadzor v nasprotju z namenom izvajanja videonadzora znotraj delovnih prostorov (prvi odstavek 77. člena tega zakona) ali
2. če izvaja videonadzor v delovnih prostorih, kjer ni potrebno varovati interesov iz prvega odstavka 76. člena tega zakona (drugi odstavek 77. člena tega zakona).

(2) Z globo od 4.000 do 10.000 eurov se kaznuje za prekršek iz prejšnjega odstavka samostojni podjetnik posameznik ali posameznik, ki samostojno opravlja dejavnost

(3) Z globo od 500 do 4.000 eurov se kaznuje za prekršek iz prvega odstavka odgovorna oseba pravne osebe, samostojnega podjetnika posameznika ali posameznika, ki samostojno opravlja dejavnost.

(4) Z globo od 500 do 4.000 eurov se kaznuje za prekršek iz prvega odstavka tega člena odgovorna oseba državnega organa ali organa samoupravne lokalne skupnosti.

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

104. člen

(kršitev določb o videonadzoru v vozilih namenjenih javnemu potniškemu prometu)

(1) Z globo od 4.000 do 10.000 eurov se kaznuje za prekršek pravna oseba, če se pravna oseba po zakonu, ki ureja gospodarske družbe, šteje za srednjo ali veliko gospodarsko družbo, pa z globo od 8.000 do 20.000 eurov:

1. če izvaja videonadzor v nasprotju z namenom izvajanja videonadzora v prevoznih sredstvih, namenjenih javnemu potniškemu prometu (prvi odstavek 78. člena tega zakona) ali
2. če v nasprotju z drugim odstavkom 78. člena tega zakona ne uniči videoposnetkov v predpisanem roku ali uporablja posnetke za druge namene od tistih, določenih v drugem odstavku 78. člena tega zakona.

(2) Z globo od 4.000 do 10.000 eurov se kaznuje za prekršek iz prejšnjega odstavka samostojni podjetnik posameznik ali posameznik, ki samostojno opravlja dejavnost

(3) Z globo od 500 do 4.000 eurov se kaznuje za prekršek iz prvega odstavka odgovorna oseba pravne osebe, samostojnega podjetnika posameznika ali posameznika, ki samostojno opravlja dejavnost.

(4) Z globo od 500 do 4.000 eurov se kaznuje za prekršek iz prvega odstavka tega člena odgovorna oseba državnega organa ali organa samoupravne lokalne skupnosti.

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

105. člen

(kršitev določb o videonadzoru na javnih površinah)

(1) Z globo od 5.000 do 20.000 eurov se kaznuje za prekršek pravna oseba, če se pravna oseba po zakonu, ki ureja gospodarske družbe, šteje za srednjo ali veliko gospodarsko družbo, pa z globo od 10.000 do 30.000 eurov:

1. če izvaja videonadzor na javnih površinah v nasprotju z nameni iz prvega odstavka 79. člena tega zakon;
2. če izvaja videonadzor tistih delov javnih površin, ki ni potreben za varovanje interesov iz prvega odstavka 79. člena tega zakona (drugi odstavek 79. člena tega zakona);
3. če izvaja videonadzor na javnih površinah s katerimi ne upravlja ali na njih zakonito ne opravlja dejavnosti (tretji odstavek 79. člena tega zakona);
4. če hrani posnetke videonadzora javnih površin več kot šest mesecev od trenutka nastanka, razen, če zakon ne določa drugače (šesti odstavek 79. člena tega zakona);
5. če nemudoma ne obvesti policije ali drugega pristojnega subjekta, ko videonadzorni sistem posname dogodek na javni površini, ki ogroža zdravje ali življenje posameznika (sedmi odstavek 79. člena tega zakona);
6. če na javnih površinah uporablja sistem za avtomatsko prepoznavo registrskih tablic ali sistemov, ki uporabljajo biometrične podatke, razen če zakon izrecno določa drugače (deseti odstavek 79. člena tega zakona).

(2) Z globo od 5.000 do 10.000 eurov se kaznuje za prekršek iz prejšnjega odstavka samostojni podjetnik posameznik ali posameznik, ki samostojno opravlja dejavnost

(3) Z globo od 500 do 5.000 eurov se kaznuje za prekršek iz prvega odstavka odgovorna oseba pravne osebe, samostojnega podjetnika posameznika ali posameznika, ki samostojno opravlja dejavnost.

(4) Z globo od 500 do 5.000 eurov se kaznuje za prekršek iz prvega odstavka tega člena odgovorna oseba državnega organa ali organa samoupravne lokalne skupnosti.

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

106. člen

(kršitev določb o biometriji v javnem sektorju)

(1) Z globo od 2.000 do 4.000 eurov se kaznuje za prekršek pravna oseba, če se pravna oseba po zakonu, ki ureja gospodarske družbe, šteje za srednjo ali veliko gospodarsko družbo, pa z globo od 3.000 do 6.000 eurov:

1. če izvaja obdelave biometričnih osebnih podatkov brez zakonske podlage iz prvega, tretjega, četrtega ali petega odstavka 81. člena tega zakona;
2. če obdeluje biometrične osebne podatke z dejanji obdelave, ki niso potrjena na način iz drugega odstavka 81. člena tega zakona.

(2) Z globo od 2.000 do 4.000 eurov se kaznuje za prekršek iz prejšnjega odstavka samostojni podjetnik posameznik ali posameznik, ki samostojno opravlja dejavnost

(3) Z globo od 500 do 4.000 eurov se kaznuje za prekršek iz prvega odstavka odgovorna oseba pravne osebe, samostojnega podjetnika posameznika ali posameznika, ki samostojno opravlja dejavnost.

(4) Z globo od 500 do 4.000 eurov se kaznuje za prekršek iz prvega odstavka tega člena odgovorna oseba državnega organa ali organa samoupravne lokalne skupnosti.

107. člen

(kršitev določb o biometriji v zasebnem sektorju)

(1) Z globo od 2.000 do 10.000 eurov se kaznuje za prekršek pravna oseba, če se pravna oseba po zakonu, ki ureja gospodarske družbe, šteje za srednjo ali veliko gospodarsko družbo, pa z globo od 4.000 do 20.000 eurov:

1. če biometrične ukrepe v zasebnem sektorju izvaja v nasprotju z nameni iz prvega odstavka 82. člena tega zakona;
2. če izvaja biometrične ukrepe nad svojimi strankami brez zakonske ali pogodbene podlage oziroma brez izrecne pisne privolitve ali če potrošniku ne omogoči načina identifikacije brez obdelave biometričnih osebnih podatkov (drugi odstavek 82. člena tega zakona);
3. če izvaja biometrične ukrepe pred prejemom odločbe nadzornega organa, s katero je izvajanje biometričnih ukrepov dovoljeno (sedmi odstavek 82. člena tega zakona).

(2) Z globo od 2.000 do 10.000 eurov se kaznuje za prekršek iz prejšnjega odstavka samostojni podjetnik posameznik ali posameznik, ki samostojno opravlja dejavnost

(3) Z globo od 500 do 4.000 eurov se kaznuje za prekršek iz prvega odstavka odgovorna oseba pravne osebe, samostojnega podjetnika posameznika ali posameznika, ki samostojno opravlja dejavnost.

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

108. 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, če se pravna oseba po zakonu, ki ureja gospodarske družbe, šteje za srednjo ali veliko gospodarsko družbo, pa z globo od 16.000 do 40.000 eurov, če v nasprotju s 83. členom tega zakona zahteva, pridobi ali nadalje obdela biometrične podatke osebe v zamenjavo za storitve.

(2) Z globo od 8.000 do 20.000 eurov se kaznuje za prekršek iz prejšnjega odstavka samostojni podjetnik posameznik ali posameznik, ki samostojno opravlja dejavnost

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

(4) Z globo od 1.000 do 4.000 eurov se kaznuje za prekršek iz prvega odstavka tega člena odgovorna oseba državnega organa ali organa samoupravne lokalne skupnosti.

(5) Z globo od 500 do 2.000 eurov se kaznuje za prekršek iz prvega odstavka tega člena posameznik.

109. člen

(kršitev določb o evidentiranju vstopov in izstopov)

(1) Z globo od 1.000 do 3.000 eurov se kaznuje za prekršek pravna oseba, če se pravna oseba po zakonu, ki ureja gospodarske družbe, šteje za srednjo ali veliko gospodarsko družbo, pa z globo od 2.000 do 6.000 eurov:

1. če v zbirki o vstopih in izstopih iz službenih prostorov obdeluje osebne podatke v nasprotju z drugim odstavkom 84. člena tega zakona;
2. če osebne podatke iz zbirke o vstopih in izstopih iz službenih prostorov hrani več kot dve leti od konca koledarskega leta po vnosu osebnih podatkov v zbirko ali osebnih podatkov ne zbriše ali uniči po poteku zakonsko določenega roka za hrambo (tretji odstavek 84. člena tega zakona).

(2) Z globo od 1.000 do 2.000 eurov se kaznuje za prekršek iz prejšnjega odstavka samostojni podjetnik posameznik ali posameznik, ki samostojno opravlja dejavnost

(3) Z globo od 400 do 1.000 eurov se za prekršek iz prejšnjega odstavka kaznuje odgovorna oseba pravne osebe, samostojnega podjetnika posameznika ali posameznika, ki samostojno opravlja dejavnost.

(4) Z globo od 400 do 1.000 eurov se kaznuje za prekršek iz prvega odstavka tega člena odgovorna oseba državnega organa ali organa samoupravne lokalne skupnosti.

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

110. člen

(kršitev določb o javnih knjigah)

(1) Z globo od 2.000 do 4.000 eurov se kaznuje za prekršek pravna oseba, če se pravna oseba po zakonu, ki ureja gospodarske družbe, šteje za srednjo ali veliko gospodarsko družbo, pa z globo od 5.000 do 20.000 eurov, če porablja osebne podatke iz javnih knjig v nasprotju z njihovim zakonskim namenom (85. člen tega zakona).

(2) Z globo od 2.000 do 4.000 eurov se kaznuje za prekršek iz prejšnjega odstavka samostojni podjetnik posameznik ali posameznik, ki samostojno opravlja dejavnost

(3) Z globo od 500 do 2.000 eurov se kaznuje za prekršek iz prvega odstavka odgovorna oseba pravne osebe, samostojnega podjetnika posameznika ali posameznika, ki samostojno opravlja dejavnost.

(4) Z globo od 500 do 2.000 eurov se kaznuje za prekršek iz prvega odstavka tega člena odgovorna oseba državnega organa ali organa samoupravne lokalne skupnosti.

(5) Z globo od 100 do 1.000 eurov se kaznuje za prekršek iz prvega odstavka tega člena posameznik.

111. člen

(kršitev določb o povezovanju uradnih evidenc in javnih knjig)

(1) Z globo od 2.000 do 4.000 eurov se kaznuje za prekršek pravna oseba, če se pravna oseba po zakonu, ki ureja gospodarske družbe, šteje za srednjo ali veliko gospodarsko družbo, pa z globo od 5.000 do 20.000 eurov;

1. če v nasprotju s prvim ali drugim odstavkom 86. člena tega zakona brez zakonske podlage izvede povezovanje uradnih evidenc ali javnih knjig;
2. če pred začetkom povezovanja zbirk iz prvega odstavka 86. člena tega zakona, nadzornega organa ne obvesti v skladu s četrtim odstavkom 86. člena tega zakona.

(2) Z globo od 2.000 do 4.000 eurov se kaznuje za prekršek iz prejšnjega odstavka samostojni podjetnik posameznik ali posameznik, ki samostojno opravlja dejavnost.

(3) Z globo od 500 do 2.000 eurov se kaznuje za prekršek iz prvega odstavka odgovorna oseba pravne osebe, samostojnega podjetnika posameznika ali posameznika, ki samostojno opravlja dejavnost.

(4) Z globo od 500 do 2.000 eurov se kaznuje za prekršek iz prvega odstavka tega člena odgovorna oseba državnega organa ali organa samoupravne lokalne skupnosti.

(5) Z globo od 100 do 1.000 eurov se kaznuje za prekršek iz prvega odstavka tega člena posameznik.

112. člen

(kršitev določb o strokovnem nadzoru)

(1) Z globo od 2.000 do 4.000 eurov se kaznuje za prekršek pravna oseba, če se pravna oseba po zakonu, ki ureja gospodarske družbe, šteje za srednjo ali veliko gospodarsko družbo, pa z globo od 4.000 do 8.000 eurov:

1. če pri izvajanju strokovnega nadzora ne varuje tajnosti osebnih podatkov ali če v poročilu ali oceni ob zaključku strokovnega nadzora zapiše več osebnih podatkov kot so nujno potrebni za dosego namena strokovnega nadzora (drugi odstavek 88. člena tega zakona);
2. če pri izvajanju strokovnega nadzora posebnih vrst osebnih podatkov ali podatkov iz kazenskih ali prekrškovnih evidenc, ne naredi uradnega zaznamka ali drugega uradnega zapisa v spisu zadeve upravljavca osebnih podatkov (90. člen tega zakona).

(2) Z globo od 1.000 do 4.000 eurov se kaznuje za prekršek iz prejšnjega odstavka samostojni podjetnik posameznik ali posameznik, ki samostojno opravlja dejavnost

(3) Z globo od 800 do 1.500 eurov se kaznuje za prekršek iz prvega odstavka odgovorna oseba pravne osebe, samostojnega podjetnika posameznika ali posameznika, ki samostojno opravlja dejavnost.

(4) Z globo od 800 do 1.500 eurov se kaznuje za prekršek iz prvega odstavka tega člena odgovorna oseba državnega organa ali organa samoupravne lokalne skupnosti.

(5) Z globo od 400 do 1.000 eurov se kaznuje za prekršek iz prvega odstavka tega člena posameznik.

113. člen

(odmerjanje sankcij za prekrške)

Poleg splošnih pravil za odmero sankcije iz zakona, ki ureja prekrške, se pri odločanju nadzornega organa o višini izrečene globe za kršitve, predpisane v četrtem do šestem odstavku 83. člena Splošne uredbe, v skladu z določbami prvega odstavka 83. člena 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 ali množične kršitve varstva osebnih podatkov ter pomen, ki bi ga za odvračanje tovrstnih kršitev varstva osebnih podatkov imela višina globe.

114. člen

(izrek globe)

Za prekrške iz Splošne uredbe in iz tega zakona se sme v hitrem postopku izreči globa tudi v znesku, ki je višji od najnižje predpisane globe, določene s Splošno uredbo ali tem zakonom.

IV. DEL
PREHODNE IN KONČNE DOLOČBE

115. člen

(rok za vzpostavitev posebnih ukrepov)

Posebni ukrepi za zagotavljanje varnosti osebnih podatkov na področju posebnih obdelav iz 22. člena tega zakona se vzpostavijo v treh letih od uveljavitve tega zakona.

116. člen

(pravilnik o zaračunavanju stroškov)

Minister, pristojen za pravosodje v soglasju z ministrom, pristojnim za zdravje, po predhodnem mnenju nadzornega organa, sprejme pravilnik o zaračunavanju stroškov iz četrtega odstavka 16. člena zakona v treh mesecih od uveljavitve tega zakona.

117. člen

(določitev pooblaščenih oseb)

Pooblaščene osebe, ki so jih do uveljavitve tega zakona določili predstojniki organov v sestavi ministrstev, nadaljujejo z opravljanjem dela pooblaščene osebe po tem zakonu.

118. člen

(prehodne določbe glede delovanja nadzornega organa)

(1) Prekrškovni postopki, ki so se začeli pri Informacijskem pooblaščencu ali na sodiščih pred uveljavitvijo tega zakona, se končajo v skladu z Zakonom o varstvu osebnih podatkov (Uradni list RS, št. 94/07 – uradno prečiščeno besedilo), razen če je ta zakon za storilca milejši. Postopki inšpekcijskega nadzora, začeti na podlagi Zakona o varstvu osebnih podatkov (Uradni list RS, št. 94/07 – uradno prečiščeno besedilo), se nadaljujejo v skladu s tem zakonom.

(2) Dosedanje odločitve Informacijskega pooblaščenca o ustreznosti varstva osebnih podatkov v tretjih državah in prenosov osebnih podatkov se z uveljavitvijo tega zakona razveljavijo.

(3) Seznam tretjih držav iz 66. člena Zakona o varstvu osebnih podatkov (Uradni list RS, št. 101/15, 11/17 in 16/17) se z uveljavitvijo tega zakona razveljavi.

(4) Ne glede na določbo drugega odstavka tega člena se dosedanje odločitve Informacijskega pooblaščenca o ustreznosti varstva osebnih podatkov v tretjih državah in prenosov osebnih podatkov uporabljajo do sprejema novih odločitev po Splošni uredbi.

(5) 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.

119. člen

(prehodne določbe glede povezovanja)

Povezovanja uradnih evidenc in javnih knjig se uskladijo s 86. členom tega zakona v štirih letih od uveljavitve tega zakona.

120. člen

(prehodne določbe glede potrjevanja)

(1) Slovenska akreditacija začne izvajati postopke akreditacije 1. januarja 2024.

(2) Do začetka izvajanja postopkov akreditacije po tem zakonu se šteje, da so dejanja obdelave upravljavcev in obdelovalcev, ki morajo po določbah tega zakona za dejanja obdelave pridobiti certifikat, ta skladna z merili iz mehanizma potrjevanja.

121. člen

(prehodne določbe glede videonadzora v prevoznih sredstvih)

Upravljavci in obdelovalci so dolžni obdelave osebnih podatkov, ki se nanašajo na videonadzor v prevoznih sredstvih, namenjenih javnemu potniškemu prometu, uskladiti z določbami 78. člena tega zakona v roku treh let od uveljavitve tega zakona.

122. člen

(upoštevanje obvestil o določitvi pooblaščenih oseb)

Upravljavcem in obdelovalcem, ki so pred začetkom uveljavitve tega zakona posredovali podatke nadzornemu organu o pooblaščenih osebah, ni treba ponovno posredovati informacij, če podatki o pooblaščenih osebah niso spremenjeni.

123. člen

(razveljavitev podzakonskih predpisov)

Z dnem uveljavitve tega zakona prenehajo veljati:

– Pravilnik o metodologiji vodenja registra zbirk osebnih podatkov (Uradni list RS, št. 28/05 in 30/11);

– Pravilnik o pridobivanju potrebnih informacij za odločanje o iznosu osebnih podatkov v tretje države (Uradni list RS, št. 79/05);

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

pravilnika o zaračunavanju stroškov iz četrtega odstavka 16. člena tega zakona, kolikor ni v nasprotju s tem zakonom.

124. člen

(uporaba določb o prekrških)

Do sprememb določb o višinah in razponih glob, ki jih določa zakon, ki ureja prekrške, se globe za kršitve, ki so določene v 83. členu Splošne uredbe, izrekajo v skladu s 83. členom Splošne uredbe.

125. člen

(prenehanje veljavnosti zakona)

Z dnem uveljavitve tega zakona preneha veljati Zakon o varstvu osebnih podatkov (Uradni list RS, št. 94/07 – uradno prečiščeno besedilo in 177/20).

126. člen

(končna določba)

Ta zakon začne veljati trideseti dan po objavi v Uradnem listu Republike Slovenije.

III. OBRAZLOŽITEV

I. del – Temeljne določbe

1. poglavje – Splošne določbe

1. poglavje I. dela predloga zakona vsebuje splošne oziroma temeljne določbe predloga zakona. Večina določb je ti. sistemske narave in so pomembne za interpretacijo predloga zakona ali za določene področne ureditve ali za uporabo določb tega zakona in Splošne uredbe. Pomembne so zlasti določbe o opredelitvi (bistva) človekove pravice do varstva osebnih podatkov, prepovedi diskriminacije, ozemeljski veljavnosti, pravne podlage za obdelavo osebnih podatkov in podobno.

K 1. členu (vsebina)

Prvi odstavek predlaganega člena navaja, da je vsebina zakona najprej določanje pravic, obveznosti, upravičenj, načel, postopkov in ukrepov pri obdelavi osebnih podatkov ter druga vprašanja tako obdelave kot varstva osebnih podatkov.

S tem se varuje in uresničuje človekovo pravico do varstva osebnih podatkov iz Ustave Republike Slovenije. Gre torej za nadaljevanje sistemskega pristopa regulacije v smeri priznavanja in spoštovanja osebne človekove pravice, kot je le-ta nadalje opredeljena v 38. členu Ustave RS. Na ta način je v določbi podana povezava oziroma interpretacija, da zakon predstavlja načine uresničevanja oziroma varstva pravic iz 38. (varstvo osebnih podatkov), 35. (varstvo pravic zasebnosti in osebnostnih pravic) in 34. (pravica do osebnega dostojanstva in varnosti) člena Ustave Republike Slovenije.

Iz določb prvega odstavka jasno izhaja, da za obdelave osebnih podatkov v Republiki Sloveniji veljajo določbe Splošne uredbe (ki se v večini lahko neposredno uporabljajo, npr. definicije, pooblaščene osebe, pravice posameznikov …) ter določbe tega sistemskega zakona o varstvu osebnih podatkov.

V drugem odstavku predlaganega člena je določeno razmerje med predlaganim zakonom in Zakonom o varstvu osebnih podatkov na področju obravnavanja kaznivih dejanj[33] (ZVOPOKD). ZVOPOKD ureja obdelave osebnih podatkov v zvezi s kaznivimi dejanji – razen vprašanj, ki jih posebej ureja ZVOP-2 in jih ZVOPOKD ne ureja – tako da ima ZVOP-2 naravo sistemskega zakona. To velja zlasti za obdelavo osebnih podatkov umrlih oseb, kazenske in prekrškovne evidence ipd. Torej je drugi odstavek izjema od sistemske ureditve v prvem odstavku in je ZVOPOKD samostojen sistem varstva osebnih podatkov, ki pa prav tako kot predlog tega zakona, temelji na 38. členu Ustave RS.

Pravico oziroma skupek pravic s področja podatkovne zasebnosti iz 38. člena Ustave Republike Slovenije (varstvo osebnih podatkov) določa kot človekovo pravico posameznika ali posameznice do varstva njegovih ali njenih osebnih podatkov. Pri tem določba izhaja iz ti. »subjektivnega pristopa« in ne iz pristopa regulacije (zakonske oziroma upravne obveznosti), v središču te ene od najbolj bistvenih pravic je namreč človek. To izhaja tudi iz prvega dela določbe, po kateri se posameznikom zagotavljajo zasebnost (38. in 35. člen Ustave Republike Slovenije) in dostojanstvo (34. člen Ustave Republike Slovenije) ob upoštevanju podatkovne samoodločbe

[33] Uradni list RS, št. 177/20.

(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.

Predlog 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«, kar je v letu 2019 posebej izpostavila tudi nova ustavnosodna presoja Ustavnega sodišča Republike Slovenije[36].

Ureditev je tudi primerljiva 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)[37]. Z navedenim zakonom namreč 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 in osebne človekove pravice (na ustavni ravni).

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

K 2. členu (prepoved diskriminacije glede obdelave osebnih podatkov)

Predlagani 2. člen ureja prepoved nedopustne diskriminacije glede varstva osebnih podatkov – natančneje: prepoved nedopustne diskriminacije, kadar se izvaja obdelava osebnih podatkov. Pri tem je pomembna povezava s 1. členom, da gre za človekovo pravico, da je osredotočeni naslovnik pravic posameznik, na katerega se nanašajo osebni podatki ter glede razlagalne »moči« glede drugih zakonov ipd. V 2. členu so glede na 14. člen Ustave Republike Slovenije ter glede na druge ustaljene formulacije pravnega reda Republike Slovenije (npr. prvi odstavek 131. člena Kazenskega zakonika[38] ter prvi odstavek 1. člena Zakona o varstvu pred diskriminacijo[39]) navedene prepovedane okoliščine diskriminacije. Določbe so nekoliko posodobljene – dodana je spolna identiteta po prvem odstavku 1. člena Zakona o varstvu pred diskriminacijo, dodana je genska (ne genetska) predispozicija, beseda »barva« iz dosedanjega 4. člena ZVOP-1 je spremenjena v »barvo kože«, omenjeno je tudi zdravstveno stanje in invalidnost (upoštevana sprememba 14. člena Ustave RS iz 2004).

Predlagani člen pomeni, da se nikogar ne sme nedopustno diskriminirati glede varstva osebnih podatkov. Natančneje – med prepovedanimi kriteriji diskriminacije (razlikovanja) sta v praksi zlasti najbolj pomembna kriterija državljanstva in prebivališča, tudi glede na 1. člen Konvencije o

[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] Glejte: Odločba US, št. U-I-152/17, 4. 7. 2019, zlasti 20. točka in opomba št. 10; objava: Uradni list RS, št. 46/19.
[37] Objava: Bundesgesetzblatt I Nr. 120/2017, Teil I.
[38] Uradni list RS, št. 50/12 – uradno prečiščeno besedilo, 6/16 – popr., 54/15, 38/16 in 27/17.
[39] Uradni list RS, št. 33/16.

varstvu posameznikov glede na avtomatsko obdelavo osebnih podatkov[40] (Sveta Evrope), ki se v tem delu v okviru reforme varstva osebnih podatkov v okviru Sveta Evrope ne spreminja.

Predlagani člen pa dopušča pod zakonsko določenimi pogoji možnost izvajanja profiliranja pri obdelavi osebnih podatkov, avtomatizirano odločanje pod zakonsko določenimi pogoji in jamstvi (npr. pravica do ugovora) – seveda, če takšna obdelava ni diskriminatorna (torej ne sme pomeniti nedopustne diskriminacije).

K 3. členu (področje uporabe)

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 2. člena 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 osebnih podatkov.

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 popolnoma 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 »popolnoma« – 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 dni ali drugih podobnih podatkov, kot so obletnice.

Pomembno je, da v primerih, kadar obdelava zadeva tako zasebne kot poslovne informacije, se izjema ne uporabi. Beseda »izključno« nakazuje na *ozko interpretacijo* te določbe in 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.«[41]

Ob upoštevanju, da se Splošna uredba uporablja neposredno, je v tretjem odstavku določeno, da za obdelave osebnih podatkov, ki jih Splošna uredba ne ureja, velja ta zakon subsidiarno, kar pomeni, da lahko področni zakoni še vedno varstvo podatkov na svojem področju uredijo drugače, vendar ne v nasprotju s Splošno uredbo.

K 4. členu (veljavnost zakona)

4. člen je eden od najpomembnejših členov predloga zakona, glede na to, da prek določanja jurisdikcije pravnega reda Republike Slovenije (prvi in drugi 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.

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

[41] 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.

Prvi odstavek primarno določa personalno veljavnost tega zakona. Zakon velja za upravljavce, obdelovalce, uporabnike in druge subjekte, ki obdelujejo osebne podatke, ne glede na to, da obdelava ne poteka na ozemlju Republike Slovenije.

Drugi odstavek določa pravila glede ozemeljske veljavnosti, pri čemer določa za katere obdelave osebnih podatkov (in s tem, za katere upravljavce oziroma obdelovalce osebnih podatkov) se uporablja določen predpis. Splošna uredba v skladu z njenim 3. členom 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 zakona svojo veljavnost določa v teh okvirih.

Prvenstveno ta zakon v skladu s prvim odstavkom predlaganega člena tako kot do sedaj velja za tiste obdelave osebnih podatkov, ki jih izvaja javni sektor ali zasebni sektor v Republiki Sloveniji (definirana v 3. in 4. točki drugega odstavka 5. člena Predloga ZVOP-2) ter za obdelave, 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[42].

Gre za že obstoječe kriterije iz (a) točke prvega odstavka člena 4 Direktive o varstvu osebnih podatkov[43] oziroma prvega odstavka 5. člena dosedanjega Zakona o varstvu podatkov[44] (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[45] 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[46], oziroma ki na ozemlju Republike Slovenije opravljajo dejansko in resnično, čeprav majhno, dejavnost, v okviru katere se izvaja ta obdelava[47].

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 do sedaj 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 95/46/ES št. 8/2010 o pravu, ki se uporablja[48] , 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 več ne uporablja.

Drugi odstavek določa, da predlog zakona velja tudi za obdelave osebnih podatkov prebivalcev Republike Slovenije, ki potekajo v okviru upravljavca s sedežem zunaj Evropske unije (izvaja jih

[42] Uvodna navedba št. 22 Splošne uredbe.
[43] UL L 281 , 23/11/1995 str. 0031 – 0050.
[44] Uradni list RS, št. 94/07 – uradno prečiščeno besedilo in 177/20.
[45] Sodba Sodišča EU v zadevi C-131/12, tč. 52, 56 in 67.
[46] Uvodna navedba št. 22 Splošne uredbe.
[47] 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*.
[48] http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2010/wp179_en.pdf

upravljavec iz tretje države), vendar se ponujajo uporabnikom iz Republike Slovenije, oziroma zadevajo profiliranje slovenskih uporabnikov. Navedena določba temelji na drugem odstavku 3. člena 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[49] (in torej za nadzor nad njim ni že tako v skladu s prvim odstavkom 3. člena 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[50] 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[51]. V takšnih primerih bo Informacijski pooblaščenec pristojen za nadzor skladnosti obdelave tujega upravljavca oz. obdelovalca s tem zakonom, ter za obravnavo pritožb posameznikov v zvezi s tem.

