

23. 1. 2018

EVA: 2017-2030-0039

## **PREDLOG ZAKONA O VARSTVU OSEBNIH PODATKOV (ZVOP-2) – ZA MEDRESORSKO IN STROKOVNO USKLAJEVANJE TER ZA DRUGI KROG JAVNE RAZPRAVE**

### **I. UVOD**

#### **1. OCENA STANJA IN RAZLOGI ZA SPREJEM PREDLOGA ZAKONA**

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

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

V času vložitve predlogov navedenih pravnih aktov je Republike Slovenije imela sistem varstva osebnih podatkov urejen v skladu z določbami 38. člena Ustave Republike Slovenije<sup>4</sup>, Direktive 95/46/ES<sup>5</sup>, Okvirnega sklepa 2008/977/PNZ<sup>6</sup> in Konvencije o varstvu posameznikov glede na avtomatsko obdelavo osebnih podatkov<sup>7</sup> (Sveta Evrope).

Republika Slovenija je iz načelnih sistemskih razlogov (pravna varnost, možnost znižanja dosežene visoke ravni varstva osebnih podatkov, pretirane obveznosti za upravljavce osebnih podatkov – tudi

<sup>1</sup> 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).

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

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

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

<sup>5</sup> 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.

<sup>6</sup> 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.

<sup>7</sup> 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.

finančne, očitno pretirane globe, nato pretirana pooblastila Evropski komisiji glede izvedbenih in delegiranih aktov, izbira vrste predloga pravnega akta, ustreznost takratnega Okvirnega sklepa 2008/977/PNZ ipd.) navedenima predlogoma pretežno ali v celoti nasprotovala<sup>8</sup>, ob tem pa navedla tudi vrsto posebej obrazloženih pridržkov. Glede takratnega Predloga Splošne uredbe o varstvu podatkov je bil bistveni zaključek iz stališča Republike Slovenije, poleg želje za spremembo vrste pravnega akta iz uredbe v direktivo - da se mora Republika Slovenija v pogajanjih v okviru Sveta Evropske unije prizadevati, da »ne bi prišlo do neutemeljenega zniževanja standardov varstva osebnih podatkov, ki bi bili nižji glede na primerljivi kazalnik – »Direktivo 95/46/ES o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem pretoku takih podatkov«, glede predloga Direktive pa, da zadošča vsebina določb takrat veljavnega Okvirnega sklepa 2008/977/PNZ iz leta 2008 in da torej sprejetje predlagane Direktive ni potrebno.

Glede vsebine Predloga Splošne uredbe so se pojavili ustavnopravni pomisleki tudi v Zvezni republiki Nemčiji, tako je leta 2012<sup>9</sup> nemški zvezni ustavni sodnik Johannes Masing objavil članek, v katerem je z vidika nemškega Temeljnega zakona (Ustava) in ustavnosodne presoje nemškega Ustavnega sodišča izredno kritično nastopil proti Osnutku Splošne uredbe o varstvu podatkov. V njem 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 ustavnosodna presoja nemškega Zveznega Ustavnega sodišča 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)**«<sup>10</sup> - 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**«<sup>11</sup> - v nadaljnjem besedilu: Direktiva.

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

<sup>8</sup> 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.

<sup>9</sup> 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 v: Masing, Johannes, Prof. dr., *Herausforderungen des Datenschutzes*, *Neue Juristische Wochenschrift*, 2012, str. 2305-2311.

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

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

<sup>12</sup> 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.

Glede na navedene ugotovitve je pripravljeno besedilo Predloga Zakona o varstvu osebnih podatkov (ZVOP-2), ki pa pri tem ustrezno upošteva tudi izkušnje in spoznanja glede uporabe dosedanjega ZVOP-1 iz leta 2004, določbe 38. člena Ustave Republike Slovenije o človekovi pravici do varstva osebnih podatkov<sup>13</sup>, obstoječo ustavnosodno presojo Ustavnega sodišča Republike Slovenije glede človekove pravice do varstva osebnih podatkov od leta 1992<sup>14</sup> dalje ter tudi določbe še veljavne (še nespremenjene) Konvencije o varstvu posameznikov glede na avtomatsko obdelavo osebnih podatkov.

## **2. CILJI, NAČELA IN POGLAVITNE REŠITVE PREDLOGA ZAKONA**

### **2.1 Cilji Predloga ZVOP-2**

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

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

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

- omogočiti ljudem (posameznice in posamezniki, na katere se nanašajo osebni podatki) ter javnopravnim organom in poslovnim subjektom (upravljavci in obdelovalci), da so sistemske norme varstva osebnih podatkov čim bolj povezane ali pojasnjevalno predpisane, tako da se omogoči čim bolj koherenten pristop k izvajanju uresničevanja in varstva pravic s področja varstva osebnih podatkov<sup>15</sup>.

### **II.2. Pravni pristop glede zakonske izvedbe obeh pravnih aktov Evropske unije s področja varstva osebnih podatkov**

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

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

<sup>14</sup> 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.

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

drugim povezano določa, da lahko države članice Evropske unije ohranijo ali uvedejo podrobnejše določbe, da bi prilagodile uporabo pravil te uredbe v zvezi z obdelavo osebnih podatkov za zagotovitev skladnosti s točkama (c) in (e) prvega odstavka, tako da podrobneje opredelijo posebne zahteve v zvezi z obdelavo ter druge ukrepe za zagotovitev zakonite in poštene obdelave.

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

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

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

Delno primerljiv zakonodajni pristop, kot je predlagan v Predlogu ZVOP-2, sta dosedaj sprejeli tudi dve drugi primerljivi državi Evropske unije, namreč Zvezna republika Nemčija<sup>16</sup> in Republika Avstrija<sup>17</sup> (državi s primerljivim pravnim redom in ustavnopravnim oziroma ustavnosodnim razumevanjem pravice do varstva osebnih podatkov) v njihovih novih zakonih o varstvu osebnih podatkov iz leta 2017, namreč dokaj širšo implementacijo določb Splošne uredbe v nacionalni zakonodaji, razširitev določb Splošne uredbe na določena vprašanja, ki jih ureja sicer Direktiva (zaradi pravne varnosti in enakosti), natančnejše ureditve namenov obdelave osebnih podatkov, ureditev posebnih določb Direktive v posebnem delu zakona ipd. Bolj primerljiv slovenskim rešitvam iz Predloga ZVOP-2 je sicer bolj garantistični pristop Slovaške republike, ki je v njenem predlogu med drugim določila celo splošno uporabo (in istočasno neposredno uporabo) temeljnih definicij s področja varstva osebnih podatkov za vsa področja varstva osebnih podatkov iz njenega Predloga Zakona o varstvu osebnih podatkov (št. UV-42294/2017, z dne 22. 9. 2017), natančno razdelala zakonska načela, ob tem da je dan poseben poudarek načelu zakonitosti, razdelala institut privolitve ter izgleda pravnosistemske izhajala iz celovite uporabe pristopa klasičnega mednarodnega zasebnega prava in postopka.

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

Prav tako utegne na dokončnejšo vsebino bodočega ZVOP-2 vplivati tudi dejstvo, da je predvidena objava popravkov uradne slovenske inačice besedil Splošne uredbe in Direktive konec leta 2017 predvidoma v prvem tromesečju leta 2018, kar velja tudi za večino drugih jezikovnih inačic Splošne uredbe in Direktive. Vpliv na določbe Predloga ZVOP-2 utegne biti še nekoliko širši, saj utegnejo biti spremenjene tudi inačici besedil Splošne uredbe in Direktive v angleški jezikovni inačici, kar ni bilo

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

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

pričakovano. Z vidika pravne varnosti bodo spremembe v slovenski (morda tudi angleški) inačici obeh besedil pravnih aktov Evropske unije lahko upoštevane le v zakonodajnem postopku v Državnem zboru RS, saj bodo objavljene v Uradnem listu Evropske unije predvidoma šele marca 2018.

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

Predlog ZVOP-2 ima po predlagani vsebini dejansko in neizbežno skorajda pomen »zakonika« (za varstvo osebnih podatkov), saj kot je že navedeno, poskuša urediti čim več sistemske ozir splošne vsebine na enem mestu (razlog pravne varnosti), upošteva direktivni pristop iz določenih delov Splošne uredbe, uvaja nujne pojasnjevalne in povezovalne norme, izvaja določbe Direktive v istem zakonu, izvaja določbe Konvencije o varstvu posameznikov glede na avtomatsko obdelavo osebnih podatkov (Sveta Evrope), ureja varstvo osebnih podatkov za področja, ki jih Splošna uredba ne ureja (npr. varstvo osebnih podatkov umrlih oseb), določa, da velja za vse obdelave osebnih podatkov v Republiki Sloveniji (npr. področje varnosti države) ter tudi glede na absolutno dolžnost upoštevanja obveznosti zakonskega urejanja varstva osebnih podatkov glede na drugi odstavek 38. in 87. člen Ustave Republike Slovenije, ureja poleg sistemskih določb tudi določene področne ureditve (npr. biometrija) ipd.. Zlasti z vidika spoštovanja načela pravne varnosti je tak pristop skupnega urejanja varstva osebnih podatkov na enem mestu (tradicionalen že od leta 1990<sup>18</sup>) – upravičen.

### **II. 3. O zakonodajni tehniki Predloga ZVOP-2**

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

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

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

### **II. 4. Načela Predloga ZVOP-2**

#### Načelo spoštovanja osebnosti in pravic človeka

Prvo vodilno načelo novega Predloga ZVOP-2 je zakonodajno urejanje v smeri individualnega pristopa, po katerem je treba izhajati iz človeka kot upravičenca (nosilca; naslovnika; subjekta) pravice do varstva osebnih podatkov in torej njemu zagotoviti dejansko uresničevanje te pravice. Prosti pretok

<sup>18</sup> Glejte: Zakon o varstvu osebnih podatkov iz leta 1990 (Uradni list RS, št. 8/90, 19/91 in 59/99 - ZVOP).

osebnih podatkov, prenosi osebnih podatkov, čezmejne obdelave osebnih podatkov, posredovanja osebnih podatkov, obdelave osebnih podatkov v druge namene ipd. lahko delujejo le, če je navedeni individualni pristop spoštovan. Pri presoji zakonodajnih ali izvedbenih posegov v pravico do varstva osebnih podatkov je treba izhajati iz ocene vpliva posega varstvo osebnih podatkov na človeka kot subjekta ter opraviti oceno z vidika spoštovanja strogega načela sorazmernosti.

#### Načelo zakonitosti

Načelo zakonitosti v Predlogu ZVOP-2 izhaja iz drugega odstavka 38. člena Ustave Republike Slovenije (»Zbiranje, obdelovanje, namen uporabe, nadzor, in varstvo tajnosti osebnih podatkov določa zakon.«) ter iz 87. člena Ustave Republike Slovenije po katerem se pravice in obveznosti lahko urejajo le z zakonom. Navedeno načelo izhaja tudi iz temeljne navedbe št. 39 Splošne uredbe, (a) točke prvega odstavka člena 5 Splošne uredbe, prvega, drugega in tretjega odstavka člena 6 Splošne uredbe, (a) točke prvega odstavka člena 4 Direktive, člena 8 Direktive in a. točke 5. člena Konvencije. Ob tem je pomembno, da drugi stavek uvodne navedbe št. 45 Splošne uredbe navaja (ne pa prepoveduje) da »Ta uredba ne zahteva posebnega zakona za vsako posamezno obdelavo.« To pomeni da lahko države članice Evropske unije glede na svojo nacionalno (zlasti ustavno) ureditev vseeno določijo vsaj splošne pravne podlage za določene vrste obdelav konkretnih osebnih podatkov v sistemskem ali v področnih zakonih, ne pomeni pa za Republiko Slovenijo, da se lahko konkretne obdelave konkretnih osebnih podatkov določa v podzakonskih predpisih (kar je nedopustno po ustaljeni ustavnosodni presoji Ustavnega sodišča Republike Slovenije od leta 1992 dalje<sup>19</sup>). Temu pristopu tako sledijo 6. točka tretjega odstavka 6. člena, 8. člen in delno 9. člen ZVOP-2. Za delovanje (odločanje, poseganje v pravice določanje obveznosti) javnega sektorja (javne oblasti) velja strogo načelo zakonitosti, za zasebni sektor je načelo nekoliko omiljeno v smislu, da lahko splošne določbe Splošne uredbe ter ZVOP-2 določajo splošna pravila za posege v varstvo osebnih podatkov, ki se jih nato konkretno uporabi v praksi preko ocene učinkov na varstvo osebnih podatkov. Tako (delno) omiljeno spoštovanje načela zakonitosti za zasebni sektor (pogodbe, storitve) je zahteva iz točk (a), (b) (d) in (f) prvega odstavka člena 6 Splošne uredbe.

#### Načelo stroge sorazmernosti

Pri izvajanju posegov v pravico do varstva osebnih podatkov je treba izhajati iz načela sorazmernosti kot ga opredeljuje Predlog ZVOP-2, konkretnije, po ustavnosodni presoji z uporabo strogega testa sorazmernosti (predvsem odločba US, št. U-I-60/03, 4. 12. 2003<sup>20</sup>, zlasti 30. v zvezi s 17. točko odločbe).

#### Načelo namenske obdelave osebnih podatkov

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

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

Za represivne posege države človekove pravice ali temeljne svoboščine in interese še vedno velja načelo »prepovedano vse, kar ni izrecno dovoljeno«<sup>21</sup>. Za posege s strani zasebnega sektorja pa je

<sup>19</sup> Odločba US, št. U-I-115/92, 24. 12. 1992; objava: Uradni list RS, št. 3/93 in OdlUS I, 105.

<sup>20</sup> Objava: Uradni list RS, št. 131/03 in OdlUS XII, 93.

<sup>21</sup> Odločba US, št. U-I-25/95, 27. 11. 1997; objava: Uradni list RS, št. 5/98 in OdlUS VI, 158.

navedeno načelo omejeno v skladu z določbami ZVOP-2 in točkami (a), (b) (d) in (f) prvega odstavka člena 6 Splošne uredbe.

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

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

Tako so nekoliko drugače (v skladu s Splošno uredbo) določena načela zakonitosti, poštenosti in sorazmernosti, ki veljajo za vse dele Predloga ZVOP-2 ter tudi za področne ureditve v drugih zakonih v Republiki Sloveniji.

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

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

Določeni drugi (dosedaj: naknadni) nameni 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.

Določena je ureditev za osebe, ki znotraj upravljavcev ali obdelovalcev zagotavljajo varstvo osebnih podatkov, zlasti ko gre za tvegane ali množične obdelave osebnih podatkov, namreč pooblaščen osebe za varstvo osebnih podatkov. Ne uvaja se reguliran poklic, ampak neodvisne osebe znotraj upravljavca ali obdelovalca, ki naj preprečijo tveganja ali kršitve varstva osebnih podatkov.

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

Posebej je v Predlogu ZVOP-2 poudarjen pomen svobode izražanja v razmerju do varstva osebnih podatkov, tako da je omogočeno zdržanje dosedanje ravni uresničevanja svobode izražanja v okviru pravnega reda Republike Slovenije<sup>22</sup>.

Nadzorni organ za varstvo osebnih podatkov Republike Slovenije po določbah ZVOP-2 ostaja

<sup>22</sup> Gre za načelen in sistemski pristop Republike Slovenije, ki v obdobju zadnjih cca 6 let ni bil izražen samo pri sprejemanju Stališč Republike Slovenije glede predlogov Splošne uredbe in Direktive leta 2012, ampak tudi širše (mednarodno prepoznavno), npr. pisna in ustna intervencija Republike Slovenije leta 2014 v postopku v primeru *Maximillian Schrems* (ti. »Facebook primer«) - sodba SEU, C-362/14, 6. 10. 2015 ter v vzdržanosti pri glasovanju Republike Slovenije (kot ene od le štirih držav, ki so se vzdržale glasovanja iz načelnih razlogov) glede Ščita z a s e b n o s t i («Privacy Shield») dne 8. julija 2016 (glejte npr.: <https://www.theguardian.com/technology/2016/jul/08/privacy-shield-data-transfer-us-european-union>) ter tudi glede vsebine določenih bilateralnih mednarodnih pogodb (npr. s področja policijskega sodelovanja).

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

Področje pravosodja in policije ter izvrševanja kazenskih sankcij in delno obrambe ter varnosti države je urejeno v posebnem delu ZVOP-2. Ustrezne specifike in izjeme, tako glede namenov obdelav osebnih podatkov, obveščanja posameznikov o njihovih osebnih podatkih, so urejene specifično, glede na določbe Direktive.

V področnih ureditvah obdelav osebnih podatkov (poseben del ZVOP-2) so npr. delno prenovljeno razdelane določbe o videonadzoru (npr. uvedba videonadzora na javnih površinah) ter o biometriji.

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

Morale so biti izvedene tudi znatne spremembe dosedanega tradicionalnega izrazoslovja s področja varstva osebnih podatkov (ustaljeno od leta 1984<sup>23</sup>) – ker je bilo treba to izvesti glede na drugačne definicije iz Splošne uredbe in Direktive.

Tako so sedanji novi temeljni izrazi zlasti:

1. zbirka (dosedaj zbirka osebnih podatkov),
2. varnost osebnih podatkov (dosedaj zavarovanje osebnih podatkov),
3. upravljavec (dosedaj upravljavec osebnih podatkov),
4. obdelovalec (dosedaj pogodbeni obdelovalec),
5. posebne vrste osebnih podatkov (dosedaj občutljivi osebni podatki),
6. prenos osebnih podatkov (dosedanji iznos osebnih podatkov v tretje države),
7. čezmejna obdelava osebnih podatkov (pomeni izmenjave in obdelave osebnih podatkom med državami članicami Evropske unije),
8. posredovanje osebnih podatkov pomeni izmenjavo osebnih podatkov med upravljavcem in uporabnikom ali upravljavcem in upravljavcem ali upravljalcem in obdelovalcem.

## **II. 6. Bistvene spremembe v besedilu določb Predloga ZVOP-2 glede na Javno razpravo (prvi krog – 4.10. 2017 – 13. 11. 2017)**

Glede na prvi sklop pripomb in predlogov z prvega kroga Javne razprave (v obdobju 4. 10. 2017 – 13. 11. 2017) so v besedilu dosedanega osnutka zakona izvedene bistvene spremembe, saj je bil znaten del pripomb iz Javne razprave upravičen.

<sup>23</sup> Dr. Lovro Šturm: *Pravni vidiki zaščite podatkov v sodobnih informacijskih sistemih*, Zbornik znanstvenih razprav XLIV, 1984, str. 117-131.



Glede na najpogostejše pripombe in želje iz Javne razprave je besedilo uvodnega dela besedila določb Predloga ZVOP-2 (temeljne določbe) sedaj spremenjeno na način, da sledi hierarhiji dosedanjih določb ZVOP-1 (vidik preglednosti in notranje povezanosti določb), da določa splošne norme glede pravnih podlag za obdelavo osebnih podatkov, da določa posebne norme glede privolitve in obdelave v druge namene, drugače definira povezovanje zbirk osebnih podatkov ipd.. Nato predlog v nadaljevanju zlasti drugače določa obdelavo osebnih podatkov v druge namene, poenostavlja pogoje, ki se uporabljajo za privolitev otroka v zvezi uporabo storitev informacijske družbe, spreminja pogoje glede pooblaščenih oseb za varstvo osebnih podatkov, vključno glede možnosti, da se v določenih primerih za javni sektor najame zunanje izvajalce, posebej vzpostavlja možnost (skladnost) neposrednega trženja, drugače ureja institut roka hrambe osebnih podatkov, drugače ureja razmerje med svobodo izražanja in varstvom osebnih podatkov (še vedno v korist svobode izražanja), posvetovanje glede uvedbe videonadzora v delovnih prostorih širi tudi na svet delavcev ali delavskega zaupnika idr.. Glede določenih sistemskih vprašanj, ki izredno vplivajo na upravljavce in obdelovalce so sedaj podane zakonske rešitve glede kriterijev za izrekanje (pre)visokih glob po Splošni uredbi ter določba o pogojnem (začasnem) upoštevanju privolitev, ki so bile podane po veljavnem ZVOP-1. Prav tako je prišlo do razdelave (dodatnih) prekrškov, ki se jih lahko predpiše z ZVOP-2. Dodatne je razdelan (popravljen) tudi IX. del Predloga ZVOP-2, ki ureja varstvo osebnih podatkov na področju policijskega ter kazensko pravosodnega delovanja, tako da so določene določbe vsebinsko bolj razdelane in povezane.

Glede na navedeno ima Predlog ZVOP-2 v vsaj nekaj pomembnih delih drugačno vsebino ali pomen, kar pomeni, da je nujno treba izvesti dodaten (drugi) krog Javne razprave, saj spremembe besedila Predloga ZVOP-2 vplivajo na bodoče pravice ali interese posameznikov in posameznic, na katere se nanašajo osebni podatki, na obveznosti ali interese upravljavcev, obdelovalcev, svobodo izražanja ipd..

## II. 7. Sprejetje zakona

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

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

Predlog zakona ne bo imel posledic za Proračun Republike Slovenije.

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

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

- ocena drugih javnih finančnih sredstev: Predlog zakona ne bo imel posledic za druga javna finančna sredstva.
- predvideno povečanje ali zmanjšanje prihodkov državnega proračuna: Zaradi predloga zakona ni predvideno povečanje ali zmanjšanje prihodkov državnega proračuna – sredstva so že zagotovljena (naslednja točka).
- predvideno povečanje ali zmanjšanje obveznosti za druga javna finančna sredstva: Zaradi predloga zakona ni predvideno povečanje ali zmanjšanje obveznosti za druga javna finančna sredstva.
- predvideni prihranki za državni proračun in druga javna finančna sredstva: Prihranki za državni proračun in druga javna finančna sredstva niso predvideni.
- sredstva bodo zagotovljena z zadolževanjem (poročstva): Zaradi predloga zakona ni potrebno zadolževanje.
- v naslednjem proračunskem obdobju bodo sredstva zagotovljena: V naslednjem proračunskem obdobju dodatnih sredstev zaradi predloga zakona ni treba zagotavljati izven že predhodno dodeljenih sredstev v naslednji točki.

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

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

Podatki o sredstvih:

##### **Leto 2018**

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

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

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

Vsi izdatki skupaj 463,800,00 EUR.

##### **Leto 2019**

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

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

Vsi izdatki skupaj 359.600,00 EUR.

## Prostorska problematika

Trenutni prostori, v katerih deluje Informacijski pooblaščenec, v prihodnosti ne bodo zadoščali za učinkovito nadzorno delo in sprejemanje strank ob obstoječem ter novem številu zaposlenih. Glede nujne zamenjave poslovnih prostorov je Informacijski pooblaščenec izvedel posvetovanja z Ministrstvom za javno upravo, ki opravlja naloge s področja systemskega urejanja ravnanja s stvarnim premoženjem države in načrtovanja ter koordiniranja prostorskih potreb organov državne uprave. Posvetovanja z Ministrstvom za javno upravo so pokazala, da ustreznih prostorov v lasti Republike Slovenije za Informacijskega pooblaščenca ni na razpolago. Informacijski pooblaščenec bo moral poslovne prostore najeti, obstoječe poslovne prostore, ki so urejeni ter v celoti opremljeni, pa prepustiti v uporabo drugim državnim organom. Informacijski pooblaščenec je v letu 2017 naredil analizo trga nepremičnin in ugotovil, da se najemnine ustreznih prostorov skupaj z obratovalnimi stroški gibljejo med 17 in 19 evri na m<sup>2</sup>. Informacijski pooblaščenec je na podlagi analize trga našel ustrezne prostore v velikosti 800 m<sup>2</sup> na lokaciji, kjer so tudi že drugi državni organi. Cena najema je 17 EUR na m<sup>2</sup>, z vključenimi vsemi stroški. Ti prostori bodo omogočali redno in kakovostno delo Informacijskega pooblaščenca, saj tako Splošna uredba kot tudi Direktiva v 52. členu izrecno določata, da mora vsaka država članica »zagotoviti, da ima vsak nadzorni organi na voljo človeške, tehnične in finančne vire, prostore ter infrastrukturo, ki jih potrebuje za učinkovito opravljanje svojih nalog in izvajanje pooblastil, tudi tistih, ki se nanašajo na medsebojno pomoč, sodelovanje in udeležbo v odboru.«. Vselitev v nove prostore je predvidena v drugi polovici leta 2018.

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

### IV. 1. Uvodno o primerjalnopravi ureditvi

V letu 2017 sta bila sprejeta le dva izvedbena zakona držav članic Evropske unije – v Zvezni republiki Nemčiji in v Republiki Avstriji. Večina preostalih držav članic Evropske unije ima pripravljene predloge ali osnutke izvedbenih zakonov ali pa jih še pripravlja<sup>24</sup>. »Modeli« oziroma »smeri« zakonodajnega urejanja iz navedenih zakonov ali predlogov ali osnutkov so si precej različne (načeloma je vsaka država dokaj razvila zakonsko izvedbeno ureditev v njej lastno smer)<sup>25</sup>, nekateri zakoni so tudi minimalistični (predlog Finske republike z dne 21. 6. 2017), nekateri zakoni so tudi vsebinsko nepopolni.

Kot možen primer - Francoska republika je sprejela delni izvedbeni zakon leta 2016<sup>26</sup> ter naknadno glede njega ocenila, da bo treba zaradi vsebinske nepopolnosti ozir. vsebinskih problemov že sprejeti zakon razveljaviti (v delu, ki se nanaša na varstvo osebnih podatkov) ter pripraviti popolnoma nov Zakon o varstvu osebnih podatkov, ki je sedaj v letu 2018 v začetni pripravi. V zakonu iz leta 2016 je tako med drugim uredila vprašanje izrekanja visokih glob po Splošni uredbi, varstvo osebnih podatkov umrlih oseb, pravico do pozabe ipd..

Dokaj možna potencialna posledica navedenih precejšnjih razlik glede »modelov« ozir. »smeri« zakonodajnega urejanja s strani držav članic Evropske unije je tudi (možna) bodoča situacija, da bo

<sup>24</sup> Osnutek zakona Kraljevine Belgije bo tako znan predvidoma konec januarja 2018.

<sup>25</sup> Glede na to, da je vsaj Splošna uredba namenjena določeni zelo močni stopnji unifikacije varstva osebnih podatkov v Evropski uniji, hitra primerjava pokaže, da so si bili dosedanja zakoni o varstvu osebnih podatkov držav članic Evropske unije, ki so bili izvedbeni zakoni po Direktivi 95/46/ES (harmonizacija!) iz leta 1995 (zakoni so bili sprejeti v obdobju 1998-2004) vsebinsko in tudi oblikovno med seboj veliko bolj podobni. Rezultat sedanjega izredno različnega zakonodajnega pristopa držav članic Evropske unije glede Splošne uredbe je z vidika skupne evropske pravne varnosti in celo varstva pravice do osebnih podatkov kot človekove pravice sporen, ni pa bil nepričakovan.

<sup>26</sup> Zakon št. 2016-1321 z dne 7. oktobra 2016 za digitalno republiko.

treba v letih 2018 in 2019 po proučitvi vseh sprejetih zakonskih rešitev večino izvedbenih zakonov držav članic Evropske unije dopolnjevati (kar velja tudi za ZVOP-2). Vse države članice pri teh zakonodajnih pristopih štejejo, da ustrezno izvajajo določbe Splošne uredbe in Direktive.

V nadaljevanju sta tako predstavljena že sprejeta nemški in avstrijski zakon (torej le **dva že sprejeta zakona držav članic Evropske unije**) ter z vidika, da gre za (še dodatno) dokaj samostojen način zakonskega urejanja – zakonski predlog Vlade Slovaške republike (**tretja primerjalnopravna ureditev države članice Evropske unije v pripravi**).

### *III.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)<sup>27</sup>. Sistemski pristop zakona je, da precej upošteva obstoječo nacionalno pravno ureditev (ustavnopravno), ustaljene rešitve iz področnih zakonov Nemčije ter tradicionalno prakso varstva osebnih podatkov v Nemčiji.

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

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

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<sup>28</sup> ali če je to potrebno za uveljavljanje, izvajanje ali obrambo civilnopravnih zahtevkov, če ne prevladujejo interesi posameznika, na katerega se nanašajo osebni podatki, za izključitev obdelave osebnih podatkov. V 35. členu so določene omejitve pravice do izbrisa osebnih podatkov – če bi bil poseg nesorazmeren ali pa gre le za minimalno korist za posameznika.

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

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

<sup>27</sup> Zakon z dne 30. junija 2017, Bundesgesetzblatt Teil I, 2097.

<sup>28</sup> Zasebni sektor npr. uporablja videonadzor in bi hotel vložiti kazensko ovadbo, saj je ocenil, da obstaja sum storitve kaznivega dejanja.

Znano je da je sprejeti Zakon o prilagoditvi in izvajanju zakonodaje o varstvu osebnih podatkov EU deležen (sicer neupoštevanih) kritik iz dela zasebnega sektorja in dela javnosti<sup>29</sup>, češ da ni dovolj v skladu z določbami Splošne uredbe - da naj bi bile občasno njegove določbe prestroge ali preširoke. Možno je, da bo Nemčija v primeru kritik z vidika domnevne neskladnosti določb Zakona o prilagoditvi in izvajanju zakonodaje o varstvu osebnih podatkov EU v razmerju do določb Splošne uredbe uporabila podlago (ugovor) varstva temeljnih pravic po Temeljnem zakonu (Ustavi) Zvezne republike Nemčije ter ustaljene ustavnosodne presoje Zveznega Ustavnega sodišča Zvezne republike Nemčije.

#### *IV.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)<sup>30</sup>.

Sprejeti zakonski okvir precej sledi dosedanji ureditvi varstva osebnih podatkov v Republiki Avstriji, Avstrija je namreč izbrala način novelacije (spremembe in dopolnitve) veljavnega zakona. 1. člen veljavnega zakona, ki ureja varstvo osebnih podatkov kot osebno človekovo pravico in ima uradno pomen ustavne norme, ni bil spremenjen zaradi neobstoja zahtevane dvotretjinske večine vseh poslancev in poslank za ustavno revizijo, kar pomeni, da je Avstrija zadržala dosedanjo širšo opredelitev varstva osebnih podatkov kot temeljne pravice – kot nadrejeno glede vseh obdelav osebnih podatkov (tudi obdelav v druge namene). Prav tako je Avstrija zadržala dosedanjo tradicionalno ureditev (po sodni praksi od leta 1951 dalje) tudi (dela) podatkov pravnih oseb, ki se obravnavajo in varujejo kot (da so) osebni podatki. Za obdelavo osebnih podatkov otrok v zvezi storitvami informacijske družbe je določena mejna starost 14 let (v predlogu je bilo 16 let). Glede osebnih podatkov v zvezi s kazenskimi obsodbami je določeno (nekoliko drugače kot v členu 10 Splošne uredbe), da se lahko ti podatki obdelujejo tudi s strani upravljavca, če ima za to legitimen interes. Avstrija ni sprejela rešitve glede kritiziranih (spornih) visokih glob po Splošni uredbi, glede katerih se zatrjuje kršitev človekovih pravic ozir. neustavnost (tudi z vidika, da tako visokih glob ne bi smel izrekat nadzorni organ – ker ni sodišče), ampak bo počakala na odločitev Ustavnega sodišča Republike Avstrije v primerljivem primeru – presoja ustavnosti previsokih glob, katere lahko izreka avstrijski Urad za finančni trg. Glede razmerja varstvo osebnih podatkov – znanstveno raziskovanje je Avstrija določila le splošne določbe, obdelave pa bodo potekale po obstoječih področnih zakonih. Ni podana jasna rešitev glede dosedanjih pridobljenih privolitvev za obdelavo osebnih podatkov, če namreč ostanejo veljavne (nespremenjene) po novi ureditvi po Splošni uredbi – le v obrazložitvi prehodnih določb je v zvezi z omembo uvodne navedbe št. 171 Splošne uredbe nekoliko nejasno navedeno, da dosedanje privolitve za obdelavo osebnih podatkov ostanejo v veljavi, če ustrezajo pogojem iz Splošne uredbe.