K 5. členu (pomen izrazov)

V 5. členu je v prvem odstavku najprej določeno, da za varstvo osebnih podatkov veljajo bistveni izrazi (»pojmi« po Splošni uredbi), torej definicije privolitve, obdelave osebnih podatkov, zbirke ipd. Rešitev je predlagana po vzorcu prvega odstavka 5. člena Zakona o varstvu fizičnih oseb glede obdelave osebnih podatkov Kraljevine Belgije iz leta 2018.

V drugem odstavku so določeni bistveni izrazi, ki veljajo tako za I. del (uredbeni del) kot II. del (področne ureditve obdelav osebnih podatkov) in ostale dele predloga zakona, npr. nadzorni organ, zakon, varnost države, kazenske evidence, javni in zasebni sektor. Gre za izraze, ki jih je treba glede na specifičnosti pravnega reda Republike Slovenije določi samostojno, npr. javni sektor, povezovalni znak (do sedaj isti povezovalni znak) ipd., ki ne odstopajo vsebinsko od dosedanjih definicij iz 6. člena ZVOP-1. Prav tako je opredeljen izraz »zadeve sodišča«, saj v njih po Splošni uredbi ni dopustno posegati v neodvisnost sodniškega odločanja.

Izraz »zakon« pomeni glede na 6. člen Splošne uredbe, 4. člen Direktive ter za izvrševanje a) in b) točke 5. člena Konvencije o varstvu posameznikov glede na avtomatsko obdelavo osebnih podatkov (Sveta Evrope) - ta (predlagani) zakon, druge zakone Republike Slovenije, obvezujoče (in torej ratificirane) mednarodne pogodbe, ki zavezujejo Republiko Slovenijo ter pravne akte ali odločitve Evropske unije, katerih določbe so enakovredne zakonom in neposredno uporabljive ali neposredno učinkovite (glede na 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[52] ter glede na določbe 87. in 153. člena Ustave Republike Slovenije). Predlagana določba upošteva tudi najnovejšo precedenčno odločbo Ustavnega sodišča Republike Slovenije[53], ki je okrepila pomen podrobne zakonske podlage za vse obdelave osebnih podatkov (kot je to bilo to razvito v ustavnosodni presoji Ustavnega sodišča Republike Slovenije že od leta 1992 dalje).

Definicija »varnosti države« je pomembna za uporabo določb o varnosti države v ZVOP-2 ter določb področnih 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

[49] Uvodna navedba št. 23 Splošne uredbe.
[50] Glede na uvodno navedbo št. 23 Splošne uredbe.
[51] Uvodna navedba št. 24 Splošne uredbe.
[52] Odločba US, št. U-I-115/92, 24. 12. 1992; objava: OdlUS I, 105 in Uradni list RS, št. 3/93.
[53] Odločba US, št. U-I-152/17, 4. 7. 2019, zlasti 32. točka; objava: Uradni list RS, št. 46/19.

klasično varnost države (obveščevalno in protiobveščevalno delovanje) ter za področje obrambe države. Navedena področja Splošna uredba izrecno izključuje iz svojega urejanja, ker Evropska unija na teh področjih nima neposrednih kompetenc. Urejanje varstva osebnih podatkov na teh področjih je torej prepuščeno državam članicam in njihovim nacionalnim ureditvam.

Zaradi potrebne povezave z 9. členom predloga zakona je določena 11. točka drugega odstavka 6. člena, ki opredeljuje storitve informacijske družbe. Navedena določba sledi 35. točki 4. člena Zakona o informacijski varnosti[54]. Ker so v 8. členu Splošne uredbe storitve informacijske družbe omenjene le splošno, brez podrobnejše opredelitve, je predlagatelj prevzel opredelitev iz obstoječe zakonodaje.

K 6. členu (pravne podlage za obdelavo osebnih podatkov)

V predlaganem 6. členu so določena temeljna načela za zakonito obdelavo osebnih podatkov (pravne podlage). Prvi odstavek se pri tem sklicuje na ureditev v neposredno veljavnih 6. in 9. členu Splošne uredbe, ki pa urejanje zakonitosti za določene vrste obdelav prepuščata nacionalnim ureditvam. Predlagana ureditev nacionalnih posebnosti sledi smerem iz dosedanjega 9. in 10. člena ZVOP-1. Bistvena razlika je, da so sedaj pravne podlage za obdelave osebnih podatkov v javnem in v zasebnem sektorju urejene v skupnem členu, s tem da je najprej poudarjena prva pravna podlaga – namreč prvi odstavek 6. člena Splošne uredbe.

Tako prvi odstavek 6. člena določa, da se osebne podatke lahko obdeluje le, če to omogočajo pravne podlage iz 6. in 9. člena Splošne uredbe. Konkretneje ta formulacija vključuje pravne podlage zlasti iz prvega odstavka 6. člena Splošne uredbe, delno pa tudi drugega in tretjega odstavka 6. člena (urejanje obdelav osebnih podatkov s področnimi zakoni). Besedilo »le in v obsegu, kadar je to v skladu« upošteva določbo drugega odstavka 38. člena Ustave Republike Slovenije o varstvu tajnosti osebnih podatkov.

Poleg 6. člena Splošne uredbe je v prvem odstavku navedena tudi pravna podlaga za obdelavo posebnih vrst osebnih podatkov – namreč 9. člen Splošne uredbe, ki pretežno zahteva zakonsko urejanje.

Predlagani drugi odstavek določa, kaj mora biti vsebina področnega zakona s področja osebnih podatkov, ki naj bi se obdelovali v javnem sektorju in zasebnem 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) ter ob upoštevanju (c) in (e) točk prvega pododstavka prvega odstavka 6. člena Splošne uredbe. Upošteva tudi merila iz drugega odstavka 6. člena Splošne uredbe ter drugega dela tretjega odstavka 6. člena Splošne uredbe. Glede (c) prvega pododstavka prvega odstavka 6. člena Splošne uredbe velja opozoriti, da je v času priprave tega besedila uradna slovenska inačica (kot je objavljena v Uradnem listu EU) netočna, saj je iz angleške (in drugih) inačice za sklepati, da pravna podlaga pomeni »izpolnjevanje pravne obveznosti« in ne »izpolnjevanje zakonske obveznosti«. Glede na pravni red RS je sicer treba upoštevati potrebo po urejanju obdelav v zakonih, vendar obstaja tudi možnost delovanja na podlagi drugih pravnih obveznosti, npr. na podlagi obvezujočih pravnih obveznosti – npr. pravnomočne sodbe sodišč.

Predlagani tretji odstavek določa posebne določbe glede možnosti uporabe privolitve v javnem sektorju (za oblastne naloge in pristojnosti). Najprej je določeno, da mora to možnost določati zakon, v drugih primerih poslovanja javnega sektorja, ko gre za neoblastno poslovanje, pa neposredno zadostuje (neposredna uporaba) podlaga iz tega tretjega odstavka. Za razliko od dosedanjega drugega odstavka 9. člena ZVOP-1 je sedaj določeno, da lahko ne samo nosilci javnih pooblastil, ampak izrecno celotni javni sektor obdelujejo osebne podatke tudi na podlagi

[54] Zakon o informacijski varnosti (Uradni list RS, št. 30/18 in 95/21).

privolitve[55], ki pa mora biti določena v zakonu (npr. narodnost, verska pripadnost – 61. člen ter prvi in drugi odstavek 41. člena Ustave Republike Slovenije). Če pa take možnosti ne določa zakon, pa lahko javni sektor obdeluje osebne podatke na podlagi privolitve le, če ne gre za izvrševanje zakonskih (dejansko: oblastvenih[56]) nalog, pristojnosti ali obveznosti 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.

Predlagani četrti odstavek pomeni dodatno izvedbo ozir. možnost izvedbe (e) točke prvega odstavka 6. člena Splošne uredbe. Po njej se izjemoma lahko obdelujejo neposredno na tej pravni podlagi, določeni v tem zakonu, osebni podatki, kadar je to potrebni za izvrševanje 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. Predlagana določba pa ne omogoča niti začasnega omogočanja določanja osebnih podatkov v podzakonskih predpisih (zlasti v pravilnikih), je kvečjemu – glede na njeno izjemnost možni »sprožilec«, da pristojno ministrstvo po izvedeni začasni konkretni obdelavi osebnih podatkov (če je to potrebno), pripravi spremembe ali dopolnitve ustreznega zakona, tako da je spoštovano pravilo iz drugega odstavka tega člena predloga zakona (ki temelji na drugem odstavku 38. člena Ustave Republike Slovenije v zvezi s 87. členom Ustave Republike Slovenije)[57]. Predlagana določba tako temelji na (e), delno pa tudi (c) točki prvega pododstavka prvega odstavka 6. člena Splošne uredbe in je primerljiva dosedanji določbi četrtega odstavka 9. člena ZVOP-1, katere uporabo sicer sodna praksa slovenskih sodišč nekoliko omejuje[58]. Gre torej za nadgradnjo vsebine dosedanjega četrtega odstavka 9. člena ZVOP-1[59]. Predlagane določbe drugega odstavka so splošne, sistemske narave (*lex generalis*).

[55] 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).«

[56] 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 […].«

[57] 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. V letu 2019 je Ustavno sodišče RS sprejelo tudi odločbo (št. U-I-26/17, U-I-87/16, U-I-105/16, 24. 10. 2019; objava: Uradni list RS, št. 67/19) z vidika spoštovanja upravne zakonitosti (drugi odstavek 120. člena Ustave Republike Slovenije), ki je tudi relevantna z vidika spoštovanja zakonitosti oziroma prepovedi predpisovanja zakonskih (originarnih) vsebin v podzakonskih aktih in v kateri je med drugim navedeno: »50. Po drugi strani splošnih aktov za izvrševanje javnih pooblastil (kot je tudi Metodologija), ki dopolnjujejo in podrobneje izpeljujejo zakonsko določbo, ni mogoče razumeti kot dejavnik, ki bi omogočal do zakonodajalca blažje razumevanje zahtev načela jasnosti in pomenske določljivosti zakonov. Nasprotno stališče bi ogrozilo zagotavljanje jamstev drugega odstavka 120. člena Ustave. Ni ustavno sprejemljivo, da bi se nerazumljivost in nejasnost zakonov (glede materije, ki mora po Ustavi biti zakonsko urejena) odpravljalo z jasnimi in razumljivimi podzakonskimi akti.«

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

[59] Glejte tudi: sodba Upravnega sodišča RS, opr. št. I U 687/2012, 19. 12. 2012, zlasti 8. točka, po kateri je ZVOP-1 (v zvezi s četrtim odstavkom 9. člena) *lex generalis*, in ZEKom-1 ni *lex specialis*. Glejte tudi odločbo IP, št.: 0612-19/2012/16, 11. 1. 2016, kjer je zamejeno pojasnjen domet uporabe določbe četrtega odstavka 9. člena ZVOP-1.

Četrti odstavek tako ureja pravno podlago za obdelave osebnih podatkov na neoblasten način v povezavi z akti poslovanja javnega sektorja (glejte npr. sklep Vrhovnega sodišča RS, opr. št. I-Up 74/2016 z dne 13. 4. 2016, ki se nanaša na akte poslovanja).

Predlagani peti odstavek najprej navaja, da gre za delni odstop od dela določbe prvega odstavka tega člena, v delu, ki omenja obdelave posebnih vrst osebnih podatkov (9. člen Splošne uredbe). Prvi stavek petega odstavka tako določa, da je obdelava osebnih podatkov o etnični ali narodni pripadnosti posameznika v javnem sektorju izjemoma dopustna, če to določa zakon, ki določa tudi dodatno pravno podlago – privolitev posameznika. Na ta način se spoštujejo določbe prvega in drugega odstavka 41. člena Ustave Republike Slovenije (svoboda vesti) in 61. člena Ustave Republike Slovenije (izražanje narodne pripadnosti). Delni odstop je na podlagi g) točke drugega odstavka 9. člena Splošne uredbe možen tudi v primeru, ko poseben zakon določa obdelavo osebnih podatkov o narodni ali etnični pripadnosti posameznika, če se posameznik glede teh podatkov svobodno opredeli.

Predlagani drugi stavek določa, da se sme obdelave teh osebnih podatkov z zakonom določiti le za primere, ko je to nujno za odločitev o osebnem stanju ali pravicah posameznika (npr. posebna volilna pravica pripadnikov in pripadnic italijanske in madžarske narodne skupnosti; odločanje o azilu ipd.). Ta določba ne omogoča, da bi se npr. pri obdelavi osebnih podatkov po Zakonu o prijavi prebivališča obdelovalo osebne podatke o narodni ali etnični pripadnosti posameznika, saj to ni pomembno za upravno odločanje o prijavi prebivališča, statistični namen kot tak pa ni dopusten (v okviru sistema upravnega odločanja). Predlagana določba pa tudi ne preprečuje, da bi se v Zakonu o popisu prebivalstva (če bi se ta izvajal na klasičen način), ki je lahko le zakon (samo) za potrebe državne raziskovalne statistike in analitike, obdelovalo teh podatkov, seveda z ustreznimi varovalkami (npr. ločen zapis podatkov, zapis na podlagi zakona in še podane privolitve, nadaljnja obdelava teh podatkov na način anonimizacije, prednostno uničenje teh zapisov ipd.).

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«[60] 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 organom mednarodnih organizacij s področja človekovih pravic in temeljnih svoboščin[61], če ni

[60] 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 odstavku 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.«.

[61] Glede morebitnega spreminjanja stališča s strani mednarodnih organizacij (v smeri delnega ukinjanja oziroma odsvetovanja zbiranja in obdelave osebnih podatkov o etnični 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

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[62] – 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. Zaradi posebne zgodovinske občutljivosti obstajajo na določenih upravnih področjih v tujini tudi znatno splošnejše rešitve anonimizacije celo neosebnih (!) podatkov, iz katerih bi se lahko (pa četudi neutemeljeno) sklepalo na narodno ali versko pripadnost posameznikov, ki so lastniki ali vozniki vozil. Npr. v Bosni in Hercegovini so tako leta 1997 v dogovoru več institucij z Visokim predstavnikom (OHR) določili, da se od leta 1998[63] na registrskih tablicah ne navaja več kratica okrožja, kjer je vozilo registrirano (npr. SA), ampak da imajo registrske tablice isto obliko in da številke na njih določi samodejno in slučajno računalniški sistem s centralnega nivoja Bosne in Hercegovine.

Še bolj zamejen (strožji) pristop velja glede zbiranja in obdelave osebnih podatkov o verski pripadnosti[64] – 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 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.

Predlagani drugi stavek konkretizira določbo prvega stavka, tako da je določeno, da se z zakonom obdelave teh podatkov določi za primere, ko je to nujno za odločitev o osebnem stanju ali pravicah posameznika, spodbudah in ugodnostih (npr. posebna pomoč pri šolanju, posebna volilna pravica itd.) ali za zagotavljanje in spodbujanje enakega obravnavanja, enakih možnosti ter zajamčenih posebnih pravic pripadnikov narodne ali etnične skupnosti v Republiki Sloveniji (npr. ukrepi pozitivne diskriminacije za zmanjšanje neutemeljenega razlikovanja med ljudmi v družbi). Predlagana rešitev jasno in nedvoumno omogoča zbiranje podatkov o enakosti (prek obdelave osebnih podatkov, npr. z anonimizacijo) kar je pogoj za vsebinsko ustrezno sprejemanje posebnih ukrepov v smislu 17. člena Zakona o varstvu pred diskriminacijo. Le-te se sme z namenom zagotavljanja enakih možnosti sprejemati tudi z akti občin, izvršilne veje oblasti in drugih subjektov, npr. posameznih delodajalcev. Na to potrebo sicer že dalj časa opozarja Zagovornik načela enakosti in je bila že predmet dosedanjih priporočil k osnutku ZVOP-2 (nazadnje št. 0070-1/2019/3 z dne 28.5.2021, glej 1. točka priporočila). Spremljanje podatkov o enakosti, ki bodo pridobljeni na podlagi obdelave osebnih podatkov bo tako dopustno ne ne le za preprečevanje in odpravljanje diskriminacije, temveč tudi za spodbujanje (dejanske, vsebinske)

---

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.«

[62] 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).

[63] Glejte: http://www.ohr.int/?p=55603

[64] 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.

enakosti v praksi, kar označuje sintagma enake možnosti (ki jo je zagovornik uporabljal že v obeh dosedanjih zgoraj navedenih priporočilih). Skladno s predlogom je mogoče tudi spremljanje uresničevanja zajamčenih posebnih pravic narodnih oz. etničnih skupnosti (ne le posameznikov, torej t.i. kolektivnih pravic) v Sloveniji. Predlagana ureditev ni samostojna pravna podlaga za obdelave osebnih podatkov, dopušča pa urejanje ustreznih podlag v področni zakonodaji.

K 7. členu (obdelava osebnih podatkov v druge namene)

Predlagani 7. člen določa obdelavo osebnih podatkov v druge namene[65] kot pravilo za delovanje (odločanje) javnega in zasebnega sektorja glede možnosti obdelav osebnih podatkov v druge namene po četrtem odstavku 6. člena 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 področni zakon in če je to v skladu z določbami četrtega odstavka 6. člena Splošne uredbe (velja načeloma za zasebni sektor). Tovrsten pristop omogočajo tudi določbe tretjega odstavka 15. člena Ustave Republike Slovenije o omejitvah človekovih pravic s pravicami drugih oseb (glede na drugi stavek prvega odstavka 38. člena Ustave Republike Slovenije).

K 8. členu (privolitev mladoletne osebe za uporabo storitev informacijske družbe)

Predlagani 8. člen ureja pogoje za obdelavo osebnih podatkov otrok v primeru uporabe storitev informacijske družbe določa v skladu z 8. členom Splošne uredbe (po vzorcu iz Zakona o zasebnosti otrok na spletu Združenih držav Amerike – (*Children's Online Privacy Protection Act - COPPA*) iz leta 1998). Otrok 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, 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[66]: »Otrok, ki dopolni 15 let, lahko sam sklepa pravne posle, če zakon ne določa drugače.«

Po predlaganem drugem odstavku privolitev mladoletne osebe ne sme biti pogojevana s pretiranimi pogoji s strani upravljavca, npr. 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. V Francoski republiki je tako v Zakonu o varstvu osebnih podatkov Francoske republike 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.

K 9. členu (posebno varstvo osebnih podatkov umrlih posameznikov)

V 9. 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

[65] 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.

[66] Uradni list RS, št. 15/17, 21/18 – ZNOrg, 22/19, 67/19 – ZMatR-C in 200/20 – ZOOMTVI.

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 v skladu s tem zakonom, na način kot ga določajo področni zakoni (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 9. člena ZVOP-2 upravljavec osebne podatke o umrlem posamezniku posreduje zakoncu, zunajzakonskemu partnerju ali partnerju iz partnerske zveze (izenačen s prej navedenimi), otrokom ali staršem ali dedičem, če umrli ni tega pisno prepovedal ali če drug zakon ne določa drugače.

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, kar je celo širše od področne ureditve iz 68. do 70. člena predloga zakona.

Predlagani peti odstavek je neposredna pravna podlaga (upravičenje) za izjemno obdelavo osebnih podatkov umrlih v knjigah, učbenikih, enciklopedijh itd, se pa ne nanaša na klasične objave oziroma članke v medijih (za te primere načeloma veljajo določbe glede razmerja do svobode izražanja po 72. členu predloga zakona), po pridobitvah privolitev po določenem izključujočem vrstnem redu. Določena je tudi ureditev objave osebnih podatkov javnih osebnosti, seveda če tega ne prepoveduje kak drug zakon.

Predlagani šesti odstavek določa, da se določbe 9. člena Predloga ZVOP-2 uporabljajo za osebne podatke umrlih posameznikov 20 let po njihovi smrti, če drug zakon ne določa drugače. Ta določba pomeni, da imajo področni zakoni pomen *lex specialis* in prevladajo nad določbami ZVOP-2. Po preteku 20 let ti podatki niso več varovani kot osebni podatki po tem zakonu in zanje veljajo določbe področne zakonodaje (npr. Obligacijski zakonik).

K 10. členu (varstvo in obdelava osebnih podatkov o odločitvah o kazenskih obsodbah ter o kaznovanjih za prekrške)

V predlaganem 10. členu je določen dodaten sklop osebnih podatkov, ki so dejansko po vsebini del posebne vrste osebnih podatkov, namreč podatkov o kazenskih obsodbah in kaznovanjih za prekrške. Predlagana ureditev izhaja iz 10. člena Splošne uredbe ter iz uvodnih navedb št. 75 in 80 Splošne uredbe, ki v zvezi s konceptom kazenske obtožbe iz prvega odstavka 6. člena Evropske konvencije omenjajo 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 se morajo obravnavati kot posebne vrste osebnih podatkov v skladu s prvim in tretjim odstavkom 9. člena Splošne uredbe.

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[67].

Predlagana 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 in to na način, da se kot identifikacijski znak uporabi enotna matična številka iz kazenske ali prekrškovne evidence. Tretji odstavek tudi posebej (področno) določa, da mora biti zlasti zagotovljeno, da se osebni podatki iz obeh evidenc in Centralnega registra prebivalstva ne obdelujejo nepooblaščeno, nezakonito razkrivajo ali drugače nepooblaščeno obdelujejo. Gre za poseben poudarek glede zagotavljanja varnosti osebnih podatkov.

Peti odstavek določa način izvedbe povezovanja, da se osebni podatki posameznikov v kazenskih evidencah in prekrškovnih evidencah ob vsaki spremembi usklajujejo s podatki iz Centralnega registra prebivalstva oziroma tako, da se pri neusklajenih podatkih pojavi opozorilo, da je pri njegovih podatkih v drugi zbirki osebnih podatkov prišlo do spremembe ali da več ne obstajajo. Tako predlagana ureditev omogoča delovanje tako imenovanega sistema samodejnih opozoril, da je pri podatkih v drugi zbirki prišlo do spremembe (ti. »*alert sistem*«).

K 11. členu (splošno sodno varstvo pravic posameznika)

Predlagani 11. člen določa sistem splošnega sodnega varstva pravic posameznika, na katerega se nanašajo osebni podatki. Ta člen je zapisan v isti smeri, kot 12. člen ZVOPOKD. Predlagana je samostojna sodna pot za varstvo pravic s področja osebnih podatkov, po kateri ni potrebno predhodno izčrpanje drugih oblik pravnega varstva po določbah ZVOP-2 ali Splošne uredbe ali področnih zakonov. S predlaganim sistemom splošnega sodnega varstva se uresničuje določba 79. člena Splošne uredbe. Predlagano sodno varstvo sledi dosedanji ureditvi iz 34. člena ZVOP-1 (kjer je tudi določena upravnosodna presoja).

Sodno varstvo po 11. členu Predloga ZVOP-2 je torej samostojno pravno sredstvo (samostojno sodno varstvo) in ni pogojeno s predhodnim izčrpanjem kateregakoli drugega pravnega sredstva ali pravice po ZVOP-2 ali Splošne uredbe ali področnih zakonov.

Po predlaganem prvem odstavku lahko vsak posameznik, na katerega se nanašajo osebni podatki in ki meni, da določena obdelava njegovih osebnih podatkov s strani upravljavca ali obdelovalca krši določbe Splošne uredbe, ZVOP-2 ali drugih (področnih) zakonov, ki urejajo obdelavo ali varstvo osebnih podatkov v zvezi s Splošno uredbo, zahteva sodno varstvo svojih pravic ves čas, dokler kršitev traja (kriterij trajajoče kršitve).

Po dopolnilnem tretjem odstavku lahko posameznik v primeru, če je kršitev iz prvega odstavka prenehala in meni da je obstajala, s tožbo zahteva ugotovitev, da je kršitev obstajala (kriterij pretekle kršitve).

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

Drugi odstavek določa, da lahko posameznik s sodnim varstvom po določbah 11. člena zahteva prenehanje kršitve, vzpostavitev zakonitega stanja (npr. izbris, popravek) oziroma povračilo škode, določene so torej materialne podlage zahtevka.

V četrtem odstavku so določene temeljne postopkovne določbe, tako da v postopku po prvem, drugem in tretjem odstavku 11. člena odloča Upravno sodišče Republike Slovenije z uporabo določb Zakona o upravnem sporu po postopku za tožbo zaradi kršitve človekovih pravic in temeljnih svoboščin, tožnik (posameznik, na katerega se nanašajo osebni podatki) pa lahko v tožbo vključi tudi odškodninski zahtevek. Podobna določba je tudi v veljavnem četrtem odstavku 12. člena ZVOPOKD.

Po petem odstavku je v postopku pred Upravnim sodiščem Republike Slovenije po tem členu javnost izključena, razen če sodišče na predlog posameznika, na katerega se nanašajo osebni podatki (tožnika), iz utemeljenih razlogov ne odloči drugače.

V šestem odstavku je določeno, da se določbe glede sistemskega sodnega varstva ne uporabljajo glede obdelav osebnih podatkov s področja varnosti države (glejte tudi definicijo varnosti države v 6. členu tega zakona, ki vključuje tudi področja obrambe države).

Za razliko od določbe šestega odstavka 12. člena ZVOPOKD predlog 11. člena ZVOP-2 ne določa, da Upravno sodišče Republike Slovenije v zadevah upravnih sporov odloči najpozneje v šestih mesecih – ker ne gre za občutljivi kontekst obdelave osebnih podatkov s področja kaznivih dejanj iz ZVOPOKD.

2. poglavje – Postopek pred upravljavcem in obdelovalcem

V 2. poglavju predloga zakona se urejajo določena postopkovna vprašanja glede zagotavljanja pravic posameznikov, na katere se nanašajo osebni podatki, in ki jih uveljavljajo neposredno na podlagi Splošne uredbe in tega ali drugega zakona pred upravljalcem ali obdelovalcem v javnem ali zasebnem sektorju. Splošna uredba določa okrepljeno odgovornost upravljavca ali obdelovalca 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. Splošna uredba se neposredno uporablja že od maja 2018, praksa pa kaže, da so uporabniki pravne ureditve varstva osebnih podatkov z rešitvami dobro seznanjeni. Predlagani členi tega poglavja urejajo določene posebnosti postopka ob hkratnem sklicevanju na določbe Splošne uredbe zaradi večje pravne varnosti in razumevanja samega postopka.

K 12. členu (splošna določba)

Predlog člena določa, da se pravice posameznikov pred upravljavcem in obdelovalcem uveljavljajo na podlagi Splošne uredbe in tega poglavja. Kot upravljavec se obravnava tudi obdelovalec, ki bi kršil Splošno uredbo s tem, ko bi nepooblaščeno sam določil namene in sredstva obdelave, kot to določa deseti odstavek 28. člena Splošne uredbe.

K 13. členu (postopkovne določbe za državne organe in organe samoupravnih lokalnih skupnosti)

Predlog prvega odstavka člena ureja postopek obravnavanja zahtevkov posameznikov pred državnimi organi in organi samoupravnih lokalnih skupnosti nekoliko drugače kot pred ostalim javnim in zasebnim sektorjem. V 6. členu predloga zakona je definiran pojem »javni sektor«, ki obsega tako državne organe, organe samoupravnih lokalnih skupnosti kot nosilce javnih pooblastil, javne agencije, javne sklade, javne zavode, univerze, samostojne visokošolske zavode in samoupravne narodne skupnosti, zasebni vrtci in zasebne osnovne ter srednje šole in druge osebe javnega prava. Postopek je za državne organe in organe samoupravnih lokalnih skupnosti

vezan na smiselno uporabo določb zakona, ki ureja splošni upravni postopek, zlasti glede odločitve o zahtevah posameznikov po III. Poglavju Splošne uredbe (informacij in dostopa do osebnih podatkov, popravka in izbrisa, omejitve obdelave itd.), ki je v obliki odločbe z vsemi sestavinami po zakonu, ki ureja splošni upravni postopek in ta zakon.

Drugi odstavek ureja obveznost seznanitve posameznika o pravici do pritožbe pri nadzornem organu ter določa rok za pritožbo na podlagi določb Splošne uredbe, ki v 57. členu določa pooblastila nadzornega organa in v 77. členu pravico do pritožbe pri nadzornem organu, in sicer v 15-ih dneh od seznanitve z rešitvijo zahtevka.

K 14. členu (obravnavanje zahtevkov posameznika v javnem in zasebnem sektorju)

Predlog člena ureja postopek obravnavanja zahtevkov posameznikov v javnem in zasebnem sektorju, ki niso državni organi ali organi samoupravne lokalne skupnosti (zanje je postopek urejen v predhodnem členu), ki ni vezan na smiselno uporabo določb zakona, ki ureja splošni upravni postopek, temveč je poenostavljen. Upravljavec ali obdelovalec po tej določbi posameznika v zvezi z njegovo zahtevo po III. Poglavju Splošne uredbe (informacije in dostop do osebnih podatkov, popravek in izbris, omejitve obdelave itd.) seznani z odločitvijo, ki je lahko v obliki obvestila, odgovora, sporočila ali uradnega zaznamka. Posamezniku se posredujejo informacije (tudi osebni podatki) na način, kot ga je ta zahteval oziroma kot je glede na vse okoliščine primerno, oziroma na način in v roku kot izhaja iz Splošne uredbe, kjer velja splošno pravilo, po katerem se na zahtevo, ki je bila vložena po elektronski poti, poda odgovor v elektronski obliki. Posameznika se lahko z osebnimi podatki seznani tudi ustno.

Prej navedena odločitev mora vsebovati navedbo razlogov in informacijo o možnosti pritožbe pri Informacijskem pooblaščencu, v skladu z določbami Splošne uredbe (podobno kot v pouku o pravnem sredstvu).

K 15. členu (sestavine odločbe)

Predlagani 15. člen se navezuje na predlog 13. člena tega zakona, ko o zahtevkih posameznikov odločajo državni organi in organi samoupravnih lokalnih skupnosti, ki pri reševanju zahtevkov smiselno uporabljalo določbe zakona, ki ureja splošni upravni postopek in izdajajo odločbe. Zaradi posebnosti delovanja teh organov, ki praviloma obdelujejo osebne podatke posameznikov na podlagi zakonske obveznosti, izvajanja nalog v javnem interesu ali izvajanja oblasti (6. člen Splošne uredbe), je postopek bolj formaliziran. Ko izdajajo odločbe lahko le-ta poleg sestavin po zakonu, ki ureja splošni upravni postopek vsebuje tudi sestavine po tem zakonu. Gre za del odločbe, ki vsebuje dovoljen obseg pregleda zbirke ali lastnih osebnih podatkov iz razlogov in pogojev iz 23. člena Splošne uredbe in so te omejitve določene z zakonom. Splošna uredba med drugim navaja razloge državne varnosti, obrambe, javne varnosti, preprečevanja, preiskovanja, odkrivanja ali pregona kaznivih dejanj ali izvrševanja kazenskih sankcij, gospodarskega in finančnega interesa, varstva posameznika, na katerega se nanašajo osebni podatki ali varstva pravic in svoboščin drugih itd., ki morajo biti v državi članici določeni z zakonom.

Odločba državnega organa ali organa samoupravne lokalne skupnosti v teh primerih ne obsega konkretnih razlogov za zavrnitev ali omejitev dostopa (drugi odstavek), niti ne obsega navedb, s katerimi bi se potrdilo ali zanikalo izvajanje ali neizvajanje prikritih preiskovalnih ukrepov iz zakona, ki ureja Slovensko obveščevalno-varnostno agencijo ali zakona, ki ureja obrambo (tretji odstavek). Predlagano je torej, da vsi posamezniki – ne glede na položaj (ali so nadzorovani preko ukrepov; ali so se v njih slučajno znašli; ali pa sploh niso nadzorovani – torej se sploh ne obdelujejo njihovi osebni podatki) – dobijo od pristojnega organa enak odgovor, iz katerega ni mogoče sklepati, ali se v zvezi z njimi osebni podatki obdelujejo ali ne. Namen določbe je zavarovati učinkovitost delovanja prikritih ukrepov preiskovalnih organov. Na ta način se preprečuje zloraba pravic, ki jih daje ta zakon za pridobivanje podatkov, ki jih posameznik sicer ne more pridobiti po določbah področne zakonodaje, ki ureja te ukrepe.

Zaradi izvajanja učinkovitega nadzora in sodnega varstva pa upravljavec ali obdelovalec konkretne razloge za zavrnitev ali omejitev dostopa navede ločeno v prilogi k odločbi ali uradnemu zaznamku, s katero se posameznika ne seznanja. Priloga mora biti opremljena s številko zadeve, datumom in podpisom pristojne uradne osebe in se ne vroča prijavitelju s posebnim položajem (glejte tudi 33. člen predloga zakona).

K 16. členu (stroški seznanitve z osebnimi podatki)

Predlagani prvi odstavek 16. člena, tako kot to ureja že Splošna uredba v 12. členu, določa, da se posameznikom na podlagi zahtev za informacije, dostopa do osebnih podatkov, popravka, izbrisa, pravice do omejitve itd., tako po Splošni uredbi kot po tem ali drugem zakonu, zagotovijo brezplačno.

Drugi odstavek določa, da le kadar so zahtevki posameznika, na katerega se nanašajo osebni podatki, očitno neutemeljeni ali pretirani zlasti ker se ponavljajo, lahko upravljavec ali obdelovalec posamezniku zaračuna razumne stroške, pri čemer upošteva materialne stroške posredovanja informacij ali sporočila ali izvajanja zahtevanega ukrepa. 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. Predlagana rešitev ne razlikuje med javnim in zasebnim sektorjem, niti ne zaračunava stroškov dela upravljavca, saj gre pri dostopu do lastnih osebnih podatkov za eno od temeljnih človekovih pravic (tretji odstavek 38. člena Ustave RS), ki ima vpliv tudi na pravice posameznika na drugih pravnih področjih.

Tretji odstavek določa, da dokazno breme, da je zahteva očitno neutemeljena ali pretirana nosi upravljavec ali obdelovalec, ki mora navesti razloge za takšno ugotovitev.

Četrti odstavek določa, da minister pristojen za pravosodje, po predhodnem mnenju nadzornega organa, predpiše pravila o zaračunavanju stroškov po Splošni uredbi in po tem zakonu. Sem sodi tudi določitev višine stroškov na področju seznanitve z lastno zdravstveno dokumentacijo in dokumentacijo umrlih pacientov ter povezana pravila o zaračunavanju, ki jih je treba zaradi pravne varnosti in različnih pristojnosti ministrstev posebej omeniti glede na področno ureditev.

Peti odstavek določa, da je o predvidenih stroških potrebno posameznika vnaprej obvestiti.

Šesti odstavek določa, da upravljavec in obdelovalec nosita stroške tehnične izvedljivosti prenosljivosti osebnih podatkov, kadar gre za zahtevo za prenos podatkov po 20. členu Splošne uredbe.

V praksi bo zaračunavanje stroškov prišlo v poštev zelo redko, običajno bo upravljavec zaradi očitne neutemeljenosti zahtevo zavrnil. Primer takšne očitno neutemeljene zahteve bi bil, ko bi posameznik od upravljavca želel potrditev, ali o njem obdeluje osebne podatke; upravljavec mu potrdi, da njegovih osebnih podatkov ne obdeluje; posameznik kljub odgovoru zahteva izbris svojih osebnih podatkov.

K 17. členu (omejitev pravic in obveznosti)

Predlagani prvi odstavek 17. člena, kot že omenjeno v krajši obrazložitvi k drugemu odstavku 15. člena, izrecno določa, da se lahko le z zakonom izjemoma omeji pravice posameznikov iz razlogov in pod pogoji iz 23. člena Splošne uredbe, v zvezi z zahtevami iz III. Poglavja Splošne uredbe, 34. člena Splošne uredbe in 1. poglavja tega zakona ali drugega zakona, ki jih Splošna uredba ne ureja. Razlogi so navedeni v prvem odstavku 23. člena Splošne uredbe (razlogi državne varnosti, obrambe, javne varnosti, preprečevanja, preiskovanja, odkrivanja ali pregona kaznivih dejanj ali izvrševanja kazenskih sankcij, vključno z varovanjem pred grožnjami javni varnosti in njihovim preprečevanjem, drugih pomembnih ciljev v splošnem javnem interesu

Republike Slovenije, zlasti pomembnega gospodarskega ali finančnega interesa, vključno z denarnimi, proračunskimi in davčnimi zadevami, javnim zdravjem in socialno varnostjo, varstva neodvisnosti sodstva in sodnega postopka, preprečevanja, preiskovanja, odkrivanja in pregona kršitev etike v zakonsko urejenih poklicih, spremljanja, pregledovanja ali urejanja, povezanega, lahko tudi zgolj občasno, z izvajanjem javne oblasti, varstva posameznika, na katerega se nanašajo osebni podatki, ali človekovih pravic in temeljnih svoboščin drugih ter uveljavljanja civilnopravnih zahtevkov). Omejitve pa se lahko določijo samo pod pogojem, da je zakonska določba, ki določa takšno omejitev, v skladu s 6. členom predloga zakona.

Drugi odstavek določa, da se lahko obveznosti in naloge upravljavcev ali obdelovalcev, ki se nanašajo na varstvo ali obdelavo osebnih podatkov, prav tako omejijo le z zakonom ter iz razlogov in pod pogoji iz 23. člena Splošne uredbe, kot to določa prejšnji odstavek.

K 18. členu (posebna pravila glede načina uveljavljanja pravic ali zahtevkov na določenih področjih)

Po predlaganem 18. členu ZVOP-2 (prvi in drugi odstavek) se pravice ali drugi zahtevki posameznikov, na katere se nanašajo osebni podatki, na področjih svobode izražanja ali dostopa do informacij javnega značaja iz 72. do 74. člena Predloga ZVOP-2 ne izvajajo v postopkih pred nadzornim organom po določbah tega zakona ali po določbah Splošne uredbe. Te pravice in drugi zahtevki iz Splošne uredbe ter pravice zasebnosti v zvezi s področji iz 72. do 74. člena Predloga ZVOP-2 se izvajajo v skladu z zakoni, ki urejajo ta področja (npr. Obligacijski zakonik, Kazenski zakonik, Zakon o medijih, Zakon o dostopu do informacij javnega značaja), ter določbami 72. do 74. člena Predloga ZVOP-2. Po tretjem odstavku ne glede na določbe prvega in drugega odstavka 18. člena predloga ZVOP-2 nadzor nad zakonitostjo posredovanja, razkritja ali omogočanja nepooblaščenega dostopa do osebnih podatkov iz zbirke za namene iz četrtega odstavka 72. člena (nepooblaščeno razkritje) izvaja Informacijski pooblaščenec.

V četrtem odstavku so urejene omejitve za zadeve sodišč – v teh zadevah zaradi varovanja sodniške neodvisnosti ni podana pristojnost Informacijskega pooblaščenca za nadzore, zato se uresničevanje pravic po Splošni uredbi in nadzor glede obdelav osebnih podatkov v sodnih postopkih, rešujejo v okviru konkretnega sodnega postopka in nadaljnjega sodnega varstva v posamezni zadevi skladno s postopkovnimi predpisi.

Po petem odstavku pa se zapolnjuje morebitna pravna praznina in se v postopku z zahtevo in pritožbo po 41., 42., in 45. členu Zakona o pacientovih pravicah, smiselno uporabljajo določbe Splošne uredbe in ZVOP-2.

K 19. členu (izjema glede uveljavljanja zahtevka posameznika preko zakonitega zastopnika)

Po predlaganem 19. členu ZVOP-2 upravljavec ali obdelovalec lahko izjemoma zavrne zahtevek posameznika iz tega dela ZVOP-2 ali dostop do posameznikove zdravstvene dokumentacije, ki je vložen 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. V tem primeru z razlogi za zavrnitev seznani pristojnega zastopnika pacientovih pravic po Zakonu o pacientovih pravicah.

Predlagana omejitev je povezana s tretjim odstavkom 38. člena Ustave Republike Slovenije v zvezi s prvim stavkom prvega odstavka 5. člena, 56. členom in tretjim odstavkom 15. člena Ustave Republike Slovenije.

K 20. členu (zavarovanje osebnih podatkov, ki so predmet postopka)

Predlagani 20. člen ureja obveznost upravljavcev in obdelovalcev, da zavarujejo vsebino in obliko osebnih podatkov, ki so predmet zahteve vse od seznanitve z uvedbo postopka po tem zakonu. Osebni podatki, ki so predmet zahteve, dnevniki obdelav in drugi zahtevani podatki se ne smejo izbrisati ali spremeniti, ne glede na potek rokov hrambe, dokler o zadevi ni odločeno, saj v nasprotnem primeru glede njih ne bi bilo mogoče ugotavljati zakonitosti obdelave.

Drugi odstavek nadalje določa, da lahko nadzorni organ v posameznem postopku glede na okoliščine posameznega primera določi tudi drugi način zavarovanja osebnih podatkov, ki so predmet zahteve oziroma odredi izdelavo kopije osebnih podatkov ali kopije postopkov obdelave. Namen določbe drugega odstavka je predvsem preprečevanje potrebe po posegih v obstoječe aplikacije, v katerih se obdelujejo osebni podatki in ki ne omogočajo zavarovanja osebnih podatkov znotraj same aplikacije. Predlagana določba tako ne posega v nadaljnje opravljanje nalog upravljavca ali obdelovalca.

3. poglavje – Varnost osebnih podatkov

Predlagano tretje poglavje ureja varnost osebnih podatkov in ukrepe za zagotavljanje varnosti. Določene so posebne obdelave osebnih podatkov, ki so zaradi svojih lastnosti posebej občutljive in zahtevajo posebno urejanje in varovanje, prav tako pa je določena obveznost priprave ocene učinka na varstvo osebnih podatkov, ob upoštevanju pristojnosti za predlaganje zakonov.

K 21. členu (vodenje dnevnikov obdelav)

Člen daje pravno podlago za vzpostavitev in hrambo dnevniških zapisov (dnevnik obdelave) in za njegovo uporabo. Predlagana ureditev vključuje štiri kategorije tako imenovanih posebnih obdelav, in sicer:

1) obdelave z uporabo avtomatiziranih sistemov obdelave osebnih podatkov, s katerim se izvajajo obsežne obdelave posebnih vrst osebnih podatkov (preprečuje se sistemska oziroma avtomatična diskriminacija);

2) obdelave, s katerimi se redno in sistematično spremlja posameznike (posebej se nadzira obdelave osebnih podatkov v zvezi s profiliranjem);

3) obdelave, glede katerih je z oceno učinka ugotovljeno tveganje, ki ga je mogoče učinkovito upravljati z vodenjem dnevnika obdelave (določba predstavlja podlago za uvedbo dnevnikov obdelave po presoji upravljavca);

4) obdelave, glede katerih tako določa zakon (določba predstavlja podlago za uvedbo dnevnikov obdelave po presoji zakonodajalca).

Dnevniki obdelav je zapis, pogosto avtomatiziran, iz katerega je razvidno, da so se podatki obdelovali, kdaj so se obdelovali, kdo jih je obdeloval, kateri podatki so se obdelovali ter komu so bili posredovani (uporabnik). Gre za zapis, ki omogoča kasnejšo analizo v primeru ugotavljanja zakonitosti obdelave, nenazadnje pa tudi zagotavljanje celovitosti in varnosti podatkov ter za odpravljanje napak v delovanju informacijskega sistema. Tipično zahtevano funkcionalnost zagotavljajo sistemi sistemskih dnevnikov (npr. strežniški dnevniki ipd.) ali sistemi za zagotavljanje revizijske sledi. Drug zakon ali notranji akt lahko določa tudi druge sestavine dnevnika, ki so potrebni za doseganje namena, če to zahteva ocena učinka v zvezi s konkretno obdelavo. Z dnevnikom obdelav se zagotavlja notranjo sledljivost obdelav osebnih podatkov.

Drugi odstavek določa nabor podatkov, ki jih je treba zapisati v dnevnik za vsako od dejanj obdelave iz seznama v prvem odstavku. Med njimi je tudi identifikacija osebe, ki je izvedla dejanje obdelave. Oseba mora biti določljiva (določiti jo mora biti mogoče v primeru nadzora), kar

pomeni, da zadošča, če se vpiše identifikator, ki omogoča naknadno ugotovitev točne identitete osebe, ki je izvedla dejanje obdelave.

Tretji odstavek določa namene uporabe dnevnikov obdelave. Izven teh namenov dnevnikov ni dopustno uporabljati.

Za namen izvajanja nadzora nad zakonitostjo obdelave osebnih podatkov morata upravljavec oziroma obdelovalec nadzorniku IP omogočiti dostop do dnevnikov na njegovo zahtevo. Pri tem je treba upoštevati tudi določbe 20. člena (zavarovanje osebnih podatkov, ki so predmet postopka), na podlagi katerega lahko nadzornik odredi hrambo podatkov, ki je daljša od v tem členu določenega roka, če je to potrebno za izvedbo postopka za namen zavarovanja dokazov.

Dnevniške zapise je dovoljeno hraniti največ dve leti od konca leta v katerem so nastali, drug zakon pa lahko določa drugačne roke. Dvoletni rok je običajno zadosten za dosego namenov iz tega člena, vendar pa predlog zakona omogoča upravljavcem, da rok na podlagi ocene učinka (35. člen Splošne uredbe) podaljšajo. V takem primeru se sme dnevnik obdelave hraniti največ 5 let.

K 22. členu (varnost osebnih podatkov na področju posebnih obdelav)

Za določene zbirke, ki so zaradi svoje velikosti, podatkov, ki se v njej obdelujejo ali drugih lastnosti, posebej občutljive, se določa poseben sistem varovanja. Lastnosti, zaradi katerih zbirka velja za posebej občutljivo so navedene v prvem odstavku predlaganega 22. člena. Prva točka določa, da so občutljive zbirke tiste, ki so določene v zakonu s področja centralnega registra prebivalstva, prijave prebivališča, finančne uprave, državljanstva, Slovenske obveščevalno-varnostne agencije, obrambe, zbirke podatkov s področja zdravstvenega varstva, področja obveznega zdravstvenega zavarovanja, uveljavljanju pravic iz javnih sredstev ter kazenskih in prekrškovnih evidenc. Prav tako so občutljive obdelave osebnih podatkov v zbirkah, ki vsebujejo osebne podatke več kot 100.000 posameznikov, posebne osebne podatke več kot 10.000 posameznikov ali več kot 200.000 posameznikov, kadar se obdelujejo podatki v javnem sektorju.

Za navedene zbirke je treba izvajati ukrepe, da se onemogoča razkritje nepooblaščenim osebam in stalno preprečuje škodo varnosti, interesom Republike Slovenije ali človekovim pravicam in svoboščinam posameznikov, na katere se podatki nanašajo. To velja tudi za zbirke v zasebnem sektorju (drugi odstavek).

Posebne obdelave iz 1.-4. točka prvega odstavka, ki jih izvajajo navedeni subjekti javnega sektorja in ki vsebujejo biometrične ali zdravstvene osebne podatke ali podatke iz kazenskih in prekrškovnih evidenc, se smejo hraniti v zasebnem računalniškem oblaku le pod pogojem, da je fizična lokacija hrambe teh podatkov stalno znana v vseh fazah hrambe ter obdelave.

Določba implementira pooblastilo, ki ga daje Splošna uredba v tretjem odstavku 6. člena ter četrtem odstavku 9. člena – »Države članice lahko ohranijo ali uvedejo dodatne pogoje, tudi omejitve, glede obdelave genetskih, biometričnih ali podatkov v zvezi z zdravjem.« ter »Države članice bi morale imeti možnost, da ohranijo ali uvedejo dodatne pogoje, tudi omejitve, glede obdelave genetskih podatkov, biometričnih podatkov ali podatkov o zdravstvenem stanju. To pa ne bi smelo ovirati prostega pretoka osebnih podatkov v Uniji, kadar ti pogoji veljajo za čezmejno obdelavo takih podatkov« (53. uvodna navedba).

K 23. členu (ocena učinka glede obdelav osebnih podatkov)

Kot določata 35. in 36. člen Uredbe, je pod določenimi pogoji treba izdelati oceno učinka in opraviti predhodno posvetovanje z nadzornim organom. Informacijski pooblaščenec lahko na podlagi četrtega in petega odstavka 35. člena Splošne uredbe določi in objavi seznam vrst dejanj

obdelave, za katere velja zahteva po oceni učinka v zvezi z varstvom podatkov. Tak seznam je Informacijski pooblaščenec že sprejel.[68]

Oceno učinka je treba pripraviti tudi pred posebnimi obdelavami osebnih podatkov (22. člen). Ker imajo kršitve varnosti za posebne obdelave lahko škodljive posledice za varnost države, je treba v takšnem primeru izdelati tudi oceno učinka obdelav osebnih podatkov na varnost države, vključno z njenimi političnimi ali gospodarskimi koristmi, če bi bili podatki iz zbirke razkriti nepooblaščenim osebam ter pripravi ustrezne ukrepe za zmanjšanje tveganja. Tveganje se lahko zmanjšuje z ustreznimi varnostnimi politikami in logično-tehničnimi kontrolami, ki jih predvidita in dosledno izvajata upravljavec in obdelovalec. Oba morata tudi skrbeti za ustrezno organizacijsko kulturo, z namenom zagotavljanja višje ravni varnosti osebnih podatkov.

Tretji odstavek določa spremembe okoliščin, ki terjajo ponovno izdelavo (osvežitev).

Za posodabljanje in dosledno izvajanje ocene učinkov, vključno z v njej predvidenimi ukrepi za zmanjšanje tveganj je odgovoren predstojnik ali vodstveni organ upravljavca ali obdelovalca.

Predlagani peti odstavek ureja izdelavo ocene učinka v okviru zakonodajnega postopka. To velja tako za vladne predloge zakonov, poslanske predloge, zakonske predloge iz ljudske iniciative, če je po tem členu pred obdelavo treba opraviti oceno učinka. Kadar se z zakonom določa obdelava osebnih podatkov, za katero je treba izdelati oceno učinka, predlagatelj predlogu zakona priloži oceno učinka predvidenih dejanj obdelave na varstvo osebnih podatkov v skladu s 35. členom Splošne uredbe, na podlagi katere Informacijski pooblaščenec izda mnenje glede obdelave osebnih podatkov. Predlagatelj zakona se mora glede mnenja Informacijskega pooblaščenca opredeliti.

Šesti odstavek določa pripravo ocene učinka kot internega dokumenta, s smiselno uporabo določb 23. člena oziroma 35. člena Splošne uredbe. V zvezi s tem ni potrebna izvedba predhodnega posvetovanja po 36. členu Splošne uredbe. Oceno učinka se pripravi le za nove obdelave po uveljavitvi tega zakona. Ocena učinka je dostopna različnim nadzornim organom, ko izvajajo zakonsko določene nadzore.

4. poglavje – Nadzori

1. oddelek – Posebnosti postopka

4. poglavje v 1. oddelku določa temeljne določbe glede postopkovnih vprašanj v zvezi z izvajanjem nadzorov ali odločanj Informacijskega pooblaščenca.

K 24. členu (uporaba določb zakona, ki ureja splošni upravni postopek)

V postopkih pred Informacijskim pooblaščencem po določbah I. in II. dela tega zakona se uporabljajo določbe Zakona o splošnem upravnem postopku, če Predlog ZVOP-2 ne določa drugače (npr. 26. člen Predloga ZVOP-2, po katerem ni dopustna stranska udeležba).

K 25. členu (izvajanje postopkovnih dejanj brez prisotnosti)

Po predlaganem 25. členu v postopku po tem poglavju lahko Informacijski pooblaščenec opravlja razgovore z osebami pri upravljavcu ali obdelovalcu in s pričami brez prisotnosti posameznika, na katerega se nanašajo osebni podatki, v celoti ali deloma, če bi takšna prisotnost škodovala izvedbi uradnih postopkov ali varstvu ali uresničevanju človekovih pravic in temeljnih svoboščin

[68] https://www.ip-rs.si/fileadmin/user_upload/Pdf/Ocene_ucinkov/Seznam_dejanj_obdelav_osebnih_podatkov__za_katere_velja_zahteva_po_izvedbi_ocene_ucinka_v_zvezi_z_varstvom_osebnih_podatkov.pdf

tretjih oseb, o čemer odloči s sklepom in obvesti tega posameznika. V tem primeru Informacijski pooblaščenec tudi ne dovoli prisotnosti pri drugih dejanjih v postopku in posameznika ne seznani z opravljanimi procesnimi dejanji.

Posebej je v drugem odstavku upoštevano, da Informacijski pooblaščenec na področjih (zadevah) varnosti države in obrambe države opravlja razgovore z osebami pri upravljavcu ali obdelovalcu brez prisotnosti posameznika, na katerega se nanašajo osebni podatki, ter ne dovoli njegove prisotnosti pri drugih dejanjih v postopku in mu ne vroča zapisnikov o teh dejanjih. Navedena omejitev velja neposredno in ne obstaja pritožba, zato se ne izda poseben sklep.

Proti sklepu, s katerim se omeji prisotnost posameznika, na katerega se nanašajo osebni podatki, pri postopkovnih dejanjih po tem členu, ni pritožbe, sklep pa se sme izpodbijati skupaj z odločitvijo o glavni zadevi. Zoper vsebino iz sklepa iz prvega odstavka ni možnosti pritožbe, je možno izpodbijati le odločitev o glavni zadevi.

K 26. členu (izključitev stranske udeležbe)

V postopku po tem poglavju ni dopustna stranska udeležba, kot jo določa Zakon o splošnem upravnem postopku. Podobno je določeno v 30. členu ZVOPOKD.

Posameznik, na katerega se nanašajo osebni podatki, ima položaj stranke v postopku, s čimer so pravice posameznika ustrezno zaščitene tudi brez instituta stranske udeležbe. Razlog za izključitev stranske udeležbe morebitnih drugih oseb, ki bi se zaradi varstva svojih interesov in pravnih koristi želeli udeleževati postopka, je v varstvu učinkovitosti in integritete postopkov upravljavcev ter zagotavljanje varnosti osebnih podatkov, ki bi se obdelovali v nadzornem postopku. Te osebe lahko svoje interese in pravne koristi varujejo v samostojnih postopkih po tem zakonu, v katerih se rešujejo vprašanja njihovih osebnih podatkov.

K 27. členu (nadzorna pooblastila)

Predlagani 27. člen določa nadzorna pooblastila Informacijskega pooblaščenca, s podobno vsebino in s podobnimi varovalkami kot je to določeno v 31. členu ZVOPOKD. Predlagani člen samostojno (ne glede na določbe ZIN ali ZUP) določa dostop do dokumentacije, poslovnih knjig, kadar pa gre za poseg v upravičeno pričakovanje zasebnosti posameznika (zamejena zasebnost na delovnem mestu), pa o tem odloča preiskovalni sodnik. Pri izvedbi določenih posegov, ki so analogni hišni preiskavi, je poleg sodnega varstva določena tudi prisotnost predstavnikov zavezanca nadzora.

Predlagani sistem glede sodnega odločanja izhaja iz odločbe Ustavnega sodišča RS iz leta 2013[69]. Predlagani člen je delno določen tudi po vzoru rešitev iz 28. in 29. člena Zakona o preprečevanju omejevanja konkurence in 429. člena Energetskega zakona.

K 28. členu (nadzorni ukrepi)

Predlagani 28. člen ZVOP-2 samostojno določa nadzorne ukrepe Informacijskega pooblaščenca, ki so (prvi odstavek) podobni tistim, ki jih določa 32. člen ZVOPOKD. Le v 6. točki omenja ukrepe po ZIN in to samo preventivne ukrepe. V drugem odstavku se zaradi varstva svobode in nevtralnosti interneta in svobode izražanja delno zadrži določba, vsebinsko podobna drugemu odstavku 54. člena ZVOP-1, tako da se ukrepi sicer lahko uporabijo, vendar morajo biti milejši in ne posegati v vsebino drugih pravic.

Četrti odstavek določa omejitve nadzornih ukrepov, ki jih nadzorni organ ne sme uporabiti tako, da bi posegal v zadeve sodišč, kar bi se lahko zgodilo, če bi se izvajal nadzor nad zadevami

[69] Odločba US, št. U-I-40/12, 11. 4. 2013, Uradni list RS, št. 39/13 in OdlUS XX, 5.

sodne uprave, učinki ukrepa pa bi lahko posegli v neodvisno odločanje sodstva. Za kazenske zadeve sodišč je to urejeno v drugem odstavku 32. člena ZVOPOKD.

Peti odstavek določa možnost nadzorne osebe, da uporabi ukrepe tudi v postopkih s prijaviteljem s posebnim položajem in v inšpekcijskem postopku.

2. oddelek – Položaj prijavitelja s posebnim položajem

K 29. členu (prijava in prijavitelj s posebnim položajem)

V predlaganem 29. členu sta definirana prijavitelj s posebnim položajem in prijava. Posameznik, ki meni, da določena obdelava njegovih osebnih podatkov krši določbe Splošne uredbe, tega zakona ali drugih zakonov, ki urejajo obdelavo ali varstvo osebnih podatkov, ima po predlaganem zakonu tudi možnost vložitve neposredne zahteve v skladu z Zakonom o splošnem upravnem postopku pri Informacijskem pooblaščencu, na podlagi katere lahko Informacijski pooblaščenec ukrepa glede obdelave njegovih osebnih podatkov, kadar odkrije kršitve, posameznik pa lahko v zahtevi za primer odkritja kršitev predlaga tudi ustrezne ukrepe (npr. izbris, popravek). Taka zahteva je poimenovana kot »prijava«. Prijava in poimenovanje »prijavitelj s posebnim položajem« kažeta na pomen tega postopka z vidika lažjega razumevanja in boljšega uresničevanja ali varovanja pravic posameznika, in to ob upoštevanju, da je treba posamezniku zagotoviti osebno zadoščenje (ne samo ugotovitev kršitve, ampak tudi druga aktivna ukrepanja, kot so npr. popravek ali izbris osebnih podatkov) ter zato nadzornemu organu zagotoviti učinkovita nadzorna pooblastila (pooblastila in ukrepi iz 27. in 28. člena predloga zakona). Položaj prijavitelja s posebnim položajem je na tak način urejen tudi v zakonu, ki ureja varstvo osebnih podatkov pri obravnavanju kaznivih dejanj.