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

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

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

<sup>29</sup> 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/>

<sup>30</sup> Bundesgesetzblatt I Nr. 120/2017, Teil I.

### *III. 4. Zakonski projekt druge države članice Evropske unije - 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.: Njegove bistvene nacionalne (sistemske) rešitve zlasti glede Splošne uredbe so predstavljene v nadaljevanju. Zelo močna sistemska rešitev iz predloga zakona je določitev splošne uporabe (in istočasno neposredne uporabe) temeljnih definicij s področja varstva osebnih podatkov za vsa področja (5. člen), kot so to npr. obdelava osebnih podatkov, privolitev ipd.. V 6. členu vzpostavlja 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 določa dokaj strogo namensko obdelavo 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 dopušča le glede arhivskih, statističnih, znanstvenih, zgodovinsko raziskovalnih namenov. V 17. členu določa, 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 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, določa, da se ne sme izvajati avtomatizirana obdelava glede posebnih vrst osebnih podatkov. III. Poglavlje II. Dela, III. Del in IV. Del Predloga zakona pa določajo zakonsko izvedbo določb Direktive (EU) 2016/680.

## **IV. Besedilo členov**

### **I.DEL TEMELJNE DOLOČBE**

#### **Pravica do varstva osebnih podatkov**

##### **1. člen**

(1) Vsaki posameznici ali posamezniku pripada osebna človekova pravica do varstva njenih ali njegovih osebnih podatkov, tako da se jim zagotavljajo zasebnost oziroma dostojanstvo ter podatkovna samoodločba.

(2) V okviru osebne človekove pravice iz prejšnjega odstavka 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.

#### **Prepoved diskriminacije glede varstva osebnih podatkov**

##### **2. člen**

Varstvo osebnih podatkov je zagotovljeno vsaki posameznici ali posamezniku (v nadaljnjem besedilu: posameznik) ne glede na narodnost, raso, barvo kože, veroizpoved, etnično pripadnost, spol, jezik, politično ali drugo prepričanje, spolno usmerjenost, spolno identiteto, premoženjsko stanje, kraj rojstva, izobrazbo, družbeni položaj, državljanstvo, kraj oziroma vrsto prebivališča, zdravstvene ali genske predispozicije ali katerokoli drugo osebno okoliščino.

#### **Vsebina zakona**

##### **3. člen**

(1) S tem zakonom se določajo pravice, obveznosti, upravičenja, načela, postopki in ukrepi, s katerimi se preprečujejo neustavni, nezakoniti ali neupravičeni posegi v zasebnost oziroma dostojanstvo oziroma druge temeljne pravice posameznika pri obdelavi osebnih podatkov, tako da se v skladu s spoštovanjem načela pravne varnosti varuje ali uresničuje pravico iz 1. člena tega zakona.

(2) S tem zakonom se v pravni red Republike Slovenije prenašajo določbe Direktive (EU) 2016/680 Evropskega parlamenta in Sveta z dne 27. aprila 2016 o varstvu posameznikov pri obdelavi osebnih podatkov, ki jih pristojni organi obdelujejo za namene preprečevanja, preiskovanja, odkrivanja ali pregona kaznivih dejanj ali izvrševanja kazenskih sankcij, in o prostem pretoku takih podatkov ter o razveljavitvi Okvirnega sklepa Sveta 2008/977/PNZ (Uradni list EU, L, št. 119/89 z dne 4. 5. 2016, str. 89–131 in .... – popr.; v nadaljnjem besedilu: Direktiva) ter zagotavlja izvajanje določb Uredbe (EU) 2016/679 Evropskega parlamenta in Sveta z dne 27. aprila 2016 o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem pretoku takih podatkov ter o razveljavitvi Direktive 95/46/ES (Splošna uredba o varstvu podatkov) (Uradni list EU, L, št. 119/1 z dne 4. 5. 2016, str. 1–88 in ... - popr.; v

nadaljnem besedilu: Splošna uredba), ki se morajo ali smejo prenesti v pravni red Republike Slovenije ter povezovalne določbe v zvezi s Splošno uredbo do določb Direktive.

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

(4) Če IX. del tega zakona ne določa drugače, določbe tega dela zakona veljajo tudi na področjih preprečevanja, preiskovanja, odkrivanja ali pregona kaznivih dejanj ali izvrševanja kazenskih sankcij.

## **Ozemeljska veljavnost zakona**

### **4. člen**

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

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

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

## **Obdelava osebnih podatkov za domače potrebe**

### **5. člen**

Določbe tega zakona ne veljajo za obdelave osebnih podatkov, ki jih izvajajo posamezniki izključno za osebno uporabo, družinsko življenje ali za druge domače potrebe.

## **Pomen izrazov**

### **6. člen**

(1) V tem zakonu uporabljeni izrazi imajo naslednji pomen in veljajo za izvajanje tega zakona ali drugih zakonov, v katerih so predpisani ti izrazi:

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



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

3. omejitev obdelave pomeni: označevanje shranjenih osebnih podatkov zaradi omejevanja njihove obdelave v prihodnosti;

4. oblikovanje profilov pomeni: vsako obliko avtomatizirane obdelave osebnih podatkov, ki vključuje uporabo osebnih podatkov za ocenjevanje nekaterih osebnih vidikov v zvezi s posameznikom, zlasti za analizo ali predvidevanje uspešnosti pri delu, ekonomskega položaja, zdravja, osebnega okusa, interesov, zanesljivosti, vedenja, lokacije ali gibanja tega posameznika;

5. psevdonimizacija pomeni: obdelavo osebnih podatkov na tak način, da osebnih podatkov brez dodatnih informacij ni več mogoče pripisati specifičnemu posamezniku, na katerega se nanašajo osebni podatki, če se take dodatne informacije hranijo ločeno ter zanje veljajo tehnični in organizacijski ukrepi za zagotavljanje, da se osebni podatki ne pripišejo določenemu ali določljivemu posamezniku;

6. zbirka pomeni: vsak strukturiran niz osebnih podatkov, ki so dostopni v skladu s posebnimi merili, niz pa je lahko centraliziran, decentraliziran ali razpršen na funkcionalni ali geografski podlagi;

7. upravljavec pomeni: fizično ali pravno osebo, javni organ, agencijo ali drugo telo, ki samo ali skupaj z drugimi določa namene in sredstva obdelave; kadar namene in sredstva obdelave določa pravo Unije ali pravo države članice, se lahko upravljavec ali posebna merila za njegovo imenovanje določijo s pravom Unije ali pravom države članice;

8. obdelovalec pomeni: fizično ali pravno osebo, javni organ, agencijo ali drugo telo, ki obdeluje osebne podatke v imenu upravjavca;

9. uporabnik pomeni: fizično ali pravno osebo, javni organ, agencijo ali drugo telo, ki so mu bili osebni podatki razkriti, ne glede na to, ali je tretja oseba ali ne. Vendar pa se javni organi, ki lahko prejmejo osebne podatke v okviru posamezne poizvedbe v skladu s pravom Unije ali pravom države članice, ne štejejo za uporabnike; obdelava teh podatkov s strani teh javnih organov poteka v skladu z veljavnimi pravili o varstvu podatkov glede na namene obdelave;

10. tretja oseba pomeni: fizično ali pravno osebo, javni organ, agencijo ali telo, ki ni posameznik, na katerega se nanašajo osebni podatki, upravljavec, obdelovalec in osebe, ki so pooblaščenice za obdelavo osebnih podatkov pod neposrednim vodstvom upravjavca ali obdelovalca;

11. privolitev posameznika, na katerega se nanašajo osebni podatki, pomeni: vsako prostovoljno, konkretno, informirano in nedvoumno ravnanje v obliki izjave ali drugačnega jasnega aktivnega delovanja, iz katerega je mogoče sklepati na želje posameznika, na katerega se nanašajo osebni podatki, s katero izrazi strinjanje z obdelavo osebnih podatkov, ki se nanašajo nanj;

12. kršitev varstva osebnih podatkov pomeni: kršitev varnosti, ki povzroči nenamerno ali nezakonito uničenje, izgubo, spremembo, nepooblaščen razkritje ali dostop do osebnih podatkov, ki so poslani, shranjeni ali kako drugače obdelani;

13. genski podatki pomeni: osebne podatke v zvezi s podedovanimi ali pridobljenimi genskimi značilnostmi posameznika, ki dajejo edinstvene informacije o fiziologiji ali zdravju tega posameznika in so zlasti rezultat analize biološkega vzorca zadevnega posameznika;

14. biometrični podatki pomeni: osebne podatke, ki so rezultat posebne tehnične obdelave v zvezi s fizičnimi, fiziološkimi ali vedenjskimi značilnostmi posameznika, ki omogočajo ali potrjujejo edinstveno identifikacijo tega posameznika, kot so podobe obraza ali daktiloskopski podatki;

15. podatki o zdravstvenem stanju pomeni: osebne podatke, ki se nanašajo na telesno ali duševno zdravje posameznika, vključno z zagotavljanjem zdravstvenih storitev, in razkrivajo informacije o njegovem zdravstvenem stanju;

16. glavni sedež pomeni:

a) v zvezi z upravljavcem, ki ima sedeže v več kot eni državi članici, kraj njegove osrednje uprave v Uniji ali, kadar se odločitve o namenih in sredstvih obdelave osebnih podatkov sprejemajo na drugem sedežu upravljavca v Uniji in ima ta sedež pooblastila za izvajanje takih odločitev, sedež, ki sprejema take odločitve;

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

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

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

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

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

21. nadzorni organ pomeni: Informacijskega pooblaščenca, določenega s tem zakonom ter zakonom, ki ureja informacijskega pooblaščenca;

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

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

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

c) je bila vložena pritožba pri tem nadzornem organu;

23. čezmejna obdelava osebnih podatkov pomeni bodisi:

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

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

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

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

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

telesa, ustanovljene z mednarodno pogodbo med Republiko Slovenijo in drugo državo ali med Republiko Slovenijo in več državami ali na podlagi take mednarodne pogodbe;

kar je navedeno tudi v skladu z zavezujočimi določbami člena 4 Splošne uredbe ter tudi pomeni izvajanje določb člena 3 Direktive in določb 2. in 5. člena Konvencije o varstvu posameznikov glede na avtomatsko obdelavo osebnih podatkov (Uradni list RS, št. 11/94 – Mednarodne pogodbe, št. 3/94 in 86/04 – ZVOP-1).

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

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

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

(3) Za učinkovito uporabo izrazov iz prvega odstavka tega člena v tem zakonu uporabljeni drugi izrazi pomenijo in veljajo za izvajanje tega zakona ali drugih zakonov:

1. javni sektor pomeni državne organe, organe samoupravnih lokalnih skupnosti, nosilce javnih pooblastil, javne agencije, javne sklade, javne zavode, univerze, samostojne visokošolske zavode in samoupravne narodne skupnosti;

2. zasebni sektor pomeni pravne in fizične osebe, ki opravljajo dejavnost po zakonu, ki ureja gospodarske družbe ali gospodarske javne službe ali obrt, in osebe zasebnega prava; zasebni sektor so tudi javni gospodarski zavodi, javna podjetja in gospodarske družbe in izvajalci javnih služb, ne glede na delež oziroma vpliv države, samoupravne lokalne skupnosti ali samoupravne narodne skupnosti;

3. povezovalni znaki – so osebna identifikacijska številka in druge z zakonom opredeljene enolične identifikacijske številke posameznika, z uporabo katerih je mogoče zbrati oziroma priklicati osebne podatke iz zbirk osebnih podatkov, v katerih so enolične identifikacijske številke obdelovane;

4. povezovanje zbirk pomeni elektronsko povezovanje dveh ali več zbirk osebnih podatkov tako, da se osebni podatki samodejno posodobijo v povezanih zbirkah (»povezovanje v ožjem smislu«) ter posredovanje podatkov na podlagi zahteve, na način, da uporabnik iz svoje zbirke osebnih podatkov neposredno prikliče osebne podatke, tako, da se priklicani osebni podatki elektronsko obdelajo in prenesejo v zbirko uporabnika, iz katere je bil opravljen priklic (»povezovanje v širšem smislu«); posamične elektronske poizvedbe za pridobitev osebnih podatkov posamezne osebe na zahtevo uporabnika, kjer uporabnik pred vsako poizvedbo posebej izkaže upravičenje za dostop do zbirke in zahtevanih osebnih podatkov, se ne štejejo za povezovanje zbirk;

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

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

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

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

## **Načela za zakonito obdelavo osebnih podatkov**

### **7. člen**

(1) Osebni podatki se:

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

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

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

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

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

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

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

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

## **Pravna podlage za obdelavo osebnih podatkov v javnem sektorju ter obdelava za drug namen**

### **8. člen**

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

(2) Ne glede na prejšnji odstavek se lahko v javnem sektorju obdelujejo osebni podatki le na podlagi privolitve posameznika, če ne gre za izvrševanje zakonitih pristojnosti, nalog ali obveznosti javnega sektorja. Zbirke osebnih podatkov, ki nastanejo na tej podlagi, morajo biti ločene od zbirk osebnih podatkov, ki nastanejo pri izvrševanju zakonitih pristojnosti, nalog ali obveznosti.

(3) Ne glede na prvi odstavek tega člena se lahko v javnem sektorju obdelujejo osebni podatki posameznika, ki je z javnim sektorjem sklenil pogodbo, ali pa je na podlagi zahteve tega posameznika

v fazi pogajanj za sklenitev pogodbe z njim, če je obdelava osebnih podatkov potrebna in primerna za izvajanje ukrepov pred sklenitvijo pogodbe ali za izvajanje pogodbe.

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

(5) Ne glede na prvi odstavek tega člena se lahko v javnem sektorju izjemoma obdelujejo tisti osebni podatki, ki so nujni za izvrševanje zakonitih pristojnosti, nalog ali obveznosti javnega sektorja, če se s to obdelavo ne poseže v upravičen interes posameznika, na katerega se osebni podatki nanašajo.

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

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

## **Pravne podlage za obdelavo osebnih podatkov v zasebnem sektorju ter obdelava za drug namen**

### **9. člen**

(1) Osebni podatki v zasebnem sektorju se lahko obdelujejo, če obdelavo osebnih podatkov in osebne podatke, ki se obdelujejo, določa zakon ali če je za obdelavo določenih osebnih podatkov podana privolitev posameznika. Če obdelavo osebnih podatkov v zasebnem sektorju določa zakon, mora ta določati: namen obdelave in vrste osebnih podatkov, ki se obdelujejo, kategorije posameznikov, na katere se nanašajo osebni podatki in rok hrambe. Zakon lahko, če je to potrebno, določi tudi morebitne druge ukrepe za zagotovitev zakonite, poštene in pregledne obdelave, omejitve namena in uporabnike in druge upravljavce osebnih podatkov, ki se jim osebni podatki lahko razkrijejo. Z zakonom se lahko določi, da se določeni osebni podatki za enega ali več določenih namenov obdelujejo le na podlagi privolitve posameznika.

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

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

(4) Ne glede na prvi odstavek tega člena se lahko v zasebnem sektorju obdelujejo osebni podatki, če je obdelava potrebna zaradi uresničevanja zakonitih upravičenih interesov, za katere si prizadeva upravljavec ali tretja oseba, razen kadar nad takimi interesi prevladajo interesi ali človekove pravice in temeljne svoboščine posameznika, na katerega se nanašajo osebni podatki, ki zahtevajo varstvo osebnih podatkov, zlasti kadar je posameznik, na katerega se nanašajo osebni podatki, otrok.

(5) Obdelava osebnih podatkov za druge namene kot tiste, za katere so bili osebni podatki prvotno zbrani, je v zasebnem sektorju dovoljena le, kadar je združljiva z nameni, za katere so bili osebni podatki prvotno zbrani ali kadar to določa ta zakon. Za ugotovitev, ali je namen nadaljnje obdelave združljiv z namenom, za katerega so bili osebni podatki prvotno zbrani, mora upravljavec, potem ko je izpolnil vse zahteve glede zakonitosti prvotne obdelave, opraviti presojo v skladu s četrtrim odstavkom

člena 6 Splošne uredbe. Presoja mora biti opravljena pred začetkom obdelave za druge namene, v pisni obliki, in je sestavni del dokumentacije po drugem odstavku člena 5 Splošne uredbe.

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

## **Posebno varstvo osebnih podatkov umrlih posameznikov**

### **10. člen**

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

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

(3) Ne glede na določbe prejšnjega odstavka upravljavec osebne podatke o umrlem posamezniku posreduje zakoncu, zunajzakonskemu partnerju ali partnerju iz partnerske zveze, otrokom ali staršem, če umrli posameznik ni predhodno pisno prepovedal posredovanja osebnih podatkov.

(4) Če zakon ne določa drugače, lahko upravljavec podatke o umrlem posamezniku posreduje tudi katerikoli drugi osebi, ki namerava te podatke uporabljati za zgodovinske raziskovalne, znanstvene raziskovalne, statistične ali arhivske namene pod pogoji iz 76. do 78. člena tega zakona.

(5) V zgodovinskih in drugih izobraževalnih publikacijah v fizični ali elektronski obliki se lahko objavljajo osebni podatki umrlih posameznikov, če izobraževalni namen objave prevlada nad upravičenimi interesi varstva zasebnosti umrlega posameznika ali če tako določa drug zakon.

## **Pogoji za privolitev mladoletne osebe za uporabo storitev informacijske družbe**

### **11. člen**

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

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

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

## Obdelava posebnih vrst osebnih podatkov

### 12. člen

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

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

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

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

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

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

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

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

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

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

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

(3) V primerih obdelav posebnih vrst osebnih podatkov iz drugega odstavka je treba poleg ukrepov iz 32. člena določiti in vzpostaviti in pisno opredeliti še primerne in posebne zaščitne ukrepe za varstvo pravic, svoboščin ali interesov posameznika, na katerega se nanašajo osebni podatki. Ob upoštevanju tehnološkega razvoja, stroškov izvajanja ter vrste, obsega, okoliščin in namenov obdelave ter različnih stopenj verjetnosti pojava tveganj, povezanih z obdelavo, za človekove pravice in temeljne svoboščine in interese posameznikov ter njihove resnosti, so ti zaščitni ukrepi najmanj naslednji:

a) politike, postopki in ukrepi za varnost osebnih podatkov, ki zagotavljajo, da obdelava poteka skladno z zahtevami iz 32. člena tega zakona,

b) ozaveščanje oseb, udeleženih v postopkih obdelave, o varnostnih politikah, postopkih in ukrepih za zagotavljanje varnosti osebnih podatkov,

c) pri zagotavljanju elektronskih storitev javnega sektorja, ki vključujejo obdelavo posebnih vrst osebnih podatkov, je za dostop do teh storitev potrebno zagotoviti takšna sredstva elektronske identifikacije, kjer se ob izdaji uradne listine ali izvedbi storitve zahteva osebno navzočnost posameznika in njegovo identiteto preveri z vpogledom v uradni osebni dokument posameznika,

č) pri prenosu posebnih vrst osebnih podatkov preko elektronskih omrežij morajo biti ti podatki šifrirani tako, da je zagotovljena njihova neprepoznavnost med prenosom in da so kontaktni podatki naslovnika predhodno preverjeni s potrditvenim sporočilom, s katerim naslovnik potrdi pravilnost podatkov za dostavo,

d) ustrezno upravljanje uporabniških pooblastil pri upravljavcih in obdelovalcih, in

e) kjer ustrezno, tudi psevdonimizacija oziroma šifriranje osebnih podatkov.

## **Varstvo in obdelava osebnih podatkov o kazenskih obsodbah ter o odločitvah o kaznovanju za prekrške**

### **13. člen**

(1) Za podatke o vpisu ali izbrisu v ali iz kazenske evidence ali evidenc, ki se upravljajo na podlagi zakona, ki ureja prekrške (v nadaljnjem besedilu: prekrškovne evidence) ter za prenose teh podatkov velja, da gre za osebne podatke, ki morajo biti varovani kot posebne vrste osebnih podatkov po drugem in tretjem odstavku 12. člena tega zakona.

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

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

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

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



## II. DEL

### PRAVICE POSAMEZNIKA, NA KATEREGA SE NANAŠAJO OSEBNI PODATKI

#### Področje uporabe tega dela zakona

#### 14. člen

Določbe tega dela zakona urejajo pravice posameznika, na katerega se nanašajo osebni podatki, in postopek uveljavljanja teh pravic iz členov 15 do 22 in 34 Splošne uredbe ter na področju preprečevanja, preiskovanja, odkrivanja ali pregona kaznivih dejanj ali izvrševanja kazenskih sankcij, če ni v tem ali IX. delu tega zakona določeno drugače.

**Pravice glede zagotavljanja preglednih informacij, informacij o posamezniku, na katerega se nanašajo osebni podatki, pravic posameznika, na katerega se nanašajo osebni podatki, do pridobitve teh podatkov ter pravice do popravka ali izbrisa osebnih podatkov, do omejitve obdelave ter pravica do pozabe**

#### 15. člen

(1) Pravice glede zagotavljanja preglednih informacij, informacij o posamezniku, na katerega se nanašajo osebni podatki, pravic posameznika, na katerega se nanašajo osebni podatki, do pridobitve teh podatkov ter pravice do popravka ali izbrisa osebnih podatkov, do omejitve obdelave ter pravica do pozabe se izvršujejo po določbah členov 16 do 19 Splošne uredbe.

(2) Upravljavec mora posamezniku, na katerega se nanašajo osebni podatki, posredovati informacije in sporočila, v skladu s členi 13 in 14 Splošne uredbe ter informacije iz členov 15 do 22 in 34 Splošne uredbe, ki se nanašajo na obdelavo osebnih podatkov, v čim bolj jedrnatih, preglednih, razumljivi in lahko dostopni obliki ter v jasnem in preprostem jeziku. Informacije in sporočila se posredujejo v posamezniku ustrezni obliki, ki je praviloma pisna, ali z drugimi sredstvi, zlasti z elektronskimi sredstvi.

(3) Upravljavec mora posamezniku, na katerega se nanašajo osebni podatki, olajšati uveljavljanje njegovih pravic, navedenih v prejšnjem odstavku tega člena.

#### Informacije za posameznika, na katerega se nanašajo osebni podatki

#### 16. člen

(1) Na področju preprečevanja, preiskovanja, odkrivanja ali pregona kaznivih dejanj ali izvrševanja kazenskih sankcij mora upravljavec posamezniku, na katerega se nanašajo osebni podatki, zagotoviti najmanj naslednje informacije:

1. imena in kontaktne podatke upravljavca in njegovega predstavnika;
2. kontaktne podatke pooblaščenih oseb, kadar ta obstaja;
3. namene, za katere se osebni podatki obdelujejo in pravno podlago za njihovo obdelavo in po potrebi morebitna pojasnila v zvezi s tem;
4. obstoj pravice do vložitve pritožbe pri Informacijskem pooblaščenču in njegove kontaktne podatke;
5. obstoj pravice do dostopa do podatkov in do tega, da upravljavec popravi ali izbriše podatke ali omeji obdelavo podatkov posameznika, na katerega se osebni podatki nanašajo.
6. zakonsko določeni rok hrambe osebnih podatkov;

7. kategorije uporabnikov osebnih podatkov, tudi uporabnikov v tretjih državah in mednarodnih organizacijah in če tako zahteva Splošna uredba dodatna pojasnila v zvezi s tem;

8. ali je zagotovitev osebnih podatkov zakonska ali pogodbeno obveznost ali pa obveznost, ki je potrebna za sklenitev pogodbe, ter ali mora posameznik, na katerega se nanašajo osebni podatki, zagotoviti osebne podatke ter kakšne so morebitne posledice, če se taki podatki ne zagotovijo, in

9. obstoj avtomatiziranega sprejemanja odločitev, vključno z oblikovanjem profilov iz prvega in četrtega odstavka člena 22 Splošne uredbe ter vsaj v takih primerih smiselne informacije o razlogih zanj, kot tudi pomen in predvidene posledice take obdelave za posameznika, na katerega se nanašajo osebni podatki.

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

(3) Kadar osebni podatki niso bili pridobljeni neposredno od posameznika, na katerega se osebni podatki nanašajo, mora upravljavec informacije po prejšnjem odstavku posamezniku zagotoviti v razumnem roku po prejemu osebnih podatkov, oziroma če se bodo osebni podatki uporabili za komuniciranje s posameznikom, najpozneje ob prvem komuniciranju s tem posameznikom, oziroma če je predvideno razkritje drugemu uporabniku, najpozneje ob prvem razkritju osebnih podatkov. Upravljavec mora pri tem poleg podatkov iz prejšnjega odstavka posamezniku zagotoviti še informacijo, od katerega upravljavca in po kateri pravni podlagi so bili posredovani osebni podatki.

(4) Obveščanje posameznika, na katerega se osebni podatki nanašajo, po drugem ali tretjem odstavku tega člena se lahko opusti, če in dokler to v posameznem primeru predstavlja nujen in očitno sorazmeren ukrep, ki mora spoštovati temeljne pravice in zakonite interese zadevnega posameznika, in je to izrecno določeno v zakonu:

1. da se onemogoči oviranje preprečevanja, preiskovanja, odkrivanja ali pregona kaznivih dejanj ali prekrškov, izvrševanja nalog in pooblastil policije, izvrševanja kazenskih sankcij, vključno s pridobivanjem ali prenosi osebnih podatkov za še nedokončane uradne postopke po tej točki;

2. zaradi zagotavljanja, da niso ovirani drugi uradni postopki, povezani s 1. točko;

3. zaradi varnosti države;

4. zaradi javne varnosti;

5. zaradi varstva obrambe države;

6. zaradi varstva človekovih pravic ali temeljnih svoboščin tretjih oseb.

## **Pravica posameznika, na katerega se nanašajo osebni podatki, do pridobitve teh podatkov**

### **17. člen**

(1) Na področju preprečevanja, preiskovanja, odkrivanja ali pregona kaznivih dejanj ali izvrševanja kazenskih sankcij ima vsak posameznik, na katerega se nanašajo osebni podatki, pravico, da od upravljavca prejme potrditev o tem, ali se v zvezi z njim obdelujejo osebni podatki in ima v tem primeru pravico pridobiti dostop do osebnih podatkov, ki se nanašajo nanj, ter naslednje informacije:

1. namene in pravno podlago za obdelavo;

2. vrste osebnih podatkov, ki se obdelujejo;

3. uporabnike ali kategorije uporabnikov, ki so jim bili ali jim bodo osebni podatki razkriti, zlasti uporabnike v tretjih državah ali mednarodnih organizacijah;
4. predvideni rok hrambe osebnih podatkov;
5. o obstoju pravice, da od upravljavca zahteva popravek ali izbris podatkov ali omejitev obdelave osebnih podatkov posameznika, na katerega se podatki nanašajo;
6. o obstoju pravice do vložitve pritožbe pri Informacijskem pooblaščenču in njegovih kontaktnih podatkih; in
7. sporočilo, ki vsebuje osebne podatke, ki so predmet obdelave, in vse razpoložljive informacije o viru osebnih podatkov.

(2) Obravnava zahteve posameznika po prejšnjem odstavku poteka v skladu s tem delom tega zakona.

(3) Omejitve pravice do pridobitve informacij iz prvega odstavka tega člena so dovoljene le pod pogoji, navedenimi v četrtem odstavku 89. člena tega zakona.

(4) V zvezi s členom 15 Splošne uredbe ima posameznik, na katerega se nanašajo osebni podatki, ki ima v drugem postopkovnem zakonu določeno zakonsko pravico do pregledovanja zadeve ali spisa, pravico pridobiti informacije tudi v skladu z določbami drugega postopkovnega zakona.

### **Pravica do popravka ali izbrisa osebnih podatkov, do omejitve obdelave ter posebni ukrepi varnosti osebnih podatkov**

#### **18. člen**

(1) Na področju preprečevanja, preiskovanja, odkrivanja ali pregona kaznivih dejanj ali izvrševanja kazenskih sankcij ima vsak posameznik, na katerega se nanašajo osebni podatki, pravico, da od upravljavca zahteva takojšnji popravek netočnih osebnih podatkov v zvezi z njim in dopolnitev nepopolnih ali neposodobljenih osebnih podatkov. Popravek ali dopolnitev se lahko po potrebi ob upoštevanju namenov obdelave izvede s predložitvijo dopolnilne izjave ali zaznamka.

(3) Na področju preprečevanja, preiskovanja, odkrivanja ali pregona kaznivih dejanj ali izvrševanja kazenskih sankcij mora upravljavec osebne podatke nemudoma izbrisati na lastno pobudo ali na podlagi zahtevka posameznika, na katerega se podatki nanašajo, če:

1. osebni podatki niso več potrebni za namene, za katere so bili pridobljeni ali drugače obdelani;
2. so bili osebni podatki obdelani nezakonito;
3. ne obstoji več prvotna pravna podlaga za obdelavo osebnih podatkov in za nadaljnje obdelave osebnih podatkov ni morebitne druge pravne podlage; ali
4. je izbris osebnih podatkov potreben zaradi izpolnitve druge obveznosti po zakonu ali po pravnomočni sodni odločbi.

(4) Na področju preprečevanja, preiskovanja, odkrivanja ali pregona kaznivih dejanj ali izvrševanja kazenskih sankcij lahko upravljavec namesto izbrisa osebnih podatkov njihovo obdelavo omeji, če:

1. posameznik, na katerega se podatki nanašajo, izpodbija točnost ali posodobljenost osebnih podatkov in pravilnosti ali nepravilnosti ni mogoče ugotoviti, vendar mora posameznika, na katerega se nanašajo osebni podatki, obvestiti pred razveljavitvijo omejitve, ali
2. je treba osebne podatke še nadalje hraniti za dokazne namene v okviru izvajanja zakonsko določene naloge.

3. upravljavec osebnih podatkov ne potrebuje več za namene obdelave, temveč jih posameznik, na katerega se nanašajo osebni podatki, potrebuje za uveljavljanje, izvajanje ali obrambo pravnih zahtevkov;

4. je posameznik, na katerega se nanašajo osebni podatki, vložil ugovor v zvezi z obdelavo v skladu s prvim odstavkom člena 21 Splošne uredbe, dokler se ne preveri, ali zakoniti razlogi upravljavca prevladajo nad razlogi posameznika, na katerega se nanašajo osebni podatki.

(5) Vsak posameznik, na katerega se nanašajo osebni podatki, ima pravico, da od upravljavca zahtevati prepoved ali omejitev obdelave v druge namene po šestem odstavku 8. člena, po petem odstavku 9. člena ali drugih določbah tega zakona ali po drugih zakonskih podlagah, ki določajo obdelavo v druge namene.

(6) Na področju preprečevanja, preiskovanja, odkrivanja ali pregona kaznivih dejanj ali izvrševanja kazenskih sankcij mora upravljavec popravek netočnih ali neposodobljenih osebnih podatkov ali omejitev ali prepoved obdelave sporočiti pristojnemu organu ali drugi organizaciji, od katerega je pridobil osebne podatke.

(7) Na področju preprečevanja, preiskovanja, odkrivanja ali pregona kaznivih dejanj ali izvrševanja kazenskih sankcij se v primerih popravka, izbrisa podatkov ali omejitve obdelave po tem členu mora upravljavec o tem obvestiti vse uporabnike osebnih podatkov. Uporabniki so zavezani osebne podatke, ki so v njihovi pristojnosti, nemudoma popraviti, izbrisati, ustrezno označiti ali omejiti njihovo obdelavo.

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

## **Obravnavanje zahteve ter sodelovanje z Informacijskim pooblaščenecem**

### **19. člen**

(1) Ta člen se nanaša na zahtevo iz členov 15 do 22 Splošne uredbe ter na zahteve za dostop, popravek, izbris in omejitev na področju preprečevanja, preiskovanja, odkrivanja ali pregona kaznivih dejanj ali izvrševanja kazenskih sankcij (člen 14 in 16 Direktive) .

(2) Če posameznik, na katerega se podatki nanašajo, zahtevo predloži elektronsko, mora biti po možnosti obveščen po isti elektronski poti, če ne navede drugega kontaktnega naslova.

(3) V postopku z zahtevo se smiselno uporabljajo določbe 67. člena zakona, ki ureja splošni upravni postopek o ravnanju z nepopolno ali nerazumljivo vlogo.

(4) Upravljavec lahko zaradi potrditve identitete osebe, ki je v skladu s tem delom tega zakona vložila zahtevek, zahteva dodatne potrebne informacije. Ugotavljanje identitete posameznika pri zahtevah, vloženih po elektronski pošti se lahko izvaja tudi:

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

(5) Upravljavec mora o zahtevi posameznika odločiti brez nepotrebnega odlašanja in v vsakem primeru v enem mesecu po prejemu zahteve. Ta rok se lahko po potrebi podaljša za največ dva dodatna meseca ob upoštevanju zapletenosti in števila zahtev. Upravljavec obvesti posameznika, na katerega se nanašajo osebni podatki, o vsakem takem podaljšanju v enem mesecu po prejemu zahteve skupaj z razlogi za zamudo in pravnim poukom.

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

(7) V zvezi s pravico dostopa do informacij o uporabnikih iz točke c prvega odstavka člena 15 Splošne uredbe ter na področju preprečevanja, preiskovanja, odkrivanja ali pregona kaznivih dejanj ali izvrševanja kazenskih sankcij ima posameznik pravico, da od upravljavca pridobi tudi informacije o tem kdaj, na kakšni podlagi in za kakšen namen ter katerim uporabnikom so bili osebni podatki razkriti. Posameznik ima tudi pravico do pridobitve evidence dejavnosti obdelave, če jo upravljavec ima.

(8) Pravica dostopa posameznika do lastnih osebnih podatkov po členu 15 Splošne uredbe ne vpliva na pravico do seznanitve z lastno zdravstveno dokumentacijo in z njo povezane pravice po zakonu, ki ureja pacientove pravice. Glede pravice do seznanitve z lastno zdravstveno dokumentacijo in pravice do seznanitve z zdravstveno dokumentacijo umrlih pacientov se za odločanje na prvi stopnji uporabljajo določbe zakona, ki ureja pacientove pravice in tretji odstavek tega člena in 24. člen tega zakona (omejitev pravic zakonitega zastopnika), ter na drugi stopnji določbe 21. do 25. člena tega zakona.

(9) Breme dokazovanja točnosti ali posodobljenosti osebnih podatkov in zakonitosti obdelave osebnih podatkov je na upravljavcu ali obdelovalcu, če osebni podatki niso bili pridobljeni izključno na podlagi navedb posameznika, na katerega se podatki nanašajo.

(10) Upravljavec in obdelovalec ter, kadar obstajajo, njuni predstavniki, na zahtevo sodelujejo z Informacijskim pooblaščenecem pri izvajanju njegovih nalog, če ne gre za vpliv na odločanje v prekrškovnem postopku.

## **Ugovor v primeru nepopolne odločitve upravljavca**

### **20. člen**

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

### **Pritožba**

### **21. člen**

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

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

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

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

## **Postopek obravnave pritožbe**

### **22. člen**

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

(2) Posameznik se lahko pritoži tudi zoper:

1. višino zaračunane razumne pristojbine iz petega odstavka člena 12 in tretjega odstavka člena 15 Splošne uredbe in
2. odločitev upravljavca o podalšanju roka za obravnavo zahtevkov posameznika iz 19. člena tega zakona. Pritožba ne vpliva na potek podalšanega roka za odločitve.

## **Pooblastila Informacijskega pooblaščenca v pritožbenem postopku**

### **23. člen**

(1) V postopku iz 22. člena tega zakona ima pooblaščen uradna oseba Informacijskega pooblaščenca, ki mora izpolnjevati pogoje za nadzornika, poleg preiskovalnih in popravljalnih pooblastil iz drugega odstavka člena 58 Splošne uredbe, tudi pooblastila iz zakona, ki ureja inšpekcijski nadzor. Druga postopkovna dejanja v upravnem postopku, vključno z dejanji iz drugega in tretjega odstavka tega člena lahko opravlja tudi pooblaščen uradna oseba, ki ne izpolnjuje pogojev za nadzornika.

(2) V postopkih iz 22. člena tega zakona lahko pooblaščen uradna oseba Informacijskega pooblaščenca opravlja ogled prostorov, osebnih podatkov in dokumentarnega gradiva ter zaslišuje osebe pri upravljavcu in priče brez prisotnosti strank postopka. Če zadostuje za odločitev o pritožbi posameznika, lahko pooblaščen uradna oseba Informacijskega pooblaščenca pridobi le pisne izjave o dejstvih ter pisna pojasnila od upravljavca, prič ter drugih oseb. Pisne ali ustne izjave odgovornih oseb upravljavca ali pooblaščen osebe se lahko štejejo kot izjave strank.

(3) V postopku iz prvega in drugega odstavka tega člena lahko pooblaščen uradna oseba Informacijskega pooblaščenca namesto izdaje upravne odločbe upravljavcu z ureditvenim predlogom predlaga prostovoljno rešitev posameznikove pritožbe v postavljenem roku, ki ne more biti daljši od enega meseca, če se z ureditvenim predlogom predhodno strinja posameznik in je to smiselno zaradi učinkovitega uresničevanja pravic posameznika. Z izpolnitvijo ureditvenega predloga je pritožbeni

postopek zaključen s sklepom o ustavitvi postopka. Zoper sklep ni dovoljena pritožba, je pa dopusten upravni spor.

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

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

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

## **Izjema glede uveljavljanja pravic posameznika preko zakonitega zastopnika**

### **24. člen**

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

## **Upravna izvršba**

### **25. člen**

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

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

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

## **Zaračunavanje stroškov**

### **26. člen**

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

(2) Kadar so zahteve posameznika, na katerega se nanašajo osebni podatki, očitno neutemeljene ali pretirane, zlasti ker se zahteve pogosto ponavljajo, lahko upravljavec s posebno obrazloženo odločitvijo izdano v skladu z 19. členom tega zakona:

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

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

(3) Višino pristojbine iz prejšnjega odstavka ter iz tretjega odstavka člena 15 Splošne uredbe in pravila o zaračunavanju predpiše Informacijski pooblaščenec, po predhodnem soglasju ministra, pristojnega za pravosodje.

(4) Višino stroškov na področju seznanitve z lastno zdravstveno dokumentacijo in dokumentacijo umrlih pacientov ter pravila o zaračunavanju predpiše Informacijski pooblaščenec, po predhodnem soglasju ministra, pristojnega za zdravje..

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

## **Omejitve pravic posameznikov**

### **27. člen**

(1) Pravice posameznika iz tega dela zakona je mogoče z zakonom izjemoma omejiti iz razlogov navedenih v prvem odstavku členu 23 Splošne uredbe.

(2) Omejitve iz prejšnjega odstavka se lahko določijo samo pod pogojem, da je zakonska določba, ki določa takšno omejitev, v skladu s prvim odstavkom 8. člena tega zakona.

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

## **Sodno varstvo pravic posameznika**

### **28. člen**

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

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

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

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

(4) Postopek je prednosten.



### III. DEL

## UPRAVLJAVEC IN OBDELOVALEC

### 1. poglavje

#### Splošne obveznosti

#### Odgovornost za skladnost obdelav osebnih podatkov

#### 29. člen

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

(2) Upravljavec, ki obdeluje velike količine posebnih vrst osebnih podatkov ali osebnih podatkov v zvezi s kazenskimi obsodbami in kaznovanji za prekrške, ali ki izvaja obdelave, pri katerih bi glede na naravo, obseg, okoliščine in namene obdelave lahko nastalo veliko tveganje za pravice in svoboščine, mora poleg ukrepov po prejšnjem odstavku vzpostaviti in izvajati še splošno politiko varstva osebnih podatkov.

(3) Upravljavec v svojih notranjih aktih predpiše ukrepe oziroma politiko iz prvih dveh odstavkov ter določi osebe, ki so odgovorne za posamezne zbirke osebnih podatkov oziroma osebe, ki lahko zaradi narave njihovega dela obdelujejo osebne podatke iz posamezne zbirke osebnih podatkov.

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

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

#### Vgrajeno in privzeto varstvo osebnih podatkov

#### 30. člen

(1) Upravljavec mora že tekom načrtovanja nove obdelave predvideti ustrezne tehnične in organizacijske ukrepe ter varovalke za zagotovitev, da bo obdelava spoštovala temeljna načela varstva podatkov iz 5. člena tega zakona, še zlasti pa načeli najmanjšega obsega podatkov ter omejitve roka hrambe. Ukrepi morajo biti primerni glede na stanje najnovejšega tehnološkega razvoja na tem področju, na naravo, obseg, okoliščine in namene obdelave ter tveganja za poseg v človekove pravice in temeljne svoboščine posameznikov, ki nastajajo pri obdelavi, lahko pa se upošteva tudi stroške njihovega izvajanja. Z izvajanjem teh ukrepov je treba pod pogoji iz prejšnjega člena nadaljevati tudi po začetku obdelave.

(2) Upravljavec mora istočasno izvesti ustrezne organizacijske ukrepe za zagotovitev, da se bodo pri vsaki posamični obdelavi po privzetem obdelovalo samo tisti nabor osebnih podatkov, ki je tudi dejansko potreben za predvideni namen te posamične obdelave, ter da pri tem ti podatki ne bodo brez potrditve osebjem upravljavca postali dostopni večjemu številu posameznikov.

## Pogodbena obdelava

### 31. člen

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

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

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

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

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

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

3. izvede vse potrebne ukrepe za varnost osebnih podatkov;

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

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

6. ob upoštevanju vrste obdelave in razpoložljivih informacij upravljavcu pomaga pri izpolnjevanju obveznosti, navedenih v 22., 44. in 75. členu tega zakona;

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

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

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

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

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

(7) Obdelovalec in vsaka oseba, podrejena upravljavcu ali obdelovalcu, ki ima dostop do osebnih podatkov, sme te podatke obdelovati izključno po navodilih upravljavca, razen če to od nje zahteva pravo Unije ali pravo države članice.

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

## **Evidenca dejavnosti obdelav**

### **31.a člen**

(1) Upravljavec in obdelovalec vodita evidenco dejavnosti obdelav v skladu s členom 30 Splošne uredbe in skrbita za točnost in posodobljenost tega kataloga.

(2) Ta obveznost se ne uporablja za upravljavce in obdelovalce, ki so fizične osebe ali ki so pravne osebe z manj kot 250 zaposlenimi, razen za tiste njihove obdelave, za katere je verjetno, da predstavljajo tveganje za človekove pravice ali temeljne svoboščine posameznikov, na katere se nanašajo osebni podatki, če ne gre le občasne obdelave ter tudi za tiste obdelave, ki vključujejo posebne vrste podatkov ali osebne podatke v zvezi s kazenskimi obsodbami ali prekrški.

(3) Izjema iz prejšnjega odstavka se ne uporablja za upravljavce in obdelovalce, ki so del javnega sektorja, notarje, odvetnike, detektive, izvršitelje, izvajalce zasebnega varovanja, zasebne zdravstvene delavce ter za izvajalce zdravstvenih storitev.

## **2. poglavje**

### **Varnost osebnih podatkov**

#### **Varnost osebnih podatkov**

### **32. člen**

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

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

(a) psevdonimizacijo in šifriranjem osebnih podatkov;

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

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

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

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

(f) ukrepe, ki omogočajo poznejše ugotavljanje, kdaj so bile posamezne vrste osebnih podatkov vnesene v zbirko osebnih podatkov, uporabljene ali drugače obdelane in kdo je to storil, in sicer za obdobje 5 let od zaključka leta, v katerem je potekala obdelava, razen če za obdelave posameznih vrst osebnih podatkov drug zakon ne določa drugače.

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

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

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

### **Obveščanja Informacijskega pooblaščenca o kršitvah varstva osebnih podatkov**

#### **33. člen**

(1) Upravljavec oziroma obdelovalec morata v skladu s členom 33 Splošne uredbe brez nepotrebnega odlašanja obvestiti Informacijskega pooblaščenca o vsaki kršitvi varstva osebnih podatkov, ki jo zaznata, če je verjetno, da bo povzročila tveganje za posege v človekove pravice in temeljne svoboščine posameznikov.

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

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

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

### **Obveščanje posameznikov o kršitvah varstva osebnih podatkov**

#### **34. člen**

(1) Upravljavec oziroma obdelovalec morata v skladu s členom 34 Splošne uredbe brez nepotrebnega odlašanja obvestiti posameznike, katerih osebni podatki so bili kršeni ali je verjetno da so bili kršeni, o kršitvi varstva osebnih podatkov, ki jo zaznata, če je verjetno, da bo povzročila velika tveganja za pravice in svoboščine posameznikov. Za obveščanje se uporablja četrti odstavek 88. člena tega zakona.

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

(3) Ne glede na določbe prejšnjega odstavka lahko upravljavec zaradi spoštovanja pravne varnosti ali bistvenih človekovih pravic ali temeljnih svoboščin opravi tudi obveščanje preko medijev.

### **3. poglavje**

#### **Ocena učinka in predhodno posvetovanje**

#### **Ocena učinka v zvezi z varstvom osebnih podatkov**

##### **35. člen**

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

(2) Oceno učinkov je vedno treba opraviti glede:

1. obdelav, ki vključujejo sistematično in obsežno vrednotenje podatkov o posameznikih s sredstvi avtomatizirane obdelave, vključno z oblikovanjem profilov, ki potem služi kot osnova za odločitve, ki imajo za posameznika pravne posledice ali nanj na podoben način znatno vplivajo,
2. obdelave posebnih vrst podatkov ali osebnih podatkov v zvezi s kazenskimi obsodbami in prekrški v velikem obsegu,
3. sistematičen nadzor javno dostopnega območja v velikem obsegu, oziroma
4. obdelav s seznama, ki ga v skladu s pogoji iz četrtega in šestega odstavka člena 35 Splošne odredbe določi in objavi Informacijski pooblaščenec.

(3) Ocene učinkov ni treba opraviti glede:

1. obdelav s seznama, ki ga v skladu s pogoji iz petega in šestega odstavka člena 35 Splošne odredbe določi in objavi Informacijskih pooblaščenec.
2. obdelav, ki jih izvajajo upravljavci iz javnega sektorja in imajo pravno podlago v zakonu, pa je bila ocena učinkov izvedena že med sprejemanjem te zakonske podlage, vendar le, če se narava, obseg, okoliščine ali namen obdelave niso v ničemer bistvenem spremenile po izdelavi ocene.

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

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

### **4. poglavje**

#### **Posebne določbe**

#### **Posredovanje podatkov, ki ga izvajajo organi javnega sektorja**

##### **36. člen**

(1) Posredovanje osebnih podatkov, ki ga izvedejo organi javnega sektorja, v druge organe javnega sektorja, je dovoljeno, če je potrebno za izvajanje nalog v pristojnosti organa, ki prenaša podatke, ali tretje osebe, ki se ji podatki prenašajo, in so izpolnjeni pogoji, ki bi dopuščali obdelavo po četrtem odstavku 8. člena in 9. členu tega zakona. Organ javnega sektorja ali tretja oseba, ki se ji podatki

prenesejo, sme osebne podatke obdelovati samo v namen, za uresničevanje katerega se ji prenašajo. Obdelava v druge namene je dovoljena pod iz šestega ali sedmega odstavka 8. člena tega zakona.

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

1. je potreben za izvajanje nalog v pristojnosti organa, ki prenaša podatke, in so izpolnjeni pogoji, ki bi dopuščali obdelavo po 14. členu tega zakona;

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

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

(3) Prenos posebnih vrst osebnih podatkov po prvem odstavku člena 9 Splošne uredbe je dovoljen, če so izpolnjeni pogoji iz prvega ali drugega odstavka tega člena in gre za dejansko stanje, ki je izjema po drugem odstavku člena 9 Splošne uredbe ali po 17. členu tega zakona.

(4) Upravljavec centralnega registra prebivalstva ali evidenc stalno in začasno prijavljenih prebivalcev mora na način, ki je določen za izdajo potrdila, posredovati upravičencu, ki izkaže pravni interes za uveljavljanje pravic pred osebami javnega sektorja, osebno ime in naslov stalnega ali začasnega prebivališča ter datum smrti posameznika, zoper katerega ali v zvezi s katerim uveljavlja svoje pravice.

## **Posredovanje podatkov, ki ga izvajajo upravljavci iz zasebnega sektorja**

### **37. člen**

(1) Upravljavec iz zasebnega sektorja posreduje osebne podatke drugemu uporabniku zgolj na podlagi utemeljene zahteve iz drugega odstavka 38. člena, iz katere že na prvi pogled izhajata veljavna pravna podlaga za pridobitev podatkov ter utemeljenost zahteve.

## **Postopek posredovanja osebnih podatkov**

### **38. člen**

(1) Upravljavec osebnih podatkov mora proti plačilu stroškov posredovanja, če zakon ne določa drugače, posredovati osebne podatke uporabnikom ali upravljavcem, ki izkažejo pravno podlago za pridobivanje zahtevanih osebnih podatkov.

(2) Zahteva za posredovanje mora vsebovati:

1. podatke o uporabniku ali upravljavcu (za fizično osebo: osebno ime, naslov opravljanja dejavnosti ali naslov stalnega ali začasnega prebivališča; za samostojnega podjetnika ter za pravno osebo: naziv oziroma firmo in naslov oziroma sedež in matično številko) ter podpis pooblaščenice osebe;

2. pravno podlago za pridobitev zahtevanih osebnih podatkov;

3. namen obdelave osebnih podatkov oziroma razloge, ki izkazujejo potrebnost in primernost osebnih podatkov za doseg namena pridobitve;

4. predmet in številko ali drugo identifikacijo zadeve, v zvezi s katero so osebni podatki potrebni;

5. vrste osebnih podatkov, ki naj se mu posredujejo; in

6. obliko in način pridobitve zahtevanih osebnih podatkov.

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

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

(5) Če je zahteva za posredovanje osebnih podatkov delno ali v celoti zavrnjena, lahko uporabnik osebnih podatkov zahteva sodno varstvo po določbah zakonov, ki urejajo sodne postopke.

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

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

(8) Revizijsko sled iz prejšnjega odstavka mora upravljavec hraniti za obdobje pet (5) let, razen če drug zakon za posredovanje posameznih vrst podatkov ne določa drugačnega roka.

## **Pravica do vpogleda v osebni dokument**

### **39. člen**

(1) Upravljavec osebnih podatkov lahko pred vnosom v zbirko osebnih podatkov preveri točnost osebnih podatkov z vpogledom v osebni dokument ali drugo ustrezno javno listino posameznika, na katerega se nanašajo. Navedeno ne posega v določbe zakonov, ki urejajo posamezne osebne dokumente, o pravici upravljavca do kopiranja osebnega dokumenta.

## **Obdelava povezovalnih znakov**

### **40. člen**

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

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

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

## **Rok hrambe osebnih podatkov, določitev roka in vezanost na rok**

### **41. člen**

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

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

(3) Po izpolnitvi namena obdelave se osebni podatki zbršejo, uničijo, blokirajo ali anonimizirajo, če zakon za posamezne vrste osebnih podatkov ne določa drugače.

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

### 1. poglavje

#### Pooblaščne osebe za varstvo podatkov

##### Opredelitev pooblaščne osebe za varstvo osebnih podatkov

#### 42. člen

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

(2) Dejanske izkušnje iz prejšnjega odstavka vključujejo vsaj tri leta delovnih izkušenj s področja varstva osebnih podatkov ali področja informacijske varnosti ali področja poslovne skrivnosti po zakonu, ki ureja gospodarske družbe ali zaupnih podatkov po zakonu, ki ureja bančništvo,

#### Obveznost imenovanja pooblaščne osebe

#### 43. člen

(1) Pooblaščen osebno morajo imenovati:

1. vsi upravljavci ali obdelovalci v javnem sektorju;

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

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

(2) Ostali upravljavci ali obdelovalci lahko prostovoljno imenujejo pooblaščen osebno.



(3) Upravljavec ali obdelovalec, ki je imenoval pooblaščen osebno, mora v roku osmih dni od imenovanja vpisati njene kontaktne podatke po členu 30 Splošne uredbe v svoji evidenci dejanj obdelave, jih javno objaviti na primeren način ter jih sporočiti Informacijskemu pooblaščenju, ki teh podatkov ne objavi javno. Prav tako s temi kontaktnimi podatki pod pogoji iz členov 13 ali 14 Splošne uredbe seznaniti posameznike, na katere se nanašajo osebni podatki, ki jih obdeluje.

## **Pogoji za imenovanje pooblaščen osebno**

### **44. člen**

(1) Za pooblaščen osebno je lahko določen posameznik ali posameznica, ki izpolnjuje pogoje iz petega odstavka člena 37 in drugega stavka šestega odstavka člena 38 Splošne uredbe ter drugega odstavka 42. člena tega zakona.

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

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

2. je poslovno sposoben,

3. ima vsaj univerzitetno izobrazbo ali končan magistrski študijski program

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

4. je zaposlen v javnem sektorju,

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

(3) Javni sektor lahko za pooblaščen osebno izjemoma s pogodbo v pisni obliki imenuje tudi posameznika ali posameznico iz zasebnega sektorja, ali pravno osebno zasebnega sektorja, če ta subjekt javnega sektorja nima več kot 20 zaposlenih (varianta: 30 zaposlenih), če njegovo delovanje ne vsebuje visoke stopnje tveganj obdelave osebnih podatkov za človekove pravice in temeljne svoboščine in interese posameznikov, ne gre za množične avtomatične obdelave osebnih podatkov, ne gre za redno, sistematično in obsežno spremljanje posameznikov ali njihovo profiliranje ter tudi za obdelavo posebnih vrst osebnih podatkov kot del primarne dejavnosti subjekta javnega sektorja.

(4) Zasebni sektor lahko za pooblaščen osebno upravljavca ali obdelovalca s pogodbo v pisni obliki imenuje tudi posameznika ali posameznico, ki ni zaposlena pri upravljavcu ali obdelovalcu, ali pravno osebno.

(5) Če se v skladu s tretjim ali četrtem odstavkom tega člena imenuje pravno osebno, morajo vsi njeni zaposleni in drugi sodelavci, ki bodo opravljali naloge pooblaščen osebno, izpolnjevati pogoje za imenovanje v pooblaščen osebno. Prav tako mora biti v pogodbi z njo določen vodilni član, ki odgovarja za delo pravne osebe in katerega kontaktni podatki bodo objavljeni v skladu določbami tretjega odstavka 31. člena tega zakona.

(6) Pooblaščen osebno lahko pri opravljanju njenih nalog pomagajo tudi druge osebe, ki so pri tem vezane na njena navodila. Te osebe morajo izpolnjevati pogoje za imenovanje za pooblaščen osebno.

(7) Za pooblaščen osebno in osebe, ki ji pomagajo pri opravljanju njenih nalog ne sme biti imenovana oseba, ki ima konflikt interesov z upravljavcem ali obdelovalcem.

(8) V javnem sektorju se šteje, da ima določena oseba konflikt interesov, če ima položaj predstojnika ali drugega funkcionarja v subjektu javnega sektorja, če je član organov upravljanja ali nadzora pri

upravljavcu ali obdelovalcu, če njene druge naloge vključujejo odločanje o obdelavi osebnih podatkov pri upravljavcu ali obdelovalcu, ali če zastopa upravljavca oziroma obdelovalca v sodnih ali arbitražnih postopkih v zvezi z vprašanji varstva osebnih podatkov. V primeru, da pooblaščen oseb izve za situacijo, ki predstavlja ali bi lahko predstavljala konflikt interesov, mora o tem takoj pisno obvestiti upravljavca oziroma obdelovalca. Upravljavec oziroma obdelovalec mora v tem primeru bodisi odpraviti konflikt bodisi pooblaščen oseb razrešiti ob upoštevanju določb tretjega in četrtega odstavka 48. člena tega zakona. Enako ravna v primeru, če se na drug način seznanijo z obstojem ali verjetnostjo obstoja konflikta interesov. Vse navedeno velja tudi za osebe, ki pooblaščen oseb pomagajo pri opravljanju njenih nalog.

## **Skupno imenovanje pooblaščen oseb**

### **45. člen**

Več upravljavcev iz javnega ali več upravljavcev iz zasebnega sektorju lahko, upošteva njihovo delovno področje, organizacijsko strukturo in velikost, imenuje skupno pooblaščen oseb. Pri tem morajo zagotoviti, da je pooblaščen oseb še vedno sposobna opravljati svoje naloge v zvezi z vsemi upravljavci ali obdelovalci, za katere je imenovana.

## **Naloge pooblaščen oseb**

### **46. člen**

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

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

(3) Pooblaščen oseb sodišča ali državnega tožilstva ne sme opravljati navedenih nalog v zvezi z obdelavami osebnih podatkov, izvršenih v okviru izvajanja neodvisnega sodniškega odločanja ali samostojnega opravljanja državnotožilske funkcije odločanja, kot ju opredeljujeta zakon, ki ureja sodišča in zakon, ki ureja državna tožilstva. Pooblaščen oseb sme opravljati te naloge samo glede zadev sodne uprave in državnotožilske uprave ter glede izvajanja varnosti osebnih podatkov.

(4) Pooblaščen oseb Ustavnega sodišča Republike Slovenije ne sme opravljati navedenih nalog v zvezi z obdelavami osebnih podatkov, izvršenih v okviru odločanja Ustavnega sodišča Republike Slovenije, kot jih opredeljuje zakon, ki ureja ustavno sodišče ali drugi zakoni. Pooblaščen oseb sme opravljati te naloge samo glede zadev uprave Ustavnega sodišča ter glede izvajanja varnosti osebnih podatkov.

(5) Pooblaščen oseb Varuha človekovih pravic ne sme opravljati navedenih nalog v zvezi z obdelavami osebnih podatkov, izvršenih v okviru delovanja Varuha človekovih pravic, kot jih opredeljuje zakon, ki ureja varuha človekovih pravic ali drug zakon, ki ureja pristojnosti ali naloge varuha človekovih pravic. Pooblaščen oseb sme opravljati te naloge samo glede zadev obdelav osebnih podatkov s področja zagovornišva otrok ter glede izvajanja varnosti osebnih podatkov.

## **Določitev pooblaščen oseb in njihove naloge v določenih državnih organih**

### **47. člen**

(1) Na Ustavnem sodišču Republike Slovenije Ustavno sodišče določi eno pooblaščen oseb, ki opravlja naloge v skladu s četrtem odstavkom 46. člena tega zakona.

(2) Varuh človekovih pravic določi eno pooblaščenno osebo, ki opravlja naloge v skladu s petim odstavkom 46. člena tega zakona.

(3) Vsak minister ali ministrica mora določiti svojo pooblaščenno osebo, ki je zaposlena na tem ministrstvu.

(4) Na področjih izvajanja obveščevalno-varnostne dejavnosti predstojnik organizacije s tega področja določi eno pooblaščenno osebo in njenega namestnika znotraj organizacije s tega področja, ki opravlja tiste naloge iz člena 39 Splošne uredbe, za katere tako določi predstojnik, med njih pa so obvezno vključene naloge glede izvajanja varnosti osebnih podatkov ter posredovanja osebnih podatkov Vladi Republike Slovenije, Predsedniku Republike Slovenije, policiji, državnim tožilstvom ali sodiščem ali pristojnemu delovnemu telesu Državnega zbora Republike Slovenije, čezmejne obdelave in prenose.

## **Položaj pooblaščenno osebe**

### **48. člen**

(1) Upravljavca ali obdelovalca pooblaščenno osebi zagotovita pogoje za učinkovito in neodvisno opravljanje njenih nalog po 46. členu tega zakona, zlasti:

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

2. ima dostop do vseh osebnih podatkov ter dejanj obdelave,

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

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

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

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

(3) Upravljavca oziroma obdelovalca pooblaščenno osebe za varstvo podatkov zaradi izvajanja njenih nalog ne sme razrešiti, je kaznovati ali je zapostavljati.

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

## **Dolžnost varstva tajnosti osebnih podatkov**

### **49. člen**

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

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

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

## **2. poglavje**

### **Kodeksi ravnanja in certificiranje**

#### **Kodeksi ravnanja**

##### **50. člen**

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

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

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

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

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

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

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

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

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

## **Certificiranje**

### **51. člen**

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

(2) Merila posameznega certifikacijskega mehanizma, ki jih pripravi upravljavec ali obdelovalec iz prvega odstavka odobri Informacijski pooblaščenec z odločbo v skladu s petim odstavkom člena 42 Splošne uredbe ali Odbor v skladu s petim odstavkom člena 42 Splošne uredbe. Zoper odločbo Informacijskega pooblaščenca iz prejšnjega stavka pritožba ni dopustna, je pa dopusten upravni spor.