K 30. členu (obravnavanje prijave)

V predlaganem prvem odstavku 30. člena je določeno, da je po tem zakonu uvedba postopka nadzora obligatorna kadar je vložena prijava iz 29. člena tega zakona. Prijava mora vsebovati vse sestavine, kot jih določa Zakon o splošnem upravnem postopku ter navedbo upravljavca ali obdelovalca in navedbo kršitev pri obdelavi ali varnosti njegovih osebnih podatkov, iz katerih izhaja kršitev predpisov iz prejšnjega člena (Splošne uredbe, tega zakona ali drugih zakonov, ki urejajo obdelavo ali varstvo osebnih podatkov, ali krši določbe s temi zakoni povezanih podzakonskih predpisov ali splošnih aktov za izvrševanje javnih pooblastil).

Drugi odstavek določa rok za odločitev nadzornega organa. Zakon o splošnem upravnem postopku določa za izvedbo upravnega postopka rok enega meseca za enostavne oziroma rok dveh mesecev za zahtevnejše postopke. Ker se bodo nadzori po določbah tega zakona nanašali tudi na zasebni sektor, ali pa bo šlo za čezmejne obdelave osebnih podatkov, predlog določa daljši rok (tri mesece) z možnostjo podaljšanja za dodaten mesec dni.

K 31. členu (pravice prijavitelja s posebnim položajem)

V predlaganem prvem odstavku 31. člena je določeno, da nadzorni organ prijavitelja na njegovo zahtevo, izraženo v prijavi ali v naknadni komunikaciji, obvešča o svojih ukrepih. Obveščanje daje prijavitelju možnost, da se seznani s stanjem postopka. Za področje varnosti države je določena izjema od obveščanje, vendar pa je zagotovljena kontradiktornost postopka po drugem odstavku istega člena.

Drugi odstavek določa, da se prijavitelj lahko vključi v postopek, ko so znane vse preliminarne ugotovitve, bistvene za odločbo. Takrat prijavitelj lahko poda pripombe ustno ali pisno v roku najmanj dveh delovnih dni, kot mu ga določi nadzorni organ. Nadzorni organ se po prejemu pripomb do njih opredeli v odločbi. Na ta način se uravnoteži pravica do kontradiktornega

postopka na eni strani in interes države po zagotavljanju integritete postopkov na drugi, kar pride v poštev le pri omejitvah pravic in obveznosti iz 23. člena Splošne uredbe, ko gre za razloge varnosti in obrambe države, prijaviteljev po sedmem odstavku 13. člena Zakona o integriteti in preprečevanju korupcije, virov prijave po Zakonu o inšpekcijskem postopku, poklicne skrivnosti, virov novinarjev itd. Možnost, da se stranka v postopku izjasni glede osnutka odločbe, ki vsebuje vse za odločitev relevantne okoliščine, zagotavlja zadostno kontradiktornost postopka.

K 32. členu (položaj nadzorovanega upravljavca ali obdelovalca)

Predlagani prvi odstavek 32. člena določa, da imata upravljavec in obdelovalec položaj stranke v postopku, saj lahko kot nosilec pravic in obveznosti uveljavlja tudi določene ugovore, pravice ipd. in ima pravico biti neposredno prisoten pri vseh postopkovnih dejanjih.

Drugi odstavek določa, da lahko upravljavec in obdelovalec na ugotovitve, bistvene za odločbo (kot tudi prijavitelj) podata pripombe, do katerih se mora nadzorni organ opredeliti. S tem se zagotavlja kontradiktornost postopka v delu, ki se nanaša na odločbo in vse okoliščine, ki so pomembne za odločitev. Predlagana ureditev zagotavlja postopkovno enakost v razmerju do zakonsko določenih pravic prijavitelja s posebnim položajem in glede možnosti sodelovanja v postopku (drugi odstavek 31. člena predloga zakona).

K 33. členu (odločba)

Predlagani prvi odstavek 33. člen določa vsebino odločbe izdane v nadzornem postopku po tem oddelku, podobno kot to že določa 15. člen za upravljavce in obdelovalce, ki so državni organi ali organi samoupravnih lokalnih skupnosti. Odločba mora poleg sestavin po zakonu, ki ureja splošni upravni postopek vsebovati še sestavine iz predlaganega 33. člena. Posebno pozornost je treba nameniti dovoljenemu obsegu pregleda spisa (3. točka prvega odstavka 33. člena) s strani prijavitelja s posebnim položajem, obvezna sestavina odločbe so tudi odrejeni ukrepi upravljavcu ali obdelovalcu in rok za njihovo izvedbo, kot sama ugotovitev o obstoju ali neobstoju zatrjevane kršitve.

Drugi odstavek določba izjemo od obveznosti obrazložitve odločbe po pravilih zakona, ki ureja splošni upravni postopek v primeru, ko bi navedba razlogov za zavrnitev ali omejitev dostopa ogrozila izvrševanje namena zavrnitve ali omejitve dostopa iz 23. člena Splošne uredbe, ki ga določa zakon. Prav tako odločba ne obsega navedb, s katerimi bi se potrdilo ali zanikalo izvajanje ali neizvajanje prikritih preiskovalnih ukrepov iz zakona, ki ureja Slovensko obveščevalno varnostno agencijo ali zakona, ki ureja obrambo.

Tretji odstavek določa, da se del obrazložitve, ki se nanaša na konkretne razloge, enako kot v četrtem odstavku 15. člena zapiše v prilogo odločbe, ki se strankam ne vroča, priloga pa mora biti opremljena s številko zadeve, datumom in podpisom pristojne uradne osebe. V primeru sodnega varstva je priloga dostopna pristojnemu sodišču.

Ker v nadzorih, izvajanih s strani Informacijskega pooblaščenca, ni drugostopenjskega upravnega organa, ki bi odločal o pritožbi, postane odločba izvršljiva z vročitvijo prijavitelju in nadzorovanemu upravljavcu ali obdelovalcu.

K 34. členu (ukrepanje glede obdelav osebnih podatkov drugih posameznikov)

Predlagani 34. člen določa, da če nadzorni organ v postopku nadzora po tem oddelku zazna sum kršitve varstva pravic glede osebnih podatkov, ki bi lahko vplivale na druge posameznike, lahko poleg že tekočega postopka, iz katerega izvirajo začetne ugotovitve, uvede tudi inšpekcijski nadzor. Postopek po prijavi prijavitelja s posebnim položajem se torej nadaljuje v skladu s predhodnimi določbami tega zakona, nadzorni organ pa se lahko odloči, da uvede sočasni

nadzor (predvidoma glede širšega kroga posameznikov) v javnem interesu, torej nadzor v povezavi z Zakonom o inšpekcijskem nadzoru.

3. oddelek – Inšpekcijski nadzor glede varstva osebnih podatkov

K 35. členu (uporaba zakona, ki ureja inšpekcijski nadzor)

Predlagani 35. člen določa, da se v inšpekcijskem nadzoru po tem zakonu neposredno uporabljajo določbe 17. člena tega zakona (omejitev pravic in obveznosti), 25.-28. člena (posebnosti postopka – izvajanje postopkovnih dejanj brez prisotnosti, izključitev stranske udeležbe, nadzorna pooblastila in nadzorni ukrepi) ter prvega, drugega in tretjega odstavka 33. člena (vsebina odločbe – glede konkretnih razlogov za zavrnitev ali omejitev dostopa in priloge k odločbi). Za vsa ostala vprašanja se uporablja Zakon o inšpekcijskem nadzoru.

K 36. členu (uvedba inšpekcijskega nadzora)

Predlagani 36. člen v prvem odstavku določa, da Informacijski pooblaščenec uvede postopek inšpekcijskega nadzora v javnem interesu (*ex offo*) skladno z Zakonom o inšpekcijskem nadzoru.

Drugi odstavek določa, da Informacijski pooblaščenec postopek, razen po prijavi (ki je posebej urejena v 29. členu predloga zakona), uvede tudi na pobudo drugih organov (državni organi, nadzorne javne agencije Republike Slovenije) in na pobudo nadzornih organov za varstvo osebnih podatkov držav članic Evropske unije in Sveta Evrope.

K 37. členu (letni načrt nadzorov in poročanje)

Zakon, ki ureja Informacijskega pooblaščenca v 14. členu že določa, da Informacijski pooblaščenec letno pripravlja poročila o svojem delu tako s področja varstva osebnih podatkov kot s področja dostopa do informacij javnega značaja in ga pošlje državnemu zboru najpozneje do 31. maja za preteklo leto ter ga objavi na svoji spletni strani.

Predlagani 37. člen v prvem odstavku nalaga Informacijskemu pooblaščencu, da pripravi letni načrt nadzorov, v katerem posebej opredeli nadzore na področju posebnih zbirk iz 22. člena tega zakona. Gre za zbirke določene v zakonih, ki urejajo centralni register prebivalstva, prijavo prebivališča, finančno upravo, državljanstvo, Slovensko obveščevalno-varnostno agencijo, obrambo, zbirke podatkov s področja zdravstvenega varstva, področja obveznega zdravstvenega zavarovanja, uveljavljanju pravic iz javnih sredstev ter kazenskih in prekrškovnih evidenc, ali kadar se na podlagi zakonov obdelujejo osebni podatki več kot 100.000 posameznikov, ali kadar upravljavec ali obdelovalec obdeluje predvsem posebne vrste osebnih podatkov, ali kadar se v zbirki obdeluje posebne vrste osebnih podatkov več kot 10.000 posameznikov, ali v zasebnem sektorju, kadar se obdelujejo osebni podatki več kot 200.000 posameznikov. Za vse omenjene zbirke veljajo posebni ukrepi, s katerimi se dodatno zagotavljata varnost in tajnost osebnih podatkov, zato je tudi zaradi zagotavljanja zaupanja v zakonito obdelavo osebnih podatkov potrebno, da se opravljalo redni načrtovani nadzori.

5. poglavje – Posebne določbe

K 38. členu (posredovanje osebnih podatkov, ki ga izvedejo osebe javnega sektorja)

Člen ureja posredovanje osebnih podatkov osebam javnega sektorja ali tretjim osebam, ki ga izvedejo osebe javnega sektorja. Za takšno posredovanje je potrebna pravna podlaga, kot jo določa 6. člen predloga ZVOP-2. Prejemniki (uporabniki) podatkov (fizične in pravne osebe) jih smejo obdelovati le za namene, za uresničevanje katerega se jim ti podatki posredujejo.

Enaki pogoji kot za posredovanje osebnih podatkov, veljajo tudi za posebne osebne podatke, poleg tega pa morajo biti izpolnjeni tudi pogoji, ki jih določa 9. člen Uredbe ali 10. člen tega zakona.

Posredovanje podatkov je brezplačno, drug zakon pa lahko določa drugačno ureditev.

Kot posebnost je urejeno posredovanje podatkov iz registra stalnega prebivalstva, matičnega registra in centralnega registra, ki se lahko posredujejo upravičencu, ki izkaže zakoniti interes za uveljavljanje pravic pred osebami javnega sektorja. Upravičenec lahko pridobi podatke o osebnem imenu in naslovu stalnega ali začasnega prebivališča oziroma stalnem ali začasnem naslovu prebivališča v drugi državi, naslovu za vročanje ali datumu smrti posameznika, če te podatke v konkretni zadevi potrebuje. Pri normiranju predlagatelj izhaja iz drugega odstavka 22. člena veljavnega ZVOP-1.

Peti odstavek določa obveznost uporabnikov podatkov iz pristojnosti Ministrstva za notranje zadeve, da na lastne stroške vzpostavijo varnostne mehanizme, ki jih zaradi posebne občutljivosti posameznih evidenc s področja upravnih notranjih zadev določi minister za notranje zadeve s pravilnikom. Te evidence so posebej varovane tudi z 22. členom tega zakona.

Šesti odstavek določa drugačen režim za podatke s področja varnosti države in obrambe. Posredovanje podatkov je treba urediti v področnih zakonih.

K 39. členu (posredovanje podatkov, ki ga izvajajo osebe zasebnega sektorja)

Člen ureja posredovanje osebnih podatkov iz zasebnega sektorja drugim osebam (subjektom javnega ali zasebnega sektorja in pravnim ali fizičnim osebam). Takšno posredovanje je dovoljeno na podlagi 40. člena, v kateri mora biti navedena pravna podlaga za pridobitev podatkov. Drug zakon lahko vprašanje posredovanja podatkov uredi drugače.

Drugi odstavek določa brezplačnost posredovanja osebnih podatkov subjektom javnega sektorja, če drug zakon ne določa drugače.

K 40. členu (postopek posredovanja osebnih podatkov)

Člen ureja postopek za posredovanje osebnih podatkov in vsebino zahteve (prvi odstavek).

Drugi odstavek določa 15 dnevni rok za posredovanje podatkov. V istem roku lahko upravljavec posredovanje zavrne in prosilca o razlogih obvesti, v istem roku pa se lahko upravljavec in vlagatelj zahteve dogovorita za podaljšanje roka.

Tretji odstavek določa pravno fikcijo zavrnitve zahteve v primeru molka (prim. molk organa; četrti odstavek 222. člena ZUP). Posebno fikcijo je treba urediti, ker ZUP ne velja za vse upravljavce.

Četrti odstavek določa obveznost prosilca, da pred zahtevo za sodno varstvo uporabi možnost pritožbe v primeru zavrnitve zahteve. Kot drugostopenjski organ v takem primeru nastopa Informacijski pooblaščenec, razen v primeru, ko Informacijski pooblaščenec nastopa kot prvostopenjski organ – v tem primeru ni drugostopenjskega organa in ima prosilec neposredno po zavrnitvi zahteve na prvi stopnji možnost tožbe v upravnem sporu. Člen ureja tudi stvarno pristojnost sodišč v zvezi z zahtevki. Upravno sodišče je pristojno za upravni spor zoper odločitve o zavrnitvi zahtev za pridobitev podatkov iz uradnih evidenc in javnih knjig. Kadar gre za druge evidence (npr. v zasebnem sektorju), je za odločanje pristojno sodišče splošne pristojnosti, ki odloča v nepravdnem postopku.

Peti odstavek določa izjemo v zvezi s sodnimi, upravnimi in drugimi uradnimi postopki. Na primer vpogled v sodni spis in pridobivanje podatkov iz spisa urejajo postopkovni zakoni (npr. ZKP, ZPP itd.).

Šesti in sedmi odstavek določata obveznost in obdobje hrambe podatkov o posredovanju osebnih podatkov. Dvoletni rok je namenjen učinkovitemu izvajanju prekrškovnih postopkov v primeru kršitve. Drugi zakoni lahko določijo drugačne roke hrambe podatkov o posredovanju.

Določbe o zunanji sledljivosti iz šestega in sedmega odstavka veljajo tudi za obdelovalce (osmi odstavek).

Deveti odstavek določa da obvezno zagotavljanje zunanje sledljivosti iz šestega in sedmega odstavka ne velja za upravljavce, ki zakonito javno objavijo osebne podatke ali so osebni podatki po zakonu javni.

K 41. členu (uporaba povezovalnih znakov)

Člen ureja omejitve pri povezovanju zbirk podatkov in pridobivanju podatkov iz njih.

Prvi odstavek določa omejitev za pridobivanje podatkov iz zbirk, ko to počne uradna oseba. Omejitev se nanaša na zbirke s področja zdravstva, varnosti države (kar vključuje tudi obrambo države), sodstva, kazenske ter prekrškovne evidence. Omejitev pomeni, da mora uradna oseba za pridobitev podatkov iz navedenih evidenc vnesti vsaj dva iskalna pogoja (npr. EMŠO in ime in ne zgolj EMŠO ali samo ime). Na ta način se doseže manjše število napak pri obdelavah osebnih podatkov (nenamerni vpogled). Omejitev se ne uporablja za avtomatsko povezovanje informacijskih sistemov, za te namene se lahko uporablja tudi samo en ustrezen povezovalni znak. Odstavek določa omejitev pridobivanja podatkov iz navedenih zbirk.

Drugi odstavek ureja izjemo od omejitve, določene v prvem odstavku. Za namen odkritja storilca ali kaznivega dejanja, ki se preganja po uradni dolžnosti ali za namen zavarovanja življenja ali telesa posameznika je dovoljeno osebne podatke iz zbirk pridobiti tudi na podlagi le enega povezovalnega znaka. Izjema je uporabna na primer pri iskanju pogrešane osebe, kjer niso znani vsi osebni podatki pogrešane osebe. Za namen zavarovanja življenja sme operater mobilne telefonije pregledati zbirke in po njih iskati tudi samo po imenu in tako pridobiti podatke o lokaciji mobilne naprave, ki pripada pogrešani osebi.

Na področju varnosti države tretji odstavek določa izjemo od prvega odstavka, in sicer mora morebitno izjemo določiti notranji akt organa. Pravila, določena z notranjim aktom, morajo omogočati sledljivost obdelav osebnih podatkov.

Četrti odstavek določa, da se določbe prvega odstavka ne uporabljajo za povezovanje navedenih zbirk z drugimi zbirkami (npr. za namen posodabljanja navedenih zbirk s podatki iz drugih zbirk).

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

Prvi odstavek določa rok hrambe osebnih podatkov v javnem sektorju. Kadar obdelave osebnih podatkov določa zakon, mora ta določiti tudi rok hrambe. Kadar se podatki v javnem sektorju obdelujejo na drugih podlagah (tretji in četrti odstavek 7. člena tega zakona), jih je dopustno hraniti do dosega namena obdelave.

Drugi odstavek določa obveznost upravljavca, da redno preverja, ali so izpolnjeni pogoji za prenehanje hrambe osebnih podatkov. Preverjanje mora biti ustrezno dokumentirano.

Tretji odstavek določa ravnanje z osebnimi podatki po prenehanju namena obdelave. Osebni podatki se izbrišejo, uničijo ali anonimizirajo, zakon pa lahko določa tudi druge načine postopanja (npr. omejevanje dostopa, blokiranje, arhiviranje).

6. poglavje – Pooblaščene osebe za varstvo osebnih podatkov

K 43. členu (pooblaščena oseba za varstvo osebnih podatkov)

Splošna uredba v določbah od 37. do 39. člena že ureja imenovanje, položaj in naloge pooblaščene osebe za varstvo osebnih podatkov. S tem zakonom se dodatno urejajo zgolj posebnosti, ki jih uredba ne ureja. Predlagani 43. člen tako le določa, da je to oseba, ki upravljavcu ali obdelovalcu v skladu z 39. členom Splošne uredbe na neodvisen način svetuje pri zagotovitvi skladnosti obdelave z zakonom.

K 44. členu (obveznost določitve pooblaščene osebe)

Predlagani prvi odstavek 44. člena ureja obveznost upravljavcev in obdelovalcev za določitev pooblaščene osebe za varstvo osebnih podatkov v javnem in zasebnem sektorju v skladu s 37. členom Splošne uredbe. Ta določa obveznost imenovanja kadar obdelavo opravljajo javni organi, razen za sodišča, kadar delujejo kot sodni organi (glej drugi odstavek 47. člena predloga zakona), za dejanja obdelave, pri katerih je treba zaradi njihove narave, obsega in/ali namenov posameznike, na katere se nanašajo osebni podatki, redno in sistematično obsežno spremljati, ali kadar temeljne dejavnosti upravljavca ali obdelovalca zajemajo obsežno obdelavo posebnih vrst podatkov v skladu z 9. členom Splošne uredbe (obdelava posebnih vrst osebnih podatkov) in osebnih podatkov v zvezi s kazenskimi obsodbami in prekrški iz 10. člena Splošne uredbe, ter obdelave iz 1. do 4. točke prvega odstavka 22. člena tega zakona (ti. posebne obdelave).

Drugi odstavek določa, da lahko ne glede na pogoje iz prvega odstavka upravljavci in obdelovalci prostovoljno določijo pooblaščeno osebo za varstvo osebnih podatkov.

Tretji odstavek ureja možnost določitve namestnika pooblaščene osebe za varstvo osebnih podatkov za čas zadržanosti ali odsotnosti, ki v tem primeru opravlja vse naloge kot jih določa Splošna uredba v 38. in 39. členu za imenovano pooblaščeno osebo za varstvo osebnih podatkov in ta zakon.

Četrti odstavek ureja obveznost vnosa podatka o pooblaščeni osebi za varstvo osebnih podatkov v evidence dejavnosti obdelave v skladu s 30. členom Splošne uredbe, objavo kontakta zlasti na spletni strani in obveznost posredovanja podatkov nadzornemu organu, ki jih za potrebe izvajanja nalog vključi v seznam pooblaščenih oseb. Ta seznam ni dostopen javnosti, namenjen je le izvajanju nalog nadzornega organa, ko se v skladu s Splošno uredbo obrača neposredno na pooblaščeno osebo pri upravljavcu ali obdelovalcu.

K 45. členu (pogoji za določitev pooblaščene osebe)

Splošna uredba v 5. odstavku 37. člena določa, da se pooblaščena oseba za varstvo podatkov imenuje na podlagi poklicnih odlik in zlasti strokovnega znanja o zakonodaji in praksi na področju varstva podatkov ter zmožnosti za izpolnjevanje nalog iz 39. člena. Predlagani prvi odstavek 45. člena podrobneje določa pogoje za določitev pooblaščene osebe za varstvo podatkov in njenega namestnika, ki morata biti poslovno sposobna, imeti znanja in praktične izkušnje s področja varstva osebnih podatkov in nista pravnomočno obsojena na kazen najmanj šestih mesecev zapora oziroma nista pravnomočno obsojena za kaznivo dejanje glede zlorabe osebnih podatkov ali kraje identitete.

Drugi odstavek posebej za pooblaščeno osebo v državnem organu postavlja pogoj, da je zaposlena v javnem sektorju. Ne velja pa ta obveznost za organe samoupravnih lokalnih skupnosti in ostalih organov javnega sektorja, zlasti pa ne za zasebni sektor. Za državne organe je tako na podlagi pooblastila iz drugega oziroma tretjega odstavka 6. člena Splošne uredbe poleg teh usmeritev še dodatni pogoj, da je zaposlena v javnem sektorju.

Tretji odstavek ureja možnost določitve pooblaščene osebe v javnem sektorju (razen državnih organov) osebo iz zasebnega sektorja s pisno pogodbo v primeru, ko je ni mogoče določiti znotraj osebe javnega sektorja ali ni mogoče določiti skupne pooblaščene osebe z drugimi upravljavci ali obdelovalci.

Četrti odstavek ureja možnost določitve pooblaščene osebe v zasebnem sektorju izmed zaposlenih ali s pisno pogodbo določijo drugega posameznika ali pravno osebo. Kadar se določi pravna oseba je potrebno v pogodbi določiti posameznika, ki odgovarja za delo pravne osebe kot pooblaščene osebe in katere kontaktni podatki se objavijo v skladu s tem zakonom.

Peti in šesti odstavek urejata primere nasprotja interesov pooblaščene osebe z interesi upravljavca ali obdelovalca ali njegovimi drugimi nalogami in položajem, ki ga ima pri upravljavcu ali obdelovalcu. Take osebe se ne sme določiti za pooblaščeno osebo. V javnem sektorju se šteje, da je v nasprotju interesov oseba, ki je na položaju predstojnika, če je član organov upravljanja ali nadzora pri upravljavcu ali obdelovalcu, če njegove naloge vključujejo sistemsko odločanje o obdelavi osebnih podatkov ali upravljavca ali obdelovalca zastopa v sodnih ali arbitražnih postopkih v zvezi s vprašanji varstva osebnih podatkov. Če taka oseba zve, da je v nasprotju interesov o tem takoj obvesti upravljavca ali obdelovalca in se jo razreši opravljanja naloge. Enako velja za namestnika. Te določbe za javni sektor se smiselno uporabljajo tudi za zasebni sektor.

K 46. členu (skupna določitev pooblaščene osebe)

V predlaganem 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, organom javnega sektorja, 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 širšem smislu samostojni in neodvisni (svobodni) poklic (prvi odstavek 137. člena Ustave Republike Slovenije) je dodan poseben odstavek, po katerem se 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. Enako je določeno tudi za notarje (javna služba po drugem odstavku 137. člena Ustave Republike Slovenije), omogočeno je, da lahko notarji v dogovoru z Notarsko zbornico Slovenije določijo skupno pooblaščeno osebo, ni pa nujno da je zaposlena na Notarski zbornici Slovenije.

K 47. členu (naloge pooblaščene osebe)

Osnovne naloge pooblaščene osebe določa 39. člen Splošne uredbe. Ta določa, da ima pooblaščena oseba za varstvo podatkov vsaj naslednje naloge: (a) obveščanje upravljavca ali obdelovalca in zaposlenih, ki izvajajo obdelavo, ter svetovanje navedenim o njihovih obveznostih v skladu s to uredbo in drugimi določbami prava Unije ali prava države članice o varstvu podatkov; (b) spremljanje skladnosti z uredbo, drugimi določbami prava Unije ali prava države članice o varstvu podatkov in politikami upravljavca ali obdelovalca v zvezi z varstvom osebnih podatkov, vključno z dodeljevanjem nalog, ozaveščanjem in usposabljanjem osebja, vključenega v dejanja obdelave, ter s tem povezanimi revizijami; (c) svetovanje, kadar je to zahtevano, glede

ocene učinka v zvezi z varstvom podatkov in spremljanje njenega izvajanja v skladu s 35. členom te uredbe; (d) sodelovanje z nadzornim organom; (e) delovanje kot kontaktna točka za nadzorni organ pri vprašanjih v zvezi z obdelavo, vključno s predhodnim posvetovanjem iz 36. člena te uredbe, in, kjer je ustrezno, posvetovanje glede katere koli druge zadeve.

Predlagani prvi odstavek 47. člena določa, da pooblaščena oseba omenjene naloge iz 39. člena Splošne uredbe opravlja na neodvisen način ter zlasti svetuje in pomaga pri ocenjevanju tveganj v zvezi z obdelavami osebnih podatkov v zbirkah, ki jih izvaja upravljavec oziroma obdelovalec za katerega je določena. Naloge pooblaščene osebe so torej omejene zgolj na obveščanje, svetovanje in pomoč upravljavcem in obdelovalcem glede njihovih obveznosti in ne pomenijo prevzema odgovornosti za zagotavljanje skladnosti obdelav osebnih podatkov. Za zagotavljanje skladnosti obdelave osebnih podatkov z določbami Splošne uredbe in zakonov se upravljavci in obdelovalci odgovornosti za kršitve skladnosti ne morejo rešiti s sklicevanjem na neustrezno delo pooblaščene osebe.

Drugi odstavek se nanaša na prepoved opravljanja omenjenih nalog pooblaščene osebe v zvezi z obdelavami osebnih podatkov v konkretnih zadevah sodišč ali zadev Ustavnega sodišča, kadar le-to obravnava zadeve sodišč.

Za Ustavno sodišče Republike Slovenije je primerljivo (kot za neodvisna sodišča) je 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.

K 48. členu (določitev pooblaščenih oseb in njihove naloge v določenih državnih organih)

V predlogu člena so glede na posebne ustavne položaje ali določene ustavne vrednote določena pravila glede določitve pooblaščenih oseb pri posameznih državnih organih.

V prvem odstavku je najprej določeno, da mora Vrhovno sodišče Republike Slovenije določiti (le) eno pooblaščeno osebo, ki opravlja naloge za vsa sodišča s splošno pristojnostjo in specializirana sodišča v Republiki Sloveniji – torej centralizirani pristop.

V drugem odstavku je določen centraliziran pristop tudi za vsa državna tožilstva ter za Državnotožilski svet, da namreč Vrhovno državno tožilstvo Republike Slovenije določi eno pooblaščeno osebo, ki opravlja naloge pooblaščene osebe zakona za vsa državna tožilstva v Republiki Sloveniji ter za Državnotožilski svet kot samostojni pravosodni državni organ.

V tretjem 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). 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 varnosti in obrambe države je v četrtem odstavku določeno, da predstojnik organa (Slovenska obveščevalno-varnostna agencija, Obveščevalno varnostna služba Ministrstva za obrambo) s tega področja določi eno pooblaščeno osebo in njenega namestnika znotraj organa s tega področja, ki opravlja tiste naloge iz člena 39 Splošne uredbe, za katere tako določi predstojnik, med njih pa so po zakonu 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 prenosov osebnih podatkov.

V petem 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 Ministrstvu za javno upravo ali v kateri od upravnih enot.

K 49. členu (dolžnost varstva tajnosti osebnih podatkov)

Predlagani 49. člen določa, da sta pooblaščena oseba in njen namestnik pri opravljanju dela pooblaščene osebe zavezana k varstvu tajnosti obdelovanih osebnih podatkov. Ta obveznost velja tudi po prenehanju delovnega razmerja ali opravljanja nalog pooblaščene osebe na drugih podlagah. Pridobljene informacije smeta uporabljati izključno za opravljanje nalog in so tudi po zaključku dejavnosti zavezane k varstvu tajnosti osebnih podatkov. Dolžnost velja zlasti v zvezi z identiteto posameznika, na katerega se nanašajo osebni podatki, ki se je obrnil na pooblaščeno osebo.

7. poglavje – Kodeksi ravnanja in potrjevanje

K 50. členu (kodeksi ravnanja)

V predlaganem 50. členu se tako ureja kodekse ravnanja - podana je pravna podlaga, ki omogoča uporabo kodeksov ravnanja, tj. pravil dobre prakse na področju posameznih vrst obdelav osebnih podatkov, ki jih pripravijo relevantna domača ali tuja združenja podjetij v določenem sektorju, in so že prilagojena posebnostim manjših, srednjih oziroma večjih podjetij. Člen predvideva uporabo kodeksov, ki so potrjeni na različnih nivojih nadzornih organov; tako s strani posameznega državnega nadzornega organa, kot tudi širše, s strani Evropskega Odbora za varstvo osebnih podatkov po 68. členu 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*)[70], 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 51. členu (potrjevanje)

V predlaganem 51. členu ZVOP-2 se ureja sistem potrjevanja (certificiranja) obdelav osebnih podatkov. V prvem odstavku je tako določena definicija potrjevanja, 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 potrjevanja (vsebinski kriterij) ter da se o ugotovitvi takšne skladnosti se upravljavcu ali obdelovalcu izda certifikat (oblastveni kriterij). Predmet potrjevanja 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 potrjevalnega mehanizma odobri z odločbo Informacijski pooblaščenec v skladu s petim odstavkom 42. člena Splošne uredbe ali Evropski

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

Odbor za varstvo osebnih podatkov v skladu s petim odstavkom 42. člena Splošne uredbe ter v zvezi s 63. členom 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 potrjevalnih mehanizmov, ki jih je odobril in ta seznam sprotno objavlja na svoji spletni strani.

K 52. členu (postopek akreditiranja teles za potrjevanje)

V predlaganem 52. členu ZVOP-2 se v skladu s 121. členom Ustave Republike Slovenije predaja javno pooblastilo za izvajanje potrjevanja 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 43. člena Splošne uredbe in Zakona o akreditaciji[71] (torej tudi pooblastilo na podlagi zakona). Dodatne zahteve glede potrjevanja v skladu s točko b prvega odstavka in tretjim odstavkom 43. člena Splošne uredbe določi Informacijski pooblaščenec.

Po drugem odstavku pred izdajo pooblastila zunanjemu potrjevalnemu telesu Slovenska akreditacija v skladu s prvim odstavkom 43. člena Splošne uredbe o vlogi zainteresiranega subjekta obvesti Informacijskega pooblaščenca, ki preveri izpolnjevanje dodatnih zahtev v skladu s točko b prvega odstavka in tretjim odstavkom 43. člena 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 potrjevanje zunanjemu potrjevalnemu telesu, če je ugotovljeno, da pogoji za pooblastilo niso ali niso več izpolnjeni, ali, da so bili ukrepi, ki jih je v postopku potrjevanja izvedlo pooblaščeno potrjevalno 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. Po prehodni določbi 120. člena Predloga ZVOP-2 pa Slovenska akreditacija začne izvajati postopke akreditacije 1. januarja 2023.

8. poglavje – Nadzorni organ za varstvo osebnih podatkov Republike Slovenije

K 53. členu (nadzorni organ za varstvo osebnih podatkov)

Predlagani člen določa institucionalno določbo, po kateri je nadzorni organ Republike Slovenije za varstvo osebnih podatkov, Informacijskega pooblaščenca, kot je bil že do sedaj (glejte tudi definicijsko 1. točko drugega odstavka 6. člena Predloga ZVOP-2). Podobno je določeno 75. členu ZVOPOKD. Po drugem odstavku predlaganega člena zoper odločitve nadzornega organa ni dovoljena pritožba, je pa dopusten upravni spor v skladu z zakonom, ki ureja upravni spor. Informacijski pooblaščenec je samostojni in neodvisni državni organ, ki je del izvršilne veje oblasti, ni pa del Vlade.

[71] Uradni list RS, št. 59/99.

K 54. členu (pristojnosti nadzornega organa)

Predlagani 54. člen ZVOP-2 v prvem odstavku določa pristojnosti Informacijskega pooblaščenca, poleg nalog, ki so že določene v 57. členu Splošne uredbe.

Po drugem odstavku Informacijski pooblaščenec izvaja pristojnosti in naloge iz prvega odstavka zaradi javnega interesa brezplačno. Po tretjem odstavku nadzore po ZVOP-2 izvajajo nadzorne osebe, pri nadzoru pa lahko sodeluje strokovno osebje nadzornega organa.

K 55. členu (javnost dela)

Po predlaganem prvem odstavku 55. člena ZVOP-2 Informacijski pooblaščenec lahko poleg nalog iz 57. člena Splošne uredbe opravlja tudi dodatne naloge, ki so navedene v tem členu. Gre predvsem za obveščanje in osveščanje javnosti.

V drugem odstavku je določena možnost sodelovanja nevladnih organizacij pri opravljanju določenih nalog nadzornega organa.

K 56. členu (omejitve pri izvajanju nadzorov)

Po predlaganem 56. členu ZVOP-2 **n**adzorne osebe Informacijskega pooblaščenca niso pristojne za nadzore glede 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. Prav tako niso pristojne za nadzore glede obdelav osebnih podatkov, izvedenih v okviru neodvisnega sodniškega odločanja Ustavnega sodišča Republike Slovenije v zadevah odločanja sodišč (ustavna pritožba zoper odločitve sodišč). Podobne rešitve so v prvem odstavku 77. člena ZVOPOKD. Tretji odstavek določa omejitve nadzorov glede delovanja oseb, ki po odredbi sodišča obdelujejo osebne podatke za namen sodnega postopka (gre za stečajne upravitelje, izvršitelje, tolmače ipd).

Četrti odstavek določa omejitve nadzornih oseb pri opravljanju nadzora in izrekanju sankcij na področju obveščevalno varnostne dejavnosti, varnostnega preverjanja oseb po zakonu, ki ureja tajne podatke in delovanja varuha človekovih pravic, kadar ta varuje človekove pravice posameznikov. V takem primeru nadzorna oseba ne sme zabeležiti, kopirati, prepisati ali drugače prevzeti identifikacijskih osebnih podatkov oziroma kopirati nobene dokumentacije glede:

Navedene omejitve ne posegajo v nadzorne pristojnosti IP na drugih področjih delovanja navedenih organov (npr. kadrovske, finančne zadeve, zagovorništvo otrok ipd.).

Omejitev nadzorov iz prve točke četrtega odstavka je določena, ker Evropska unija nima pristojnosti na področju varnosti države, urejanje varstva osebnih podatkov na tem področju je prepuščeno državam članicam. Omejitev nadzorov iz druge točke izhaja iz potrebe po posebnem varovanju virov podatkov v zvezi z varnostno preverjanimi osebami, ki se izvaja v zvezi z varnostjo in obrambo države. Omejitev nadzorov iz tretje točke izhaja iz pristojnosti Varuha, da varuje človekove pravice šibkejših nasproti državi in njenim delom, raznolikosti področij, ki jih nadzoruje Varuh in zaupnosti in občutljivosti osebnih podatkov, ki jih Varuh obdeluje kot del neformalnega varstva človekovih pravic.

V petem odstavku je določeno, da lahko izjemoma nadzorne osebe na področjih iz prejšnjega odstavka pri izvajanju nadzora po ZVOP-2 zabeležijo, kopirajo, prepišejo ali drugače prevzamejo identifikacijske osebne podatke oziroma druge podatke, če je prijavo glede svojih osebnih podatkov podal prijavitelj s posebnim položajem, pri opravljanju nadzora pa vseeno ni dopustno razkriti podatkov o delovanju upravljavca iz vseh točk prejšnjega odstavka v konkretni zadevi. Podobne rešitve so v drugem odstavku 77. člena ZVOPOKD.

Po šestem odstavku se sme v primeru izvajanju nadzora nad osebnimi podatki, ki se obdelujejo za namene zagotavljanja varnosti države, ki so jih organom Republike Slovenije, pristojnim za področji varnosti države ali obrambe države posredovali tuji organi, pristojni za ti področji, ali ki so bili pridobljeni v sodelovanju z njimi, izvesti vpogled, kopiranje, prepis ali drugi prevzem le tistih podatkov, za katere je tuji organ, ki je podatke posredoval ali pridobil, podal jasno in izrecno predhodno soglasje za vpogled ali drug prevzem.

Sedmi odstavek določa možnost Varuha človekovih pravic, da sam zahteva uvedbo inšpekcijskega nadzora.

K 57. členu (sodelovanje z drugimi organi)

Po predlaganem 57. členu Predloga ZVOP-2 Informacijski pooblaščenec pri svojem delu sodeluje z državnimi organi, Evropskim odborom za varstvo osebnih podatkov iz 68. člena Splošne uredbe, drugimi pristojnimi organi Evropske unije za varstvo posameznikov pri obdelavi osebnih podatkov ter podobnimi organi Sveta Evrope, drugimi mednarodnimi organizacijami, nadzornimi organi tretjih držav za varstvo osebnih podatkov, zavodi, združenji, nevladnimi organizacijami s področja varstva osebnih podatkov ali zasebnosti ter drugimi organizacijami in organi glede vprašanj, ki so pomembna za varstvo osebnih podatkov. Nadzorni organ je pristojen tudi za čezmejno sodelovanje ali izvajanje nadzorov z drugimi nadzornimi organi držav. V tretjem odstavku pa je podana ureditev, ki določa, da v okviru postopkov skupnega ukrepanja po 62. členu Splošne uredbe člani ali osebje nadzornega organa druge države članice Evropske unije izvajajo nadzor tako, da nadzor vodi nadzorni organ, če se nadzor izvaja na ozemlju Republike Slovenije ali v okviru pristojnosti nadzornega organa v skladu s tem zakonom, pri čemer lahko uporabljajo le nadzorna pooblastila iz tega zakona in Splošne uredbe, če jih je za to pooblastil nadzorni organ. Člani ali osebje nadzornega organa druge države članice Evropske unije krijejo svoje stroške.

K 58. členu (opravljanje nadzorov)

Predlog 58. člena določa, da nadzorne osebe Informacijskega pooblaščenca opravljajo nadzore po ZVOP-2 neposredno, torej jih ne morejo opravljati na posredni (oddaljeni) način. Pri nadzorih lahko sodeluje strokovno osebje Informacijskega pooblaščenca.

K 59. členu (službena izkaznica)

Predlog 59. člena ZVOP-2 določa službene izkaznice nadzornih oseb in njeno vsebino. Drugi odstavek določa, da obliko določi informacijski pooblaščenec, kot predstojnik nadzornega organa in jo objavi v Uradnem listu Republike Slovenije. V tretjem odstavku je določeno, da izkaznico izda nadzorni organ.

K 60. členu (varovanje tajnosti)

Predlog 60. člena določa posebna pravila glede varovanja tajnosti s strani nadzornih oseb.

9. poglavje – Zunanji nadzor nad delovanjem nadzornega organa

K 61. členu (letno poročilo nadzornega organa)

Predlog 61. člena (v razdelku glede zunanjega nadzora nadzornega organa) določa pravila glede vsebine Letnega poročila Informacijskega pooblaščenca. 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. To

poročilo je del skupnega Letnega poročila v skladu z zakonom, ki ureja Informacijskega pooblaščenca. Poročilo se posreduje tudi Evropski komisiji in Odboru ter je dostopno javnosti.

V zvezi z nadzori, katere opravlja Informacijski pooblaščenec, je torej prek obravnave Letnega poročila Informacijskega pooblaščenca v Državnem zboru zagotovljen tudi dodatni (prvi) zunanji nadzorni mehanizem (sistem zavor in ravnovesij) glede njegovega delovanja, tako da se ne bo postavljalo vprašanje "Kdo bo varoval varuhe?"[72].

K 62. členu (pristojnosti varuha človekovih pravic)

V 62. členu Predloga ZVOP-2 je določen dodatni (drugi) zunanji kontrolni mehanizem – določitev 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.

Navedba pristojnosti Varuha človekovih pravic pomeni, da je določen drugi zunanji kontrolni mehanizem.

Tretji odstavek določa, da je del letnega poročila varuha tudi ocena stanja na področju varstva osebnih podatkov.

Četrti odstavek določa, da lahko varuh v okviru svojih splošnih pristojnosti (3. člen Zakona o varuhu človekovih pravic) predlaga Informacijskemu pooblaščencu izvedbo nadzora s področja pravice do varstva osebnih podatkov (glejte tudi drugi odstavek 61. člena).

K 63. členu (pristojnosti državnega zbora)

V predlogu 63. člena ZVOP-2 je določen tretji zunanji kontrolni mehanizem. Najprej (prvi odstavek) je določeno, da stanje na področju varstva osebnih podatkov in izvrševanje določb tega zakona spremlja Državni zbor Republike Slovenije. Predlog zakona v tem delu sledi veljavni ureditvi iz 61. člena ZVOP-1.

Po drugem odstavku pristojno delovno telo Državnega zbora za nadzor obveščevalnih in varnostnih služb lahko sodeluje z nadzornim organom, poleg tega pa lahko na lasten predlog ali na pobudo nadzornega organa sodelujeta tudi glede sprememb zakonov ali drugih predpisov ali pa kadar je v določenih primerih potrebna izmenjava tajnih podatkov ali drugih informacij o poteku ali o ugotovitvah nadzornih postopkov.

10. poglavje – Prenosi določenih osebnih podatkov državam članicam Evropske unije, tretjim državam ali mednarodnim organizacijam

K 64. členu (splošne določbe)

Predlagani 64. člen ZVOP-2 določa, da se prenosi osebnih podatkov iz Republike Slovenije v tretje države ali mednarodne organizacije se izvajajo le v skladu z določbami V. Poglavja Splošne uredbe. Določbe o pogojih in izjemah glede prenosov se nahajajo v določbah navedenega poglavja Splošne uredbe, ki se neposredno uporablja. Za postopke odločanja o prenosih se uporablja ZUP, če zakon ali Splošna uredba ne določata drugače.

[72] "*Quis custodiet ipsos custodes?*"

K 65. členu (posebni prenosi)

Predlagani 65. člen Predloga ZVOP-2 določa za določena področja, ki so popolnoma ali delno v samostojni pristojnosti Republike Slovenije (npr. podatki o umrlih, podatki s področja varnosti in obrambe države ipd.) posebna pravila za prenose osebnih podatkov v druge države ali mednarodne organizacije.

K 66. členu (odstopanja v posebnih primerih)

Predlagani 66. člen Predloga ZVOP-2 določa posebna pravila za primere, ko se osebni podatki iz 66. člena Predloga ZVOP-2 posredujejo v tretjo državo ali mednarodno organizacijo, za katero ne obstaja sklep o ustreznosti iz 45. člena Splošne uredbe oziroma niso bili sprejeti ustrezni zaščitni ukrepi. Za ta vprašanja se uporabijo določbe prvega odstavka 49. člena Splošne uredbe, razen glede javnega sektorja, kjer se ne uporabljajo točke a) do c) prvega odstavka 49. člena Splošne uredbe.

II. del – Področne ureditve obdelave osebnih podatkov

1. poglavje – Posebna pravila glede obdelave osebnih podatkov za znanstvenoraziskovalne, zgodovinskoraziskovalne, statistične in arhivske namene

K 67. členu (obdelava osebnih podatkov v znanstvenoraziskovalne, zgodovinskoraziskovalne in statistične namene)

V 67. členu Predloga ZVOP-2 se ureja obdelava osebnih podatkov v znanstvenoraziskovalne, zgodovinske raziskovalne in statistične namene – gre za sistemska pravila glede obdelave. Navedena področja so načeloma z vidika varstva osebnih podatkov dobro urejena v področni zakonodaji – v Zakonu o varstvu dokumentarnega in arhivskega gradiva ter arhivih[73], v Zakonu o državni statistiki[74] (kjer bi morda vseeno bilo potrebno urediti področno povezovanje zbirk) ter v Zakonu o raziskovalni in razvojni dejavnosti[75] (ki pa bi ga bilo treba širše spremeniti ozir. dopolniti z vidika urejanja varstva osebnih podatkov). Te določbe veljajo tudi za področje ZVOPOKD, kolikor področna zakonodaja (npr. ZDT-1) ne določa drugače.

Po prvem odstavku je dovoljena obdelava osebnih podatkov za namene znanstvenega, zgodovinskega in statističnega raziskovanja, ki ga izvajajo organizacije ali posamezniki, ki pri svojem delovanju uporabljajo etična načela in metodologijo s področja raziskovanja. Za raziskovalce in raziskovalne organizacije se ne zahteva, da so registrirani skladno z zakonodajo s področja raziskovanja, pogoj za obravnavo po tem poglavju je, da pri svojem delovanju uporabljajo etična pravila in metodologijo. Med raziskovalce tako štejemo tudi posameznike, ki opravljajo raziskave v okviru javnih in zasebnih raziskovalnih institucij (npr. univerza).

Drugi odstavek vzpostavlja domnevo, da je namen obdelave osebnih podatkov za raziskovanje skladen z namenom njihovega zbiranja. Namena torej nista v nasprotju (glej drugi odstavek 38. Člena Ustave RS).

K 68. členu (pogoji obdelave osebnih podatkov v raziskovalne namene)

Prvi odstavek določa pogoje, pod katerimi se osebne podatke lahko obdeluje za raziskovalne namene. To je dovoljeno, če tako obdelavo dovoljuje zakon, če posameznik tega ni prepovedal

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

(splošna prepoved) ali če posameznik ni prepovedal obdelave za konkretno raziskavo (posebna prepoved). V primeru posebnih podatkov, ki pomenijo poklicno skrivnost mora posameznik za obdelovanje v raziskovalni namen podati pisno soglasje.

Drugi odstavek določa pogoje, pod katerimi lahko raziskovalec pridobi osebne podatke. Predložiti je treba opis raziskave z vsemi elementi, ki so navedeni v seznamu iz drugega odstavka. Namen opisa raziskave je omogočiti upravljavcu, da se seznani z raziskavo, njenimi nameni, potrebnimi podatki in na tej podlagi sprejme informirano in utemeljeno odločitev o posredovanju osebnih podatkov. Raziskovalec navede tudi obliko, v kateri želi podatke (lahko so tudi anonimizirani, torej niso več osebni podatki), lahko so psevdonimizirani, lahko so v izvirni obliki. Prav tako mora navesti razlog za določeno obliko, ki jo potrebuje, saj je na ta način omogočeno, da lahko upravljavec v odločanju zlasti po 2. in 3. točki četrtega odstavka 68. člena oceni in odloči, ali bo podatke posredoval v zahtevani obliki ali jih ne bo posredoval.

Tretji odstavek določa obveznost priprave ocene učinkov in posvetovanja z Informacijskim pooblaščencem v primeru, ko so za to izpolnjeni pogoji po Splošni uredbi.

V četrtem odstavku so določeni pogoji za zavrnitev posredovanja osebnih podatkov, pri tem je pomembna povezava z drugim odstavkom, kot je že bila predstavljena zgoraj.

Peti odstavek določa omejitve obveščanja posameznikov o obdelavah njihovih osebnih podatkov po 12.-14. členu Splošne na podlagi (e) točke prvega odstavka 23. člena Splošne uredbe. Pomemben cilj v splošnem javnem interesu v tem primeru je napredek znanstvenega raziskovanja.

Šesti odstavek določa ravnanje z osebnimi podatki, po tem, ko je raziskava zaključena.

Sedmi odstavek določa objavo osebnih podatkov v okviru rezultatov raziskave.

V osmem odstavku so opredeljene možnosti dostopa posameznika do lastnih osebnih podatkov, ki jih obdeluje raziskovalec in pravica do ugovora. Določba vzpostavlja sorazmerje glede na omejeno obveščanje posameznikov o obdelavah osebnih podatkov.

Deveti odstavek določa brezplačnost posredovanja osebnih podatkov s strani subjektov javnega sektorja.

K 69. členu (kontaktiranje posameznikov)

Predlagani 69. člen ZVOP-2 določa pravila glede obdelave osebnih podatkov za kontaktiranje posameznikov v raziskovalne 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 stroškov obdelave osebnih podatkov kontaktira posameznike z namenom pridobivanja privolitev za potrebe raziskovanja.

Gre torej za primere, ko raziskovalec želi pridobiti privolitev, pa nima osebnih podatkov, zato kontaktiranje posameznika, na katerega se nanašajo osebni podatki, za njega izvede upravljavec in to proti plačilu stroškov ter le za namene iz prvega in drugega odstavka.

Po tretjem odstavku se v okviru obdelave obdelujejo samo osebno ime, naslov stalnega ali začasnega prebivališča, kontaktna telefonska številka ali kontaktni naslov elektronske pošte (uporabljeno načelo sorazmernosti ter določen namen obdelave).

K 70. členu (obdelava podatkov za namene arhivskega delovanja)

V predlaganem 70. členu ZVOP-2 je določena obdelava podatkov za namene arhiviranja v javnem interesu. Po prvem odstavku je obdelava osebnih podatkov za namene arhivskega delovanja dovoljena, če je to 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 15. členu 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[76]. Posameznik, na katerega se nanašajo osebni podatki nima pravice zahtevati izvedbe izbrisa v skladu s pravico do pozabe iz 17. člena Splošne uredbe ipd. Gre za omejitev pravic posameznikov, ki jih dopušča 23. člen Splošne uredbe.

Po tretjem odstavku ima posameznik, na katerega se nanašajo osebni podatki, v primeru ko navaja netočnost in neposodobljenost svojih osebnih podatkov, možnost podati dopolnilno izjavo z nasprotnim prikazom dejstev. Pristojni arhiv mora dopolnilno izjavo priložiti dokumentom ali ustrezno označiti na njih, kje se ta izjava nahaja (posebna vrsta uradnega zaznamka).

Četrti odstavek določa razmerje do področne zakonodaje s področja varstva dokumentarnega in arhivskega gradiva.

K 71. členu (obdelava podatkov za namene statističnega raziskovanja)

71. člen predloga zakona ureja obdelavo podatkov za namene statističnega raziskovanja. Obdelava osebnih podatkov v ta namen je dovoljena, če je to v javnem interesu, ki ga določa zakon.

Drugi odstavek določa omejitve pravic posameznika, na katerega se nanašajo osebni podatki.

V tretjem odstavku je določeno razmerje do zakona, ki ureja delovanje državne statistike.

2. poglavje – Varstvo svobode izražanja ter dostopa do informacij v razmerju do varstva osebnih podatkov

2. poglavje II. dela zakona ureja razmerja med človekovo pravico do varstva osebnih podatkov (38. člen Ustave Republike Slovenije) ter svobodo izražanja iz prvega odstavka 39. člena in dostopom do informacij javnega značaja iz drugega odstavka 39. člena Ustave Republike Slovenije.

K 72. členu (varstvo svobode izražanja v razmerju do pravice do varstva osebnih podatkov)

V predlaganem 72. členu 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[77]. Treba je upoštevati, da je

[76] Glejte: Sklep Višjega sodišča v Ljubljani, opr. št. I Cp 490/2000, 11. 4. 2001.

[77] 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

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[78]) 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 (oziroma določbe celotnega člena) je formuliran tako, da se ne nanaša 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[79]. Posredno (posledično) pa pokriva predlagani člen tudi področje svobode komuniciranja[80] po 37. členu Ustave Republike Slovenije.

V drugem odstavku je natančneje določeno varstvo svobode izražanja v razmerju do varstva osebnih podatkov za namene obveščanja javnosti s strani medijev, književnega, umetniškega ustvarjanja, resne kritike, obrambe kakšne pravice ali varstva upravičene koristi ter izobraževanja, ali izobraževanja preko javno dostopnih objav in publikacij, kar vključuje pravice, da se osebni podatki uporabijo, objavijo ali drugače razkrijejo za namene uresničevanja svobode izražanja pod pogoji, navedenimi v drugem odstavku.

1. če je posameznik za obdelavo, objavo ali razkritje osebnih podatkov podal privolitev,
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),
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 nujna za utemeljitev mnenja ali vrednostne ocene[81] (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 je npr. nekdo drug zakonito objavil, raziskovalno novinarstvo, povzetek objave iz čezmejne obdelave ipd.),

---

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....«.

[78] 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.

[79] 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.

[80] 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.

[81] 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..

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[82]).

Po tretjem odstavku uveljavljanje pravic v zvezi z določbami tega člena zagotavlja samo sodna oblast (sodišča) v skladu z določbami Splošne uredbe in zakonov, ki urejajo svobodo izražanja in sodne postopke ali urejajo sodno varstvo (po določbah Zakona o medijih, po splošnih določbah Zakona o pravdnem postopku, Obligacijskega zakonika, Zakona o kazenskem postopku, delno pa tudi Zakona o upravnem sporu, in ne gre pa za sistemsko sodno varstvo kot je določeno v 11. členu ZVOP-2).

Četrti odstavek določa, da upravljavci ali obdelovalci ne smejo subjektom za namene svobode izražanja nezakonito posredovati, nezakonito razkriti ali nezakonito omogočiti nepooblaščenega dostopa do vsebine osebnih podatkov.

K 73. členu (varstvo pravice do dostopa do informacij javnega značaja v razmerju do pravice do varstva osebnih podatkov)

Podobno kot za varstvo svobode izražanja v 72. členu predloga zakona je v predlaganem 73. členu predloga zakona določena posebna ureditev za varstvo oziroma 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.

Po predlaganem prvem odstavku lahko zavezanci po Zakonu o dostopu do informacij javnega značaja[83] 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 Zakona o dostopu do informacij javnega značaja ali npr. Zakona o zunanjih zadevah (drugi odstavek 45.a člena)[84], Zakona o javnem naročanju (četrti odstavek 35. člena)[85], Zakona o integriteti in preprečevanju korupcije (drugi odstavek 23. člena)[86], Zakona o sistemu plač v javnem sektorju (šesti odstavek 38. člena)[87] itd.

Po drugem odstavku za namene uresničevanja javnega interesa na področju sodelovanja javnosti, zagotavljanja transparentnosti dela ali spremljanja njihove prakse, zavezanci iz prvega odstavka po postopku iz Zakona o dostopu do informacij javnega značaja, lahko proaktivno javno objavijo tudi osebne podatke iz dokumentov, ki niso zajeti v prvem odstavku tega člena, in predstavljajo informacijo javnega značaja, na način delnega dostopa in praviloma v psevdonimizirani obliki.

Tretji odstavek ureja možnost, da v primerih, ko zakon določa javnost podatkov in ko gre za podatke, ki so informacija javnega značaja, da jih upravljavec lahko tudi javno objavi npr. na spletnih straneh.

---

[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, 23/17 – ZSSve, 36/19 in 139/20.

[83] Uradni list RS, št. 51/06 – uradno prečiščeno besedilo, 117/06 – ZDavP-2, 23/14, 50/14, 19/15 – odl. US, 102/15 in 7/18.

[84] Uradni list RS, št. 113/03 – uradno prečiščeno besedilo, 20/06 – ZNOMCMO, 76/08, 108/09, 80/10 – ZUTD, 31/15 in 30/18 – ZKZaš.

[85] Uradni list RS, št. 91/15 in 14/18.

[86] Uradni list RS, št. 69/11 – uradno prečiščeno besedilo in 158/20.

[87] Uradni list RS, št. 108/09 – uradno prečiščeno besedilo, 13/10, 59/10, 85/10, 107/10, 35/11 – ORZSPJS49a, 27/12 – odl. US, 40/12 – ZUJF, 46/13, 25/14 – ZFU, 50/14, 95/14 – ZUPPJS15, 82/15, 23/17 – ZDOdv, 67/17 in 84/18.

K 74. členu (izjema glede obveščanja posameznika)

V predlaganem 74. členu je za upravljavce in obdelovalce določeno, da če so osebni podatki javni na podlagi zakona (npr. po določbah ZDIJZ, 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 12. do 14. členu Splošne uredbe in po določbah Zakona o splošnem upravnem postopku[88] (npr. šesti odstavek 143. člena o vabljenju k stranski udeležbi v postopku).

3. poglavje – Videonadzor

K 75. členu (splošne določbe o videonadzoru in varstvu osebnih podatkov)

Člen ureja videonadzor in varstvo osebnih podatkov. Ureditev se nanaša tako na javni kot na zasebni sektor, ne velja pa za videonadzor, ki ga izključno za domače namene izvajajo posamezniki.

Prvi odstavek določa, da se poglavje tega zakona o videonadzoru uporablja, če drug zakon ne določa drugače (subsidiarna uporaba).