(3) Certifikat se lahko uporablja za izkazovanje, da so dejanja obdelave osebnih podatkov s strani upravljavca ali obdelovalca skladna s Splošno uredbo, pri čemer pa posedovanje certifikata ne posega v odgovornosti upravljavca ali obdelovalca za skladnost njunih delovanj obdelave osebnih podatkov s Splošno uredbo in ne posega v naloge in pristojnosti Informacijskega pooblaščenca za ugotavljanje te skladnosti.

(4) Certifikat se izda upravljavcu ali obdelovalcu za obdobje največ treh let in se pod enakimi pogoji lahko tudi podaljša, če so zahtevani pogoji certifikacijskega mehanizma še naprej izpolnjeni.

(5) Upravljavec ali obdelovalec, ki svoje obdelave osebnih podatkov predloži v mehanizem certifikacije, mora telesu, ki izvaja certifikacijo, zagotoviti dostop do vseh informacij oziroma dostope do svojih dejanj obdelave, ki so potrebne za izvedbo postopka certifikacije.

(6) Informacijski pooblaščenec lahko z odločbo razveljavi certifikat, če ugotovi, da zahteve v zvezi z njim niso bile ali niso več izpolnjene. Zoper odločbo iz prejšnjega stavka pritožba ni dopustna, je pa dopusten upravni spor.

(7) Informacijski pooblaščenec pripravlja in upravlja seznam pravnomočnih certifikacijskih mehanizmov, ki jih je odobril ter ga sproti objavlja na svoji spletni strani.

## **Postopek akreditiranja teles za certificiranje**

### **52. člen**

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

(2) Pred izdajo pooblastila zunanjemu certifikacijskemu telesu Slovenska akreditacija v skladu s prvim odstavkom člena 43 Splošne uredbe o vlogi telesa obvesti Informacijskega pooblaščenca, ki preveri izpolnjevanje dodatnih zahtev v skladu s točko b prvega odstavka in tretjim odstavkom člena 43

Splošne uredbe in o tem izda odločbo. Zoper odločbo iz prejšnjega stavka pritožba ni dopustna, je pa dopusten upravni spor.

(3) Nacionalni akreditacijski organ na lastno pobudo ali na predlog Informacijskega pooblaščenca prekliče pooblastilo za certificiranje zunanjemu certifikacijskemu telesu, če je ugotovljeno, da pogoji za pooblastilo niso ali niso več izpolnjeni, ali, da so bili ukrepi, ki jih je v postopku certifikacije izvedlo pooblaščenno certifikacijsko telo, v neskladju s Splošno uredbo.

## V. DEL

### PRENOS OSEBNIH PODATKOV TRETJIM DRŽAVAM ALI MEDNARODNIM ORGANIZACIJAM TER GLEDE ČEZMEJNE OBDELAVE

#### **Splošna pravila za prenos osebnih podatkov ter za čezmejno obdelavo**

#### **53. člen**

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

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

1. je prenos potreben za namene iz 82. člena tega zakona;
2. se osebni podatki posredujejo upravljavcu v tretji državi ali mednarodni organizaciji, ki je pristojni organ za izpolnitev enega od namenov iz 82. člena tega zakona;
3. je pristojna država članica v primerih, ko se osebni podatki posredujejo iz druge države članice Evropske unije ali tej dajo na razpolago, prenos vnaprej odobrila;
4. je Evropska komisija v skladu s 54. členom tega zakona sprejela sklep o ustreznosti ali, če tak sklep ne obstaja, so bili predloženi oziroma obstajajo ustrezni ukrepi v smislu 55. člena tega zakona ali je, če ne obstaja sklep o ustreznosti v skladu s 54. členom tega zakona in niso predložena ustrezna zagotovila v smislu 55. členom tega zakona, možno v skladu s 56. členom tega zakona uporabiti izjeme za določene primere in
5. je zagotovljeno, da je nadaljnji prenos tretji državi ali drugi mednarodni organizaciji dovoljen le na podlagi predhodne odobritve pristojnega organa, ki je izvedel prvotni prenos podatkov, in ob primernem upoštevanju vseh tehničnih meril, vključno z naravo ali težo kaznivega dejanja ali prekrška, namenom prvotnega prenosa osebnih podatkov in stopnjo varstva osebnih podatkov v tretji državi ali mednarodni organizaciji, ki se ji posredujejo osebni podatki oziroma jih posreduje naprej.

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

## **Prenos podatkov na podlagi sklepa o ustreznosti varstva osebnih podatkov**

### **54. člen**

(1) Prenos osebnih podatkov v tretjo državo ali mednarodno organizacijo je dovoljen, če je Evropska komisija v skladu s tretjim odstavkom člena 36 Direktive na podlagi izvedbenega akta odločila, da zadevna tretja država, njena regija oziroma eden ali več specifičnih sektorjev v tej tretji državi ali zadevna mednarodna organizacija nudi ustrezno stopnjo varstva osebnih podatkov. Za tak prenos podatkov ni potrebna posebna odobritev. Določbe prejšnjega stavka ne posegajo v obveznost pridobitve dovoljenja v skladu s 3. točko prvega odstavka 53. člena tega zakona.

(2) Sklep Evropske komisije, sprejet v skladu s petim odstavkom člena 36 Direktive o preklicu, spremembi ali odložitvi sklepa po tretjem odstavku člena 36 Direktive ne vpliva na prenose osebnih podatkov tretji državi, regiji oziroma enemu ali več specifičnim sektorjem v tretji državi oziroma mednarodni organizaciji v skladu z 55. in 56. členom tega zakona.

## **Prenos podatkov z uveljavljanjem ustreznih ukrepov varstva osebnih podatkov**

### **55. člen**

(1) Če ne obstaja sklep v skladu s prvim odstavkom 54. člena tega zakona, je prenos osebnih podatkov v tretjo državo ali mednarodno organizacijo dopusten, če:

1. so v ustreznem pravnem aktu, ki je pravno obvezujoč, določeni ustrezni ukrepi za varstvo osebnih podatkov ali
2. je upravljavec po oceni vseh okoliščin, ki so pri prenosu pomembne, ugotovil, da dejansko obstajajo ustrezni ukrepi za varstvo osebnih podatkov.

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

(3) Prenose v skladu z 2. točko prvega odstavka je treba dokumentirati, dokumentacijo, ki vključuje datum in čas prenosa, informacije o pristojnemu organu prejemniku, utemeljitev prenosa in prenešene osebne podatke, pa je treba na zahtevo dati na razpolago Informacijskemu pooblaščenču.

## **Izjeme**

### **56. člen**

(1) Če ne obstajata ne sklep o ustreznosti v skladu s 54. členom tega zakona in tudi ne primeren ukrep v skladu s 55. členom tega zakona, je prenos osebnih podatkov tretji državi ali mednarodni organizaciji dopusten le, če je prenos potreben:

1. za zaščito življenjsko pomembnih interesov posameznika;
2. če je to predvideno zaradi varovanja zakonitih interesov posameznikov, na katere se nanašajo osebni podatki;
3. za odvrnitev neposredne in resne nevarnosti za javno varnost države članice Evropske unije ali tretje države;
4. v posameznem primeru za namene, navedene v 82. členu tega zakona, ali

5. v posameznem primeru za uveljavljanje, izvajanje ali obrambo pravnih zahtevkov v povezavi z nameni, navedenimi v 82. členu tega zakona.

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

(3) Za prenose v skladu s prvim odstavkom veljajo določbe tretjega odstavka 55. člena tega zakona.

## VI. DEL

### NADZORNI ORGAN ZA VARSTVO OSEBNIH PODATKOV REPUBLIKE SLOVENIJE

#### 1. poglavje

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

#### **Nadzorni organ za varstvo osebnih podatkov Republike Slovenije**

#### **57. člen**

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

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

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

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

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

#### **Temeljne pristojnosti Informacijskega pooblaščenca**

#### **58. člen**

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

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



(3) Informacijski pooblaščenec je pristojen za izvajanje inšpekcijskih nadzorov nad vsemi obdelavami osebnih podatkov v Republiki Sloveniji, razen glede obdelav, za katere je po določbah Splošne uredbe pristojen nadzorni organ druge države članice Evropske unije.

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

## **Izjeme glede pristojnosti Informacijskega pooblaščenca**

### **59. člen**

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

1. obdelav osebnih podatkov, izvršenih v okviru izvajanja neodvisnega sodniškega odločanja, kot to opredeljuje zakon, ki ureja sodišča,
2. obdelav osebnih podatkov, izvršenih v okviru opravljanja samostojne državnotožilske funkcije odločanja ali delovanja, kot to opredeljuje zakon, ki ureja državno tožilstvo,
3. obdelav osebnih podatkov, izvršenih v okviru odločanja Ustavnega sodišča Republike Slovenije, kot jih opredeljuje zakon, ki ureja ustavno sodišče ali drugi zakoni,
4. obdelav osebnih podatkov, izvršenih v okviru delovanja Varuha človekovih pravic, kot jih opredeljuje zakon, ki ureja varuha človekovih pravic ali drug zakon, ki ureja pristojnosti ali naloge varuha človekovih pravic, razen glede zadev obdelav osebnih podatkov s področja zagovornišva otrok,
5. obdelav osebnih podatkov na področjih predkazenskega postopka ali obveščevalno-varnostne dejavnosti, iz katerih bi bilo lahko razvidno, da v postopku delujejo ali sodelujejo tajni delavci oziroma sodelavci po določbah zakona, ki ureja kazenski postopek, zakona, ki ureja obrambo ali zakona, ki ureja Slovensko obveščevalno-varnostno agencijo oziroma bi bila lahko razkrita identiteta teh posameznikov,
6. obdelav osebnih podatkov na področju zaščiteneh prič po določbah zakona, ki ureja zaščito prič, iz katerih bi bila lahko razkrita identiteta teh posameznikov.

(2) Informacijski pooblaščenec je ne glede na prejšnji odstavek tega člena pristojen za opravljanje inšpekcijskega nadzora zvezi z zadevami sodne uprave, državnotožilske uprave, uprave Ustavnega sodišča Republike Slovenije, uprave Varuha človekovih pravic ter glede izvajanja ukrepov in postopkov s področja varnosti osebnih podatkov ter sledljivosti obdelav in posredovanj osebnih podatkov po sedmem odstavku 38. člena tega zakona vseh državnih organov iz prejšnjega odstavka tega člena.

## **Naloge Informacijskega pooblaščenca glede posvetovanj o uvedbah obdelav osebnih podatkov**

### **60. člen**

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

(2) Organi in nosilci javnih pooblastil iz prejšnjega odstavka so se dolžni pravočasno, v skladu z določbami o rokih iz drugega odstavka člena 36 Splošne uredbe, predhodno posvetovati z

Informacijskim pooblaščenecem po določbah prejšnjega odstavka, kadar je v predlaganem predpisu določena vzpostavitev nove zbirke, njena sprememba ali prenos osebnih podatkov iz obstoječe zbirke. Kadar se vrste obdelav, ki jih ureja predlagani predpis, nanašajo na primere iz 41. člena tega zakona, mora predlagatelj predpisa v okviru posvetovanja Informacijskemu pooblaščenecu predložiti oceno učinka iz sedmega odstavka člena 35 Splošne uredbe.

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

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

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

(6) Drugi upravljavci so se dolžni predhodno posvetovati z Informacijskim pooblaščenecem, s smiselno uporabo določb prvega do četrtega odstavka tega člena, kadar je iz ocene učinka na varstvo osebnih podatkov iz 41. člena tega zakona razvidno, da bi obdelava osebnih podatkov povzročila veliko tveganje za posameznike, na katere se nanašajo osebni podatki, če upravljavec ne bi sprejel ukrepov za ublažitev tveganja.

## **Sodelovanje z drugimi organi**

### **61. člen**

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

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

(3) V okviru delovanja po prejšnjem odstavku so člani ali osebje drugega nadzornega organa dolžni izvajati nadzor tako, da nadzor vodi Informacijski pooblaščenec, če se nadzor izvaja na ozemlju Republike Slovenije ali v okviru pristojnosti Informacijskega pooblaščenca po tem zakonu. Člani ali osebje drugega nadzornega organa krijejo svoje stroške.

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

## **2. poglavje**

### **Inšpekcijski nadzor in javnost delovanja**

#### **Uporaba predpisov, ki urejajo opravljanje inšpekcijskega nadzora**

### **62. člen**

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

## **Obseg inšpekcijskega nadzora**

### **63. člen**

V okviru inšpekcijskega nadzora Informacijski pooblaščenec:

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

## **Neposredno opravljanje inšpekcijskega nadzora**

### **64. člen**

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

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

## **Preiskovalna pooblastila**

### **65. člen**

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

1. pregledovati vsebino zbirk ne glede na njihovo tajnost ali drugo vrsto zaupnosti;
2. pregledovati dokumentacijo, ki se nanaša na obdelavo osebnih podatkov, ne glede na njeno zaupnost ali tajnost, ter na prenos osebnih podatkov v tretjo državo in posredovanje uporabnikom osebnih podatkov iz tretjih držav, ne glede na njeno tajnost ali drugo vrsto zaupnosti;
3. brez predhodne najave in brez navzočnosti zavezanca, njegovega zakonitega zastopnika oziroma pooblaščenca opraviti pregled vsebine in preveriti način delovanja zavezančevih spletnih strani in drugih elektronsko dostopnih storitev;
4. preverjati postopke in ukrepe ter pregledovati dokumentacijo in akte, ki se nanašajo na varnost osebnih podatkov oziroma na njeno izvajanje;
5. pregledovati prostore, v katerih se obdelujejo osebni podatki, računalniško in drugo opremo ter tehnično dokumentacijo;

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

7. opravljati druga preiskovalna pooblastila, določena z zakonom.

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

## **Popravljalna pooblastila in ukrepi nadzornika**

### **66. člen**

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

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

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

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

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

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

(2) Ukrepov iz prejšnjega odstavka ni mogoče odrediti zoper osebo, ki v elektronskem komunikacijskem omrežju opravlja storitev izključnega prenosa podatkov, vključno z začasnim shranjevanjem podatkov in drugimi delovanji v zvezi s podatki, ki so izključno v funkciji opravljanja ali olajšanja prenosa podatkov po omrežjih, če ta oseba sama nima interesa, povezanega z vsebino teh podatkov, in ne gre za osebo, ki lahko sama ali skupaj z omejenim krogom z njo povezanih oseb učinkovito nadzoruje dostop do teh podatkov.

## **Odločitev, da se postopek ne uvede**

### **67. člen**

Nadzornik v primerih, kadar je iz prijave posameznika, na katerega se nanašajo osebni podatki očitno, da glede na podatke iz prijave ni možno sklepati na kršitev varstva osebnih podatkov po Splošni uredbi, tem zakonu ali drugem zakonu oziroma predpisu, ki ureja obdelavo in varstvo osebnih podatkov, s sklepom odloči, da se inšpekcijski postopek ne uvede. Nadzornik v obrazložitvi sklepa navede razloge za neuvedbo postopka.

## **Obveščanje prijavitelja**

### **68. člen**

Nadzornik je dolžan prijavitelja po opravljenem nadzoru in sprejetem zadnjem ukrepu oziroma ustavitvi postopka obvestiti o vseh pomembnejših ugotovitvah in dejanjih v postopku inšpekcijskega nadzora.

## **Pravno sredstvo zoper odločitve Informacijskega pooblaščenca**

### **69. člen**

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

## **Ukrepanje ob zaznavi kaznivih dejanj ali prekrškov**

### **70. člen**

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

(2) Če nadzornik pri izvrševanju svojih pristojnosti ugotovi, da obstaja sum storitve kaznivega dejanja ali prekrška iz pristojnosti drugega prekrškovnega organa, poda kazensko ovadbo v skladu z zakonom, ki ureja kazenski postopek oziroma izvede postopke v skladu z zakonom, ki ureja prekrške.

## **Varovanje tajnosti**

### **71. člen**

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

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

## **Javnost dela in dodatna svetovanja**

### **72. člen**

(1) Informacijski pooblaščenec lahko:

1. izdaja notranje glasilo ter strokovno literaturo;
2. na spletni strani ali na drug primeren način pravočasno objavlja mnenja iz 44. člena tega zakona;
3. na spletni strani oziroma na drug primeren način objavlja odločbe in sklepe Ustavnega sodišča Republike Slovenije o zahtevah ocene ustavnosti, ki jih je vložil Informacijski pooblaščenec ter odločitve Ustavnega sodišča Republike Slovenije o njih;

4. na spletni strani oziroma na drug primeren način objavlja odločbe in sklepe sodišč s splošno pristojnostjo in upravnega sodišča, ki se nanašajo na varstvo osebnih podatkov, tako da iz njih ni možno razbrati osebnih podatkov strank, oškodovancev, prič ali izvedencev z uporabo psevdonimizacije;
5. daje mnenja o skladnosti kodeksov poklicne etike, splošnih pogojev poslovanja oziroma njihovih predlogov s predpisi s področja varstva osebnih podatkov;
6. daje neobvezna mnenja, pojasnila in stališča o vprašanih s področja varstva osebnih podatkov in jih objavlja na spletni strani ali na drug primeren način;
7. pripravlja in daje neobvezne smernice in priporočila glede varstva osebnih podatkov na posameznem področju;
8. po potrebi daje izjave za javnost o izvedbi posamičnih zadev po tem zakonu;
9. izvaja konference za medije v zvezi z delom Informacijskega pooblaščenca ter prepise izjav ali posnetke izjav s konferenc za medije objavi na spletni strani;
10. obdeluje kontaktne podatke za izvajanje izobraževanj, posvetovanj, javnih dogodkov;
11. na spletni strani objavlja druga pomembna obvestila.

(2) Informacijski pooblaščenec lahko za opravljanje pristojnosti iz 5., 6., in 7. točke prejšnjega odstavka pozove k sodelovanju tudi predstavnike društev in drugih nevladnih organizacij s področja varstva osebnih podatkov, zasebnosti ter potrošnikov.

### **3. poglavje**

#### **Zunanji nadzor delovanja Informacijskega pooblaščenca in sodelovanje**

##### **Letno poročilo Informacijskega pooblaščenca**

###### **73. člen**

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

(2) Poročilo iz prejšnjega odstavka se posreduje tudi Evropski komisiji, Odboru ter je dostopno javnosti.

##### **Pristojnosti Varuha človekovih pravic**

###### **74. člen**

(1) Varuhinja oziroma 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, ki ureja varuha človekovih pravic.

(2) Varstvo osebnih podatkov je posebno delovno področje varuha, za katerega je zadolžen eden od namestnikov varuha.

## **Pristojnosti Državnega zbora Republike Slovenije**

### **75. člen**

(1) Stanje na področju varstva osebnih podatkov in izvrševanje določb tega zakona, v skladu s 73. členom tega zakona, spremlja pristojno delovno telo državnega zbora.

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

## **VII. DEL**

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

#### **Obdelava osebnih podatkov v znanstvene raziskovalne, zgodovinske raziskovalne in statistične namene**

### **76. člen**

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

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

(2) Registrirane znanstveno-raziskovalne organizacije in registrirani raziskovalci po zakonu, ki ureja raziskovalno in razvojno dejavnost, lahko za namen obdelave iz prejšnjega odstavka pri upravljavcu osebnih podatkov vpogledajo oziroma pridobijo posebne vrste osebnih podatkov ali druge osebne podatke praviloma v psevdonimizirani obliki, če predložijo predstavitveni elaborat raziskave, s katerim izkažejo:

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

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

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

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

Elaboratu mora biti priložena ocena učinkov v zvezi z varstvom osebnih podatkov, kot je opredeljena v 35. členu tega zakona.

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

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

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

### **Obdelava naslovov za kontaktiranje posameznikov v znanstvene raziskovalne, zgodovinske raziskovalne in statistične namene**

#### **77. člen**

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

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

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



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

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

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

## **Obdelava podatkov za namene arhiviranja v javnem interesu**

### **78. člen**

(1) Obdelava osebnih podatkov za namene arhivskega delovanja je dovoljena, če je v javnem interesu, v skladu 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.

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

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

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

## **VIII. DEL**

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

#### **Varstvo svobode izražanja v razmerju do pravice do varstva osebnih podatkov**

### **79. člen**

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

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

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

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

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

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

### **Varstvo pravice do dostopa do informacij javnega značaja v razmerju do pravice do varstva osebnih podatkov**

#### **80. člen**

(1) Zavezanci po zakonu, ki ureja dostop do informacij javnega značaja, javnosti posredujejo osebne podatke, če so ti po zakonu javni ali če je za njihovo razkritje podan prevladujoč javni interes po določbah zakona, ki ureja dostop do informacij javnega značaja, zakona, ki ureja medije ali drugega zakona.

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

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

## **Izjema glede obveščanja posameznika**

### **81. člen**

Če so osebni podatki javni na podlagi zakona, posameznika ni treba obveščati po členu 13. ali 14. Splošne uredbe, 15. do 17. členu tega zakona in po določbah zakona, ki ureja splošni upravni postopek.

## IX. DEL

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

## 1. poglavje

### Splošne določbe

#### Področje uporabe tega dela zakona

#### 82. člen

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

(2) Če ta del zakona ne določa drugače, veljajo za konkretne vrste osebnih podatkov, konkretne zbirke, obdelave osebnih podatkov ter njihova posredovanja, prenose in čezmejne obdelave določbe zakonov, ki urejajo naloge in pooblastila policije, kazenski postopek, državno tožilstvo, sodišča, sodniško službo, obrambo, obveščevalno-varnostno dejavnost ter izvrševanje kazenskih sankcij.

#### Temeljna načela obdelave podatkov

#### 83. člen

Osebni podatki:

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

## Razvrščanje osebnih podatkov po vrstah ter kakovost osebnih podatkov

### 84. člen

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

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

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

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

(4) Pri vsakem posredovanju, čezmejni obdelavi ali prenosu osebnih podatkov jim je treba po možnosti priložiti informacije, na podlagi katerih lahko prejemnik oceni oceno aktualnost, pravilnost, popolnost in zanesljivost.

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

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

## **Zakonitost obdelave osebnih podatkov**

### **85. člen**

Obdelava osebnih podatkov po tem delu zakona je zakonita le, če je določena z zakonom, ali če je potrebna zaradi varstva življenja ali telesa posameznika ter je potrebna in sorazmerna za izpolnitev določenih nalog, ki jih pristojni organ izvaja v skladu z nameni iz 82. člena tega zakona.

## **Posebne določbe o obdelavi osebnih podatkov za druge namene in prenos osebnih podatkov**

### **86. člen**

(1) Obdelava osebnih podatkov po določbah tega dela zakona s strani istega ali drugega upravljavca in za drug namen obdelave od tistega, za katerega so bili podatki pridobljeni, je dovoljena le, če ta drug namen spada na področje iz 82. člena ter izpolnjuje pogoje iz 84. in 85. člena tega zakona.

(2) Prenos, posredovanje ali čezmejna obdelava osebnih podatkov, obdelanih skladno z določbami tega glavnega dela, za namen, ki ni naveden v 82. členu tega zakona, so dovoljeni le, če je to izrecno določeno v zakonski podlagi ter je prejemnik po svojih predpisih pooblaščen za obdelavo teh osebnih podatkov za ta drug namen.

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

## **Avtomatizirano odločanje v posameznem primeru**

### **87. člen**

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

(2) Odločitve iz prvega odstavka lahko v skladu z 82. členom tega zakona izjemoma temeljijo na posebnih vrstah osebnih podatkov samo, če so bili sprejeti posebni ustrezni ukrepi za varstvo človekovih pravic in temeljnih svoboščin ter upravičenih interesov posameznika, na katerega se nanašajo osebni podatki. Odločitve po prejšnjem stavku, ki bi lahko vodile do diskriminacije posameznika, na katerega se nanašajo osebni podatki, ali njemu bližnjih oseb, so prepovedane.

## **2. poglavje**

### **Pravice posameznika, na katerega se nanašajo osebni podatki**

## **Splošna pravila**

### **88. člen**

(1) Upravljavec mora posamezniku, na katerega se nanašajo osebni podatki, posredovati informacije in sporočila, v skladu s 89. do 91. členom tega zakona, ki se nanašajo na obdelavo osebnih podatkov, podajati v čim bolj točni, razumljivi in lahko dostopni obliki ter v jasnem in preprostem jeziku, če to posameznik zahteva. Informacije in sporočila se posredujejo v posamezniku ustrezni obliki.

(2) Upravljavec mora posamezniku, na katerega se nanašajo osebni podatki, olajšati uveljavljanje njegovih pravic iz 89. do 91. člena tega zakona.

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

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

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

(6) Informacije iz 89. člena ter vsa sporočila in ukrepi v skladu s 90. in 91. členom tega zakona se zagotovijo brezplačno. Pri očitno neutemeljenih ali pretiranih zahtevah posameznika, na katerega se podatki nanašajo, zlasti če se zahteve pogosto ponavljajo, lahko upravljavec s posebno obrazložitvijo odkloni ukrepanje na podlagi zahtevka. Obrazložitev iz prejšnjega stavka mora vsebovati vsaj povzetek razlogov glede očitne neutemeljenosti ali pretirano narave zahtevka.

(7) Upravljavec lahko zaradi potrditve identitete posameznika, na katerega se nanašajo osebni podatki, ki je v skladu z 90. ali 91. členom tega zakona vložil zahtevek, zahteva dodatne potrebne informacije od posameznika, kar vključuje glede na konkretne okoliščine poleg osebnega imena tudi navedbo datuma rojstva oziroma navedbo enotne matične številke občana, zahtevek pa mora biti podpisan lastnoročno ali v elektronski obliki z ustreznim digitalnim potrdilom.

(8) V primerih iz četrtega odstavka 89. člena, tretjega odstavka 90. člena in četrtega odstavka 91. člena tega zakona ima posameznik, na katerega se podatki nanašajo, pravico, da zahteva preverjanje zakonitosti zadevne omejitve njegovih pravic s strani Informacijskega pooblaščenca. Upravljavec mora posameznika, na katerega se nanašajo osebni podatki, izrecno poučiti o tej pravici.

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

## **Dajanje informacij posamezniku, na katerega se nanašajo osebni podatki**

### **89. člen**

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

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

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

1. pravno podlago obdelave;
2. rok hrambe osebnih podatkov ali, če to izjemoma ni možno, merila za določitev tega roka v skladu z 41. členom tega zakona;
3. po potrebi navesti kategorije prejemnikov osebnih podatkov, tudi prejemnikov v tretjih državah in mednarodnih organizacijah;
4. po potrebi druge informacije, zlasti če so bili osebni podatki pridobljeni brez vednosti posameznika, na katerega se nanašajo.

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

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

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

### **Pravica posameznika, na katerega se nanašajo osebni podatki, do pridobitve teh podatkov**

#### **90. člen**

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

1. namenov obdelave in njihovi pravni podlagi;
2. vrstah osebnih podatkov, ki se obdelujejo;



3. prejemnikih ali kategorijah prejemnikov, ki so jim bili podatki razkriti, zlasti če gre za prejemnike v tretjih državah ali mednarodnih organizacijah;
4. če je mogoče, predvideni roku hrambe osebnih podatkov ali, če to izjemoma ni možno, merilih za določitev tega roka v skladu z 41. členom tega zakona;
5. obstoju pravice, da upravljavec popravi ali izbriše podatke ali omeji obdelavo osebnih podatkov posameznika, na katerega se podatki nanašajo;
6. obstoju pravice do vložitve prijave pri Informacijskem pooblaščenču in njegovih kontaktnih podatkih;
7. sporočilih o osebnih podatkih, ki so predmet obdelave, in vseh razpoložljivih informacijah o viru osebnih podatkov, razen njegove konkretne identifikacije, če je identiteta vira varovana kot tajna ali zaupna po določbah drugega zakona.

(2) Za informacije iz prvega odstavka veljajo roki po določbah člena 12 Splošne uredbe. Omejitve pravice do pridobitve informacij so dovoljene le pod pogoji, navedenimi v četrtem odstavku 66. člena tega zakona.

(3) V primeru neizdaje informacij v skladu z drugim odstavkom mora upravljavec posameznika, na katerega se nanašajo podatki, nemudoma pisno obvestiti o zavrnitvi ali omejitvi informacij in razlogih, na katerih to temelji. Ta določba se ne uporablja, če je zagotovitev teh informacij v nasprotju z enim od namenov iz četrtega odstavka 89. člena tega zakona. Upravljavec mora posameznika, na katerega se nanašajo podatki, obvestiti o možnosti vložitve pritožbe na organ za varstvo podatkov.

(4) Upravljavec mora dokumentirati razloge za odločitev o neizdaji informacij v skladu z drugim odstavkom. Ti podatki morajo biti dostopni Informacijskemu pooblaščenču in pooblaščenim osebam.

(5) V obsegu, v katerem ima posameznik, na katerega se nanašajo osebni podatki, v drugem zakonu določeno zakonsko pravico do vpogleda v njegove osebne podatke, ki se obdelujejo, ima pravico pridobiti informacije v skladu z določbami drugega zakona, ki urejajo pravico do vpogleda.

## **Pravica do popravka ali izbrisa osebnih podatkov in do omejitve obdelave**

### **91. člen**

(1) Vsak posameznik, na katerega se nanašajo osebni podatki, ima pravico, da od upravljavca zahteva takojšnji popravek svojih netočnih osebnih podatkov in dopolnitev nepopolnih ali neposodobljenih osebnih podatkov. Popravek ali dopolnitev se lahko po potrebi izvede z dodatno priloženo izjavo ali zaznamkom, če je naknadna sprememba nezdržljiva z namenom dokumentiranja glede na fazo določenega postopka. Upravljavec je dolžan dokazati točnost ali posodobljenost osebnih podatkov, če osebni podatki niso bili pridobljeni izključno na podlagi navedb posameznika, na katerega se podatki nanašajo.

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

1. osebni podatki niso več potrebni za namene, za katere so bili pridobljeni ali drugače obdelani;
2. so bili osebni podatki obdelani nezakonito ali
3. je izbris osebnih podatkov potreben zaradi izpolnitve druge obveznosti po zakonu ali po pravnomočni sodni odločbi.

(3) Namesto izbrisa osebnih podatkov lahko upravljavec njihovo obdelavo omeji, če:

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

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

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

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

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

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

## X. DEL

### PODROČNE UREDITVE OBDELAV OSEBNIH PODATKOV

#### 1. poglavje

#### Neposredno trženje

#### Pravice in dolžnosti upravljavca na področju neposrednega trženja

##### 92. člen

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

(2) Za namene izvajanja neposrednega trženja lahko upravljavec uporablja le naslednje osebne podatke, ki jih je zbral v skladu s prejšnjim odstavkom: osebno ime, naslov stalnega ali začasnega prebivališča, telefonsko številko, naslov elektronske pošte ter številko telefaksa. Na podlagi privolitve posameznika lahko upravljavec obdeluje tudi druge osebne podatke, posebne vrste osebnih podatkov pa le, če ima za to privolitev posameznika, ki je izrecna in praviloma pisna.

(3) Upravljavec mora neposredno trženje izvajati tako, da posameznika ob izvajanju neposrednega trženja jasno in ločeno od katerihkoli drugih informacij obvesti o njegovih pravicah iz 15. in 16. člena tega zakona.

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

#### Pravica posameznika glede prenehanja obdelave osebnih podatkov s področja neposrednega trženja

## **93. člen**

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

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

## **2. poglavje**

### **Videonadzor**

#### **Splošne določbe o videonadzoru in varstvu osebnih podatkov**

## **94. člen**

(1) Če z zakonom ni drugače določeno, se določbe tega poglavja uporablja za vse vrste videonadzora, in tudi v primerih, ko se z videonadzorom zgolj spremlja neposredno dogajanje pred kamerami.

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

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

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

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

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

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

(7) Posnetki videonadzora se lahko hranijo največ 3 mesece od trenutka nastanka posnetka, če zakon ne določa drugače.

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

## **Uporaba videonadzora glede dostopa v uradne službene oziroma poslovne prostore**

### **95. člen**

- (1) Javni in zasebni sektor lahko izvajata videonadzor dostopa v njihove uradne službene oziroma poslovne prostore, če je to potrebno za varnost ljudi ali premoženja, zaradi zagotavljanja nadzora vstopa ali izstopa v ali iz službenih oziroma poslovnih prostorov ali če zaradi narave dela obstaja možnost ogrožanja zaposlenih.
- (2) Videonadzor se lahko izvaja le na takšen način, da se ne izvaja niti snemanje notranjosti stanovanjskih stavb, ki nimajo vpliva na dostop do njihovih prostorov, niti snemanje vhodov v stanovanja.
- (3) O izvajanju videonadzora je potrebno pisno obvestiti vse zaposlene v osebi javnega ali zasebnega sektorja, ki opravljajo delo v nadzorovanem prostoru.
- (4) Zbirka osebnih podatkov po tem členu vsebuje posnetek posameznika (slika oziroma glas), datum in čas vstopa in izstopa iz prostora, lahko pa tudi osebno ime posnetega posameznika, naslov njegovega stalnega ali začasnega prebivališča, zaposlitev, številko in podatke o vrsti njegovega osebnega dokumenta ter razlogu vstopa, če se navedeni osebni podatki zbirajo poleg ali s posnetkom videonadzornega sistema.

## **Videonadzor in večstanovanjske stavbe**

### **96. člen**

- (1) Videonadzor v večstanovanjskih stavbah je dovoljen samo, če za to obstaja privolitev lastnikov, ki imajo v lasti več kot 70 odstotkov solastniških deležev na skupnih delih.
- (2) Videonadzor se lahko v večstanovanjski stavbi uvede le, kadar je to potrebno za varnost ljudi in premoženja.
- (3) Privolitev iz prvega odstavka mora biti pisna, pri čemer je treba na listini izrecno navesti, kateri lastniki so podali privolitev k uvedbi videonadzora.
- (4) Upravljavec po tem členu je upravnik večstanovanjske stavbe. Če večstanovanjska stavba nima upravnika, je upravljavec oseba, ki jo izmed sebe pisno določijo lastniki, ki so podali privolitev za uvedbo videonadzora in se ta oseba s tem pisno strinja.
- (5) Če upravljavec oziroma oseba iz prejšnjega odstavka ni določen, se šteje, da je upravljavec videonadzora v večstanovanjski stavbi skupnost lastnikov, ki so privolili v izvajanje videonadzora. Pravice in obveznosti, ki izvirajo iz uvedbe videonadzora in prekrškovno odgovornost nosijo samo tisti lastniki, ki so se strinjali z uvedbo videonadzora.
- (6) Prepovedano je omogočiti ali izvajati sprotno ali naknadno pregledovanje dogajanja v območju izvajanja videonadzora preko interne kableske televizije, javne kableske televizije, svetovnega spleta ali s pomočjo drugega elektronskega komunikacijskega sredstva, ki lahko prenaša te posnetke.
- (7) Prepovedano je z videonadzornim sistemom snemati vhode v posamezna stanovanja. Prepovedano je izvajati videonadzor nad hišniškim stanovanjem ter delavnico za hišnika.
- (8) Izjemoma je dovoljeno omogočiti združitev videonadzornega sistema z napravami, ki jih uporabljajo lastniki za potrebe vstopa v večstanovanjsko stavbo, kot sta na primer domofon ali video domofon, razen če te naprave omogočajo snemanje ali spremljanje dogajanja v območju izvajanja videonadzora na posamezni napravi. Spremljanje dogajanja v območju izvajanja videonadzora mora onemogočiti upravljavec videonadzora.

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

## **Delovni prostori**

### **97. člen**

(1) Izvajanje videonadzora znotraj delovnih prostorov se lahko izvaja le v izjemnih primerih, kadar je to nujno potrebno za varnost ljudi ali premoženja ali za varovanje tajnih podatkov ter poslovne skrivnosti, tega namena pa ni možno doseči z milejšimi sredstvi.

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

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

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

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

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

## **Videonadzor na javnih površinah**

### **98. člen**

(1) Videonadzor na javnih površinah je dovoljen le v izjemnih primerih, kadar je to nujno potrebno, ker obstaja resna in utemeljena nevarnost za življenje ali zdravje ljudi, varnost premoženja ali varovanje tajnih podatkov in tega namena ni mogoče doseči z milejšimi sredstvi, ali za potrebe varovanja prostorov, zgradb ali območij, ki jih je potrebno varovati na podlagi zakona in sicer samo v obsegu in trajanju, ki je za dosego teh namenov nujno potreben.

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

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

## **3. poglavje**

### **Obdelava osebnih podatkov z uporabo biometrije**

#### **Biometrični ukrepi v javnem sektorju**

### **99. člen**

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

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

## **Biometrični ukrepi v zasebnem sektorju**

### **100. člen**

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

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

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

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

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

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

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

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

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

## **4. poglavje**

### **Evidentiranje vstopov in izstopov**

#### **Evidentiranje vstopov in izstopov iz službenih prostorov**

### **101. člen**

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

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

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

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

## **5. poglavje**

### **Javne knjige in varstvo osebnih podatkov**

#### **Zakoniti namen javne knjige**

##### **102. člen**

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

## **6. poglavje**

### **Povezovanje zbirk osebnih podatkov**

#### **Povezovanje uradnih evidenc in javnih knjig**

##### **103. člen**

(1) Uradne evidences in javne knjige se lahko povezujejo med seboj ali z drugimi zbirkami le, če tako določa zakon, 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.

(2) Upravljavci ali upravljavec, ki povezuje dve ali več zbirk iz določb prejšnjega odstavka, so dolžni o tem predhodno pisno obvestiti Informacijskega pooblaščenca.

(3) Če vsaj ena zbirka, ki naj bi se jo povežalo, vsebuje osebne podatke iz 17. ali 18. člena tega zakona, ali če bi povezovanje imelo za posledico njihovo razkritje ali je za izvedbo povezovanja potrebna uporaba povezovalnega znaka, povezovanje ni dovoljeno brez predhodnega dovoljenja Informacijskega pooblaščenca.

(4) Informacijski pooblaščenec dovoli povezavo iz prejšnjega odstavka na podlagi pisne vloge upravljavca, če ugotovi, da upravljavci zagotavljajo ustrezno varnost osebnih podatkov.

(5) Zoper odločbo iz prejšnjega odstavka ni pritožbe, dovoljen pa je upravni spor.

## **7. poglavje**

### **Strokovni nadzor**

#### **Uporaba določb tega poglavja**

##### **104. člen**

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

#### **Splošne določbe**

##### **105. člen**

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

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

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

#### **Strokovni nadzor in dodatna obdelava osebnih podatkov**

##### **106. člen**

(1) Izvajalec strokovnega nadzora lahko pri opravljanju strokovnega nadzora, pri katerem v skladu s prvim odstavkom 105. člena tega zakona obdeluje osebne podatke, pisno obvesti posameznika, na katerega se nanašajo osebni podatki, da izvaja strokovni nadzor in ga obvesti, da lahko pisno ali ustno poda svoja stališča.

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

#### **Strokovni nadzor in posebne vrste osebnih podatkov**

##### **107. člen**



Če se pri izvajanju strokovnega nadzora obdelujejo podatki iz 17. ali 18. člena tega zakona, izvajalec strokovnega nadzora o tem naredi uradni zaznamek ali drug uradni zapis v spisu zadeve upravljavca osebnih podatkov.

## XI. DEL KAZENSKE DOLOČBE

### **Uporaba določb Splošne uredbe glede upravnih kazni in glob ter odločanje o prekrških po tem delu zakona**

#### **108. člen**

(1) V skladu s prvim odstavkom 70. člena tega zakona Informacijski pooblaščenec odloča o predpisanih kršitvah in upravnih globah iz člena 83 Splošne uredbe kot o prekrških v okviru pristojnosti prekrškovnega organa po določbah zakona, ki ureja prekrške, kolikor ta zakon ne določa drugače.

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

(3) Višine in razponi upravnih glob, ki so za pravne osebe, samostojne podjetnike posameznike in posameznike, ki samostojno opravljajo dejavnost, za kršitve, predpisane v členu 83 Splošne uredbe, določene v 109. in 110. členu tega zakona, se uporabljajo ne glede na določbe o razponih glob iz zakona, ki ureja prekrške.

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

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

### **Kršitve iz četrtega odstavka člena 83 Splošne uredbe**

#### **109. člen**

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

1. če krši obveznosti upravljavca in obdelovalca v skladu s členi 8, 11, 25 do 39 ter 42 in 43 Splošne uredbe;
2. če krši obveznosti organa za potrjevanje v skladu s členoma 42 in 43 Splošne uredbe;

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

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

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

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

### **Kršitve iz petega odstavka člena 83 Splošne uredbe**

#### **110. člen**

(1) Z globo od 4.000 do 20.000.000 eurov ali v primeru gospodarske družbe v znesku 4 % skupnega svetovnega letnega prometa v preteklem proračunskem letu, odvisno, kateri je višji, se kaznuje za prekršek pravna oseba, samostojni podjetnik posameznik ali posameznik, ki samostojno opravlja dejavnost:

1. če krši temeljna načela za obdelavo, vključno s pogoji za privolitev, v skladu s členi 5, 6, 7 in 9 Splošne uredbe;

2. če krši pravice posameznika, na katerega se nanašajo podatki, v skladu s členi 12 do 22 Splošne uredbe;

3. če krši določbe v zvezi s prenosi osebnih podatkov uporabniku v tretji državi ali mednarodni organizaciji, v skladu s členi 44 do 49 Splošne uredbe;

4. če ne upošteva odredbe ali začasne ali dokončne omejitve obdelave ali prekinitve prenosa podatkov, ki jo izda Informacijski pooblaščenec v skladu z drugim odstavkom člena 58 Splošne uredbe, ali če ne zagotovi dostopa, s čimer se krši prvi odstavek člena 58 Splošne uredbe.

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

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

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

### **Kršitev določb o neposrednem trženju**

#### **111. člen**

(1) Z globo od 2.000 do 4.000 eurov se kaznuje za prekršek pravna oseba, samostojni podjetnik posameznik ali posameznik, ki samostojno opravlja dejavnost, če v skladu s tem zakonom obdeluje osebne podatke za namene neposrednega trženja in ne ravna v skladu z 92. ali 93. členom tega zakona.

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

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

### **Kršitev splošnih določb o videonadzoru**

#### **111. člen**

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

1. če ne objavi obvestila na način iz tretjega odstavka 94. člena tega zakona;
2. če obvestilo ne vsebuje informacij iz četrtega odstavka 94. člena tega zakona;
3. če ne zavaruje videonadzornega sistema, s katerim se izvaja videonadzor, v nasprotju s šestim odstavkom 94. člena tega zakona.

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

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

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

(5) Z globo od 5.000 do 15.000 eurov se kaznuje za prekršek pravna oseba, samostojni podjetnik posameznik ali posameznik, ki samostojno opravlja dejavnost, če izvaja nedovoljeni videonadzor v nasprotju s sedmim ali osmim odstavkom 80. člena tega zakona.

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

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

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

### **Kršitev določb o videonadzoru glede dostopa v uradne službene oziroma poslovne prostore**

#### **112. člen**

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

1. če izvaja videonadzor brez pravne podlage iz prvega odstavka 95. člena tega zakona;

2. če izvaja videonadzor tako, da izvaja snemanje notranjosti stanovanjskih stavb, ki nimajo vpliva na dostop do njihovih prostorov ali posnetke vhodov v stanovanja (drugi odstavek 81. člena tega zakona);

3. če pisno ne obvesti zaposlenih (tretji odstavek 95. člena tega zakona).

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

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

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

### **Kršitev določb o videonadzoru pri večstanovanjskih stavbah**

#### **113. člen**

(1) Z globo od 2.000 do 8.000 eurov se kaznuje za prekršek pravna oseba, samostojni podjetnik posameznik ali posameznik, ki samostojno opravlja dejavnost, ki izvaja videonadzor v nasprotju s 96. členom tega zakona.

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

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

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

### **Kršitev določb o videonadzoru v delovnih prostorih**

#### **114. člen**

(1) Z globo od 4.000 do 12.000 eurov se kaznuje za prekršek pravna oseba, samostojni podjetnik posameznik ali posameznik, ki samostojno opravlja dejavnost, ki izvaja videonadzor v delovnih prostorih v nasprotju s 97. členom tega zakona.

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

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

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

### **Kršitev določb o videonadzoru na javnih površinah**

#### **115. člen**

(1) Z globo od 4.000 do 12.000 eurov se kaznuje za prekršek pravna oseba, samostojni podjetnik posameznik ali posameznik, ki samostojno opravlja dejavnost, ki izvaja videonadzor na javnih površinah v nasprotju z 98. členom tega zakona.

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

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

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

### **Kršitev določb o biometriji v javnem sektorju**

#### **116. člen**

(1) Z globo od 4.000 do 12.000 eurov se kaznuje za prekršek pravna oseba javnega sektorja, ki izvaja biometrijske ukrepe v nasprotju z 99. členom tega zakona.

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

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

### **Kršitev določb o biometriji v zasebnem sektorju**

#### **117. člen**

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

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

### **Kršitev določb o evidentiranju vstopov in izstopov**

#### **118. člen**

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

1. ki uporablja evidenco vstopov in izstopov kot uradno evidenco v nasprotju s tretjim odstavkom 101. člena tega zakona;
2. ki ravna v nasprotju s četrtim odstavkom 101. člena tega zakona.

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

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

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

### **Kršitev določb o javnih knjigah**

#### **119. člen**

(1) Z globo od 2.000 do 4.000 eurov se kaznuje za prekršek pravna oseba, samostojni podjetnik posameznik ali posameznik, ki samostojno opravlja dejavnost, ki uporablja osebne podatke v nasprotju z zakonskim namenom iz 102. člena tega zakona.

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

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

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

#### **120. člen**

### **Kršitev določb o povezovanju uradnih evidenc in javnih knjig**

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

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

#### **121. člen**

### **Kršitev določb o strokovnem nadzoru**

(1) Z globo od 4.000 do 8.000 eurov se kaznuje za prekršek pravna oseba:

1. če izvaja strokovni nadzor v nasprotju z drugim odstavkom 105. člena tega zakona;
2. če ne napravi uradnega zaznamka ali drugega uradnega zapisa v nasprotju s 107. členom tega zakona.

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

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

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

## **XII. DEL**

### **PREHODNE IN KONČNE DOLOČBE**

#### **Prehodne določbe**

##### **122. člen**

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

(2) Upravljavci in obdelovalci so dolžni v roku enega leta od začetka uporabe tega zakona izvesti ustrezne ukrepe prilagoditve glede uporabe privolitve kot pravne podlage za obdelavo osebnih podatkov. Za obdobje iz prejšnjega stavka se šteje, da če obdelovalec in upravljavec izvajata ustrezne ukrepe prilagoditve in je bila dosedanja privolitve v skladu z dosedanjimi pravili iz Zakona o varstvu osebnih podatkov (Uradni list RS, št. 94/07 – uradno prečiščeno besedilo), da izvajata ustrezne popravljalne ukrepe, ki za obdobje iz prvega stavka preprečujejo nastanek kaznivosti za prekršek.

(3) V Zakonu o spremembah in dopolnitvah Zakona o izvrševanju kazenskih sankcij – ZIKS-1F (Uradni list RS, št. 54/15) se z dnem uporabe tega zakona črta 88. člen.

(4) Postopki odločanja ali obdelave osebnih podatkov, ki so se pred začetkom uporabe tega zakona začeli pri Informacijskem pooblaščenca, na sodiščih in drugih državnih organih ter pri upravljavcih osebnih podatkov in pogodbenih obdelovalcih, se nadaljujejo in končajo po določbah Zakona o varstvu osebnih podatkov (Uradni list RS, št. 94/07 – uradno prečiščeno besedilo), najpozneje do roka enega leta od začetka uporabe tega zakona.

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

(6) Skladno z osmim odstavkom 18. člena tega zakona so upravljavci ali obdelovalci, ki za izvajanje svojega delovanja pridobivajo osebne podatke iz registrov ali evidenc s področja upravnih notranjih zadev, dolžni v roku dveh let po začetku uporabe tega zakona vzpostaviti ustrezne varnostne mehanizme po predhodnem soglasju ministrstva, pristojnega za notranje zadeve.

#### **Končna določba**

##### **123. člen**

Ta zakon začne veljati naslednji dan po objavi v Uradnem listu Republike Slovenije, uporabljati pa se začne 25. maja 2018.

## V. Obrazložitev členov

Besedilo Predloga ZVOP-2 še ne upošteva sprememb (popravkov) v besedilu določb slovenskih in različnih Splošne uredbe in Direktive, ker le-te še niso objavljene v Uradnem listu Evropske unije ter tako tudi še niso mogle biti upoštevane v obrazložitvi členov. Kot je že navedeno v uvodni obrazložitvi, utegne biti vpliv na določbe Predloga ZVOP-2 še nekoliko širši, saj utegneta biti delno spremenjeni tudi različni besedil Splošne uredbe in Direktive v angleški jezikovni različici (objava v Uradnem listu Evropske unije predvidoma marca 2018).

### 1. K I. delu Predloga ZVOP-2:

#### K 1. členu:

1. člen v prvem odstavku določa bistvo človekove pravice do varstva osebnih podatkov. Pravico oziroma skupek pravic iz varstva osebnih podatkov iz 38. člena Ustave Republike Slovenije določa kot osebno človekovo pravico posameznika ali posameznice do varstva njegovih ali njenih osebnih podatkov. Pri tem izhaja iz ti. »subjektivnega pristopa« in ne iz pristopa regulacije (zakonske ozir. upravne obveznosti), v središču te ene od najbolj bistvenih pravic je človek. To izhaja tudi iz zadnjega dela določbe, po kateri se posameznicam in posameznikom zagotavljajo zasebnost (38. in 35. člen Ustave Republike Slovenije) oziroma (torej: in/ali) dostojanstvo (34. člen Ustave Republike Slovenije) ter podatkovna samoodločba (38. člen Ustave Republike Slovenije).

V drugem odstavku je določeno, da se v okviru osebne človekove pravice po prvem odstavku zagotavlja, da ima vsaka posameznica ali posameznik upravičenje, da se z zakonom ter pošteno in na pregleden način ureja in zagotavlja obdelava njenih ali njegovih osebnih podatkov, tajnost njenih ali njegovih osebnih podatkov, ter njene ali njegove pravice do seznanitve z lastnimi osebnimi podatki, do popravka lastnih podatkov oziroma do uresničevanja drugih pravic iz tega ali drugega zakona. Glede dela določbe o tajnosti osebnih podatkov določba izhaja iz drugega odstavka 38. člena Ustave Republike Slovenije, po katerem »varstvo tajnosti (!) osebnih podatkov določa zakon«.

Predlagani 1. člen predloga zakona je tudi primerljiv določbi 1. člena Zakona o varstvu osebnih podatkov Republike Avstrije, kot je bil spremenjen z Zveznim zakonom, s katerim se spreminja Zakon o varstvu osebnih podatkov iz leta 2000 (Zakon o prilagoditvi varstva osebnih podatkov 2018)<sup>31</sup>, kjer ni prišlo do posega v 1. člen veljavnega zakona, ki temeljno ureja človekovo pravico od varstva osebnih podatkov – zaradi neobstoja dvotretjinske ustavne večine za revizijo, kar pomeni, da tudi Avstrija zadrži dosedanjo širšo opredelitev varstva osebnih podatkov kot temeljne človekove pravice (na ustavni ravni).

1. člen ima pomen za razlago vseh določb tega predloga zakona, področne zakonodaje glede varstva osebnih podatkov ter za uporabo določb Splošne uredbe, tako da mora osredotočeni naslovniki pravic biti posameznik, na katerega se nanašajo osebni podatki (subjekt varstva pravice do tajnosti osebnih podatkov).

Glede na dosedanji 1. člen ZVOP-1 novi 1. člen ZVOP-2 torej vsebuje posodobljene formulacije, s posebnim pomenom za interpretacijo ZVOP-2, kot je opisan zgoraj.

#### K 2. členu:

---

<sup>31</sup> Objava: Bundesgesetzblatt I Nr. 120/2017, Teil I.



Predlagani 2. člen ureja prepoved diskriminacije glede varstva osebnih podatkov. Pri tem je pomembna povezava s 1. členom, da gre za osebno človekovo pravico, da je osredotočeni naslovnik pravic posameznik, na katerega se nanašajo osebni podatki ter glede razlagalne »moči« glede drugih zakonov ipd.. V 2. členu so glede na 14. člen Ustave Republike Slovenije ter glede na druge ustaljene formulacije pravnega reda Republike Slovenije (npr. prvi odstavek 131. člena Kazenskega zakonika<sup>32</sup> ter prvi odstavek 1. člena Zakona o varstvu pred diskriminacijo<sup>33</sup>) navedene prepovedane okoliščine diskriminacije. Določbe so nekoliko posodobljene – dodana spolna identiteta po prvem odstavku 1. člena Zakona o varstvu pred diskriminacijo, dodana genska (ne genetska) predispozicija, beseda »barva« iz dosedanjega 4. člena ZVOP-1 je spremenjena v »barvo kože«.

Predlagani člen pomeni, da se nikogar ne sme diskriminirati glede varstva osebnih podatkov, kar med drugim vključuje tudi prebivališče (vpliv glede 4. člena predloga zakona – ozemeljska veljavnost). Natančneje – med prepovedanimi kriteriji diskriminacije (razlikovanja) sta zlasti pomembna kriterija državljanstva in prebivališča, glede na 1. člen Konvencije o varstvu posameznikov glede na avtomatsko obdelavo osebnih podatkov<sup>34</sup> (Sveta Evrope), ki se v tem delu v okviru še nedokončane reforme varstva osebnih podatkov v okviru Sveta Evrope ne spreminja.

### **K 3. členu:**

Prvi odstavek predlaganega 3. člena navaja, da je vsebina zakona najprej določanje pravic, obveznosti, upravičenj, načel, postopkov in ukrepov, s katerimi se preprečujejo neustavni, nezakoniti ali neupravičeni posegi v zasebnost oziroma dostojanstvo oziroma druge temeljne pravice posameznika oziroma posameznice pri obdelavi osebnih podatkov, tako da se v skladu s spoštovanjem načela pravne varnosti varuje ali uresničuje pravico iz 1. člena tega zakona. Gre torej za nadaljevanje sistemskega pristopa glede osebne človekove pravice, kot je opredeljena v 1. členu predloga ZVOP-2.

V drugem odstavku je določeno, da se v pravni red Republike Slovenije prenašajo določbe Direktive (EU) 2016/680 Evropskega parlamenta in Sveta z dne 27. aprila 2016 o varstvu posameznikov pri obdelavi osebnih podatkov, ki jih pristojni organi obdelujejo za namene preprečevanja, preiskovanja, odkrivanja ali pregona kaznivih dejanj ali izvrševanja kazenskih sankcij, in o prostem pretoku takih podatkov ter o razveljavitvi Okvirnega sklepa Sveta 2008/977/PNZ ter tudi prenašajo in zagotavlja izvajanje določb Uredbe (EU) 2016/679 Evropskega parlamenta in Sveta z dne 27. aprila 2016 o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem pretoku takih podatkov ter o razveljavitvi Direktive 95/46/ES (Splošna uredba o varstvu podatkov), ki se morajo ali smejo prenesti v pravni red Republike Slovenije ter tudi povezovalne določbe v zvezi s Splošno uredbo do določb Direktive. Navedena zapletena formulacija pove, da se določbe navedene Direktive izvršuje z zakonom, da delno podobno velja glede določb Splošne uredbe, ki se lahko izvršijo ali morajo izvršiti z zakonom Republike Slovenije, da pa za določene neposredno uporabne določbe Splošne uredbe (kadar se zlasti prekrivajo z določbami Direktive) velja sistem informativnega prepisa in ne neposredne uporabnosti, saj se jih načeloma ne razdeli, temveč le prepíše (npr. prvi odstavek 6. člena Predloga ZVOP-2 o splošnih definicijah). Namen tovrstnega prepisa v zvezi z razlago njegovega pomena ne predstavlja kršitve določb Splošne uredbe, niti ne z vidika uvodne navedbe št. 8 Splošne uredbe, temveč le zagotavljanje pravne varnosti, pa četudi le na informativni način (v tem primeru). Pri navedbah obeh Uradnih listov Evropske unije za oba pravna akta Evropske unije je še vedno puščen dodaten prazen prostor, saj še niso bili izdani popravki in sicer v slovenskem jeziku.

V tretjem odstavku je določeno (glede na prvi odstavek člena 2 Splošne uredbe), da določbe ZVOP-2 veljajo za popolnoma ali delno avtomatizirano obdelavo osebnih podatkov ter za drugačne obdelave osebnih podatkov, ki so vključeni ali so namenjeni vključitvi v zbirko.

V četrtem odstavku je določeno, da če VIII. del tega zakona ne določa drugače, določbe tega dela zakona veljajo tudi na področjih preprečevanja, preiskovanja, odkrivanja ali pregona kaznivih dejanj ali izvrševanja kazenskih sankcij (področje izvrševanja določb »Direktive (EU) 2016/680 Evropskega parlamenta in Sveta z dne 27. aprila 2016 o varstvu posameznikov pri obdelavi osebnih podatkov, ki

<sup>32</sup> Uradni list RS, št. 50/12 – uradno prečiščeno besedilo, 6/16 – popr., 54/15, 38/16 in 27/17.

<sup>33</sup> Uradni list RS, št. 33/16.

<sup>34</sup> Uradni list RS, št. 11/94 – Mednarodne pogodbe, št. 3/94 in 86/04 – ZVOP-1.

jih pristojni organi obdelujejo za namene preprečevanja, preiskovanja, odkrivanja ali pregona kaznivih dejanj ali izvrševanja kazenskih sankcij, in o prostem pretoku takih podatkov ter o razveljavitvi Okvirnega sklepa Sveta 2008/977/PNZ«).

#### **K 4. členu:**

4. člen je en od najpomembnejših členov predloga zakona, glede na to, da preko določanja jurisdikcije pravnega reda Republike Slovenije (prvi in tretji odstavek), njenega nadzornega organa (Informacijski pooblaščenec) ter sodnega varstva pred sodišči Republike Slovenije določa raven varstva pravic posameznikov glede njihovih osebnih podatkov.

Ozemeljska veljavnost določa, za katere obdelave osebnih podatkov (in s tem, za katere upravljavce oziroma obdelovalce osebnih podatkov) se uporablja določen predpis. Splošna uredba v skladu s členom 3 tako velja za tiste obdelave, ki jih izvajajo upravljavci in obdelovalci iz Evropske unije, ter v določenem delu tudi obdelave tujih upravljavcev in obdelovalcev, če imajo ti namen obdelovati osebne podatke prebivalcev Evropske unije. Predlog ZVOP-2 svojo veljavnost določa prav v teh okvirih, poleg tega pa jo v okviru pooblastil iz Splošne uredbe<sup>35</sup> določa tudi za nekatere posebne primere obdelav osebnih podatkov prebivalcev Republike Slovenije, za katere bi bila sicer podana veljavnost nacionalnega zakona katere druge države članice. Cilj tako široko začrtane veljavnosti je preprečiti, da bi bili prebivalci Evropske unije oziroma Republike Slovenije izključeni iz varstva, ki ga zagotavlja Splošna uredba oziroma tak zakon, oziroma da bi upravljavec oziroma obdelovalec to varstvo zaobšla<sup>36</sup> z izbiro kraja ustanovitve.

Prvenstveno ta zakon v skladu s prvim odstavkom tega člena tako kot dosedaj velja za tiste obdelave osebnih podatkov, ki potekajo v okviru opravljanja dejavnosti upravljavca ali obdelovalca, ki ima sedež, hčerinsko družbo, podružnico ali drugačno poslovno enoto na ozemlju Republike Slovenije, in to ne glede na to, ali sama dejanja obdelave dejansko potekajo na ozemlju Republike Slovenije ali ne<sup>37</sup>.

Gre za že obstoječe kriterije iz (a) točke prvega odstavka člena 4 Direktive o varstvu osebnih podatkov oziroma prvega odstavka 5. člena dosedanje ZVOP-1. Pri tem pri ugotavljanju, ali se neka obdelava izvaja v okviru dejavnosti določene poslovne enote, v skladu z sodno prakso Sodišča Evropske unije<sup>38</sup> 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<sup>39</sup>, oziroma ki na ozemlju Republike Slovenije opravljajo dejansko in resnično, čeprav majhno, dejavnost, v okviru katere se izvaja ta obdelava<sup>40</sup>.

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

<sup>35</sup> Npr. drugi stavek prvega odstavka člena 8 (privolitvena starost otrok), uvodna navedba št. 27 (obdelave osebnih podatkov umrlih oseb), četrti odstavek člena 9 (obdelave genskih, biometričnih ali podatkov v zvezi z zdravjem) ali člen 10 (obdelava osebnih podatkov v zvezi s kazenskimi obsodbami in prekrški).

<sup>36</sup> Glejte: razdelek št. 54 sodbe Sodišča EU v zadevi C-131/12 z dne 13. 5. 2014, *Google Spain SL, Google Inc. proti Agencia Española de Protección de Datos (AEPD)*.

<sup>37</sup> Uvodna navedba št. 22 Splošne uredbe.

<sup>38</sup> Sodba Sodišča EU v zadevi C-131/12, tč. 52, 56 in 67.

<sup>39</sup> Uvodna navedba št. 22 Splošne uredbe.

<sup>40</sup> 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*.

mednarodnega prava (tretji odstavek 3. člena Splošne uredbe oziroma četrti odstavek 5. člena ZVOP-1).

Pravila za razmejevanje veljave zakonov posameznih držav članic so sicer podrobneje pojasnjena v mnenju Delovne skupine po členu 29 Direktive o varstvu osebnih podatkov št. 8/2010 o pravu, ki se uporablja<sup>41</sup>, upošteva je okoliščino, da se kriterij opreme za obdelavo ((c) točka prvega odstavka člena 4 Direktive oz. drugi odstavek 5. člena ZVOP-1) z začetkom uporabe Splošne uredbe ne uporablja več.