Drugi odstavek dodatno določa, da se videonadzor uvede z ustrezno odločitvijo pristojne osebe (funkcionar, predstojnik, direktor subjekta javnega ali zasebnega sektorja, ki izvaja videonadzor). Odločitev mora biti pisna in obrazložena.

Tretji odstavek določa obveznost objave obvestila o izvajanju videonadzora. Obvestilo mora biti objavljeno na takšen način, da se lahko oseba, ki vstopa v nadzorovano območje pred vstopom odloči, ali želi, da se njeni osebni podatki (podoba, glas itd.) obdelajo v video-nadzornem sistemu. Obvestilo se običajno objavi v obliki obvestilne table, nalepke ali na drug primeren način.

Četrti odstavek določa vsebino obvestila, peti odstavek pa za določene informacije določa, da so lahko objavljene na spletnih straneh upravljavca, namesto na samem obvestilu, vendar mora biti v tem primeru na obvestilu zapisan naslov, kjer posameznik lahko najde zahtevane informacije. Namen možnosti, da se določene informacije objavijo na spletnih straneh je predvsem v stalnem ažuriranju podatkov in v zmanjšanju količine podatkov, ki jih je treba zapisati v obvestilo.

Šesti odstavek določa pravno domnevo seznanitve posameznikov z obdelavo osebnih podatkov v okviru izvajanja video nadzora, če so izpolnjeni pogoji iz prejšnjih odstavkov. Na podlagi tega lahko upravljavec sklepa, da osebe, ki so vstopile v nadzorovano območje, soglašajo z obdelavo njihovih podatkov v mejah obvestila.

Sedmi odstavek določa nabor podatkov, ki se obdelujejo za namen videonadzora v zbirki posnetkov video-nadzornega sistema.

Osmi odstavek določa obveznost zavarovanja videonadzornega sistema.

Deveti odstavek določa rok hrambe videonadzornih posnetkov na največ eno leto. Podatke je potrebno izbrisati, ko je dosežen namen obdelave, kar je lahko tudi že pred potekom enega leta. Drug zakon lahko določa drugačen rok hrambe. V primeru, ko se posnetki predajo policiji za namen preiskave kaznivega dejanja, se za posnetke uporablja področna zakonodaja, ki ureja ravnanje z dokazi.

Deseti odstavek določa omejitve izvajanja videonadzora. Prepovedan je videonadzor v prostorih, kjer posamezniki utemeljeno pričakujejo višjo stopnjo zasebnosti (dvigala, sanitarije, garderobe, hotelske sobe in drugi in podobni prostori), seznam je torej odprt.

[88] Uradni list RS, št. 24/06 – uradno prečiščeno besedilo, 105/06 – ZUS-1, 126/07, 65/08, 8/10, 82/13 in 175/20 – ZIUOPDVE.

Enajsti odstavek določa omejitev uporabe videoposnetkov izključno za namene, ki so bili navedeni v obvestilu ob nastanku posnetkov. Drugi zakoni lahko določijo drugače.

Upravljavec videonadzornega sistema mora zagotavljati dnevnik obdelav, iz katerega mora biti mogoče ugotoviti v katere posnetke je bilo vpogledano, kdaj in kako so bili uporabljeni ali komu so bili posredovani, kdo je izvedel ta dejanja obdelave, kdaj in s kakšnim namenom ali na kateri pravni podlagi. Dnevniški zapis se hrani dve leti, drug zakon pa lahko določa drugačno obdobje hrambe.

K 76. členu (videonadzor dostopa v uradne službene oziroma poslovne prostore)

Člen določa omejitve videonadzora dostopa v uradne službene oziroma poslovne prostore. Prvi odstavek določa splošno pravno podlago za uvedbo videonadzora v zasebnem sektorju, pred uvedbo takšnega nadzora je treba izkazati potrebo po videonadzoru zaradi varnosti ljudi ali premoženja, zaradi zagotavljanja nadzora vstopa ali izstopa v ali iz uradnih službenih oziroma poslovnih prostorov.

Drugi odstavek določa omejitve glede načina izvajanja video nadzora v zasebnem sektorju v stanovanjskih stavbah, v katerih so tudi uradni službeni oziroma poslovni prostori, in sicer se ta lahko izvaja le tako, da se snema vhodov v stanovanja.

Tretji odstavek določa obveznost upravljavca video nadzornega sistema, da zaposlene, ki opravljajo delo v nadzorovanih prostorih o tem obvesti. Prav tako jih mora obvestiti o podatkih, ki jih hrani v zbirki osebnih podatkov nadzornega sistema (četrti odstavek).

Četrti odstavek določa soglasje lastnikov nepremičnine za snemanje v skupnih prostorih.

Peti odstavek določa vsebino zbirke podatkov, ki jo sme hraniti nadzorni sistem.

K 77. členu (videonadzor znotraj delovnih prostorov)

Člen določa omejitve pri video nadzoru znotraj delovnih prostorov. Prvi odstavek določa možnost za izvajanje video nadzora v delovnih prostorih le pod pogojem, da je to nujno potrebno (pogoj nujnosti, ki je višji standard v primerjavi s standardom potrebnosti; glej prvi odstavek 75. člena) 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, ob dodatnem pogoju, da teh namenov ni mogoče doseči z milejšimi sredstvi.

Drugi odstavek določa prostorsko omejitev videonadzora znotraj delovnih prostorov in omejitev po namenu, in sicer na tiste dele prostorov, kjer se varuje interese iz prvega odstavka.

Tretji odstavek določa prepoved snemanja običajnih delovnih mest, razen če je to nujno potrebno, skladno s prvim odstavkom.

Četrti odstavek določa pogoje, pod katerimi je dopustno neposredno spremljanje dogajanja pred kamerami. Dovoljeno je le za primere, če takšno spremljanje izvaja izrecno pooblaščeno osebje.

Peti odstavek določa obveznost upravljavca video nadzornega sistema, da zaposlene o videonadzoru v naprej pisno obvesti.

Šesti odstavek kot pogoj za uvedbo video-nadzornega sistema v organizaciji javnega ali zasebnega sektorja določa obveznost, da se delodajalec posvetuje z reprezentativnimi sindikati pri delodajalcu ter svetom delavcev oziroma delavskim zaupnikom, če obstajajo. Rok za posvetovanje je najmanj 30 dni, lahko je daljši. Po prejetju odgovora se delodajalec odloči o uvedbi videonadzora. Kadar gre za videonadzor znotraj delovnih prostorov, je rok za posvetovanje daljši, najmanj 60 dni. Določbe tega odstavka se ne uporabljajo na področju obveščevalno-varnostne dejavnosti države in varovanja tajnih podatkov najvišjih stopenj tajnosti (sedmi odstavek).

Osmi odstavek določa pogoj za vzpostavitev video nadzora v skupnih prostorih. Pogoj je, da z videonadzorom soglašajo lastniki 70 odstotkov skupnih prostorov.

Deveti odstavek določa smiselno uporabo določb tega člena tudi za nadzor vstopa ali izstopa v ali iz uradnih službenih oziroma poslovnih prostorov, ali če zaradi narave dela obstaja možnost varnostnega ogrožanja zaposlenih (76. člen).

K 78. členu (videonadzor v prevoznih sredstvih, namenjenih javnemu potniškemu prometu)

Predlog zakona v 78. členu ureja področje videonadzora v prevoznih sredstvih v javnem potniškem prometu. To se sme izvajati le v zamejenem obsegu in ob kratkotrajni hrambi posnetkov.

K 79. členu (videonadzor na javnih površinah)

Člen določa omejitve videonadzora na javnih površinah. Videonadzor na javnih površinah je dovoljen le kadar je to potrebno zaradi obstoja resne in utemeljene nevarnosti za življenje, osebno svobodo, telo ali zdravje ljudi, nato tudi varnost premoženja upravljavca (torej ne premoženja vseh prebivalcev v lokalni skupnosti) ali varovanje tajnih podatkov upravljavca ali obdelovalca in tega namena ni mogoče doseči z milejšimi sredstvi, dodatno pa ob omejitvah obsega in trajanja še za namene varovanja varovanih oseb ter posebnih objektov in okolišev objektov, ki jih varuje policija, Slovenska vojska, pravosodna policija, oziroma varovanja drugih prostorov, zgradb ali območij, ki jih je treba varovati na podlagi zakona. Prvi odstavek določa še omejitev uporabe posnetkov, in sicer je ta dovoljena le za navedene namene (namenska raba).

Drugi odstavek določa prostorsko zamejitev videonadzora na javnih površinah, in sicer na tiste dele in v obsegu, kjer je treba varovati interese iz prvega odstavka.

Tretji odstavek določa upravljavce video-nadzornih sistemov, in sicer so to lahko osebe javnega ali osebe zasebnega prava, ki upravlja z javno površino ali na njej zakonito opravljajo dejavnost. Odstavek določa še pogoje za izvajanje videonadzora, in sicer ga smejo za javni sektor izvajati le uradne osebe ali pooblaščeno varnostno osebje, za zasebni sektor pa pooblaščeno varnostno osebje. Osebe ali osebje mora biti izrecno pooblaščeno za izvajanje videonadzora.

Videonadzor se lahko izvaja tako, da se ob snemanju spremlja izvajanje dogajanja v živo (četrti odstavek).

Peti odstavek določa, da se pod določenimi pogoji videonadzor lahko opravlja tudi z uporabo telesnih kamer (ang. *bodycam*). Predlog daje neposredno podlago za uporabo telesne kamere za namen varovanja prenosa tajnih podatkov (kurir), za namen varovanja telesa (telesni stražar), poslovnih skrivnosti ali premoženja večje vrednosti. V vseh ostalih primerih je za uporabo telesnih kamer potrebna izrecna zakonska določba.

Šesti odstavek določa rok hrambe posnetkov nadzornega sistema, in sicer je hramba omejena na šest mesecev od trenutka nastanka posnetka. Drugi zakoni lahko določijo drugačne roke hrambe.

Sedmi odstavek določa obveznost upravljavca video-nadzornega sistema, s katerim se izvaja videonadzor javnih površin, da v primeru, ko sistem posname dogodek, ki ogroža zdravja ali življenje posameznika, o tem nemudoma obvesti policijo ali drug pristojni subjekt. Gre za obveznost sporočanja dogodkov v »realnem času«, ki zahteva bodisi spremljanje dogajanja pred kamerami v živo (četrti odstavek) ali drug način prepoznave življenjsko ogrožajočih dogodkov (npr. prepoznava prometnih nesreč na posnetku z uporabo umetne inteligence).

Osmi odstavek določa možnost upravljavca cest, da na posameznih, v naprej določenih odsekih uvede videonadzor. Pri tem je treba upoštevati tudi Zakon o cestah. Namen videonadzora cestnih površin je učinkovito varovanje cestnega prometa ali njegovo upravljanje.

Deveti odstavek določa obveznost izdelave ocene učinka in izvedbe posvetovanja z nadzornim organom.

Deseti odstavek določa prepoved uporabe sistemov za avtomatsko prepoznavo registrskih tablic (ANPR) in sistemov, ki prepoznavajo biometrične značilnosti posameznikov. Drug zakon lahko določa drugače (glej tudi 80. člen – omejitev biometrije).

4. poglavje – Obdelava osebnih podatkov z uporabo biometrije

K 80. členu (omejitev biometrije)

Prvi odstavek določa prepoved obdelave biometričnih osebnih podatkov, ki bi bila v nasprotju z določbami tega poglavja, ki določa minimalne standarde za uvedbo tovrstnih obdelav.

Drugi odstavek določa izrecno prepoved uvedbe biometričnih ukrepov brez zakonske podlage.

Tretji odstavek določa prepoved povezovanja zbirk, ki vsebujejo biometrične podatke ter omogočati prenosljivost teh podatkov, razen pod pogojem, da posameznik, na katerega se nanašajo ti podatki, v takšne obdelave privoli.

K 81. členu (biometrija v javnem sektorju)

Prvi odstavek določa obvezno zakonsko urejanje uporabe biometričnih ukrepov v javnem sektorju. Dodaten pogoj za uporabo biometričnih ukrepov je, da je to nujno potrebno za varnost ljudi, varnost premoženja ali za varovanje tajnih podatkov, za identifikacijo pogrešanih ali umrlih posameznikov ali varovanja poslovne skrivnosti, teh namenov pa ni možno doseči z milejšimi sredstvi.

Drugi odstavek določa dopustnost obdelav biometričnih osebnih podatkov v javnem sektorju, če so dejanja obdelave (torej informacijski sistemi, ki jih obdelujejo) potrjeni po postopku iz 51. člena tega zakona. Zagotovljena mora biti uporaba in obdelava podatkov pod izključnim nadzorom ali oblastjo posameznika, hkrati mora biti posamezniku omogočeno, da izrecno dovoli obdelavo teh podatkov tudi drugim obdelovalcem in upravljavcem za namen dokazovanja točnosti svoje identitete.

Tretji odstavek določa možnost, da se z zakonom predpišejo biometrični ukrepi, če to obveznost določa mednarodni akt, podobno je določeno tudi v drugem odstavku 79. člena ZVOP-1.

Četrti odstavek določa možnost obdelave biometričnih osebnih podatkov v postopku izdaje sredstev elektronske identifikacije v skladu z zakonom, ki ureja sredstva elektronske identifikacije. Določba predstavlja samostojno pravno podlago, ki je izjema od prvega odstavka. Obdelava je načeloma prostovoljna (posameznik jo lahko zahteva) vendar temelji na zakonu. Dopuščen je tudi drug način identifikacije, če se posameznik ne strinja z obdelavo biometričnih osebnih podatkov v tem konkretnem postopku.

Peti odstavek določa možnost uporabe biometričnih ukrepov v zvezi z vstopom v stavbo ali dele stavbe v zasebnem sektorju. Izvajanje takšnih ukrepov mora biti smiselno skladno z 82. členom tega zakona.

K 82. členu (biometrija v zasebnem sektorju)

Člen ureja izvajanje obdelave biometričnih osebnih podatkov v zasebnem sektorju.

Prvi odstavek predstavlja sistemsko določbo, drugi in tretji odstavek določata samostojni podlagi za obdelavo biometričnih osebnih podatkov, četrti do deveti odstavek pa določajo postopek odločanja o uvedbi obdelave biometričnih osebnih podatkov.

Po prvem odstavku je obdelave biometričnih osebnih podatkov dovoljeno izvajati le, če so nujno potrebne za opravljanje dejavnosti, za varnost ljudi, varnost premoženja, varovanje tajnih podatkov, varstvo poslovne skrivnosti ali za varstvo točnosti identitete strank.

Obdelave biometričnih osebnih podatkov lahko oseba zasebnega sektorja v svojih prostorih izvaja tako za svoje zaposlene, kot tudi za zaposlene svojih pogodbenih partnerjev. Osebe, pri katerih se bo izvajalo biometrične ukrepe, morajo biti o tem predhodno pisno obveščene (drugi odstavek).

Tretji odstavek določa dopustnost obdelav biometričnih osebnih podatkov v zasebnem sektorju, če so dejanja obdelave (torej informacijski sistemi, ki jih obdelujejo) potrjeni po postopku iz 51. člena tega zakona. Zagotovljena mora biti uporaba in obdelava podatkov pod izključnim nadzorom ali oblastjo posameznika, hkrati mora biti posamezniku omogočeno, da izrecno dovoli obdelavo teh podatkov tudi drugim obdelovalcem in upravljavcem za namen dokazovanja točnosti svoje identitete. Če so dejanja obdelav potrjena na način, določen v tem odstavku, odločba Informacijskega pooblaščenca ni potrebna (deveti odstavek).

Četrti odstavek določa obveznost obveščanja posameznikov in predhodno posvetovanje z zaposlenimi glede nameravanih obdelav biometričnih osebnih podatkov.

Peti odstavek določa obveznost osebe iz zasebnega sektorja, ki namerava izvajati biometrične ukrepe, pred uvedbo ukrepov posreduje nadzornemu organu opis nameravanih ukrepov in razloge za njihovo uvedbo. Nadzorni organ o vlogi odloči v dveh mesecih in uvedbo biometričnih ukrepov z odločbo dovoli ali zavrne (upravni postopek; šesti odstavek). Zoper odločbo ni pritožbe, dovoljen pa je upravni spor (osmi odstavek). Pritožba ni dovoljena, ker Informacijski pooblaščenec nima nadrejenega drugostopenjskega organa.

Šele po prejemu pozitivne odločbe sme oseba zasebnega sektorja začeti izvajati biometrične ukrepe (sedmi odstavek).

Deveti odstavek določa izjemo pri izvajanju biometričnih ukrepov v zasebnem sektorju, če se biometrični ukrepi izvajajo na način, da so biometrične značilnosti ali matematične pretvorbe biometričnih značilnosti vedno pod nadzorom ali oblastjo posameznika, na katerega se nanašajo osebni podatki in je posameznik za izvedbo teh ukrepov podal privolitev.

K 83. členu (prepoved pridobivanja biometričnih osebnih podatkov v zvezi s trženjem)

Člen določa prepoved pridobivanja in obdelave biometričnih osebnih podatkov v okviru trženja ali v zameno za določene storitve, četudi so storitve za posameznika brezplačne (npr. ponujanje brezplačnih analiz DNK vzorca za pridobitev genealoških podatkov, prepoved identifikacije s prepoznavo obraza ali prstnega odtisa za namen trženja ali druge podobne poslovne dejavnosti – npr. menjava za brezplačne elektronske storitve).

5. poglavje – Evidentiranje vstopov in izstopov

K 84. členu (evidentiranje vstopov in izstopov iz službenih prostorov)

Člen ureja evidentiranje vstopa in izstopa iz službenih prostorov (evidenca prisotnosti, evidenca obiskovalcev ipd.). 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:

- osebno ime,
- številka in vrsta osebnega dokumenta,

- naslov prebivališča,
- zaposlitev,
- vrsta in registrska številka vozila,
- datum, ura in razlog vstopa ali izstopa v ali iz prostorov.

Po potrebi lahko osebne podatke preveri tudi z vpogledom v osebni dokument posameznika.

Tretji odstavek določa rok hrambe podatkov, in sicer največ dve leti od konca koledarskega leta po vnosu podatkov v zbirko. Podatke je po poteku roka treba izbrisati ali na drug način uničiti (npr. če se vodijo v knjigi gostov). Drugi zakoni lahko določijo drugačne roke hrambe in postopanje s podatki po izteku rokov.

6. poglavje – Javne knjige in varstvo osebnih podatkov

K 85. členu (zakoniti namen javne knjige)

V 85. členu Predloga ZVOP-2 je določeno, da se lahko osebni podatki iz javne knjige, urejene z zakonom (npr. zemljiška knjiga), uporabljajo le v skladu z namenom[89], 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.

7. poglavje – Povezovanje zbirk osebnih podatkov

K 86. členu (povezovanje uradnih evidenc in javnih knjig)

Predlagani 86. člen o povezovanju uradnih evidenc in javnih knjig predstavlja nadaljevanje in v določeni meri tudi nadgradnjo obstoječe ureditve povezovanja zbirk osebnih podatkov iz dosedanjega 84. člena ZVOP-1. Bistvo ureditve tako ostaja - omejuje se vsako količinsko oz. kakovostno znatnejše povezovanje uradnih evidenc med sabo ali z zunanjimi evidencami zgolj na tiste primere, ko sta to posebej dovolila zakonodajalec oziroma v nekaterih 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, zahteve po dovoljenju Informacijskega pooblaščena pa ni več), ureditev manj tveganih pa blažje (ni več potrebe po obveščanju ali pridobivanju dovoljenja Informacijskega pooblaščenca).

Razlog za tak sorazmerno restriktivni pristop je 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 EMŠO) 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

[89] 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.

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 hack-erski ali celo nezakoniti 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 ti. nastanek/omogočanje »totalne nadzorovalne družbe«. Predlagani preprečevalni pristop izhaja iz francoske »*afere SAFARI*« iz leta 1974[90], 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 preklican zaradi nasprotovanja javnosti oziroma razumevanja, da uvedba takšne totalne družbe nadzora nikakor ne more biti dopustna v razmerah, ki niso ne izredno niti vojno stanje, pa še takrat bi lahko tovrstna ureditev bila dopustna le začasno in v skladu z načelom sorazmernosti.

Posebna zakonska ureditev povezovanja osebnih podatkov je določena tudi 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.

Povezovanje je načelno opredeljeno v samem členu (tretji odstavek), pri čemer je po novem določena tehnološko nevtralno oz. bolj splošno, tako da lahko vključuje različne tehnične načine izvajanja povezovanja zbirk, ki so se pojavila v zadnjih desetih letih. Opredelitev 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). 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 enako 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 do sedaj 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.

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

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 (torej določitev v zakonu)[91], 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).

Ni pa več treba pridobiti dovoljenja Informacijskega pooblaščenca (upravna odločba), zadostuje, da upravljavec, ki načrtuje izvedbo povezovanja, o tem predhodno (rok 30 dni) obvesti Informacijskega pooblaščenca, ki pa lahko v tej predhodni fazi oceni, da 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, ne določa pa obveznosti notifikacije Informacijskega pooblaščenca oziroma pridobivanja njegovega dovoljenja. Navedeno sledi splošni premisi nove ureditve varstva osebnih podatkov (Splošna uredba), da morajo biti ukrepi in postopki varstva osebnih podatkov primerni naravi obdelovanih osebnih podatkov ter tveganjem, ki pri tem nastajajo.

Predlog zakona tako po eni strani predvideva, da bodo številna manj tvegana povezovanja po novem bistveno enostavnejša. Za povezovanje s podatki v matičnih registrih (Centralni register prebivalstva, 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 posamezne namene pridobivati tudi določene podatke iz matičnega registra.

Po drugi 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. Navedena strožja ureditev se bo tako uveljavljala le postopoma. V vmesnem času bodo lahko bolj tvegana povezovanja potekala na enaki zakonski podlagi kot manj tvegana (se pravi, zakon mora določati vsaj možnost pridobivanja podatkov iz zadevnih uradnih evidenc), pri čemer je še vedno treba pridobiti dovoljenje Informacijskega pooblaščenca (četrti odstavek člena, za katerega prehodno obdobje ne velja).

V roku štirih let bo torej treba poskrbeti za prilagoditev zakonske podlage, sicer bo lahko nastopila situacija, da bo Informacijski pooblaščenec nadaljnje povezovanje prepovedal.

[91] Glejte tudi sodbo Upravnega sodišča RS, opr. št. I U 1715/2011, 18. 4. 2012, kjer je med drugim navedeno:
[…] Sodišče meni, da je zakonodajalec s tem, ko je ministrstvu zgolj dal možnost take povezave, ni pa navedel, da se te zbirke morajo povezati, predvidel, da tako povezovanje lahko pride v poštev, če ni katere druge ovire, ki bi tako povezovanje preprečila. V konkretnem primeru pa tak zadržek obstaja, to je določilo 199. člena ZZK-1, ki onemogoča tak način povezovanja. V ponovljenem postopku bo morala tožena stranka upoštevati stališča sodišča glede uporabe materialnega prava, kot so navedena v tej sodbi. […]«

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 – gre za 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) – gre za povezovanje, velja strožja ureditev po prvem odstavku;
- pridobivanje podatkov zaradi odločanja o vlogah za dodelitev neprofitnih stanovanj po 11.a členu Stanovanjskega zakona – gre za 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 – gre za povezovanje; zanj velja milejši režim po drugem odstavku;
- aplikacije e-RISK, e-Poizvedbe, eMRVL - dostop do podatkov v registru MRVL – ne gre za povezovanje, če pa se posamezne evidence povezujejo preko spletnih servisov, npr. prekrškovna evidenca redarskih služb, pa gre za 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) – gre za 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) – ne gre za 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, zapiše podatke na CD ali jih odloži na neko spletno mesto za prevzem - gre za povezovanje odvisno od podatkov, ki se pridobivajo, velja strožji ali milejši režim.

8. poglavje – Strokovni nadzor

K 87. členu (strokovni nadzor)

V 87. členu Predloga ZVOP-2 je določena uvodna določba za posebno poglavje II. dela predloga zakona 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 v izogib morebitni pravni praznini na tem področju (kajti veljavni področni zakoni ne vsebujejo vedno določb o obdelavi osebnih podatkov pri opravljanju strokovnega nadzora) določa ustrezna ureditev. 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 drugim odstavkom 6. člena Predloga ZVOP-2 (načelo zakonitosti glede obdelave osebnih podatkov).

K 88. členu (splošne določbe)

V 88. členu Predloga ZVOP-2 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 tudi prekrškovne določbe.

Besedilo tretjega odstavka za področje varnosti države določa sistemske omejitve pri izvajanju strokovnih nadzorov.

K 89. členu (obveščanje posameznika in pridobivanje podatkov)

V 89. členu Predloga ZVOP-2 je določeno obveščanje posameznika (prvi odstavek) in dodatna obdelava osebnih podatkov v okviru strokovnega nadzora (drugi odstavek), kot je to že določeno v 89. členu ZVOP-1.

K 90. členu (posebne vrste osebnih podatkov)

V 90. členu Predloga ZVOP-2 so določeni strokovni nadzor v razmerju do obdelave posebnih vrst osebnih podatkov, kot je to določeno v dosedanjem 90. členu ZVOP-1. S tem členom so povezane prekrškovne določbe.

9. poglavje – Obdelava kontaktnih podatkov in osebnih dokumentov

K 91. členu (javni kontaktni podatki)

Predlagani 91. člen Predloga ZVOP-2 določa objavo kontaktnih podatkov za potrebe delovanje oseb javnega ali zasebnega sektorja, kot je to določeno že v drugem odstavku 106. člena ZVOP-1 (prehodna določba).

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

V 92. členu Predloga ZVOP-2 se ureja posebna pravna podlaga za obdelavo osebnih podatkov za izvajanje določenih dejavnosti javnega sektorja, zlasti za organiziranje določenih običajnih uradnih dogodkov. Konkretneje gre za ureditev vprašanja kako pridobiti (in nadalje obdelovati) osebne podatke za udeležbo na državnih proslavah in drugih uradnih dogodkih (tudi medijske konference, izdaje raznih knjig, usposabljanja, izobraževanja ipd.).

V tem primeru ne gre za izvrševanje oblastvenih[92] 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 (e) točki drugega odstavka 9. člena Splošne uredbe – prostovoljno razkritje posebne vrste osebnih podatkov. V isti smeri je določeno, da so tej pravni podlagi

[92] Za okvirno opredelitev neoblastvenih delovanj državnega organa 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 […].«

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. 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. Določba je ti. *lex specialis* v razmerju do ti. *lex generalis* predvsem v četrtem odstavku 6. člena ZVOP-2.

Tretji odstavek za namene obveščanja javnosti dovoljuje obdelovanje osebnih podatkov, pridobljenih na dogodkih osebe javnega ali zasebnega sektorja (npr. fotografije, video posnetke in podobno).

K 93. členu (obdelava osebnih podatkov iz uradnega identifikacijskega dokumenta)

V predlaganem 93. členu se določa seznam uradnih identifikacijskih dokumentov in njihova uporaba. Člen je podoben 60. členu ZVOPOKD, ki pa sicer velja le za obdelave po ZVOPOKD.

III. del – Kazenske določbe

K 94. členu (sankcije za kršitve, ki jih predpisuje Splošna uredba)

Predlagani 94. člen najprej umešča sistem upravnih sankcij in upravnih glob v sistem prekrškovnega prava Republike Slovenije, torej Zakona o prekrških, s tem, da od njega odstopa v delu, ko pripoznava drugačne razpone glob, kot so določene v Splošni uredbi ter da samostojno ureja odmerjanje sankcij za prekrške oziroma namen kaznovanja za prekrške v 112. členu predloga ZVOP-2. Umestitev upravnih sankcij in upravnih glob v področje prekrškov je primerna tudi glede na sodno prakso sodišč Republike Slovenije že po začetku veljavnosti Splošne uredbe[93].

Predlagani člen zaradi pravne varnosti prav tako določa naslovnikom (nadzornemu organu, bodočim kršiteljem), da se določbe četrtega, petega in šestega odstavka 83. člena Splošne uredbe o varstvu osebnih podatkov (v nadaljevanju: Splošna uredba) uporabljajo neposredno, in sicer zaradi pravne narave (Splošne) uredbe, ki se kot akt unifikacije v državah članicah EU uporablja brez implementacije v pravni red.

Določba 94. člena predloga zakona na ta način določa vsebino, ki na prvi pogled »manjka« v 95. in 96. členu predloga zakona – in sicer prekrške z globami za pravno osebo, samostojnega podjetnika posameznika in posameznika, ki samostojno opravlja dejavnost, če ti izpolnijo znake prekrškov, ki jih (izvorno) določajo četrti, peti in šesti odstavek 83. člena Splošne uredbe:

1) četrti odstavek 83. člena Splošne uredbe kot kršitve:

(a) obveznosti upravljavca in obdelovalca v skladu s členi 8, 11, 25 do 39 ter 42 in 43

[93] Glejte: Sodba Vrhovnega sodišča RS, opr. št. IV Ips 2/2021, 16. 3. 2021, zlasti 12.-16. točka ter Sklep Višjega sodišča v Ljubljani, opr. št. PRp 215/2021, 22. 6. 2021, zlasti 6.-10. točka.

(b) obveznosti organa za potrjevanje v skladu s členoma 42 in 43 Splošne uredbe ali

(c) obveznosti organa za spremljanje v skladu s členom 41(4) Splošne uredbe.

2) peti odstavek 83. člena Splošne uredbe kot kršitve:

(a) osnovnih načel obdelave, vključno s pogoji za privolitev, v skladu s členi 5, 6, 7 in 9;

(b) pravic posameznika, na katerega se nanašajo podatki, v skladu s členi 12 do 22;

(c) prenosov osebnih podatkov uporabniku v tretji državi ali mednarodni organizaciji, v skladu s členi 44 do 49;

(e) neupoštevanje odredbe ali začasne ali dokončne omejitve obdelave ali prekinitve prenosa podatkov, ki jo izda nadzorni organ v skladu s členom 58(2), ali nezagotovitev dostopa, s čimer se krši člen 58(1).

3) šesti odstavek 83. člena Splošne uredbe, če kršitelj ne upošteva odredbe (popravljalnih ukrepov), ki jo izda nadzorni organ iz v skladu z drugim odstavkom 58. člena Splošne uredbe.

Glede na olajševalne in obteževalne okoliščine (glej drugi odstavek 83. člena Splošne uredbe in 109. člen predloga zakona – odmerjanje sankcij za prekrške) se za prekršek:

a) iz četrtega odstavka 83. člena Splošne uredbe pravna oseba, samostojni podjetnik posameznik ali posameznik, ki samostojno opravlja dejavnost kaznuje z globo v znesku [od 200][94] do 10.000.000 EUR ali v znesku do 2 % skupnega svetovnega letnega prometa v preteklem proračunskem letu, odvisno od tega, kateri znesek je višji ter

b) iz petega in šestega odstavka 83. člena Splošne uredbe pravna oseba, samostojni podjetnik posameznik ali posameznik, ki samostojno opravlja dejavnost kaznuje z globo v znesku [od 200] do 20.000.000 EUR ali v primeru družbe v znesku do 4 % skupnega svetovnega letnega prometa v preteklem proračunskem letu, odvisno od tega, kateri znesek je višji.

Ob tem predlagatelj dodatno še pojasnjuje:

a) da z vidika izraza »družbe« (angl. *undertaking*) kot storilec prekrška iz četrtega in petega odstavka 83. člena Splošne uredbe štejejo le naslednje kategorije storilcev prekrškov, ki jih sicer v pravnem redu Republike Slovenije določa drugi odstavek 17. člena Zakona o prekrških[95] (v nadaljevanju: ZP-1), in sicer: pravna oseba, samostojni podjetnik posameznik in posameznik, ki samostojno opravlja dejavnosti ter,

b) *Administrative fines* (upravne globe) oziroma *administrative sanctions* (upravne sankcije) z vidika izrazoslovja, ki se uporablja v pravnem redu Republike Slovenije, pomenijo prekrške.

c) Pravna oseba, samostojni podjetnik posameznik in posameznik, ki samostojno opravlja dejavnost, so v skladu s 14. oziroma 14.a členom ZP-1 **akcesorno** odgovorni za prekršek, ki ga pri opravljanju dejavnosti stori storilec v njenem imenu ali za njen račun ali v njeno korist ali z njenimi sredstvi. Če samostojni podjetnik posameznik ali posameznik, ki samostojno opravlja dejavnost, sam stori prekršek, pa zanj odgovarja (sama) pod pogoji iz 9. člena ZP-1 (drugi odstavek 14.a člena ZP-1). Ker četrti, peti in šesti odstavek 83. člena Splošne uredbe določata le prekrške »podjetij«, 92. in 93. člen predloga zakona določata »manjkajoče« kategorije storilcev predmetnih prekrškov – prekrške odgovornih oseb.

[94] Spodnje mere glob sistemsko določa drugi odstavek 17. člena Zakona o prekrških.

[95] Uradni list RS, št. 29/11 – uradno prečiščeno besedilo, 21/13, 111/13, 74/14 – odl. US, 92/14 – odl. US, 32/16, 15/17 – odl. US, 73/19 – odl. US, 175/20 – ZIUOPDVE in 5/21 – odl. US.

K 95. členu (kršitve določb iz četrtega odstavka 83. člena Splošne uredbe)

Glede na obrazložitev 94. člena predloga zakona, ki »določa« prekrške pravne osebe, samostojnega podjetnika posameznika ali posameznika, ki samostojno opravlja dejavnosti, če ti izpolnijo znake prekrškov iz četrtega odstavka 83. člena Splošne uredbe, prvi odstavek 95. člena predloga zakona določa istovrstne prekrške, ki jih v imenu, na račun, v korist ali s sredstvi stori neposredni storilec – odgovorna oseba pravne osebe ali odgovorna oseba samostojnega podjetnika posameznika ali odgovorna oseba posameznika, ki samostojno opravlja dejavnost.

Odgovorne osebe so namreč obvezni »sestavni« del pravnih oseb, državnih organov, organov lokalnih skupnosti (lahko so tudi pri samostojnem podjetniku posamezniku ali posamezniku, ki samostojno opravlja dejavnosti), saj ti subjekti svoje volje in ravnanj v pravnem in poslovnem prometu ne morejo izražati sami, temveč to po naravi stvari poteka le prek fizičnih oseb – odgovornih oseb, ki jih za potrebe vodenja prekrškovnih postopkov določa 15. člen ZP-1:

»(1) Odgovorna oseba je tista oseba, ki je pooblaščena opravljati delo v imenu, na račun, v korist ali s sredstvi pravne osebe, samostojnega podjetnika posameznika ali posameznika, ki samostojno opravlja dejavnost, državnega organa ali organa samoupravne lokalne skupnosti.

(2) Odgovorna oseba je tudi tista oseba, ki je pri subjektu iz prejšnjega odstavka pooblaščena izvajati dolžno nadzorstvo, s katerim se lahko prepreči prekršek.«.

Ker pa so prekrški iz četrtega odstavka 83. člena Splošne uredbe lahko storjeni tudi v državnih organih ali v samoupravnih lokalnih skupnostih, določba drugega odstavka 95. člena predloga zakona kot storilca prekrška določa odgovorno osebo državnega organa ali organa samoupravne lokalne skupnosti, saj država in lokalne skupnosti skladno 13.a členom ZP-1 ne odgovarjajo za prekrške (zakon pa lahko določi, da odgovarja za prekršek odgovorna oseba v državnem organu ali v samoupravni lokalni skupnosti).

Znaki prekrškov, ki jih lahko zaradi kršitve določb iz četrtega odstavka 83. člena Splošne uredbe izpolnijo odgovorna oseba pravne osebe, odgovorna oseba samostojnega podjetnika posameznika oziroma posameznika, ki samostojno opravlja dejavnost, so enaki kot so določeni v četrtem odstavku 83. člena Splošne uredbe in so naslednji:

1. če krši obveznosti upravljavca ali 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.

V zvezi s predmetnimi prekrški predlagatelj pojasnjuje, da so tako prekrški v četrtem odstavku 83. člena Splošne uredbe kot tudi prekrški v prvem odstavku 95. člena predloga zakona določeni v nedovršni obliki, kar pomeni, da so določeni kot t. i. kolektivni prekrški, kjer gre po teoriji za navidezen realni stek – storilec z več ravnanji izpolni znake enega prekrška. Analogijo s kaznivimi dejanji je mogoče najti npr. pri kaznivem dejanju neupravičene proizvodnje in prometa s prepovedanimi drogami, nedovoljenimi snovmi v športu in predhodnimi sestavinami za izdelavo prepovedanih drog – 184. člen Kazenskega zakonika;[96] v nadaljevanju: KZ-1, kjer je storilec kaznovan za eno kaznivo dejanje neupravičene proizvodnje in prometa s prepovedanimi drogami, nedovoljenimi snovmi v športu in predhodnimi sestavinami za izdelavo prepovedanih drog, čeprav je 2g heroina prodal v ponedeljek, 2g kokaina pa v petek.

Prekrškovni organ bo npr. odgovorni osebi pravne osebe, ki je kršila določbo prvega odstavka 8. člena Splošne uredbe v zvezi z 10.000 otroci, ker (v 10.000 primerih) ni pridobila privolitve staršev za obdelavo osebnih podatkov, zaradi storitve prekrška iz 1. točke prvega odstavka 92.

[96] Uradni list RS, št. 50/12 – uradno prečiščeno besedilo, 6/16 – popr., 54/15, 38/16, 27/17, 23/20, 91/20 in 95/21

člena predloga zakona, ob upoštevanju olajševalnih in obteževalnih okoliščin (glejte tudi 109. člen predloga zakona), lahko izrekel globo za en prekršek v razponu od 100 do 5.000 eurov.

Razpona glob za odgovorno osebo pravne osebe, samostojnega podjetnika posameznika ali posameznika, ki samostojno opravlja dejavnost in odgovorno osebo državnega organa ali organa samoupravne lokalne skupnosti sta enaka (od 100 do 5.000 eurov), saj imajo kršitve četrtega odstavka 83. člena Splošne uredbe enako težo, če so storjene v zasebnem ali javnem sektorju.

K 96. členu (kršitve določb iz petega in šestega odstavka 83. člena Splošne uredbe)

96. člen predloga zakona iz enakih razlogov kot določba 95. člena predloga zakona določa prekrške naslednjih kategorij storilcev prekrška – odgovorne osebe pravne osebe, odgovorne osebe samostojnega podjetnika posameznika, odgovorne osebe posameznika, ki samostojno opravlja dejavnost ter odgovorne osebe državnega organa ali organa samoupravne lokalne skupnosti. Ker je storilec prekrškov iz petega in šestega odstavka 83. člena Splošne uredbe lahko tudi »navadna fizična oseba«, tretji odstavek 96. člena predloga zakona kot kategorijo storilca prekrška določa tudi »posameznika«.

Glede na to, da je teža prekrškov iz četrtega od šestega odstavka 83. člena Splošne uredbe enaka za vse »odgovorne osebe, je za to kategorijo storilca prekrška predlagan razpon globe od 100 do 5.000 eurov, za posameznika pa ob upoštevanju načela sorazmernosti razpon globe od 100 do 1.000 eurov.

Znaki prekrškov iz petega in šestega odstavka 83. člena Splošne uredbe so naslednji:

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 nadzorni organ v skladu z drugim odstavkom 58. člena Splošne uredbe, ali če ne zagotovi dostopa, s čimer se krši prvi odstavek 58. člena Splošne uredbe;
5. če ne upošteva popravljalnih ukrepov, ki jih naloži pristojni nadzorni organ v skladu z drugim odstavkom 58. člena Splošne uredbe.

V zvezi z zgoraj navedenimi prekrški predlagatelj pojasnjuje, da so prekrški v petem odstavku 83. člena Splošne uredbe kot tudi prekrški iz 1. do 4. alineje prvega odstavka 93. člena predloga zakona določeni z uporabo glagola nedovršni obliki, kar pomeni, da so tudi ti prekrški določeni kot t. i. kolektivni prekrški, kjer gre po teoriji za navidezen realni stek (storilec z več ravnanji izpolni znake enega prekrška). Če bo kršitelj npr. kršil osnovna načela obdelave osebnih podatkov iz 5. člena Splošne uredbe in obdeloval osebne podatke 20.000 oseb, bo izvršil en prekršek, globa pa se bo v skladu s pravili za odmero sankcije (glej 112. člen predloga zakona) določila v razponu, ki je predpisan za posamezno kategorijo storilca prekrška.

Prekršek iz šestega odstavka 83. člena Splošne uredbe in 5. točke prvega odstavka 93. člena predloga zakona pa ni določen kot kolektivni prekršek, kar pomeni, da bo prekrškovni organ za vsak posamezen neupoštevan popravljalni ukrep kršitelju izrekel globo v predpisanem razponu ob upoštevanju olajševalnih ali obteževalnih okoliščin – 109. člen predloga zakona.

K 97. členu (kršitve temeljnih določb tega zakona)

97. člen predloga zakona določa tri prekrške, ki pomenijo kršitev temeljnih določb zakona. Kršitelj se bo kaznoval z globo:

1. če v nasprotju z 21. členom predloga zakona ne bo uvedel ukrepov za zagotavljanje sledljivosti obdelave osebnih podatkov;
2. če v nasprotju s četrtim odstavkom 22. člena tega zakona ne bo imenoval osebe, pristojne za nadzor in usmerjanje varnostnih ukrepov v zvezi z izvajanjem obdelave osebnih podatkov, če obdeluje podatke iz 1. do 4. točke prvega odstavka 22. člena tega zakona;
3. če v nasprotju s šestim odstavkom 40. členom tega zakona ne bo uvedel ukrepov sledljivosti posredovanja osebnih podatkov.

Globe za prekrške iz 97. člena predloga zakona so ob upoštevanju teže kršitev in (ustavnega) načela sorazmernosti (2. člen v zvezi s tretjim odstavkom 15. člena Ustave) predpisane v naslednjih okvirih:

- za pravno osebo v razponu od 4.000 do 12.000 eurov, če pa se pravna oseba po zakonu, ki ureja gospodarske družbe, šteje za srednjo ali veliko gospodarsko družbo, pa z globo v razponu od 8.000 do 36.000 eurov;
- za samostojnega podjetnika posameznika ali posameznika, ki samostojno opravlja dejavnost, v razponu od 3.000 do 9.000 eurov;
- odgovorna oseba pravne osebe, samostojnega podjetnika posameznika ali posameznika, ki samostojno opravlja dejavnost, ter odgovorna oseba v državnem organu ali v samoupravni lokalni skupnosti v razponu od 400 do 4.000 eurov;
- za posameznika pa v razponu od 400 do 2.000 eurov.

K 98. členu (kršitev določb o posredovanju osebnih podatkov v zvezi s svobodo izražanja)

98. člen predloga zakona kot prekršek določa kršitev četrtega odstavka 72. člena zakona, ki se glasi: »Upravljavci ali obdelovalci ne smejo za namene izvajanja svobode izražanja nezakonito razkriti, nezakonito posredovati ali omogočiti nepooblaščenega dostopa do osebnih podatkov.«.

Če bo upravljavec ali obdelovalec za namene izvajanja svobode izražanja nezakonito posredoval, nezakonito razkril ali nezakonito omogočil nepooblaščen dostop do osebnih podatkov, se bodo kršitelji lahko kaznovali v naslednjih razponih glob:

- pravna oseba v razponu od 4.000 do 12.000 eurov, če pa se pravna oseba po zakonu, ki ureja gospodarske družbe, šteje za srednjo ali veliko gospodarsko družbo, pa z globo v razponu od 8.000 do 36.000 eurov;
- samostojni podjetnik posameznik ali posameznik, ki samostojno opravlja dejavnost, v razponu od 3.000 do 9.000 eurov;
- odgovorna oseba pravne osebe, samostojnega podjetnika posameznika ali posameznika, ki samostojno opravlja dejavnost, ter odgovorna oseba v državnem organu ali v samoupravni lokalni skupnosti v razponu od 400 do 4.000 eurov;
- posameznik pa v razponu od 400 do 2.000 eurov.

Predlagatelj ocenjuje, da so glede na težo kršitve in ob upoštevanju vidika načela sorazmernosti kot ustrezni določeni enaki razponi glob, kot so določeni za prekrške, ki pomenijo kršitve temeljnih določb tega zakona (glej 97. člen predloga zakona).

K 99. členu (kršitve določb o uporabi povezovalnega znaka)

99. člen predloga zakona določa tri prekrške v zvezi z uporabo povezovalnih znakov. Kršitelj se bo kaznoval z globo:

1. če bo v nasprotju s prvim odstavkom 41. člena tega zakona pri pridobivanju osebnih podatkov iz zbirk osebnih podatkov s področja zdravstva, obrambe države, sodstva ter iz kazenske ali prekrškovnih evidenc uporabljal samo en povezovalni znak.
2. če v nasprotju z drugim odstavkom 41. člena tega zakona ne bo napravil uradnega zaznamka ali drugega ustreznega zapisa o nujnosti uporabe izključno enega povezovalnega znaka za predpisane namene.
3. če bo v nasprotju s tretjim odstavkom 41. člena tega zakona na področju varnosti države povezovalni znak uporabljal v nasprotju z notranjim aktom o varnosti osebnih podatkov.

Kršitelji se bodo lahko za kršitve 41. člena zakona, ki so določeni kot prekrški, kaznovali v naslednjih razponih glob:

- pravna oseba v razponu od 1.000 do 8.000 eurov, če pa se pravna oseba po zakonu, ki ureja gospodarske družbe, šteje za srednjo ali veliko gospodarsko družbo, pa z globo v razponu od 8.000 do 36.000 eurov;
- samostojni podjetnik posameznik ali posameznik, ki samostojno opravlja dejavnost, v razponu od 400 do 2.000 eurov;
- odgovorna oseba pravne osebe, samostojnega podjetnika posameznika ali posameznika, ki samostojno opravlja dejavnost, ter odgovorna oseba v državnem organu ali v samoupravni lokalni skupnosti (13.a člen ZP-1) v razponu od 400 do 2.000 eurov;
- posameznik pa v razponu od 200 do 1.000 eurov.

Razponi glob so v primerjavi z razponi glob za prekrške, ki pomenijo kršitev temeljnih določb zakona, določeni nižje, razen v primeru, če prekršek stori pravna oseba, ki po zakonu, ki ureja gospodarske družbe, šteje za srednjo ali veliko gospodarsko družbo – razpon globe je v tem primeru višji, kar naj bi na potencialne kršitelje (velike gospodarske družbe) učinkoviteje vplivalo z vidika generalne prevencije.

V zvezi s prekrškoma iz 1. in 3. točke prvega odstavka 99. člena predloga zakona predlagatelj pojasnjuje, da gre zaradi uporabe nedovršne oblike glagola za t. i. kolektivni prekršek, kar pomeni, da bo pristojni prekrškovni organ kršitelja kaznoval v predpisanem razponu globe za en prekršek.

K 100. členu (kršitev splošnih določb o videonadzoru)

Določba 100. člena predloga zakona kot prekrške določa kršitve splošnih določb o videonadzoru iz 75. člena predloga zakona. Kršitelj se bo kaznoval z globo:

1. če bo v nasprotju z drugim odstavkom 75. člena zakona ne bo sprejel pisne odločitve o uvedbi videonadzora;
2. kršitev v nasprotju z tretjim odstavkom 75. člena zakona v primeru izvajanja videonadzora ne bo objavil obvestila na način, ki omogoča posamezniku, da se seznani z izvajanjem videonadzora preden se nad njim začne izvajati videonadzor;
3. če v nasprotju z četrtim odstavkom 75. člena zakona obvestilo o izvajanju videonadzora ne bo določalo vseh predpisanih informacij;
4. če videonadzorni sistem v nasprotju z osmim odstavkom 75. člena zakona ne bo zavarovan pred dostopom nepooblaščenih oseb.

Glede na to, da ne gre za težje prekrške s področja izvajanja videonadzora, se bodo kršitelji kaznovali v naslednjih razponih glob:

- pravna oseba v razponu od 4.000 do 10.000 eurov, če pa se pravna oseba po zakonu, ki ureja gospodarske družbe, šteje za srednjo ali veliko gospodarsko družbo, pa z globo v razponu od 8.000 do 20.000 eurov;
- samostojni podjetnik posameznik ali posameznik, ki samostojno opravlja dejavnost, v razponu od 1.000 do 2.000 eurov;
- odgovorna oseba pravne osebe, samostojnega podjetnika posameznika ali posameznika, ki samostojno opravlja dejavnost, ter odgovorna oseba v državnem organu ali v samoupravni lokalni skupnosti (13.a člen ZP-1) v razponu od 500 do 2.000 eurov;
- posameznik pa v razponu od 100 do 1.000 eurov.

K 101. členu (težje kršitve določb o videonadzoru)

Določba 101. člena predloga zakona kot težja prekrška na področju izvajanja videonadzora določa kršitvi devetega in desetega odstavka 75. člena predloga zakona. Kršitelj se kaznuje z globo:

1. če bo v nasprotju z devetim odstavkom 75. člena predloga zakon posnetke videonadzora hranil več kot eno leto od trenutka nastanka posnetka, razen če drug zakon določa drugače;
2. če bo v nasprotju z desetim odstavkom 75. člen predloga zakona izvajal videonadzor v dvigalih, sanitarijah, prostorih za preoblačenje, hotelskih sobah in drugih podobnih prostorih, v katerih lahko posameznik utemeljeno pričakuje višjo stopnjo zasebnosti.

Ker gre po oceni predlagatelja z vsebinskega vidika kot rečeno za precej težje kršitve na področju varstva osebnih podatkov, so predlagani razponi glob cca. 2x višji od razponov glob, ki se predpisane za kršitve splošnih določb o izvajanju videonadzora. Kršitelj se bodo za storjeni prekršek kaznovali v naslednjih razponih glob:

- pravna oseba v razponu od 8.000 do 20.000 eurov, če pa se pravna oseba po zakonu, ki ureja gospodarske družbe, šteje za srednjo ali veliko gospodarsko družbo, pa z globo v razponu od 16.000 do 40.000 eurov;
- samostojni podjetnik posameznik ali posameznik, ki samostojno opravlja dejavnost, v razponu od 4.000 do 10.000 eurov;
- odgovorna oseba pravne osebe, samostojnega podjetnika posameznika ali posameznika, ki samostojno opravlja dejavnost, ter odgovorna oseba v državnem organu ali v samoupravni lokalni skupnosti (13.a člen ZP-1) v razponu od 1.000 do 4.000 eurov;
- posameznik pa v razponu od 400 do 3.000 eurov.

Kršitev desetega odstavka 75. člena predloga zakona je zaradi uporabe nedovršne oblike glagola določena kot t. i. trajajoči prekršek.

K 102. členu (kršitev določb o videonadzoru glede dostopa v uradne službene oziroma poslovne prostore)

Določba 102. člena predloga zakona določa kršitve določb o videonadzoru glede dostopa v uradne službene oziroma poslovne prostore (76. člen predloga zakona), ki z vsebinskega vidika niso tako zavržni kot npr. kršitev prepovedi snemanja prostorov, v katerih posameznik utemeljeno pričakuje višjo stopnjo zasebnosti. Kot prekršek so določene naslednje kršitve:

1. če kršitelj izvaja videonadzor brez pravne podlage ali obdeluje posnetke v nasprotju z nameni iz prvega odstavka 76. člena tega zakona, kar pomeni, da kršitelj izvaja videonadzor dostopa v uradne službene oziroma poslovne prostore z drugimi nameni kot jih določa prvi odstavek 76. člena predloga zakona.

   Dopustni nameni snemanja dostopa v uradne službene oziroma poslovne namene so namreč le naslednji: če gre za zagotavljanje varnosti ljudi ali premoženja, zaradi zagotavljanja nadzora vstopa ali izstopa v ali iz uradnih službenih oziroma poslovnih prostorov ali če zaradi narave dela obstaja možnost ogrožanja zaposlenih.

2. če kršitelj v nasprotju z drugim odstavkom 76. člena izvaja videonadzor dostopa v uradne službene oziroma poslovne prostore v notranjosti stanovanjskih stavb, ki nimajo vpliva na dostop do teh prostorov, ali snema vhode v stanovanja;

3. če kršitelj v nasprotju s tretjim odstavkom 76. člena pisno ne obvesti zaposlenih o izvajanju videonadzora v uradne službene oziroma poslovne prostore (tretji odstavek 76. člena).

Kršitelji se bodo za kršitve prvega, drugega ali tretjega odstavka 76. člena predloga zakona kaznovali z globo v naslednjih razponih:

- pravna oseba v razponu od 2.000 do 5.000 eurov, če pa se pravna oseba po zakonu, ki ureja gospodarske družbe, šteje za srednjo ali veliko gospodarsko družbo, pa z globo v razponu od 2.000 do 8.000 eurov;
- samostojni podjetnik posameznik ali posameznik, ki samostojno opravlja dejavnost, v razponu od 2.000 do 5.000 eurov;
- odgovorna oseba pravne osebe, samostojnega podjetnika posameznika ali posameznika, ki samostojno opravlja dejavnost, ter odgovorna oseba v državnem organu ali v samoupravni lokalni skupnosti (13.a člen ZP-1) v razponu od 500 do 2.000 eurov;
- posameznik pa v razponu od 100 do 500 eurov.

K 103. členu (kršitev določb o videonadzoru znotraj delovnih prostorov)

Določba 103. člena predloga zakona določa dva prekrška na področju izvajanja videonadzora znotraj delovnih prostorov, pri čemer sta kot prekrška določeni dve kršitvi 77. člena predloga zakona:

1. kršitelj se kaznuje z globo, če izvaja videonadzor v nasprotju z namenom izvajanja videonadzora znotraj delovnih prostorov.

   Prvi odstavek 77. člena tega zakona namreč določa le naslednje zakonite namene snemanja delovnih prostorov: če 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, in teh namenov ni možno doseči z milejšimi sredstvi. Kršitelj bo tako storil prekršek iz 1. točke prvega odstavka 100. člena zakona, če bo npr. izvajal videonadzor delovnega mesta zaradi spremljanja dela delavca v času delovnega časa.

2. kršitelj se kaznuje z globo, če v nasprotju z drugim odstavkom 77 člena predloga zakona izvaja videonadzor v delovnih prostorih, kjer ni potrebno varovati interesov iz prvega odstavka 76. člena tega zakona.

Kršitelj bo tako storil prekršek 2. točke prvega odstavka 103. člena zakona, če bo izvajal videonadzor delovnih prostorov, kjer to ni potrebno za namene iz prvega odstavka 77. člena predloga zakona, npr. če bi izvajal videonadzor v sobi z odpadnim papirjem.

Predlagatelj ocenjuje, da gre v primeru kršitev 77. člena predloga zakona za srednje težke prekrške povezane z videonadzorom (poseganje v zasebnost delavcev), zato so razponi glob višji kot npr. pri prekrških v zvezi z videonadzorom glede dostopa v uradne službene oziroma poslovne prostore. Storilci prekrškov se tako za predmetna prekrška kaznujejo v naslednjih razponih glob:

- pravna oseba v razponu od 4.000 do 10.000 eurov, če pa se pravna oseba po zakonu, ki ureja gospodarske družbe, šteje za srednjo ali veliko gospodarsko družbo, pa z globo v razponu od 8.000 do 20.000 eurov;
- samostojni podjetnik posameznik ali posameznik, ki samostojno opravlja dejavnost, v razponu od 4.000 do 10.000 eurov;
- odgovorna oseba pravne osebe, samostojnega podjetnika posameznika ali posameznika, ki samostojno opravlja dejavnost, ter odgovorna oseba v državnem organu ali v samoupravni lokalni skupnosti (13.a člen ZP-1) v razponu od 500 do 4.000 eurov;
- posameznik pa v razponu od 200 do 2.000 eurov.

K 104. členu (kršitev določb o videonadzoru v vozilih namenjenih javnemu potniškemu prometu)

Določba 104. člena predloga zakona določa dva prekrška na področju izvajanja videonadzora v vozilih namenjenih javnemu potniškemu prometu, pri čemer sta kot prekrška določeni dve kršitvi 78. člena predloga zakona:

3. kršitelj se kaznuje z globo, če izvaja videonadzor v nasprotju z namenom izvajanja videonadzora v prevoznih sredstvih, namenjenih javnemu potniškemu prometu.

   Prvi odstavek 78. člena tega zakona namreč določa le naslednje zakonite namene snemanja v delih prevoznega sredstva, namenjenih potnikom: za namen varnosti potnikov in premoženja, če tega ni mogoče doseči z drugimi ukrepi, ki manj posegajo v pravice iz prvega odstavka 1. člena tega zakona.

4. kršitelj se kaznuje z globo, če v nasprotju z drugim odstavkom 78. člena tega zakona ne uniči videoposnetkov v predpisanem roku ali uporablja posnetke za druge namene od tistih, določenih v drugem odstavku 78. člena tega zakona.

   Kršitelj bo tako storil prekršek 2. točke prvega odstavka 104. člena zakona, če posnetkov videonadzora v prevoznih sredstvih, namenjenih javnemu potniškemu prometu, ne bo izbrisal v roku sedmih dni po njihovem nastanku, ali če bo te posnetke uporabljal za druge namene kot za uveljavljanje ali obrambo pravnih zahtevkov ali za izvrševanje nalog policije.