Dodatno ta zakon v skladu z drugim odstavkom tega člena velja tudi za obdelave osebnih podatkov prebivalcev Republike Slovenije, ki ne potekajo v okviru upravljavca s sedežem zunaj Evropske unije (ampak jih izvaja upravljavec iz tretje države), vendar se ponujajo slovenskih uporabnikom, oz. zadevajo profiliranje slovenskih uporabnikov. Navedena določba temelji na členu 3(2) 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<sup>42</sup> (in torej za nadzor nad njim ni že tako v skladu z členom 3(1) pristojen kateri od državnih nadzornih organov držav članic). 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<sup>43</sup> 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<sup>44</sup>. V takšnih primerih bo Informacijski pooblaščenec pristojen za nadzor skladnosti obdelave tujega upravljavca oz. obdelovalca s tem zakonom, ter za obravnavo pritožb posameznikov v zvezi s tem.

Končno posamezne določbe tega zakona v skladu s tretjim odstavkom tega člena veljajo tudi za obdelave osebnih podatkov, za katere bi po kriteriju ustanovitve iz prvega odstavka sicer v celoti veljal zakon druge države članice, vendar pa Splošna uredba pooblašča državo članico, da vseeno določi obvezno veljavo svojega zakona. To t.i. načelo rezidenčnosti omogoča Republikli Sloveniji, da npr. glede starosti privolitve slovenskih mladoletnih oseb zahteva od upravljavcem na npr. Irskem, da upoštevajo pri nas določeno minimalno starost 15 let. Vse primeri rabe tega načela so v tem odstavku posebej naštet. V njih bo slovenski državni nadzorni organ (Informacijski pooblaščenec) pristojen sprejeti pritožbe posameznika, ter na tej podlagi sprožiti sodelovanje s pristojnim državnim nadzornim organom druge države članice Evropske unije, zato, da pri tem doseže spoštovanje določb slovenskega zakona za obdelave osebnih podatkov prebivalcev Republike Slovenije. Smisel takšnega pristopa je, da se tudi za te obdelave zagotovi spoštovanje visoke ravni varstva osebnih podatkov, ki jo je že dosedaj določal ZVOP-1, kar je glede na občutljivost in tveganost izbranih področij po presoji predlagatelja nujno in tudi smiselno. Pri vsem tem velja dodati, da v teh primerih veljava tega zakona torej ne pomeni tudi izključne pristojnosti (jurisdikcije) slovenskega državnega nadzornega organa, Informacijskega pooblaščenca.

Med vrstami osebnih podatkov v tretjem odstavku niso določeni osebni podatki umrlih oseb (10. člen Predloga ZVOP-2), ker le-teh Splošna uredba ne ureja (na to področje ne posega), ampak prepušča to urejanju s strani držav članic samih (popolna jurisdikcija vsake države članice v polju njene proste zakonodajne presoje ozir. v okviru bistvenih osnov njenega pravnega reda – npr. raven varstva spoštovanja pravice do pietete) – glede na uvodno navedbo št. 27 Splošne uredbe.

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

<sup>41</sup>[http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2010/wp179\\_en.pdf](http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2010/wp179_en.pdf)

<sup>42</sup> Navedba št. 23 Splošne uredbe.

<sup>43</sup> Navedba št. 23 Splošne uredbe.

<sup>44</sup> Navedba št. 24 Splošne uredbe.

Primer št. 2: upokojenec z začasnim prebivališčem v Sloveniji. O njem avstrijski medij piše nekaj neprijetnega. Ta posameznik se bo pritožil v Avstriji avstrijskemu nadzornemu organu za varstvo osebnih podatkov. Izdajatelj medija bo imel pravico zahtevati, da se Informacijski pooblaščenec Republike Slovenije vključi v postopek in zahteva uporabo bolj garantističnih določb slovenskega ZVOP-2 o razmerju svobode izražanja do varstva osebnih podatkov – v korist spoštovanja svobode izražanja.

Določbe dosedanjega tretjega odstavka 5. člena ZVOP-1 (predstavniki tujega upravljavca) so urejena neposredno v Splošni uredbi (člen 27).

#### **K 5. členu:**

Predlagani 5. člen določa splošno izjemo od veljave zakona, namreč obdelava osebnih podatkov za domače potrebe, kar vključuje zlasti obdelave osebnih podatkov, ki jih izvajajo posamezniki izključno za osebno uporabo, družinsko življenje. Pri uporabi tega člena je treba biti pazljiv v dve smeri – sicer široko tolmačiti domače potrebe, vendar v okviru besede »izključno« - da ne pride do kombinacije med domačo potrebo 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 dnevo ali drugih podobnih datumov, kot so obletnice.

Mora se opozoriti, da če obdelava zadeva tako zasebne kot poslovne informacije, se izjema ne uporabi. Beseda »izključno« nakazuje na *ozko interpretacijo* te določbe, Poslovna aktivnost bi morala vključevati kakršnokoli aktivnost ne glede na to, ali je odplačna, kot tudi pripravljala delovanja za njo, kot so npr. ukrepi trženja ali trgovanje z osebnimi podatki za to, da se dobi storitev.«<sup>45</sup>

#### **K 6. členu:**

V 6. členu je v prvem odstavku najprej zapisan dobesedni prepis temeljnih izrazov iz Splošne uredbe in iz Direktive, ki so zaradi prekrivanja med določbami obeh pravnih aktov Evropske unije, kot so osebni podatki, obdelava, zbirka, upravljavec, psevdonimizacija, oblikovanje profilov...

Dodane so le dokaj male dopolnitve, npr. nadzorni organ države je konkretiziran, kadar se nanaša na Republiko Slovenijo – zapisan kot Informacijski pooblaščenec). Pomembno pa je, da je izjemoma popravljena definicija privolitve, ne glede na besedilo veljavne slovenske inačice Splošne uredbe, saj bi zadržanje uradne inačice pomenilo drugačno pravno razumevanje privolitve kot enega od bistvenih institutov / pravnih podlag za obdelavo osebnih podatkov. Tudi ta popravek bo moral biti upoštevan v popravljani slovenski inačici Splošne uredbe.

Pomembna sprememba pa je definicija privolitve (11. točka prvega odstavka 6. člena), katera se sedaj glasi: »privolitev posameznika, na katerega se nanašajo osebni podatki, pomeni: vsako prostovoljno, konkretno, informirano in nedvoumno ravnanje v obliki izjave ali drugačnega jasnega aktivnega delovanja, iz katerega je mogoče sklepati na želje posameznika, na katerega se nanašajo osebni podatki, s katero izrazi strinjanje z obdelavo osebnih podatkov, ki se nanašajo nanj«. Navedena določba je očitno drugačna od (11). točke člena 4 Splošne uredbe, ki se glasi: »„privolitev posameznika, na katerega se nanašajo osebni podatki“ pomeni vsako prostovoljno, izrecno, informirano in nedvoumno izjavo volje posameznika, na katerega se nanašajo osebni podatki, s katero z izjavo ali jasnim pritrdilnim dejanjem izrazi soglasje z obdelavo osebnih podatkov, ki se nanašajo nanj«. V tem primeru predlagatelj šteje, da ni imel druge izbire, kot da že v tem predlogu zakona popravi definicijo privolitve še preden pride do popravka besedila slovenske jezikovne inačice Splošne

<sup>45</sup> 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.

uredbe v tem delu. Če bi bilo prepisano sedanje objavljeno napačno besedilo glede definicije privolitve, bi to pomenilo škodo pravni varnosti.

Zapisi temeljnih definicij s področja varstva osebnih podatkov (npr. osebni podatki, obdelava...) – kolikor se nanašajo na definicije iz Splošne uredbe, so na koncu prvega odstavka pojasnjeni z navedbo, da gre (samo) za navedbo »v skladu z zavezujočimi določbami člena 4 Splošne uredbe«. To pomeni, da je navedeni zapis (prepis) le informativne ozir. povezovalne narave v korist pravne varnosti in ne pomeni reguliranja izven dometa Splošne uredbe (tudi glede na uvodno navedbo št. 8 Splošne uredbe). V delu, ko se isti zapisi temeljnih definicij nanašajo na Direktivo in so spet enaki določbam Splošne uredbe, pa je na koncu prvega odstavka za razliko od prej navedene zaključne formulacije glede Splošne uredbe navedeno, da [to] »tudi pomeni izvajanje določb člena 3 Direktive«. Dodatno pa je upoštevana tudi mednarodna obveznost s področja Sveta Evrope - navedeno je, da ta člen pomeni tudi izvajanje določb 2. in 5. člena Konvencije o varstvu posameznikov glede na avtomatsko obdelavo osebnih podatkov (Sveta Evrope)<sup>46</sup>. Za področja, kateri Splošna uredba ali Direktiva ne urejajo (npr. varstvo osebnih podatkov umrlih oseb, varnost države, obramba države...) prav tako v celoti veljajo te temeljne definicije (razlog pravne varnosti).

V delu, ko gre za prej navedeni prepis temeljnih definicij iz Splošne uredbe, primerjalnopravna ureditev trenutno kaže (ob upoštevanju, da sta sprejeta le dva zakona – avstrijski in nemški), da ima slovaški predlog zakona z dne 22. 9. 2017 tudi v 5. členu prepis določb Splošne uredbe, vendar ne vsebuje zamejitev (glede Splošne uredbe), kot je predlagano na koncu besedila prvega odstavka 6. člena ZVOP-2.

V predlaganem drugem odstavku 6. člena so za potrebe izvrševanja IX. dela tega zakona določene definicije pristojnih organov.

V predlaganem tretjem odstavku 6. člena pa so določeni še nekateri izrazi, katere se lahko glede na specifičnosti pravnega reda Slovenije določi samostojno, npr. javni sektor, povezovalni znak (dosedaj isti povezovalni znak) ipd., ki ne odstopajo vsebinsko od dosedanjih definicij iz 6. člena ZVOP-1.

V 4. točki tretjega odstavka je dodana nova definicija povezovanje zbirk osebnih podatkov, ki je dosedaj ni bilo v ZVOP-1. Namen definiranja in urejanja pogojev za povezovanje zbirk osebnih podatkov je omejiti visoka tveganja za pravico posameznika do varstva osebnih podatkov, ki nastanejo, če je omogočen enostaven dostop do velike količine osebnih podatkov posameznika na enem mestu. Takšna situacija lahko nastane zlasti, ko so zbirke osebnih podatkov medsebojno tehnološko tako povezane, da lahko uporabnik podatkov pri delu v svojem informacijskem okolju z enostavno poizvedbo (npr. z vnosom povezovalnih znakov/enoličnih identifikatorjev, kot je npr. EMŠO), pridobi osebne podatke posameznika iz večjega števila medsebojno povezanih zbirk (primer obsežnega povezovanja je sistem eSociala, ki povezuje 44 zbirk osebnih podatkov). Takšna enostavna dostopnost podatkov pomeni veliko razgaljenost posameznika in s tem veliko moč odločanja o posamezniku ter zaradi centralizacije večje možnosti zlorab (povišana tveganja za notranjo in zunanjo nenamensko uporabo, okrepljeni motivi za vdor v informacijski sistem, pridobitev velike količine podatkov idr.) ter tudi nevarnost profiliranja – kar očitno terja ustrezno stroge varovalke na drugi strani. Povezovanje je lahko izvedeno *samodejno* (npr. da informacijski sistemi medsebojno čez noč posodablajo osebne podatke ob spremembah kot v primeru Centralnega registra prebivalstva) ali pa *na zahtevo* uporabnika (primer eSociala, kjer sistem na zahtevo uporabnika z uporabo različnih centralnih gradnikov pridobi osebne podatke posameznika iz 44 zbirk) – posledice so za posameznika iste, v praksi pa celo več povezovanja poteka na zahtevo. Prav tako z vidika tveganj ni razlike, ali se podatki združijo šele pri uporabniku ali na kakšnem mestu pred njim (primer rešitve ti. »Pladenj«). Vendar pa za povezovanje ne bi smeli šteti primerov, ko se pooblaščen uporabnik v okviru upravnega ali drugega individualnega postopka prijavi v zbirko osebnih podatkov, iz katere je pooblaščen pridobiti osebne podatke posameznika (primeri aplikacij za posamične poizvedbe v centralnih registrih, kot je e-RISK v primeru Centralnega registra prebivalstva ali e-Poizvedbe na področju zdravstvenega zavarovanja). Definicija povezovanja mora zajeti primere implementacij, ki temeljijo na veliki pogostosti posameznih poizvedb ali po uporabo enotnih prijavnih mehanizmov za dostop do različnih zbirk (angl. single-sign-on), saj gre za enako visoka tveganja za

<sup>46</sup> Uradni list RS, št. 11/94 – Mednarodne pogodbe, št. 3/94 in 86/04 – ZVOP-1.

pravice posameznika. Prav tako mora definicija povezovanja zajeti možnosti deloma ali v celoti elektronskega *paketnega pridobivanja* podatkov za večje število posameznikov, saj gre za primerljivo visoka tveganja (pridobivanje podatkov na zalogo, večja možnost napak, množičnost obravnave zlasti na prekrškovno-kazenskem področju). Obstajajo torej zelo raznolike možnosti tehnične implementacije povezovanja zbirk podatkov, zato je možno ločnico med povezovanjem in pridobivanjem podatkov postaviti le na funkcionalni in ne na tehnični ravni.

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. Povezovanje zbirk osebnih podatkov ima lahko za posameznika, državo in gospodarstvo tudi koristi v smislu enostavnosti pridobivanja lastnih osebnih podatkov, odprave administrativnih ovir, preglednosti porabe javnih sredstev ter ekonomičnosti in učinkovitosti postopkov, zato povezovanje zbirk ni prepovedano, temveč je zaradi visokih tveganj za temeljne človekove pravice (zlasti s področja varstva osebnih podatkov, dostojanstva, zasebnosti in osebnostnih pravic) dopustno, če je bila za to v zakonodajnem postopku po splošni in strokovni razpravi sprejeta ustrezna in specifična zakonska podlaga ter nato v posameznem postopku izdana odločba Informacijskega pooblaščenca.

Možni primeri:

- eSociala I/O modul in namenski spletni servisi – **JE POVEZOVANJE**;
- eSociala asinhroni modul (uporabnik na CSD prek ISCS2 sistema in Pladnja posreduje zahtevo bankam, banke grede po zahtevkah na pladenj, vsak zahtevek obdelajo ročno in poizvedbe ne spustijo v svoj sistem, pripravijo podatke in jih čez nekaj časa odložijo na Pladenj, kjer so na voljo uporabniku na CSD-ju) – **JE POVEZOVANJE**;
- aplikacije e-RISK, e-Poizvedbe, eMRVL - dostop do podatkov v registru MRVL – **NI POVEZOVANJE**;
- informacijski sistem TIRS, ki inšpektorju omogoča, da se posebej prijavi (avtenticira) v CRP in za določeno osebo pridobi njene podatke – **NI POVEZOVANJE**;
- informacijski sistem TIRS, ki inšpektorju omogoča, da v tem sistemu brez posebne prijave v CRP za določeno osebo iz CRP pridobi njene podatke ali hkrati pridobi podatke za večje število oseb – **JE POVEZOVANJE**;
- spletni servis, kjer se uporabnik na občini pred poizvedbo posebej avtenticira za dostop do zbirke osebnih podatkov in **dobi podatke hkrati za več posameznikov** – paketna poizvedba (npr. vsi, ki imajo 50 let) – **JE POVEZOVANJE**;
- spletni servis, kjer se uporabnik na občini pred poizvedbo posebej avtenticira za dostop do zbirke osebnih podatkov in **pridobi podatke za enega posameznika** (posamična poizvedba) – **NI POVEZOVANJE**;
- spletni servis, kjer se uporabnik na občini pred poizvedbo posebej avtenticira za dostop do zbirke osebnih podatkov **hkrati za več posameznikov** (oseba na občini pripravi podatke, naredi izvoz, zapeče podatke na CD ali jih odloži na neko mesto za prevzem - **JE POVEZOVANJE**.

V 5. točki tretjega odstavka 6. člena je podana definicija izbrisa osebnih podatkov, po kateri le-ta pomeni trajno odstranitev ali uničenje osebnega podatka, tako da ga več ni mogoče obnoviti, pri tem pa je zaradi zagotavljanja sledljivosti obdelave osebnih podatkov dopustno zabeležiti zaznamek, da je bil v zvezi osebnimi podatki določenega posameznika izveden izbris, pri čemer pa zaznamek ne sme vsebovati podatkov, ki bi omogočali obnovo izbrisanega podatka. Izraz trajna odstranitev pomeni elektronski izbris podatka, izraz uničenje pa pomeni fizično uničenje podatka v papirnati obliki. Z zakonom se sicer lahko določi drugačna uporaba instituta izbrisa (na izrecen način!), da se po izbrisu osebni podatek lahko arhivira v ti. neaktivno« arhivsko zbirko (evidenco).

V 6. točki tretjega odstavka 6. člena je podana definicija skupnih upravljavcev, ki pomeni situacijo ali stanje ali odločitev ali odločanje, kadar dva ali več upravljavcev skupaj določijo namene in sredstva obdelave (za skupne ali ločene zbirke, z deljenimi vlogami upravljavskega tipa).

V 8. točki tretjega odstavka 6. člena je podana skupna definicija pojma zakon ali zakonska podlaga glede na 87. člen, drugi odstavek 38. člena in tretji odstavek 3.a člena Ustave Republike Slovenije. Le-ta pomeni glede na člen 6 Splošne uredbe, člen 4 Direktive ter a) in b) točko 5. člena Konvencije o varstvu posameznikov glede na avtomatsko obdelavo osebnih podatkov (Sveta Evrope) - ta zakon, druge zakone Republike Slovenije, obvezujoče (in torej ratificirane) mednarodne pogodbe, ki zavezujejo Republiko Slovenijo ter pravne akte ali odločitve Evropske unije, katerih določbe so enakovredne zakonom in neposredno uporabljive ali neposredno učinkovite (glede na tretji odstavek 3.a člena Ustave Republike Slovenije), niso pa vključeni podzakonski predpisi (glede na drugi odstavek 38. člena Ustave Republike Slovenije ter z njim povezano ustaljeno ustavnosodno presojo Ustavnega sodišča Republike Slovenije od leta 1992 dalje<sup>47</sup>).

#### **K 7. členu:**

V predlaganem 7. členu so določena temeljna načela za zakonito obdelavo osebnih podatkov, ki zlasti sledijo določbam člena 5 Splošne uredbe. V a) točki prvega odstavka so glede na načelo zakonitosti glede varstva osebnih podatkov iz drugega odstavka 38. člena Ustave Republike Slovenije v zvezi z 87. členom Ustave Republike Slovenije (ter glede na ustaljeno ustavnosodno presojo Ustavnega sodišča Republike Slovenije zlasti po 38. členu Ustave Republike Slovenije) določena obvezna merila za zakonodajno urejanje – kadar se obdelavo osebnih podatkov za javni sektor ali tudi za zasebni sektor ureja z zakonom, pri čemer je upoštevan zadnji del tretjega odstavka člena 6 Splošne uredbe. Točke b), c), d), in f) urejajo omejitev namena obdelave, vključno glede vprašanja nezdržljivosti, minimizacijo obdelave osebnih podatkov, točnost in posodobljenost (dosedanji izraz za posodobljenost: ažurnost), pri tem sledijo točkam iz prvega odstavka člena 5 Splošne uredbe. Načelo sorazmernosti je vsebovano v c) točki, v delni povezavi z b) točko. V f) točki se nahaja koncept varnosti osebnih podatkov (dosedaj: zavarovanje osebnih podatkov), ki je nadalje razdelana v ZVOP-2 v členih o varnosti osebnih podatkov in je z vidika informacijske varnosti ključna.

V drugem odstavku je določena obveznost dokumentiranja skladnosti obdelav osebnih podatkov za upravljavca in obdelovalca z določbami prvega odstavka, ter morata v skladu s tem voditi tudi predpisano dokumentacijo v skladu z zakonom – kar tudi pomeni, da ko se odloča o nezdržljivosti obdelave – in oceni, da je možna obdelava v druge namene, da je to del splošne dokumentacije o skladnosti obdelave. To se dokaže zlasti z izvedbo ocene učinkov ter notranjo in zunanjo sledljivostjo po določbah tega zakona.

V tretjem odstavku je z vidika lažje povezave določb v zakonu dodano, da je načelo sorazmernosti (poimenovano kot tako) vsebovano v c) točki, v delni povezavi z b) točko prvega odstavka 7. člena ZVOP-2.

#### **K 8. členu:**

Predlagani 8. člen najprej določa pravne podlage za obdelavo osebnih podatkov v javnem sektorju in pri temu precej sledi smerem iz dosedanjega 9. člena ZVOP-1. Ob tem v zadnjem (šestem) odstavku določa tudi pravilo glede obdelave v druge namene. Dejansko novi vsebini pa sta torej v predlaganem drugem in šestem odstavku.

Predlagani prvi odstavek določa, kaj mora biti vsebina področnega zakona s področja osebnih podatkov, ki naj bi se obdelovali v javnem sektorju, glede na določbe drugega odstavka 38. člena Ustave Republike Slovenije v zvezi z 87. členom Ustave Republike Slovenije (ter glede na ustaljeno ustavnosodno presojo Ustavnega sodišča Republike Slovenije zlasti po 38. členu Ustave Republike Slovenije). Upošteva tudi merila iz drugega odstavka člena 6 Splošne uredbe ter drugega dela tretjega

---

<sup>47</sup> Odločba US, št. U-I-115/92, 24.12.1992; objava: OdlUS I, 105 in Uradni list RS, št. 3/93.

odstavka člena 6 Splošne uredbe ter drugega odstavka člena 23 Splošne uredbe. V razmerju med prvim in šestim odstavkom 8. člena velja, da podajanje kazenskih ovadb ali naznanitev kaznivih dejanj in s tem povezana posredovanja osebnih podatkov ne šteje za dodatni namen – na to namreč napotuje zadnja poved uvodne navedbe 50 Splošne uredbe. V Sloveniji je to urejeno drugače, načeloma na sistemski ravni: ovaditelj ima bodisi zakonsko pravico (145. do 147. člen Zakona o kazenskem postopku) ali posebne dolžnosti sporočanja kršitev (68.–69. člena Zakon o preprečevanju pranja denarja in financiranja terorizma) podaje ovadbe, če pa je morda na kakem področju nima določene, pa jo podaja na podlagi varstva upravičenih interesov (upravljavca ali obdelovalca).

Zadnji stavek prvega odstavka določa pravno podlago za razliko od dosedanjega drugega odstavka 9. člena ZVOP-1, tako da lahko ne samo nosilci javnih pooblastil, ampak izrecno celotni javni sektor po definiciji iz 5. člena ZVOP-2 deluje na podlagi privolitve, ki pa mora biti določena v zakonu (npr. narodnost, verska pripadnost – 61. člen ter prvi in drugi odstavek 41. člena Ustave Republike Slovenije).

Predlagani drugi odstavek določa, da se lahko v javnem sektorju tudi obdelujejo osebni podatki - le (!) na podlagi privolitve posameznika<sup>48</sup>, če ne gre za izvrševanje zakonitih pristojnosti, nalog ali obveznosti javnega sektorja. 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. To je 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 predstavništvi ali drugih državljanov ali diplomatov za uradne sprejeme, vodenje osebnih imen staršev zaradi vabil na ti. »nadstandardne« šolske aktivnosti – npr. eAsistent.

Predlagani tretji odstavek določa, da se ne glede na prvi odstavek 8. člena lahko v javnem sektorju obdelujejo tudi osebni podatki posameznika, ki je z javnim sektorjem sklenil pogodbo, ali pa je na podlagi zahteve tega posameznika v fazi pogajanj za sklenitev pogodbe z njim, če je obdelava osebnih podatkov potrebna in primerna za izvajanje ukrepov pred sklenitvijo pogodbe ali za izvajanje pogodbe.

Predlagani četrti odstavek določa, da se ne glede na prvi odstavek tega člena lahko v javnem sektorju izjemoma obdelujejo tisti osebni podatki, ki so potrebni za zaščito življenjskih interesov posameznika, na katerega se nanašajo osebni podatki, ali druge fizične osebe. Poudarek je na besedi »izjemoma«, življenjski interesi posameznika pa so nekoliko širši od samo varovanja življenja in telesa – primerljivo določbam 43. člena Zakona o nalogah in pooblastilih policije o iskanju oseb in delno primerljivo tudi določbam 153. člena Zakona o elektronskih komunikacijah, vendar tudi širše, saj gre lahko tudi za dajanje pravne pomoči neuki stranki, preprečevanje nastanka hujše škode (npr. nujna medsosedska pomoč) ipd..

Predlagani peti odstavek določa, da se ne glede na prvi odstavek tega člena lahko v javnem sektorju izjemoma obdelujejo tisti osebni podatki, ki so nujni za izvrševanje zakonitih pristojnosti, nalog ali obveznosti javnega sektorja, če se s to obdelavo ne poseže v upravičen interes posameznika, na katerega se osebni podatki nanašajo. Ponovno je dan poudarek na besedi »izjemoma«, gre pa za izvedbo e) točke prvega odstavka člena 6 Splošne uredbe in nekoliko tudi za izvedbo četrtega odstavka člena 6 Splošne uredbe. Izjemoma pomeni tudi začasno, omejeno na konkretno nujno obdelavo osebnih podatkov (torej ne more iti za dalj časa trajajočo množično obdelavo osebnih podatkov, ki bi dobila sistemski pomen), ki ne posega v (široko) razumljen upravičen interes posameznika glede tajnosti njegovih osebnih podatkov. Predlagana določba pa ne omogoča niti začasnega omogočanja določanja osebnih podatkov v podzakonskih aktih (zlasti v pravilnikih), je kvečjemu na njeno izjemnost lahko »sprožilec«, da pristojno ministrstvo po izvedeni začasni konkretni obdelavi osebnih podatkov, pripravi spremembe ali dopolnitve ustreznega zakona, tako da je

<sup>48</sup> 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).«



spoštovano pravilo iz prvega odstavka 8. člena (in drugi odstavek 38. člena Ustave Republike Slovenije v zvezi s 87. členom Ustave Republike Slovenije). Gre za nadgradnjo vsebine dosedanjega četrtega odstavka 9. člena ZVOP-1.

Predlagani šesti odstavek določa obdelavo osebnih podatkov v druge namene<sup>49</sup> kot pravilo za delovanje (odločanje) javnega sektorja. Po predlagani določbi obdelava osebnih podatkov za drug namen kot za tistega, za katerega so bili zbrani, v javnem sektorju ni dopustna, razen če to določa ta zakon ali če to zaradi izvrševanja ciljev iz prvega odstavka člena 23 Splošne uredbe in pod pogoji iz prvega odstavka 8. člena določa drug področni zakon. Primeri so npr. zlasti arhiviranje po področni zakonodaji, znanstveno raziskovanje, statistično raziskovanje.

Predlagani sedmi odstavek določa posebno pravilo glede uporabe privolitve v druge namene za potrebe javnega sektorja. Določeno je, da je obdelava osebnih podatkov v javnem sektorju za drug namen kot za tistega, za katerega so bili zbrani, prepovedana (ni dopustna) na podlagi prvotne privolitve, če je bila ta privolitev podana za določen namen, ki sicer lahko vsebuje eno ali več delovanj obdelave v skladu z **določenim namenom**. Če je načrtovana obdelava osebnih podatkov za drug (nov) namen na podlagi privolitve, se lahko izvede le na podlagi nove privolitve posameznika, na katerega se nanašajo osebni podatki, če druga zakonska podlaga izrecno (glede na načelo zakonitosti iz drugega odstavka 38. in 87. člena Ustave Republike Slovenije) ne določa drugače. To dodatno pravilo izhaja iz besedila Predloga Smernic glede privolitve po Uredbi 2016/679<sup>50</sup> z dne 28. 11. 2017, ki jih je pripravila Delovna skupina po členu 29 Direktive 95/46/ES (združenje evropskih nadzornih organov za varstvo osebnih podatkov Evropske unije). Gre za dodatno (originarno) razlago po kateri privolitev velja le za en namen, ki ima sicer lahko različne opcije obdelave – če so za isti namen, ni pa možna obdelava v druge namene – in nato je za obdelavo v drug namen potrebno pridobiti dodatno privolitev – skladno s členom 6, četrtem odstavkom Splošne uredbe ter členom 5, (b) točko prvega odstavka iste uredbe ter glede na uvodno navedbo št. 32 uredbe.

#### **K 9. členu:**

Predlagani 9. člen najprej določa pravne podlage za obdelavo osebnih podatkov v zasebnem sektorju in pri temu precej sledi smerem iz dosedanjega 10. člena ZVOP-1. Ob tem v petem odstavku določa tudi sistemsko pravilo glede obdelave v druge namene v zasebnem sektorju.

Prvi odstavek določa, da se osebni podatki v zasebnem sektorju lahko obdelujejo, če obdelavo osebnih podatkov in osebne podatke, ki se obdelujejo, določa zakon ali če je za obdelavo določenih osebnih podatkov podana privolitev posameznika. Če obdelavo osebnih podatkov v zasebnem sektorju določa zakon, mora ta določati: namen obdelave in vrste osebnih podatkov, ki se obdelujejo, kategorije posameznikov, na katere se nanašajo osebni podatki in rok hrambe. Zakon pa lahko, če je to potrebno, določi tudi morebitne druge ukrepe za zagotovitev zakonite, poštene in pregledne obdelave, omejitve namena in uporabnike in druge upravljavce osebnih podatkov, ki se jim osebni podatki lahko razkrijejo. Z zakonom se lahko določi, da se določeni osebni podatki za enega ali več določenih namenov obdelujejo le na podlagi privolitve posameznika. Bistvo glede prvega odstavka je seveda pravna podlaga privolitve, zakonska ureditev pride v poštev, kadar to zaradi varovanja javnega interesa (npr. tudi regulacija poklica, sporočanje kršitev zakona) predpiše zakonodajalec (npr. po c) točki prvega odstavka člena 6 Splošne uredbe).

Predlagani drugi odstavek določa, da se ne glede na prvi odstavek lahko v zasebnem sektorju obdelujejo osebni podatki posameznika, ki je z zasebnim sektorjem sklenil pogodbo, ali pa je na podlagi zahteve tega posameznika v fazi pogajanj za sklenitev pogodbe z njim, če je obdelava osebnih podatkov potrebna in primerna za izvajanje ukrepov pred sklenitvijo pogodbe ali za izvajanje pogodbe.

<sup>49</sup> 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.

<sup>50</sup> »Guidelines on Consent under Regulation 2016/679«, 17/EN, WP259, Adopted on 28 November 2017, str. 12.