Predlagatelj ocenjuje, da gre v primeru kršitev 78. člena predloga zakona za srednje težke prekrške povezane z videonadzorom (poseganje v zasebnost posameznikov), zato so razponi glob višji kot npr. pri prekrških v zvezi z videonadzorom glede dostopa v uradne službene oziroma poslovne prostore. Storilci prekrškov se tako za predmetna prekrška kaznujejo v naslednjih razponih glob:

- pravna oseba v razponu od 4.000 do 10.000 eurov, če pa se pravna oseba po zakonu, ki ureja gospodarske družbe, šteje za srednjo ali veliko gospodarsko družbo, pa z globo v razponu od 8.000 do 20.000 eurov;

- samostojni podjetnik posameznik ali posameznik, ki samostojno opravlja dejavnost, v razponu od 4.000 do 10.000 eurov;
- odgovorna oseba pravne osebe, samostojnega podjetnika posameznika ali posameznika, ki samostojno opravlja dejavnost, ter odgovorna oseba v državnem organu ali v samoupravni lokalni skupnosti (13.a člen ZP-1) v razponu od 500 do 4.000 eurov;
- posameznik pa v razponu od 200 do 2.000 eurov.

K 105. členu (kršitev določb o videonadzoru na javnih površinah)

Določba 105. člena predloga zakona kot prekrške določa kršitve 79. člena predloga zakona, ki ureja videonadzor na javnih površinah. Kršitelj se kaznuje z globo:

1. če v nasprotju z nameni iz prvega odstavka 79. člena tega zakona izvaja videonadzor na javnih površinah.

   Zakoniti nameni izvajanja videonadzora na javnih površinah so naslednji: kadar je to potrebno zaradi obstoja resne in utemeljene nevarnosti za življenje, osebne svobode, telesa ali zdravja ljudi, zaradi varnosti premoženja ali varovanja tajnih podatkov in tega namena ni mogoče doseči z milejšimi sredstvi. Videonadzor na javnih površinah je dovoljen tudi za namene varovanja varovanih oseb ter posebnih objektov in okolišev objektov, ki jih varuje policija, vojaška policija, pravosodna policija, oziroma varovanja drugih prostorov, zgradb ali območij, ki jih je treba varovati na podlagi zakona.
2. če v nasprotju z drugim drugi odstavkom 79. člena tega zakona izvaja videonadzor tistih delov javnih površin, ki ni potreben za varovanje interesov iz prvega odstavka 979. člena tega zakona.
3. če v nasprotju s tretjim odstavkom 79. člena tega zakona izvaja videonadzor na javnih površinah s katerimi ne upravlja ali na njih zakonito ne opravlja dejavnost;
4. če v nasprotju s petim odstavkom 79. člena tega zakona hrani posnetke videonadzora javnih površin več kot šest mesecev od trenutka nastanka, razen, če zakon ne določa drugače;
5. če v nasprotju s šestim odstavkom 79. člena tega zakona nemudoma ne obvesti policije ali drugega pristojnega subjekta, ko videonadzorni sistem posname dogodek na javni površini, ki ogroža zdravje ali življenje posameznika;
6. če v nasprotju s sedmim odstavkom 79. člena tega zakona na javnih površinah uporablja sistem za avtomatsko prepoznavo registrskih tablic ali sistemov, ki uporabljajo biometrične podatke, razen če zakon izrecno določa drugače.

Glede na to, da so predlagani prekrški povezani z izvajanjem videonadzora javnih površin, predlagatelj ocenjuje, da gre z vidika načela sorazmernosti za težje prekrške kot so npr. prekrški s področja kršitev določb o videonadzoru znotraj delovnih prostorov. Storilci prekrškov se tako za predmetne prekrške kaznujejo v naslednjih razponih glob:

- pravna oseba v razponu od 5.000 do 20.000 eurov, če pa se pravna oseba po zakonu, ki ureja gospodarske družbe, šteje za srednjo ali veliko gospodarsko družbo, pa z globo v razponu od 10.000 do 30.000 eurov;
- samostojni podjetnik posameznik ali posameznik, ki samostojno opravlja dejavnost, v razponu od 5.000 do 10.000 eurov;
- odgovorna oseba pravne osebe, samostojnega podjetnika posameznika ali posameznika, ki samostojno opravlja dejavnost, ter odgovorna oseba v državnem organu ali v samoupravni lokalni skupnosti (13.a člen ZP-1) v razponu od 500 do 5.000 eurov;

- posameznik pa v razponu od 200 do 2.000 eurov.

V zvezi s prekrški iz 1., 2., 3. in 6. točke prvega odstavka 101. člena predloga zakona predlagatelj pojasnjuje, da gre zaradi uporabe nedovršne oblike glagola za t. i. trajajoči prekršek.

K 106. členu (kršitev določb o biometriji v javnem sektorju)

106. člen predloga zakona kot prekršek določa kršitev določb o biometriji v javnem sektorju, kar pomeni, da bo kršitelj, ki je glede na predlagano določbo del javnega sektorja, kaznovan z globo, če bo biometrične ukrepe uporabljal brez zakonske podlage.

Glede na to, da gre pri predmetnem prekršku za kršitelje, ki tvorijo javni sektor, se storilci predmetnega prekrška kaznujejo z globo v naslednjih razponih:

- pravna oseba v razponu od 2.000 do 4.000 eurov, če pa se pravna oseba po zakonu, ki ureja gospodarske družbe, šteje za srednjo ali veliko gospodarsko družbo, pa z globo v razponu od 3.000 do 6.000 eurov;
- samostojni podjetnik posameznik ali posameznik, ki samostojno opravlja dejavnost, v razponu od 2.000 do 4.000 eurov;
- odgovorna oseba pravne osebe, samostojnega podjetnika posameznika ali posameznika, ki samostojno opravlja dejavnost, ter odgovorna oseba v državnem organu ali v samoupravni lokalni skupnosti (13.a člen ZP-1) v razponu od 500 do 4.000 eurov.

Predlagatelj v zvezi s predmetnim prekrškom pojasnjuje, da gre glede na uporabo nedovršne oblike glagola za t. i. kolektivni prekršek, kar pomeni, da kršitelj izvrši en prekršek, čeprav npr. brez zakonske podlage izvaja biometrične ukrepe 5.385 oseb.

K 107. členu (kršitev določb o biometriji v zasebnem sektorju)

107. člen predloga zakona kot prekrške določa kršitve določb o biometriji v zasebnem sektorju. Kršitelj se kaznuje z globo:

1. če v nasprotju z nameni iz prvega odstavka 82. člena predloga zakona izvaja biometrične ukrepe.

   Zakoniti nameni izvajanja biometričnih ukrepov v zasebnem sektorju so povečini enaki kot nameni izvajanja biometričnih ukrepov v javnem sektorju in so naslednji: če so ti nujni za opravljanje dejavnosti, za zagotavljanje varnosti ljudi, varnosti premoženja, varovanja tajnih podatkov, varstva poslovne skrivnosti ali za varstvo točnosti identitete strank.

2. če v nasprotju s drugim odstavkom 82. člena tega zakona izvaja biometrične ukrepe nad svojimi strankami brez zakonske ali pogodbene podlage oziroma brez izrecne pisne privolitve ali če potrošniku ne omogoči načina identifikacije brez obdelave biometričnih osebnih podatkov;

3. če v nasprotju s sedmim odstavkom 82. člena tega zakona zvaja biometrične ukrepe pred prejemom odločbe nadzornega organa, s katero je dovoljeno izvajanje biometričnih ukrepov.

V zvezi s predmetnim prekrškom predlagatelj pojasnjuje, da prekršek ne bo storjen, če bo oseba iz zasebnega sektorja biometrične ukrepe izvajala v skladu z devetim odstavkom 82. člena predloga zakona, ki določa kdaj se ti lahko izvajajo brez odločbe pristojnega nadzornega organa.

Glede na to, da gre pri predmetnem prekršku za kršitelje iz zasebnega sektorja, se storilci predmetnega prekrška kaznujejo z globo v naslednjih razponih:

- pravna oseba v razponu od 2.000 do 10.000 eurov, če pa se pravna oseba po zakonu, ki ureja gospodarske družbe, šteje za srednjo ali veliko gospodarsko družbo, pa z globo v razponu od 4.000 do 20.000 eurov;
- samostojni podjetnik posameznik ali posameznik, ki samostojno opravlja dejavnost, v razponu od 2.000 do 10.000 eurov;
- odgovorna oseba pravne osebe, samostojnega podjetnika posameznika ali posameznika, ki samostojno opravlja dejavnost, ter odgovorna oseba v državnem organu ali v samoupravni lokalni skupnosti (13.a člen ZP-1) v razponu od 500 do 4.000 eurov;
- posameznik pa v razponu od 200 do 2.000 eurov.

Spodnje meje razponov glob so enake kot so predlagane spodnje meje glob za kršitev določb o biometriji v javnem sektorju, ker gre za pomembno področje varstva osebnih podatkov, pa so zgornje meje glob za tovrstne prekrške v zasebnem sektorju določene višje kot v javnem sektorju.

Predlagatelj v zvezi s predmetnimi prekrški pojasnjuje, da gre glede na uporabo nedovršne oblike glagola za t. i. kolektivne prekrške, kar pomeni, da kršitelj izvrši en prekršek, če npr. svojim 2.000 potrošnikom ni omogočil načina identifikacije brez obdelave biometričnih osebnih podatkov.

K 108. členu (kršitev določb o prepovedi pridobivanja biometričnih osebnih podatkov v zvezi s trženjem)

108. člen predloga zakona kot prekršek določa kršitev določbe o prepovedi pridobivanja biometričnih osebnih podatkov v zvezi s trženjem. 83. člen predloga zakona namreč določa, da se v okviru trženja ali podobne druge poslovne dejavnosti ne sme zahtevati, pridobiti ali nadalje obdelovati biometričnih osebnih podatkov v zamenjavo za določene storitve, čeprav so te storitve za posameznika, na katerega se nanašajo osebni podatki, brezplačne.

Storilci predmetnega prekrška se bodo lahko za prekršek kaznovali v naslednjih razponih glob:

- pravna oseba v razponu od 8.000 do 20.000 eurov, če pa se pravna oseba po zakonu, ki ureja gospodarske družbe, šteje za srednjo ali veliko gospodarsko družbo, pa z globo v razponu od 16.000 do 40.000 eurov;
- samostojni podjetnik posameznik ali posameznik, ki samostojno opravlja dejavnost, v razponu od 8.000 do 20.000 eurov;
- odgovorna oseba pravne osebe, samostojnega podjetnika posameznika ali posameznika, ki samostojno opravlja dejavnost, ter odgovorna oseba v državnem organu ali v samoupravni lokalni skupnosti (13.a člen ZP-1) v razponu od 1.000 do 4.000 eurov;
- posameznik pa v razponu od 500 do 2.000 eurov.

Predlagani razponi glob so za prekršek pridobivanja biometričnih podatkov v zvezi s trženjem predlagane v visokih zneskih, saj predlagatelj kot ustrezno ocenjuje visoko predpisane globe. Gre namreč za (prekrškovnopravno) varstvo biometričnih podatkov kot osebnega podatka, ki je za posameznika (praktično nespremenljivo) enak vse življenje.

Glede na navedeno so znaki prekrška – če v nasprotju s83. členom tega zakona zahteva, pridobi ali nadalje obdela biometrične podatke osebe v zamenjavo za storitve – določeni z uporabo dovršne oblike glagolov, kar pomeni, da bo kršitelj z vsakim pridobljenim biometričnim podatkov v zameno za (brezplačno) storitev storil prekršek – 10 biometričnih podatkov pridobljenih v

nasprotju s 83. členom predloga zakona bo pomenilo storitev 10 prekrškov iz prvega odstavka 108. člena predloga zakona.

Prekrškovni organ bo v tem primeru izrekel globo v steku ob uporabi sistemskih določbo ZP-1 o steku, predvsem drugega odstavka 27. člena ZP-1, ki določa: »Če so za prekrške, storjene v steku, določene sankcije iste vrste, se izreče enotna sankcija, ki je enaka njihovemu seštevku, vendar enotna sankcija ne sme presegati dvakratne največje mere posamezne vrste sankcije po tem zakonu. Če to opravičujejo okoliščine iz drugega, tretjega in petega odstavka prejšnjega člena, se za istovrstne prekrške v steku, za katere je izdana ena odločba o prekršku (56. člen), lahko storilcu izreče enotna sankcija, ki ne dosega seštevka določenih sankcij ali ne presega največje mere posamezne vrste sankcije po tem zakonu.«.

K 109. členu (kršitev določb o evidentiranju vstopov in izstopov)

109. člen predloga zakona kot prekrška določa dve kršitvi določb o evidentiranju vstopov in izstopov. Kršitelj se bo z globo kaznoval v dveh primerih, in sicer:

1. če bo v nasprotju z drugim odstavkom 84. člena tega zakona v zbirki o vstopih in izstopih iz službenih prostorov obdeloval več osebnih podatkov kot jih predvideva drugi odstavek 84. člena predloga zakona.

   Skladno s predmetno določbo se namreč v zvezi z vstopi in izstopi iz službenih prostorov obdeluje izključno naslednje podatke: 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.

2. če bo v nasprotju s tretjim odstavkom 84. člena predloga zakona osebne podatke iz zbirke o vstopih in izstopih iz službenih prostorov hranil več kot dve leti od konca koledarskega leta po vnosu osebnih podatkov v zbirko ali če osebnih podatkov ne bo izbrisal ali uničil po poteku zakonsko določenega roka za hrambo, razen, če bi drug zakon določal drugače.

Predlagatelj meni, da predlagana prekrška nista posebej nevarna, zato predlagani razponi glob niso visoki. Kršitelji se bodo tako v primeru storitve prekrška lahko kaznovali v naslednjih razponih glob:

- pravna oseba v razponu od 1.000 do 3.000 eurov, če pa se pravna oseba po zakonu, ki ureja gospodarske družbe, šteje za srednjo ali veliko gospodarsko družbo, pa z globo v razponu od 2.000 do 6.000 eurov;
- samostojni podjetnik posameznik ali posameznik, ki samostojno opravlja dejavnost, v razponu od 1.000 do 2.000 eurov;
- odgovorna oseba pravne osebe, samostojnega podjetnika posameznika ali posameznika, ki samostojno opravlja dejavnost, ter odgovorna oseba v državnem organu ali v samoupravni lokalni skupnosti (13.a člen ZP-1) v razponu od 400 do 1.000 eurov;
- posameznik pa v razponu od 200 do 400 eurov.

Predlagatelj v zvezi s prekrškom iz 1. točke prvega odstavka 109. člena predloga zakona pojasnjuje, da gre glede na uporabo nedovršne oblike glagola za t. i. kolektivni prekršek, kar pomeni, da kršitelj z več dejanji izvrši en prekršek, npr. če bi v nasprotju z drugim odstavkom 81. člena predloga zakona v knjigo vstopov in izstopov vpisal več osebnih podatkov 420 oseb, bi bil kaznovan za en prekršek, pri čemer bi moralo biti v opisu dejanskega stanja zajetih vseh 420 oseb.

K 110. členu (kršitev določb o javnih knjigah)

110. člen predloga zakona kot prekršek določa kršitev sistemske določbe 85. člena predloga zakona, ki določa, da se lahko osebni podatki iz javnih knjig, ki so urejeni z zakonom, 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.[97]

Storilci predmetnega prekrška se bodo lahko za storitev predmetnega prekrška kaznovali v naslednjih razponih glob:

- pravna oseba v razponu od 2.000 do 4.000 eurov, če pa se pravna oseba po zakonu, ki ureja gospodarske družbe, šteje za srednjo ali veliko gospodarsko družbo, pa z globo v razponu od 5.000 do 20.000 eurov;
- samostojni podjetnik posameznik ali posameznik, ki samostojno opravlja dejavnost, v razponu od 2.000 do 4.000 eurov;
- odgovorna oseba pravne osebe, samostojnega podjetnika posameznika ali posameznika, ki samostojno opravlja dejavnost, ter odgovorna oseba v državnem organu ali v samoupravni lokalni skupnosti (13.a člen ZP-1) v razponu od 500 do 2.000 eurov;
- posameznik pa v razponu od 100 do 1.000 eurov.

Predlagatelj v zvezi s predmetnim prekrškom še pojasnjuje, da gre glede na uporabo nedovršne oblike glagola za t. i. kolektivni prekršek, kar pomeni, da kršitelj z več dejanju izvrši en prekršek, npr. če bi kršitelj uporabil osebne podatke 5.216 oseb iz zemljiške knjige, ki bi jih uporabil v nasprotju z nameni te javne knjige, ki je sicer namenjana vpisu in javni objavi podatkov o pravicah na nepremičninah in pravnih dejstvih v zvezi z nepremičninami, bi bil kaznovan za en prekršek, pri čemer bi moralo biti v opisu dejanskega stanja zajetih vseh 5.216 oseb, globa pa bi se izrekla v razpon za kategorijo storilca prekrška kot jo določa zakon

K 111. členu (kršitev določb o povezovanju uradnih evidenc in javnih knjig)

111. člen predloga zakona kot prekršek določa kršitve 86. člena predloga zakona. Kršitelj se bo z globo kaznoval v naslednjih primerih, in sicer:

1. če bo v nasprotju s prvim ali drugim odstavkom 86. člena tega zakona brez zakonske podlage izvedel povezovanje uradnih evidenc ali javnih knjig;
2. če pred začetkom povezovanja zbirk iz prvega odstavka 86. člena tega zakona, nadzornega organa ne bo obvesti v skladu s četrtim odstavkom 86. člena tega zakona (torej ne ob obvestl pravočasno ali pa prijava ne podrobna).

Bistveno za kršitev iz 1. točke prvega odstavka 110. člena predloga zakona je, da se uradne evidence in javne knjige lahko povezujejo izključno v primeru, ko povezovanje »dveh zbirk (osebnih) podatkov« določa zakon, npr., če bi šlo za povezovanje zemljiške knjige in zemljiškega katastra.

Storilci predmetnega prekrška se bodo lahko za prekršek kaznovali v naslednjih razponih glob, ki so enaki kot razponi glob pri prekrških v zvezi s kršitvijo določb o javnih knjigah:

[97] Glejte: odločba US, št. U-I-98/11, 26. 9. 2012, zlasti točka 17. in opomba št. 10 (objava: Uradni list RS, št. 79/12).

- pravna oseba v razponu od 2.000 do 4.000 eurov, če pa se pravna oseba po zakonu, ki ureja gospodarske družbe, šteje za srednjo ali veliko gospodarsko družbo, pa z globo v razponu od 5.000 do 20.000 eurov;
- samostojni podjetnik posameznik ali posameznik, ki samostojno opravlja dejavnost, v razponu od 2.000 do 4.000 eurov;
- odgovorna oseba pravne osebe, samostojnega podjetnika posameznika ali posameznika, ki samostojno opravlja dejavnost, ter odgovorna oseba v državnem organu ali v samoupravni lokalni skupnosti (13.a člen ZP-1) v razponu od 500 do 2.000 eurov;
- posameznik pa v razponu od 100 do 1.000 eurov.

K 112. členu (kršitev določb o strokovnem nadzoru)

112. člen predloga zakona kot prekrška določa dve kršitvi, in sicer kršitev drugega odstavka 88. člena predloga zakona in 90. člena predloga zakona. Kršitelj se bo za prekršek kaznoval z globo:

1. če v nasprotju z drugim odstavkom 88. člena tega zakona pri izvajanju strokovnega nadzora ne bo varoval tajnosti osebnih podatkov ali če bo v poročilu ali oceni ob zaključku strokovnega nadzora zapisal več osebnih podatkov kot so sicer nujno potrebni za dosego namena strokovnega nadzora;
2. če v nasprotju z 90. členom tega zakona pri izvajanju strokovnega nadzora posebnih vrst osebnih podatkov ali podatkov iz kazenskih ali prekrškovnih evidenc, izvajalec ne bo naredil uradnega zaznamka ali drugega uradnega zapisa v spisu zadeve upravljavca osebnih podatkov.

Storilci predmetnega prekrška se bodo lahko za prekrška kaznovali v naslednjih razponih glob:

- pravna oseba v razponu od 2.000 do 4.000 eurov, če pa se pravna oseba po zakonu, ki ureja gospodarske družbe, šteje za srednjo ali veliko gospodarsko družbo, pa z globo v razponu od 4.000 do 8.000 eurov;
- samostojni podjetnik posameznik ali posameznik, ki samostojno opravlja dejavnost, v razponu od 1.000 do 4.000 eurov;
- odgovorna oseba pravne osebe, samostojnega podjetnika posameznika ali posameznika, ki samostojno opravlja dejavnost, ter odgovorna oseba v državnem organu ali v samoupravni lokalni skupnosti (13.a člen ZP-1) v razponu od 800 do 1.500 eurov
- posameznik pa v razponu od 400 do 1.000 eurov.

K 113. členu (odmerjanje sankcij za prekrške)

113. člen predloga zakona na področju varovanja osebnih podatkov dopolnjuje splošna pravila za odmero (prekrškovnih) sankcij, ki jih sicer sistemsko določa 26. člena ZP-1.

Pri tem se upoštevajo vse okoliščine, ki vplivajo na to, ali naj bo sankcija manjša ali večja (olajševalne in obteževalne okoliščine), zlasti pa: stopnjo storilčeve odgovornosti za prekršek, nagibe, iz katerih je prekršek storil, stopnjo ogrožanja ali kršitve zavarovane dobrine, okoliščine, v katerih je bil prekršek storjen, prejšnje življenje storilca, njegove osebne razmere, njegovo obnašanje po storjenem prekršku, zlasti, ali je poravnal škodo – drugi odstavek 26. člena ZP-1.

Pri odmeri globe se upošteva tudi storilčevo premoženjsko stanje, višino njegove plače, njegove druge dohodke, njegovo premoženje in njegove družinske obveznosti, pri prekrških s področja davkov in carin pa tudi sorazmerje višine globe z višino prikrajšane dajatve – tretji odstavek 26. člena ZP-1.

Pri odmeri globe pravni osebi in samostojnemu podjetniku posamezniku se upošteva gospodarsko moč in prej izrečene sankcije – peti odstavek 26. člena ZP-1.

Glede na to, da morajo biti globe v prekrškovnem postopku v vsakem posameznem primeru učinkovite, sorazmerne in odvračilne, se na področju varstva osebnih podatkov pri odmeri sankcije za prekršek upoštevajo tudi naslednja primeroma našteta (dodatna) merila:

1. 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,
2. ali je obstajal namen koristoljubnosti ali namen škodovanja posameznikom, na katere se nanašajo osebni podatki,
3. v primeru izvajanja popravljalnih ukrepov s strani upravljavca ali obdelovalca njihovo učinkovitost ali samostojno ukrepanje še pred uvedbo nadzora,
4. glede fizičnih oseb se upošteva zlasti splošna raven dohodkov v Republiki Sloveniji ter njihov ekonomski položaj,
5. ali gre za ponavljajoče ali množične kršitve varstva osebnih podatkov ter pomen, ki bi ga za odvračanje tovrstnih kršitev varstva osebnih podatkov imela višina globe.

K 114. členu (izrek globe)

114. člen predloga zakona določa pooblastilo iz tretjega odstavka 52. člena ZP-1, in sicer, da se sme v hitrem postopku izreči globa tudi v znesku, ki je višji od najnižje predpisane globe. Posebnost predlagane določbe pa je v tem, da bo lahko pristojni prekrškovni organ (Informacijski pooblaščenec) izrekel globo v razponu tako za prekrške iz tega zakona, kot tudi za prekrške, ki jih izvorno določata četrti, peti in šesti odstavek 83. člena Splošne uredbe.

Glede na to, da so v Splošni uredbi določene le zgornje meje glob za prekrške, spodnje meje razpona glob za storilca prekrškov pravno osebo, samostojnega podjetnika posameznika ali posameznika, ki samostojno opravlja dejavnost, sistemsko določata druga in tretja alineja drugega odstavka 17. člena ZP-1, in sicer v višini 200 eurov za vse tri kategorije storilcev prekrškov.

IV. del – Prehodne in končne določbe

K 115. členu (rok za vzpostavitev posebnih ukrepov)

Predlagani 115. člen ureja rok za sprejem pravilnika o zaračunavanju stroškov iz četrtega odstavka 17. člena. Rok je določen na 3 mesece.

K 116. členu (pravilnik o zaračunavanju stroškov)

Predlagani 125. člen določa rok, v katerem Minister za pravosodje izda pravilnik o zaračunavanju stroškov. Rok je določen na tri mesece po uveljavitvi zakona.

K 117. členu (določitev pooblaščenih oseb)

Določba 117. člena določa nadaljnje opravljanje dela že imenovanih oseb organov v sestavi ministrstev, tudi če jih ni imenoval minister. Zgolj zaradi nove določbe, ki pristojnost za imenovanje podeljuje ministru, že imenovanih oseb ni treba zamenjati.

K 118. členu (prehodne določbe glede delovanja nadzornega organa)

Predlagani 118. člen ureja prehodne določbe glede delovanja Informacijskega pooblaščenca. Predlagani prvi odstavek določa, da se prekrškovni postopki, ki tečejo pred Informacijskim pooblaščencem ali pred sodiščem končajo skladno s prej veljavnim zakonom, razen, če je nov zakon milejši od prejšnjega.

Drugi odstavek se nanaša na odločitve Informacijskega pooblaščenca glede ustreznosti varstva osebnih podatkov v tretjih državah. Odločitve ostanejo v veljavi do njihove spremembe. Enako velja tudi za seznam tretjih držav, za katere je Informacijski pooblaščenec ugotovil, da imajo v celoti ali delno zagotovljeno ustrezno raven varstva osebnih podatkov, ali da te nimajo zagotovljene (tretji odstavek).

Četrti odstavek določa ukinitev Registra zbirk osebnih podatkov, ki ga vodi Informacijski pooblaščenec. Vsebina registra se arhivira, po enem letu jo prevzame Arhiv Republike Slovenije in jo hrani kot trajno arhivsko gradivo.

K 119. členu (prehodne določbe glede povezovanja)

Predlagani 119. člen določa prehodno obdobje za prilagoditev obstoječih zbirk osebnih podatkov in javnih knjig. V štiriletnem obdobju bo treba prilagoditi njihovo delovanje, da bo skladno z zahtevami iz 84. člena.

K 120. členu (prehodne določbe glede potrjevanja)

Predlagani 114. člen določa, da Slovenska akreditacija začne izvajati postopke akreditiranja teles za potrjevanje iz 51. člena s 1. januarjem 2024. Daljše prehodno obdobje je potrebno za vzpostavitev mehanizmov akreditacije.

Drugi odstavek za navedeno prehodno obdobje določa, da so dejanja obdelave do izteka tega roka skladna z zahtevami iz mehanizma potrjevanja, predvsem z namenom, da se jih v prehodnem obdobju ne onemogoči (npr. biometrija v zasebnem sektorju).

K 121. členu (prehodne določbe glede videonadzora v prevoznih sredstvih)

Predlagani 121. člen določa prehodno obdobje treh leto, v katerem morajo upravljavci videonadzora v prevoznih sredstvih, namenjenih javnemu potniškemu prometu, uskladiti videonadzor z določbami tega zakon. Prehodno obdobje je dovolj dolgo, da nova ureditev ne bo imela posebnih finančnih posledic.

K 122. členu (upoštevanje obvestil o določitvi pooblaščenih oseb)

Predlagani 122. člen določa nadaljnjo veljavo obstoječih obvestil o imenovanju pooblaščenih oseb za varstvo podatkov. Zaradi sprejema novega zakona oseb za varstvo osebnih podatkov ni potrebno ponovno imenovati.

K 123. členu (razveljavitev podzakonskih predpisov)

Predlagani 123. člen razveljavlja podzakonske akte, in sicer

- Pravilnik o metodologiji vodenja registra zbirk osebnih podatkov (glej četrti odstavek 114. člena predloga in drugi odstavek 83. člena Zakona o varstvu osebnih podatkov na področju obravnavanja kaznivih dejanj (ZVOPOKD));

- Pravilnik o pridobivanju potrebnih informacij za odločanje o iznosu osebnih podatkov v tretje države;
- Pravilnik o zaračunavanju stroškov pri izvrševanju pravice posameznika do seznanitve z lastnimi osebnimi podatki (predviden je sprejem novega pravilnika, kljub razveljavitvi je predvidena uporaba obstoječega pravilnika do sprejema novega).

K 124. členu (uporaba določb o prekrških)

Predlagani 124. člen določa neposredno uporabo določb o globah v Splošni uredbi, dokler ne bodo določbe o tovrstnih globah sistemsko urejene v Zakonu o prekrških.

K 125. členu (prenehanje veljavnosti zakona)

Predlagani 125. člen izrecno določa prenehanje veljavnosti do sedaj veljavnega Zakona o varstvu osebnih podatkov z dnem uveljavitve novega.

K 126. členu (končna določba)

Predlagani 126. člen določa *vacatio legis* 30 dni po objavi v Uradnem listu Republike Slovenije. Daljši rok je določen, ker gre za zakon, ki je delno sistemske narave in 15 dnevni rok ne bi bil primeren. Splošna uredba, ki ureja bistvena vprašanja, se uporablja že od maja 2018, zato dodatno podaljšanje uveljavitvenega roka ni potrebno.

IV. PRILOGE

- Osnutek Pravilnika o zaračunavanju stroškov
- MSP test