Predlagani tretji odstavek določa, da se ne glede na prvi odstavek 9. člena ZVOP-2 lahko v zasebnem sektorju obdelujejo tisti osebni podatki, ki so potrebni za zaščito življenjskih interesov posameznika, na katerega se nanašajo osebni podatki, ali druge fizične osebe – podobno kot v četrtem odstavku 8. člena ZVOP-2. Na ta način je podana paralelna obveznost, da je upravljavec ali obdelovalec v zasebnem sektorju dolžan posredovati osebne podatke za izvrševanje pristojnosti javnega sektorja po četrtem odstavku 8. člena ZVOP-2.

Predlagani četrti odstavek določa, da se ne glede na prvi odstavek tega člena lahko v zasebnem sektorju obdelujejo osebni podatki, če je obdelava potrebna zaradi uresničevanja zakonitih upravičenih interesov, za katere si prizadeva upravljavec ali tretja oseba, razen kadar nad takimi interesi prevladajo interesi ali človekove pravice in temeljne svoboščine posameznika, na katerega se nanašajo osebni podatki, ki zahtevajo varstvo osebnih podatkov, zlasti kadar je posameznik, na katerega se nanašajo osebni podatki, otrok. Npr. zasebni sektor lahko obdelava na tej podlagi osebne podatke, ki jih zakonito ima, za potrebe pravnega postopka, ne gre pa za obdelavo osebnih podatkov za namene neposrednega trženja, saj je to posebno (področno) urejeno v poglavju tega zakona.

Predlagani peti odstavek določa obdelavo v druge namene v zasebnem sektorju. Določeno je, da je obdelava osebnih podatkov za druge namene kot tiste, za katere so bili osebni podatki prvotno zbrani, v zasebnem sektorju dovoljena le, kadar je združljiva z nameni, za katere so bili osebni podatki prvotno zbrani. Za ugotovitev, ali je namen nadaljnje obdelave združljiv z namenom, za katerega so bili osebni podatki prvotno zbrani, mora upravljavec, potem ko je izpolnil vse zahteve glede zakonitosti prvotne obdelave, opraviti presojo v skladu s četrtem odstavkom člena 6 Splošne uredbe. Presoja mora biti opravljena pred začetkom obdelave za druge namene, v pisni obliki, in je sestavni del dokumentacije po drugem odstavku člena 5 Splošne uredbe.

Predlagani šesti odstavek tudi določa dodatno pravilo glede uporabe privolitve v druge namene za potrebe zasebnega sektorja. Določeno je, da je obdelava osebnih podatkov v zasebnem sektorju za drug namen kot za tistega, za katerega so bili zbrani - prepovedana (ni dopustna) na podlagi prvotne privolitve, če je bila ta privolitev podana za določen namen, ki lahko vsebuje eno ali več delovanj obdelave v skladu z določenim namenom. Če je načrtovana obdelava za drug (torej nov) namen na podlagi privolitve, se lahko izvede le na podlagi nove privolitve posameznika, na katerega se nanašajo osebni podatki, če druga zakonska podlaga ne določa drugače. Enako kot pri sedmem odstavku 8. člena ZVOP-2 to dodatno pravilo izhaja iz Predloga Smernic glede privolitve po Uredbi 2016/679 z dne 28. 11. 2017, ki jih je pripravila Delovna skupina po členu 29 Direktive 95/46/ES. Gre za dodatno (originarno) razlago po kateri privolitev velja le za en namen<sup>51</sup>, ki ima sicer lahko različne opcije obdelave – če so za isti namen, ni pa možna obdelava v druge namene – in nato je za obdelavo v drug namen potrebno pridobiti dodatno privolitev – skladno s členom 6, četrtem odstavkom Splošne uredbe ter členom 5, (b) točko prvega odstavka iste uredbe ter glede na uvodno navedbo št. 32 uredbe.

#### **K 10. členu:**

V 10. členu je predlagana posebna ureditev glede varstva osebnih podatkov umrlih posameznikov, na katere so se nanašali v preteklosti zbrani in obdelani osebni podatki. Gre že za tradicionalno slovensko ureditev (glejte veljavni 23. člen ZVOP-1) z vidika zadržanja dosedanje višje stopnje varstva osebnih podatkov. Podobna ureditev obstaja ali pa bo prenovljena vsaj v Avstriji, na Slovaškem 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).

---

<sup>51</sup> S tega vidika je morda relevantna tudi določba tretjega odstavka člena 7 Splošne uredbe, po kateri lahko posameznik uvede umik privolitve kadarkoli – glejte: Voigt, Paul, von dem Bussche, Axel, *The EU General Data Protection Regulation (GDPR) : A Practical Guide*, Springer International Publishing AG, Cham, 2017, str. 97, razdelek 4.2.1.5. Umik.

Predlagani prvi odstavek določa, da se osebni podatki umrlih posameznikov varujejo po tem zakonu in drugih zakonih (npr. Obligacijski zakonik, Zakon o varstvu dokumentarnega in arhivskega gradiva ter arhivih).

Predlagani drugi odstavek določa, da upravljavec podatke o umrlem posamezniku posreduje le tistim uporabnikom, ki so za obdelavo osebnih podatkov pooblašeni z zakonom (s področja javnega ali zasebnega sektorja) in tistim osebam, ki izkažejo pravni interes za uveljavljanje pravic pred osebami javnega sektorja.

Predlagani tretji odstavek določa, da ne glede na določbe drugega odstavka 10. člena ZVOP-2 upravljavec osebne podatke o umrlem posamezniku posreduje zakoncu, zunajzakonskemu partnerju ali partnerju iz partnerske zveze, otrokom ali staršem, če umrli posameznik ni predhodno pisno prepovedal posredovanja osebnih podatkov. Upoštevano je z vidika interesov pietete bližnjih, da imajo dostop do teh podatkov, razen, če je posameznik predhodno (v oporoki ali drugače, lahko tudi z navadnim zapisom) prepovedal posredovanje njegovih osebnih podatkov.

Predlagani četrti odstavek določa, da če drug zakon ne določa drugače, lahko upravljavec podatke o umrlem posamezniku posreduje tudi katerikoli drugi osebi, ki namerava te podatke uporabljati za zgodovinske raziskovalne, znanstvene raziskovalne, statistične ali arhivske namene pod pogoji iz 76. do 78. člena tega zakona.

Predlagani peti odstavek je neposredna pravna podlaga (upravičenje) za izjemno objavo podatkov umrlih v knjigah, učbenikih, enciklopedijah itd, se pa ne nanaša na klasične članke v medijih (za te primere načeloma velja svoboda izražanja po 79. členu predloga zakona).

#### **K 11. členu:**

Predlagani 11. člen določa v skladu s členom 8 Splošne uredbe (po vzorcu iz Zakona o zasebnosti otrok na spletu Združenih držav Amerike – (Children's Online Privacy Protection Act - COPPA) iz leta 1998) pogoje za obdelavo osebnih podatkov otrok v primeru uporabe storitev informacijske družbe (opredelitev storitev informacijske družbe je vsebovana v 25. točki prvega odstavka 6. člena Predloga ZVOP-2). Storitve informacijske družbe so opredeljene v 25. točki prvega odstavka 6. člena ZVOP-2, otrok pa je v tem primeru v skladu z odprtimi določbami Splošne uredbe naveden kot mladoletna oseba, ki je stara 15 let ali več. Kar tudi pomeni (glede na predlagani prvi odstavek 11. člena), da veljajo strogi pogoji v zvezi s privolitvijo po tem členu le za otroke, ki še niso stari 15 let. Starost 15 let je izbrana (določena) glede na sistemsko vodilo iz prvega odstavka 146. člena Družinskega zakonika<sup>52</sup>: »Otrok, ki dopolni 15 let, lahko sam sklepa pravne posle, če zakon ne določa drugače.«.

Nadalje prvi odstavek določa, da gre za vprašanje urejanja privolitve mladoletne osebe za uporabo storitev informacijske družbe, ki se jih ponuja neposredno mladoletnim osebam oziroma za katere se lahko verjetno domneva, da jih bodo uporabljale mladoletne osebe – torej upravljavcu daje obveznost preverjanja in vzpostavljanja informacijskih sistemov, ki naj bi preprečili, da bi privolitev lahko podala mladoletna oseba, ki še ni stara 15 let. V primeru, če je mladoletna oseba mlajša od 15 let, je privolitev veljavna le, če jo poda ali odobri eden od staršev mladoletne osebe oziroma njen rejnik ali skrbnik.

Po predlaganem drugem odstavku je upravljavec dolžan ves čas nudenja storitve ob upoštevanju razpoložljive tehnologije v primerih iz drugega stavka prejšnjega odstavka izvajati dolžan izvajati razumna prizadevanja, s katerimi preveri, ali je starš, rejnik ali skrbnik za otroka mladoletno osebo podal ali odobril privolitev. Razumna prizadevanja so lahko različna, zakonska določba z uporabo besede »zlasti« (torej enumerativni - odprti pristop) omenja možnost kontaktiranja staršev, rejnikov ali skrbnikov.

Po predlaganem tretjem odstavku privolitev mladoletne osebe iz prvega odstavka 11. člena ZVOP-2 (ki je torej stara 15 let ali več) ne sme biti pogojevana s pretiranimi pogoji s strani upravljavca, zlasti da bi bila omogočena udeležba mladoletnih oseb v igri, ponujanje nagrade, vključitve v družbeno omrežje ali druge podobne dejavnosti, tako da bi mladoletna oseba morala posredovati več osebnih podatkov

---

<sup>52</sup> Uradni list RS, št. 15/17.

(kršitev načela sorazmernosti), kot je potrebno za namen opravljanje takšne dejavnosti. Prepoved velja tudi v primerih iz drugega stavka prvega odstavka 11. člena ZVOP-2.

Predlagani člen izhaja (enako tudi določbe člena 8 Splošne uredbe) iz COPPA, ki nima podrobnejših kriterijev, kaj se šteje za razumna prizadevanja, razen da gre (vsaj posredno) za kontaktiranje staršev ob uporabi razpoložljive tehnologije (SEC. 1302., deveti odstavek). Navedeni zakon sicer načeloma v praksi ni znan kot učinkovit zakon.

#### **K 12. členu:**

V 12. (dejansko pa tudi v povezanem 13.) členu se urejajo obdelave posebnih vrst osebnih podatkov (dosedaj: občutljivi osebni podatki).

V predlaganem prvem odstavku je najprej podana stroga (tradicionalna) prepoved obdelave posebnih vrst osebnih podatkov, sedaj glede na prvi odstavek člena 9 Splošne uredbe ter smiselno (po zapisu drugače, rezultat pa je vsebinsko enak) iz člena 10 Direktive ter glede na še nespremenjeni 6. člen Konvencije o varstvu posameznikov glede na avtomatsko obdelavo podatkov (Sveta Evrope). Določeno je, da so posebne vrste osebnih podatkov naslednje: osebni podatki o rasnem ali etničnem poreklu, političnem mnenju, verskem ali filozofskem prepričanju ali članstvu v sindikatu, genski podatki, biometrijskih podatki za namene edinstvene identifikacije posameznika, podatki v zvezi z zdravjem ali podatki v zvezi s posameznikovim spolnim življenjem ali spolno usmerjenostjo.

Drugi odstavek, podobno kot dosedanji 13. člen ZVOP-1, določa pravne podlage za obdelavo posebnih vrst osebnih podatkov, z določenimi podrobnejšimi določbami. Tako je npr. določeno, da se posebne vrste osebnih podatkov lahko obdelujejo tudi, če je to potrebno zaradi uveljavljanja ali izvajanja pravnih zahtevkov ali obrambo pred njimi – vendar v okviru zakonsko določenih uradnih postopkov – torej, upravni postopki, sodni postopki, nadzorni postopki ipd., ki morajo biti urejeni z zakonom. V h) točki pa je razdelana tudi še dodatna omejitev, ki je usmerjena na področne zakone, namreč z vidika sorazmernosti je določeno, da lahko obdelavo posebnih vrst osebnih podatkov določi drug zakon zaradi izvrševanja bistvenega javnega interesa, kar mora biti sorazmerno z zastavljenim ciljem, spoštovati bistvo pravice do varstva podatkov ter zagotavljati ustrezne in posebne ukrepe za varstvo človekovih pravic in temeljnih svoboščin ali interesov posameznika, na katerega se nanašajo osebni podatki.

V tretjem odstavku je določeno, da je treba v primerih obdelav posebnih vrst osebnih podatkov po drugem odstavku poleg ukrepov iz 29. člena ZVOP-2 določiti in vzpostaviti in pisno opredeliti še primerne in posebne zaščitne ukrepe za varstvo pravic, svoboščin ali interesov posameznika, na katerega se nanašajo osebni podatki. Ob upoštevanju tehnološkega razvoja, stroškov izvajanja ter vrste, obsega, okoliščin in namenov obdelave ter različnih stopenj verjetnosti pojava tveganj, povezanih z obdelavo, za človekove pravice in temeljne svoboščine in interese posameznikov ter njihove resnosti, so ti zaščitni ukrepi najmanj tisti, ki so urejeni v točkah tretjega odstavka. Po točki a) so to politike, postopki in ukrepi za varnost osebnih podatkov (nekdanje zavarovanje osebnih podatkov), ki zagotavljajo, da obdelava poteka skladno z zahtevami iz 29. člena ZVOP-2. Za posebne vrste osebnih podatkov bodo torej veljala splošna pravila, za ti. navadne osebne podatke pa po 29. členu ter dodatni ukrepi varnosti osebnih podatkov po tem členu. V b) točki je naveden ukrep ozaveščanja oseb, udeleženih v postopkih obdelave, o varnostnih politikah, postopkih in ukrepih za zagotavljanje varnosti osebnih podatkov. V c) točki je za področje zagotavljanja elektronskih storitev javnega sektorja, ki vključujejo obdelavo posebnih vrst osebnih podatkov, določen ukrep, da je za dostop do teh storitev potrebno zagotoviti takšna sredstva elektronske identifikacije, kjer se ob izdaji zahteva osebno navzočnost posameznika in se njegovo identiteto preveri z vpogledom v uradni osebni dokument posameznika. V č) točki je določeno, da je treba pri prenosu posebnih vrst osebnih podatkov preko elektronskih omrežij te podatke šifrirati tako, da je zagotovljena njihova neprepoznavnost med prenosom in da so kontaktni podatki naslovnika predhodno preverjeni s potrditvenim sporočilom, s katerim naslovnik potrdi pravilnost podatkov za dostavo. Elektronski podpis ni več zahtevan, ker dejansko niti ne zagotavlja nečitljivosti podatkov.

*Možni primer:* pošiljanje izvidov pacientom po e-pošti.

V d) točki je določen ukrep ustreznega upravljanja uporabniških pooblastil pri upravljavcih in obdelovalcih, v e) točki pa – da, kjer je to ustrezno, tudi psevdonimizacija oziroma šifriranje osebnih podatkov.

Glede posebnega vidika glede podatkov o narodni pripadnosti - statistični namen zbiranja teh osebnih podatkov:

Republika Slovenija ima že ustavnopravno dokaj strogo pozicijo glede izražanja narodne pripadnosti – namreč v 61. členu Ustave Republike Slovenije, po katerem se narodno pripadnost izraža svobodno. Glede na navedeni člen Ustave mora biti vsak poseg v smer pridobivanja osebnega podatka o narodni pripadnosti razumno utemeljen, mora spoštovati svobodo človeka in biti v skladu s temeljnim ustavnim načelom sorazmernosti (2. člen v zvezi s tretjim odstavkom 15. člena Ustave Republike Slovenije) – spoštovano mora biti torej strogo načelo sorazmernosti. Torej zbiranja in obdelave osebnih podatkov ni možno opravičiti s potrebami statističnega poročanja ali raziskovanja (izjema so glede na posebne varovalke lahko popisi prebivalstva – npr. Popis prebivalstva, gospodinjstev in stanovanj v Republiki Sloveniji leta 2002), če ni opravičen (utemeljen) že primarni namen za zbiranje podatka o narodni in etnični pripadnosti za potrebe določenega postopka ali odločanja (npr. prosilci za mednarodno zaščito – preganjanje zaradi narodne pripadnosti). Prav tako, če se odmisli prej navedeni primarni namen zbiranja (za potrebe postopka ozir. odločanja), bi bilo zbiranje in obdelava podatkov o pripadnosti na podlagi osebne privolitve načeloma nesmiselno, saj nikoli ne bi dovolj ljudi dalo privolitve za to, da bi vzorec dejansko bil reprezentativen in lahko kaj pomenil z vidika ocene delovanj ali odločanj o ljudeh v raznih uradnih (zakonsko določenih) postopkih.

Seveda pa pravni red Republike Slovenije ne preprečuje, da nevladne organizacije ali raziskovalne organizacije ne raziskujejo same, na podlagi uporabe arhivskega gradiva, kakšna so določena razmerja/vpliv glede narodne pripadnosti v zvezi z uradnimi postopki, storitvami ipd. v Sloveniji.

### **K 13. členu:**

V predlaganem 13. členu je določena dodatna vrsta posebne vrste osebnih podatkov, namreč podatkov o kazenskih obsodbah in kaznovanjih za prekrške – glede na člen 10 Splošne uredbe ter glede na uvodni navedbi št. 75 in 80, ki v zvezi s konceptom kazenske obtožbe iz prvega odstavka 6. člena Evropske konvencije omenja poleg kaznivih dejanj tudi prekrške (kar je del skupnega koncepta kaznivih ravnanj). V prvem odstavku je tako določeno, da za podatke o vpisu ali izbrisu v ali iz kazenske evidence ali evidenc, ki se upravljajo na podlagi Zakona o prekrških ter za prenose teh osebnih podatkov velja, da gre za osebne podatke, ki morajo biti varovani kot posebne vrste osebnih podatkov po drugem in tretjem odstavku 12. člena ZVOP-2.

Drugi odstavek najprej v prvem stavku določa, da za obdelave določenih (kategorij) 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 Zakona o izvrševanju kazenskih sankcij, Zakona o kazenskem postopku ter Kazenskega zakonika. Prav tako določa, da za obdelave določenih (kategorij) osebnih podatkov iz prekrškovnih evidenc po Zakonu o prekrških veljajo primerljiva pravila iz Zakona o prekrških glede zakonsko določenih namenov obdelave, rokov hrambe ter prenosov javnemu ali zasebnemu sektorju. Zaključno je za obe vrsti evidenc tudi določeno, da za prenose teh osebnih podatkov iz navedenih evidenc organom drugih držav ali mednarodnim organizacijam (za zakonsko določene namene) veljajo tudi pravila po drugih zakonskih podlagah.

Predlagani tretji in četrti odstavek določata, da se kazenske evidence in prekrškovne evidence lahko povezujejo s Centralnim registrom prebivalstva tako, da se zagotovi točnost in posodobljenost osebnih podatkov v kazenskih ali prekrškovnih evidencah ter da se povezovanje izvede tako, da je možno samodejno posodabljanje podatkov v evidencah oziroma na način, da povezovanje omogoča vsaj, da se v evidencah pri osebnih podatkih določenega ali določljivega posameznika pojavi samodejno opozorilo, da je pri njegovih podatkih v drugi zbirki osebnih podatkov prišlo do spremembe. V petem odstavku je glede povezovanja zaključno določeno, da se za državljane Republike Slovenije ali osebe

s prebivališčem v Republiki Sloveniji kot identifikacijska znaka uporabita osebno ime in njihova enotna matična številka, za tujca pa njegovo osebno ime in njegova enotna matična številka ali drug ustrezen identifikacijski znak iz kazenske evidence.

## **2. K II. delu Predloga ZVOP-2:**

### **K 14. členu:**

14. člen je uvodna določba II. dela Predloga ZVOP-2. V njem se ureja področje uporabe tega dela zakona, navedeno je, da se urejajo pravice posameznika, na katerega se nanašajo osebni podatki, in postopek uveljavljanja teh pravic iz členov 15 do 22 in iz člena 34 Splošne uredbe ter tudi (delno) za področja preprečevanja, preiskovanja, odkrivanja ali pregona kaznivih dejanj ali izvrševanja kazenskih sankcij, če ni v tem ali IX. delu tega zakona določeno drugače (če ta del o določenem vprašanju ne navede izrecno, da je relevanten tudi IX. del tega zakona).

### **K 15. členu:**

Predlagani 15. člen ZVOP-2 v uvodnem (prvem) odstavku ureja pravice glede zagotavljanja preglednih informacij, informacij o posamezniku, na katerega se nanašajo osebni podatki, pravic posameznika, na katerega se nanašajo osebni podatki, do pridobitve teh podatkov ter pravice do popravka ali izbrisa osebnih podatkov, do omejitve obdelave ter pravica do pozabe, tako da naredi sklic na neposredno uporabne določbe Splošne uredbe.

V drugem odstavku ureja konkretne načine, s katerimi upravljavec posamezniku, na katerega se nanašajo osebni podatki, posreduje informacije in sporočila, v skladu s členi 13 in 14 Splošne uredbe ter informacije iz členov 15 do 22 in 34 Splošne uredbe, ki se nanašajo na obdelavo osebnih podatkov, da morajo namreč biti posredovane v čim bolj jedrnatih, preglednih, razumljivih in lahko dostopnih oblikah ter v jasnem in preprostem jeziku. Informacije in sporočila se posredujejo v posamezniku ustrezni obliki, ki je praviloma pisna, ali z drugimi sredstvi, zlasti z elektronskimi sredstvi. V tretjem odstavku je določeno, da mora upravljavec posamezniku, na katerega se nanašajo osebni podatki, olajšati uveljavljanje njegovih pravic, navedenih v prejšnjem odstavku tega člena.

### **K 16. členu:**

V predlaganem 16. členu je urejeno dajanje informacij za posameznika, na katerega se nanašajo osebni podatki, za področje izvajanja IX. dela tega zakona, gre za klasične podatke o identiteti upravljavca ipd.. V četrtem odstavku so urejene izjeme glede obveščanja posameznika (s sklicem na »zakonsko klavzulo«), za naslednje namene:

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

Posameznik načeloma nima pritožbe zaradi kršitve pravice do obveščanja, oziroma seznanitve, tako da bi jo vložil pri Informacijskem pooblaščenca. To pritožbo mora uveljavljati znotraj zadevnega

kaznovalnega ali drugega uradnega postopka (npr. preprečevanje pranja denarja in financiranja terorizma). V tem so preiskovalni organi izenačeni z neodvisnimi sodišči, v tem, da sami presojujejo zakonitost obdelave osebnih podatkov v okviru kaznovalne funkcije. Ne glede na to pa Informacijski pooblaščenec ostaja pristojen za nadzor nad zakonitostjo pridobivanja podatkov, hrambe in obdelave podatkov v evidencah, oziroma vpogledov v te evidence.

#### **K 17. členu:**

V 17. členu so urejene pravice posameznika, na katerega se nanašajo osebni podatki, do pridobitve teh podatkov. Po prvem odstavku se za namene iz IX. dela tega zakona (82. člen) določa, da ima vsak posameznik, na katerega se nanašajo osebni podatki, pravico, da od upravljavca prejme potrditev o tem, ali se v zvezi z njim obdelujejo osebni podatki in ima v tem primeru pravico pridobiti dostop do osebnih podatkov, ki se nanašajo nanj, ter naslednje informacije:

1. namene in pravno podlago za obdelavo;
2. vrste osebnih podatkov, ki se obdelujejo;
3. uporabnike ali kategorije uporabnikov, ki so jim bili ali jim bodo osebni podatki razkriti, zlasti uporabnike v tretjih državah ali mednarodnih organizacijah;
4. predvideni rok hrambe osebnih podatkov;
5. o obstoju pravice, da od upravljavca zahteva popravek ali izbris podatkov ali omejitev obdelave osebnih podatkov posameznika, na katerega se podatki nanašajo;
6. o obstoju pravice do vložitve pritožbe pri Informacijskem pooblaščenцу in njegovih kontaktnih podatkih; in
7. sporočilo, ki vsebuje osebne podatke, ki so predmet obdelave, in vse razpoložljive informacije o viru osebnih podatkov.

#### **K 18. členu:**

V 18. členu so urejene pravice do popravka ali izbrisa osebnih podatkov, do omejitve obdelave ter posebni ukrepi varnosti osebnih podatkov za potrebe IX. dela tega zakona.

#### **K 19. členu:**

V 19. členu je za potrebe izvajanja Splošne uredbe in Direktive določen postopek obravnavanja zahteve za dostop, popravek, izbris in omejitev glede delovanja Informacijskega pooblaščenca in sodelovanja z njim glede na člene 15 do 22 Splošne uredbe ter glede na člene 14 in 16 Direktive.

V desetem odstavku je določena posebnost postopka, po njej so upravljavec in obdelovalec ter, kadar obstajajo, njuni predstavniki, na zahtevo sodelujejo z Informacijskim pooblaščencom pri izvajanju njegovih nalog, če ne gre za vpliv na odločanje v prekrškovnem postopku. Kar pomeni, da je treba pred uvedbo prekrškovnega postopka je treba iz spisa zadeve izločiti tista dokazila, ki bi lahko kršila privilegij zoper samoobtožbo.<sup>53</sup>

#### **K 20. členu:**

---

<sup>53</sup> Glejte: odločba US, št. U-I-40/12, 11. 4. 2013; objava: Uradni list RS, št. 39/2013 in OdlUS XX, 5.

V 20. členu je določen ugovor v primeru nepopolne odločitve upravljavca glede posredovanja osebnih podatkov. Predlagano je, da če posameznik po prejeti odločitvi upravljavca meni, da osebni podatki, ki jih je prejel, niso osebni podatki, ki jih je zahteval, ali da ni prejel vseh zahtevanih osebnih podatkov, lahko pred vložitvijo pritožbe pri upravljavcu vloži obrazložen ugovor v roku 15 dni. Upravljavec mora o ugovoru odločiti kot o novi zahtevi v 5 delovnih dneh.

#### **K 21. členu:**

V 21. členu je določeno, da če upravljavec ne odloči o zahtevi posameznika v roku iz 19. člena ZVOP-2, lahko posameznik pri Informacijskem pooblaščenca vloži pritožbo zaradi molka. Če upravljavec zahtevo zavrne, lahko posameznik pri upravljavcu, če gre za javni sektor oziroma pri Informacijskem pooblaščenca, če gre za zasebni sektor vloži obrazloženo pritožbo v roku 15 dni od prejema obvestila ali odločbe upravljavca. Po drugem odstavku pravica strank do pregledovanja dokumentov v zadevah odločanja o posameznikovi pritožbi po določbah Zakona o splošnem upravnem postopku, do pravnomočnosti odločbe Informacijskega pooblaščenca - ne more vključevati pregledovanja upravne zadeve v delu, ki se nanaša na dokumente, ki so predmet zahteve in drugih dokumentov zadeve, iz katerih bi se dalo razbrati ali sklepati na vsebino zahtevanih osebnih podatkov. Smiselno enaka omejitev glede omejitev pravic do pregledovanja upravne zadeve velja tudi pri odločanju o zahtevi pri upravljavcu.

#### **K 22. členu:**

V 22. členu je določen postopek obravnavanja pritožbe, da namreč odloča Informacijski pooblaščenec ter kaj so dodatni možni pritožbeni razlogi.

#### **K 23. členu:**

V 23. členu so določena pooblastila Informacijskega pooblaščenca v pritožbenem postopku, konkretno glede državnih nadzornikov za varstvo osebnih podatkov, tako glede uporabe pooblastil iz Splošne uredbe, Zakona o inšpekcijskem nadzoru, dostopa do dokumentacije ipd. V šestem odstavku je določen možen ekonomičen pristop obravnavanja pritožb, za primere, ko tako narekuje učinkovitost postopka, lahko Informacijski pooblaščenec o pritožbi odloči z odločbo s skrajšano obrazložitvijo, v kateri poleg izreka navede le pravno podlago in temeljni razlog odločitve ter pravni pouk. Če po prejemu odločbe s skrajšano obrazložitvijo prosilec, organ ali stranski udeleženec najkasneje v 8 dneh neobvezujoče napove upravni spor zoper odločitev Informacijskega pooblaščenca, ta izda odločbo s polno obrazložitvijo v 15 dneh, s katero tudi razveljavi odločbo s skrajšano obrazložitvijo.

**K 24. členu:** V 24. členu so določene izjeme glede uveljavljanja pravic posameznika preko zakonitega zastopnika na področju zdravstvene dokumentacije. Omejitve so dopustne glede na določbe tretjega odstavka 38. člena Ustave Republike Slovenije<sup>54</sup>.

#### **K 25. členu:**

25. člen določa, da je za izvedbe upravne izvršbe v zvezi z odločbami, izdanimi v postopku v pritožbenem postopku je pristojen Informacijski pooblaščenec. Po drugem odstavku se upravna izvršba opravi na predlog posameznika na podlagi izvršljive odločbe in sklepa o dovolitvi izvršbe, in

---

<sup>54</sup> Glejte: odločba US, št. U-I 60/03, 4. 12. 2003, zlasti 30. točka; objava: Uradni list RS, št. 131/03 in OdlUS XII, 93.



sicer s prisilitvijo zoper upravljavca. Po tretjem odstavku zoper sklep o dovolitvi izvršbe ni pritožbe, dovoljen pa je upravni spor.

#### **K 26. členu:**

Bistvo 26. člena o stroških je, da se po prvem odstavku informacije in sporočila ter ukrepi iz II. dela zakona zagotavljajo brezplačno. Po drugem odstavku pa so določene izjeme, da se v določenih primerih očitno neutemeljenih zahtev ali njihove pretiranosti lahko zaračunajo razumne pristojbine, pri čemer se upoštevajo administrativni stroške posredovanja informacij ali sporočila oziroma izvajanja zahtevanega ukrepa po tem delu zakona. Posebni odstavki določajo, da izda pravilnike o zaračunavanju stroškov neodvisni in samostojni državni organ (Informacijski pooblaščenec), po predhodnem soglasju pristojnih ministrov.

#### **K 27. členu:**

Predlagani 27. člen ZVOP-2 določa omejitve pravic posameznikov. Po prvem odstavku se pravice posameznika iz tega dela zakona je mogoče z zakonom izjemoma omejiti iz razlogov navedenih v prvem odstavku členu 23 Splošne uredbe. Omejitve pa se lahko določijo samo pod pogojem, da je zakonska določba, ki določa takšno omejitev, v skladu s prvim odstavkom 8. člena ZVOP-2 (zakonska določba). Prav tako je določena sistemska izjema, da se ne glede na določbe prvega odstavka in še zlasti v primerih obdelave osebnih podatkov v okviru strokovnih mnenj, izdelanih v skladu z določbami zakonov, ki urejajo sodne ali upravne ali nadzorne postopke, v primeru, kadar se posameznik, na katerega se nanašajo osebni podatki, navaja netočnost in neposodobljenih svojih osebnih podatkov, posamezniku dati na razpolago možnost za nasprotni prikaz dejstev, v okviru njegove pravice do ugovora. Upravljavec mora nasprotni prikaz dejstev priložiti dokumentom (posebni uradni zaznamek) ali ustrezno označiti na njih, kje se ta prikaz nahaja.

#### **K 28. členu:**

V 28. členu je posebej urejeno sodno varstvo posameznika. V prvem odstavku je določeno, da posameznik, ki ugotovi, da so kršene njegove pravice, določene s tem zakonom, lahko zahteva sodno varstvo ves čas, dokler kršitev traja. V drugem odstavku je določeno, da če je kršitev iz prvega odstavka prenehala, lahko posameznik vloži tožbo za ugotovitev, da je kršitev obstajala, če mu v zvezi s kršitvijo ni zagotovljeno drugo sodno varstvo. V tretjem odstavku je določeno, da v sodnem postopku odloča pristojno sodišče po določbah Zakona o upravnem sporu, kolikor ta zakon ali drug zakon ne določa drugače (zoper javnopravnega upravljavca se toži pred Upravnim sodiščem Republike Slovenije po določbah Zakona o upravnem sporu, zoper zasebnopravnega pa pred okrožnim ali okrajnim sodiščem in se uporabljajo določbe Zakona o pravnem postopku ter deloma tudi določbe Obligacijskega zakonika). Po tretjem odstavku je možno izključiti javnost iz sodne postopka, razen če sodišče na predlog posameznika, na katerega se nanašajo osebni podatki, iz utemeljenih razlogov ne odloči drugače. Sodni postopek je prednosten (ni pa nujen).

### **5. K IV. delu Predloga ZVOP-2:**

#### **K 29. členu:**

Ena od ključnih novosti Splošne uredbe v primerjavi z veljavno Direktivo je uzakonitev obveznosti upravljavca, da ves čas izvajanja obdelav skrbi za skladnost teh obdelav s pravili te uredbe oziroma drugih predpisov o varstvu osebnih podatkov, ter da to izvajanje tudi ustrezno dokumentira.

Upravljavec mora v ta namen v svojih internih aktih določiti postopke in ukrepe za zagotovitev skladnosti (kar je dosedaj veljalo zgolj za ukrepe za zavarovanje osebnih podatkov oz. za pogodbeno

obdelavo - drugi odstavek 25. člena oz. drugi odstavek 11. člena ZVOP-1). V primeru bolj tveganih obdelav mora določiti tudi splošno politiko varstva osebnih podatkov, ki naj vključuje ukrepe kot so ozaveščanje in usposabljanje svojih zaposlenih, upravljanje njihovih pooblastil za dostop do oz. za obdelavo podatkov, določitev odgovornih oseb za posamezne zbirke osebnih podatkov ter pravila za izvajanje revizij. Primerne postopek oziroma ukrepe, oziroma vsebino politike varstva osebnih podatkov določi na podlagi tveganosti posamezne obdelave, v skladu s kriteriji, kot so določeni v uvodnih navedbah št. 75 in 76 Splošne uredbe. Pri najbolj tveganih ukrepih se priporoča uporaba katerega od veljavnih mednarodnih standardov na tem področju.

Upravljavca mora tako predpisane ukrepe tudi ves čas izvajati in o tem voditi vsaj potrebno dokumentacijo, s katero lahko skladnost dokazuje tudi za nazaj. Ta dokumentacija naj vsebuje zlasti evidenco obdelav pri upravljavcu, oceno učinkov teh obdelav za varstvo osebnih podatkov (izdelano po ustrezni metodologiji, upošteva tveganost obdelave), popis sredstev obdelave, popis dostopnih pravic zaposlenih, pogodbenih partnerjev in drugih uporabnikov, ter rezultate rednih revizij skladnosti obdelave podatkov. Upravljavca lahko za pripravo in hrambo te dokumentacije pooblasti tudi pooblaščen osebo za varstvo osebnih podatkov, najame zunanje strokovnjake, oziroma pribavi ustrezno in za to namenjeno programsko opremo.

V skladu z usmeritvijo Splošne uredbe veljajo vse navedene obveznosti tudi za obdelovalce osebnih podatkov (glejte tudi obrazložitev k 31. členu). Navedeni glede njih odgovarjajo samostojno, ob tem pa za njih posebej odgovarja še upravljavca.

### **K 30. členu:**

Upravljavca mora po novem že pri snovanju novih obdelav preveriti, katere podatke resnično potrebuje za učinkovito izvajanje posamezne obdelave, ter potem te obdelave zasnovati tako, da ne zahtevajo zbiranja dodatnih podatkov (vgrajeno varstvo osebnih podatkov).

Obenem mora upravljavca svoje obdelave v čim večji meri zasnovati tudi tako, da v vsakem posamičnem primeru pridobijo in obdelajo samo tiste podatke, ki so potrebni v tem primeru. To pri obdelavah, ki se izvajajo s sredstvi informacijske tehnologije pomeni še zlasti, da se pred začetkom vsake obdelave ne naloži vseh podatkov, ki bi bili potrebni za tipično obdelavo te vrste, ampak, kolikor je le mogoče, zgolj tiste podatke, ki jih potrebuje ta konkretna obdelava (privzeto varstvo osebnih podatkov).

### **K 31. členu:**

Tako kot že dosedaj (11. člen ZVOP-1) lahko upravljavca posamezna opravila v zvezi z obdelavo osebnih podatkov prepusti obdelovalcu (dosedanjemu "pogodbenemu obdelovalcu"). Podobno kot dosedaj mora njuna medsebojna razmerja še vedno urediti v pisni pogodbi ali drugem podobnem sporazumu, pri čemer pa mora ta pogodba zdaj zagotoviti izvajanje vseh obveznosti po tem zakonu, ne zgolj obveznosti varstva (zavarovanja) obdelave, kot dosedaj. Po novem namreč za obdelovalca veljajo enake obveznosti kot za upravljavca, razen tistih obveznosti, ki so posebej pridržane upravljavcu.

Upravljavca ne sme skleniti takšnega sporazuma z obdelovalcem, ki ni sposoben dati zagotovila, da bo lahko zagotovil spoštovanje teh obveznosti. Prav tako obdelovalec ne sme dalje prenesti posameznih opravil na druge obdelovalce, brez da bi mu upravljavca do izrecno dovolil, ali vsaj bil s tem seznanjen in imel možnost izbiri podobdelovalca nasprotovati.

Vsebina sporazuma med upravljavcem in obdelovalcem ostaja podobna kot dosedaj, seveda z dodanimi novostmi Splošne uredbe.

### **K 32. členu:**

Navedeni člen posodablja dosedanji sistem zavarovanja osebnih podatkov iz 24. člena ZVOP-1, vse ob upoštevanju tehnološkega razvoja in z njim nastalih dodatnih tveganj, ki so nastala v letih po uveljavitvi dosedanjega zakona o varstvu osebnih podatkov. Za tovrstne postopke in ukrepe se po novem uporablja izraz "varnost podatkov", ter pri tem našteva vse sodobne poslovne procese na tem področju, kot so psevdonimizacija, blokiranja oziroma šifriranje podatkov, zagotavljanje celovitosti podatkov, zagotavljanje razpoložljivosti podatkov, ter zagotavljanje varnosti podatkov.

Navedeno se zagotavlja zlasti z namenskimi informacijskimi orodji, kot so

- orodja, tehnike in mehanizmov za zagotavljanje zaupnosti, celovitosti in razpoložljivosti komunikacijskih omrežij,
- orodja za preverjanje identitete uporabnikov,
- orodja za upravljanje pooblastil za dostop,
- orodja za zaščito pred zlonamernimi kodami,
- orodja za beleženje dejavnosti kritične informacijske infrastrukture in pomembnih informacijskih sistemov, njihovih uporabnikov in administratorjev,
- orodja za zaznavanje poskusov vdorov in preprečevanje incidentov,
- orodja za šifriranje, anonimiziranje, psevdonimiziranje oziroma blokiranje podatkov.

### **K 31.a členu**

Splošna uredba prinaša pomembno administrativno razbremenitev za večino upravljavcev, in sicer, da Informacijskega pooblaščenca več ne bo potrebno vnaprej obveščati o vzpostavitvi novih zbirk osebnih podatkov oziroma spremembah obstoječih zbirk (25. in 26. člen ZVOP-1 v zvezi s 7. členom - izjeme za manjše upravljavce). Nova ureditev tako predvideva zgolj še obveznost vodenja evidence dejavnosti obdelav, pa še to zgolj za večje upravljavce (z vsaj 250 zaposlenimi) oziroma upravljavce, ki redno izvajajo tvegane obdelave. Obvezna vsebina evidence je zdaj bistveno ožja kot prej, saj vsebuje le še 8 točk namesto prejšnjih 13, pri čemer gre pri vseh za že obstoječe kategorije, kar bo omogočalo migracijo obstoječih katalogov zbirk osebnih podatkov v novo evidenco.

Namen evidence je zlasti pomagati pri dokazovanju skladnosti obdelav (29. člen predloga) v morebitnih kasnejših postopkih nadzora s strani Informacijskega pooblaščenca, prav tako pa ostaja koristna tako za lasten pregled dejavnosti obdelave osebnih podatkov, kot tudi za obravnavo zahtev posameznikov za pridobitev lastnih osebnih podatkov (17. člen). Člen je trenutno (v tej fazi) označen kot 31.a člen, v končni verziji bo moral biti predstavljen v obliko normalnega običajnega številčenja.

### **K 32. členu**

Zadevni člen nadomešča dosedanji izraz "zavarovanje osebnih podatkov" (24. člen ZVOP-1) s pojmom "varnost osebnih podatkov". Sprememba seveda ni samo terminološka, ampak je vezana zlasti na spremenjene tehnološke realnosti, ki so nastopile v času od uveljavitve ZVOP-1. Vsesplošna informatizacija postopkov obdelave osebnih podatkov je namreč poleg številnih prednosti prinesla tudi nekatere probleme, zlasti glede zagotavljanja varnosti obdelav.

Uvodna konstrukcija člena ostaja enaka kot pri dosedanjem ZVOP-1, in sicer se poudarja, da je skrb za varnost zaveza tako obdelovalca kot upravljavca, gre pa za to, da podvzameta ustrezne tehnične ukrepe, da se v čim večji meri prepreči kršitve varstva osebnih podatkov.

Drugi odstavek primeroma našteva nekatere najbolj tipične varnostne ukrepe, tj. uporabo psevdonimiziranja oziroma šifriranja, izvajanje glavnih premis informacijske varnosti (zaupnost, celovitost, dostopnost sistemov), izdelovanje varnostnih kopij in sposobnost njihove obnove, ter

zavarovanje osebnih podatkov med prenosom po telekomunikacijskem omrežju. Novi, oziroma točneje, izrecno določeni sta tako zgolj alineja d), ki zahteva, da se navedene ukrepe varstva osebnih podatkov periodično pregleduje, ter tč. f) zadosti dolgo vodenje dnevniških sledi o dejanjih obdelave osebnih podatkov.

Zadnje navedena novost je predlagana zlasti na pobudo Informacijskega pooblaščenca oziroma njegovih pomislekov iz prakse, kjer se pri številnih nadzornih postopkih pri večjih upravljavcih še vedno dogaja, da kljub izvajanju tveganih obdelav še vedno ne vodijo revizijskih sledi v takšni kvaliteti, ki bi v primeru zlorab omogočali odgovor na vprašanje, katera oseba je kdaj dostopala do katerih podatkov, ter kakšen okvirni namen je pri tem imela. Iz tega razloga se obveznost vodenja revizijskih sledi izrecno predpisuje v minimalnem roku 5 let od preteka leta, v katerem se je zgodila obdelava, razen če področni zakon določa drug rok.

### **K 33. členu**

Ti. "*breach notification*" (obvestilo o kršitvi) v slovensko zakonodajo o varstvu osebnih podatkov prihaja sorazmerno pozno (zvezna država Združenih držav Amerike Kalifornija je to za področje varstva osebnih podatkov uvedla že leta 2003<sup>55</sup>). Poznata ga npr. že 81. člen (zlasti četrti odstavek) Zakona o elektronskih komunikacijah ozir. zdaj še aktualni Predlog Zakona o informacijski varnosti. Gre za pravilo da morajo upravljavci v primeru odkritih varnostnih napadov oz. drugih incidentov le te sporočiti Informacijskemu pooblaščenca, da ta lahko ukrepa in določi primerne ukrepe za ustavitev oziroma razrešitev varnostnega incidenta.

Pri tem Informacijskega pooblaščenca ne bo potrebno obveščati o vsakem odkritem (ali osumljenem) varnostnem incidentu, ampak zgolj o tistih, za katere je verjetno, da so oz. še bodo povzročili tveganje za posege v človekove pravice in temeljne svoboščine posameznikov. Ključna razlika bo zlasti v primerih napadov na dosegljivost informacijskega sistema (ti. »availability napadi«, med njimi zlasti DDOS), kjer gre za varnostni incident, ni pa nujno, da je prišlo tudi do kršitve varstva osebnih podatkov.

Rok za obveščanje je čim prej po odkritju incidenta ("brez nepotrebnega odlašanja"), vendar najkasneje v 72 urah, po tem pa le, če za zamik obstajajo opravičljivi razlogi. Bistvo tega roka je, da lahko Informacijski pooblaščenec čim prej odredi morebitne ukrepa za varstvo osebnih podatkov, kot tudi v tem, da v primeru najresnejših kršitev skupaj z upravljavcem oziroma obdelovalcem, pri katerem je prišlo do incidenta, premisli, ali je potrebno o njem obvestiti tudi končne uporabnike, zato da lahko podvzamejo ustrezne ukrepa za zaščito njihovih osebnih podatkov.

Obveščati je zatorej treba tudi v primerih, ko upravljavec incidenta še ni povsem raziskal, in ko tudi morda še ne ve dokončno, ali sploh je, ter v kakšnem obsegu, prišlo do zlorabe (zlasti odtujitve) osebnih podatkov. Takšen pristop izvira iz izkušenj z informacijsko-varnostne sfere, saj bi čakanje na dokončno raziskanost incidenta lahko povzročilo znatno dodatno škodo posameznikom zaradi zlorab njihovih podatkov v vmesnem času.

Dodatna novost pa je še v tem, da mora upravljavec takoj po odkritju varnostne grožnje pristopiti k zavarovanju dokazov o dogodku, za primer, če bi bilo kasneje potrebno za ugotavljanje okoliščin in dometa vloma.

Dodajamo, da je posamezne vidike notifikacijske dolžnosti že obravnavala Delovna skupina po členu 29 Direktive 95/46/ES, in o tem izdala svoje mnenje<sup>56</sup>.

### **K 34. členu**

<sup>55</sup> Glejte: Database Breach Notification Security Act ("SB 1386") iz leta 2003 (zadnjič spremenjen leta 2015).

<sup>56</sup> Glejte: WP250 z dne 3.10.2017, Guidelines on Personal data breach notification under Regulation 2016/679.

V primerih suma hujših incidentov, tj. ko je med preiskavo incidenta verjetno, da če da so ozir. bodo nas tala velika tveganja za človekove pravice in temeljne svoboščine posameznikov, mora upravljavec o incidentu obvestiti tudi svoje uporabnike, zato da lahko podvzamejo ustrezne zaščitne ukrepe.

### **K 35. členu**

Za večje in z vidika obdelave osebnih podatkov bolj intenzivne nove projekte bo v skladu s Splošno uredbo potrebno že v fazi načrtovanja pripraviti poseben dokument z oceno vseh učinkov na pravice posameznikov, katerih podatki se bodo obdelovali. Takšnemu dokumentu se pravi Ocena učinkov v zvezi z varstvom osebnih podatkov, oz. angl. Data Protection Impact Assessment, DPIA). Gre za ukrep, ki se močno povezuje z obveznostjo vgrajenega in privzetega varstva osebnih podatkov (30. člen), zato ga je treba izvesti še v fazi načrtovanja projekta obdelave osebnih podatkov.

DPIA ni obvezna za vse projekte. Dobro pravilo je, da bodo upravljavci, ki bomo morali imeti pooblaščen osebno za varstvo osebnih podatkov, za vsaj nekatere od svojih projektov potrebovali tudi DPIO. Splošna uredba to izrecno pripozna in upravljavca napotuje, da pri sestavi pridobi pomoč te osebe.

Bistvo DPIE ni v popisu obdelav osebnih podatkov oziroma iskanju pravne podlage za njih, ampak v identifikaciji, kategorizaciji ter ovrednotenju tveganj, ki bi lahko nastala pri obdelavah, ter potem iskanju rešitev, ki bi, vsaka posebej oziroma vse skupaj, prispevale k zmanjšanju tako najdenih tveganj.

Podrobnosti za izvedbo ocene razlaga Informacijski pooblaščenec v svojih smernicah iz novembra 2017<sup>57</sup>.

### **K 36, 37. in 38. členu**

Trojica členov ureja vprašanje posredovanja osebnih podatkov drugemu upravljavcu, zaradi namenov, ki so pod njegovo kontrolo. V praksi gre pri tem zlasti za zahteve odvetnikov, policije, tožilstva in sodišč za posredovanje podatkov, relevantnih v tej ali oni zadevi.

Izhodiščno pravilo za posredovanje je, da gre zgolj za eno od oblik obdelave osebnih podatkov, in da mora torej zanj obstajati veljavna pravna podlaga, ki upravljavca zavezuje ali mu vsaj dovoljuje posredovanje. Naloga, da določi to pravno podlago, ter njeno podanost ustrezno izkaže, je na prosilcu za podatke. Ta mora imetniku podatkov poslati zahtevek, v katerem utemelji svojo pravno podlago. Šele na podlagi takšnega dopisa pa je potem mogoče pripraviti zaprosene podatke in jih tudi posredovati.

Dodatno se posebej zahteva vodenje revizijskih sledi o posredovanjih.

### **K 39. členu**

V navedenem členu se ohranja obstoječa pravica iz drugega odstavka 18. člena ZVOP-1. Pravica do vpogleda v osebni dokument tako ostaja definirana sorazmerno široko (vedno, ko je potrebno potrditi identiteto posameznika), medtem ko pravica fotokopiranja tega dokumenta ostaja pridržana bankam in drugim finančnim institucijam.

### **K 40. členu**

V navedenem členu se ohranja obstoječe omejitve pri povezovanju z nekaterimi evidencami posebnih vrst osebnih podatkov, in sicer, da je treba poleg EMŠO-a ozir. davčne številke kot vezni kriterij vnesti

---

<sup>57</sup> Glejte: [https://www.ip-rs.si/fileadmin/user\\_upload/Smernice\\_o\\_ocenah\\_ucinka\\_\\_DPIA\\_\\_nov2017.pdf](https://www.ip-rs.si/fileadmin/user_upload/Smernice_o_ocenah_ucinka__DPIA__nov2017.pdf)

vsaj še en drug podatek (priimek, rojstni datum, idr.). navedeno služi kot varovalka pred prehitrim in napačnim pripisovanjem dejstev iz teh evidenc napačni osebi.

#### **K 41. členu**

V navedenem členu se konkretizira obveznosti upravljavca do spoštovanja načela najkrajšega roka hrambe oziroma do spoštovanja obveznosti vgrajenega in privzetega varstva osebnih podatkov. Upravljavec je zlasti dolžan redno preverjati, ali sta nabor in čas hrambe podatkov še vedno sorazmerna, ter o tem voditi dokumentacijo za potrebe nadzor s strani Informacijskega pooblaščenca.

#### **K 42. členu:**

V 1. poglavju IV. delu Predloga ZVOP-2 se urejajo novi subjekti na področju varstva osebnih podatkov - pooblaščenec osebe za varstvo podatkov (*»data protection officers«*) ter certificiranje obdelav osebnih podatkov. Obveznost imenovanja pooblaščenec osebe za varstvo podatkov, njene naloge, ter njen položaj so urejeni v členih 37 do 39 Splošne uredbe. Določbe so v določenem delu neposredno uporabljive oziroma učinkovite, v določenem delu pa zahtevajo oziroma dovoljujejo podrobnejše urejanje v nacionalnih zakonih o varstvu osebnih podatkov. Glede pooblaščenec oseb za varstvo podatkov se najprej podrobno ureja delo in vloga oseb, ki znotraj upravljavcev ali obdelovalcev zagotavljajo varstvo osebnih podatkov, zlasti ko gre za tvegane ali množične obdelave osebnih podatkov. V skladu s prenovljenim pravnim okvirom varstva osebnih podatkov v Evropski uniji bodo upravljavci in obdelovalci primorani vprašanju skladnosti njihovih obdelav osebnih podatkov s pravili varstva osebnih podatkov namenjati več pozornosti in sredstev - še zlasti pa bodo morali v primerih, ko izvajajo večje število bolj tveganih obdelav osebnih podatkov, imenovati tudi osebo (zaposlenega ali zunanjo osebo), katere glavna (ne pa nujno edina) naloga bo skrbeti za izvajanje te skladnosti, odgovarjati na zahteve posameznikov v zvezi z obdelavami njihovih podatkov, ter vzdrževati določeno pojasnjevalno komunikacijo z državnim nadzornim organom za varstvo osebnih podatkov (Informacijskim pooblaščencom) – sodelovanje nižje intenzitete.

S predlagano ureditvijo se ne vzpostavlja reguliran poklic, temveč neodvisne osebe znotraj upravljavca ali obdelovalca, ki naj preprečijo tveganja ali kršitve varstva osebnih podatkov. Te pooblaščenec osebe so individualne osebe, delajo neodvisno, lahko jim pomagajo druge osebe, vendar je vedno lahko le ena oseba odgovorna za ti. notranje varstvo osebnih podatkov. Zakon tudi omogoča izbiro (imenovanje) zunanjih pooblaščenec oseb, omogoča tudi fleksibilnost, da lahko skupine gospodarskih družb, društva ipd. določijo eno pooblaščenec osebo, ki skrbi za notranje varstvo osebnih podatkov v več institucijah. Ta nova oseba bo po svojem delovanju in vplivu podobna dosedanjim notranjim revizorjem ali pooblaščenec osebam za skladnost poslovanja (*»compliance officer«*).

Imenovanje pooblaščenec osebe vsebinsko in stroškovno ni nujno (in zato tudi ne smiselno) za vse upravljavce in obdelovalce. Temu primerno Predlog ZVOP-2 v 43. členu (po vzoru člena 37 Splošna uredbe) imenovanje pooblaščenec osebe zahteva zgolj za upravljavce in obdelovalce v javnem sektorju (katerih obdelave se, ker se izvajajo neodvisno od privolitve posameznika, že na splošno morajo presojati strožje), ter za tiste upravljavce iz zasebnega sektorja, ki izvajajo bolj tvegane obdelave osebnih podatkov. Pod slednjim so mišljene takšne obdelave, ki zajemajo obsežno in številčno profiliranje ali podobno sledenje večjega števila posameznikov, oziroma v večjem obsegu obdelujejo posebne vrste osebnih podatkov (nekdanji občutljivi osebni podatki). Primeri takšnih obdelav bi lahko zajemali zlasti oblikovanje profilov obiskovalcev spleta za potrebe oglaševanja, spremljanje nakupovalnih navad potrošnikov na podlagi kartic zvestobe, ali obdelava medicinskih podatkov posameznika v okviru zdravstvene dejavnosti.

V prvem odstavku 42. člena ZVOP-2 so določene splošne (sistemske) opredelitve pomena (poslanstva) pooblaščenec oseb za varstvo podatkov. Pooblaščenec oseba za varstvo podatkov je tako le oseba z ustreznimi poklicnimi odlikami in zlasti strokovnim znanjem ter dejanskimi izkušnjami o zakonodaji in praksi na področju varstva osebnih podatkov ali na primerljivem področju, ki upravljavcu ali obdelovalcu na neodvisen način pomaga pri zagotavljanju skladnosti obdelave osebnih podatkov s

pravili Splošne uredbe ter določbami tega zakona in drugih zakonov, ki urejajo obdelavo in varstvo osebnih podatkov. Po drugem odstavku dejanske izkušnje iz prvega odstavka vključujejo vsaj tri leta delovnih izkušenj s področja varstva osebnih podatkov ali področja informacijske varnosti ali področja poslovne skrivnosti po zakonu, ki ureja gospodarske družbe ali zaupnih podatkov po zakonu, ki ureja bančništvo. Predlog, ki ne določa samo delovne izkušnje s področja varstva osebnih podatkov, upošteva tudi sorodna področja, če so le-ta zadevala tudi področje varstva osebnih podatkov. Pri tem upošteva usmeritev iz petega odstavka člena 37 Splošne uredbe, po katerem se pooblaščen oseba imenuje na podlagi poklicnih odlik in zlasti (!) strokovnega znanja o zakonodaji in praksi na področju varstva podatkov ter zmožnosti za izpolnjevanje nalog iz člena 39 in del določbe uvodne navedbe št. 97, kjer je določeno: »Določiti bi bilo treba stopnjo potrebnega strokovnega znanja, zlasti glede na izvedena dejanja obdelave podatkov in varstvo, ki je potrebno pri osebnih podatkih, obdelanih s strani upravljavca ali obdelovalca.«

V 42. členu je tako podana opredelitev pooblaščen osebe, pri čemer je jasno poudarjeno, da gre za osebo, ki zgolj pomaga upravljavcu ali obdelovalcu zagotavljati skladnost njegovih obdelav osebnih podatkov z določbami Splošne uredbe. Obveznost zagotavljanja skladnosti obdelave osebnih podatkov z določbami Splošne uredbe, Direktive, ZVOP-2, področnih zakonov tako ostaja na upravljavcu oziroma obdelovalcu, oziroma se ta odgovornosti za kršitve skladnosti ne more rešiti s sklicevanjem na neustrezno delo pooblaščen osebe.

#### **K 43. členu:**

43. člen ZVOP-2 določa v prvem odstavku, da morajo pooblaščen osebo za varstvo podatkov imenovati vsi upravljavci ali obdelovalci v javnem sektorju (1. točka) – tukaj gre za pristop pomena oblastvene funkcije (pa četudi gre za nosilce javnih pooblastil). Po 2. točki istega odstavka morajo to osebo imenovati tudi tisti upravljavci ali obdelovalci v zasebnem sektorju, katerih temeljne dejavnosti zajemajo takšne obdelave osebnih podatkov, ki zaradi svoje narave, obsega oziroma namenov vključujejo redno, sistematično in obsežno spremljanje posameznikov, na katere se nanašajo osebni podatki. Presojajo, ali gre za takšne obdelave, je treba posebej opraviti pri upravljavci in pri obdelovalcu. Tako je možno, da bosta k imenovanju pooblaščen osebe zavezana oba, lahko pa samo eden od njiju. Npr. v primeru, ko manjši upravljavec uporablja določeno storitev obdelovalca, ki sicer je invazivna, vendar je ne uporablja v velikem obsegu, ta upravljavec ne bo zavezan k imenovanju pooblaščen osebe, obdelovalec, ki pa isto storitev ponuja številnim upravljavcem in jo zato opravlja v velikem obsegu, pa bo.

Natančnejša merila glede tega, kdaj se določene obdelave štejejo v temeljne dejavnosti, ter kdaj gre za obsežne in bolj invazivne obdelave, so podrobneje pojasnjena v Smernicah Delovne skupine po členu 29 Direktive 95/46/ES<sup>58</sup> na to temo.

Velika večina upravljavcev in obdelovalcev bo torej prosta te obveznosti. Bodo pa še vedno lahko pooblaščen osebo imenovali na prostovoljni podlagi, torej v primeru, če ocenjujejo, da jo potrebujejo. Zakon tudi ne predvideva dodatnih primerov, ko bi bilo imenovanje obvezno, lahko pa takšno možnost določijo posamezni področni zakoni.

Po 3. točki prvega odstavka morajo pooblaščen osebo imenovati tudi tisti upravljavci ali obdelovalci osebnih podatkov, katerih temeljne dejavnosti zajemajo obsežne obdelave posebnih vrst osebnih podatkov ali obsežne obdelave osebnih podatkov v zvezi s kazenskimi obsodbami in prekrški.

Po drugem odstavku lahko tudi ostali upravljavci ali obdelovalci prostovoljno imenujejo pooblaščen osebo in na ta način izkažejo kakovost njihovih obdelav osebnih podatkov.

Po tretjem odstavku morata upravljavec ali obdelovalec, ki sta imenovala pooblaščen osebo, v roku osmih dni od imenovanja vpisati njene kontaktne podatke po členu 30 Splošne uredbe v svoji evidenci dejanj obdelave, jih javno objaviti na primeren način ter jih sporočiti Informacijskemu pooblaščenju, ki teh podatkov ne objavi. Prav tako morata upravljavec ali obdelovalec s temi kontaktnimi podatki pod

---

<sup>58</sup> WP 243 rev.01, 5. 4. 2017, dostopne na: [http://ec.europa.eu/newsroom/document.cfm?doc\\_id=44100](http://ec.europa.eu/newsroom/document.cfm?doc_id=44100)

pogoji iz členov 13 ali 14 Splošne uredbe seznaniti posameznike, na katere se nanašajo osebni podatki – katerih osebne podatke obdeluje.

#### **K 44. členu:**

V 44. členu ZVOP-2 so določeni pogoji za imenovanje pooblaščenih oseb za varstvo podatkov. Po prvem odstavku je za pooblaščen osebno lahko določen posameznik ali posameznica, ki izpolnjuje pogoje iz petega odstavka člena 37 in drugega stavka šestega odstavka člena 38 Splošne uredbe in drugega odstavka 42. člena tega zakona.

Po drugem odstavku je dodatno za javni sektor določeno, da je pooblaščen osebno lahko imenovan posameznik, ki poleg pogojev iz prvega odstavka izpolnjuje še naslednje pogoje, da je namreč:

1. državljan Republike Slovenije ali države članice Evropske unije ali države članice Evropskega gospodarskega prostora in aktivno obvlada slovenski jezik,
2. poslovno sposoben,
3. ima vsaj univerzitetno izobrazbo ali končan magistrski študijski program
4. ima vsaj tri leta delovnih izkušenj s področja varstva osebnih podatkov ali področja informacijske varnosti ali področja poslovne skrivnosti po zakonu, ki ureja gospodarske družbe ali zaupnih podatkov po zakonu, ki ureja bančništvo (podobno kot v drugem odstavku 42. člena ZVOP-2),
4. je zaposlen v javnem sektorju, ter
5. ni bil pravnomočno obsojen na kazen najmanj šestih mesecev zapora, oziroma ni bil pravnomočno obsojen za kaznivo dejanje glede zlorabe osebnih podatkov ali kraje identitete.

Za javni sektor torej drugi odstavek 32. člena v skladu s splošno pooblastilno klavzulo iz drugega odstavka člena 6 Splošne uredbe določa še nekatere dodatne pogoje za imenovanje pooblaščenih oseb.

V tretjem odstavku je določena razumna izjema za javni sektor glede zaposlitve pooblaščenih oseb v javnem sektorju, da lahko namreč javni sektor lahko za pooblaščen osebno izjemoma s pogodbo v pisni obliki imenuje tudi posameznika ali posameznico iz zasebnega sektorja, ali pravno osebo zasebnega sektorja, če ta subjekt javnega sektorja nima več kot 20 zaposlenih (varianta: 30 zaposlenih) ter če njegovo delovanje ne vsebuje visoke stopnje tveganj obdelave osebnih podatkov za človekove pravice in temeljne svoboščine in interese posameznikov, ne gre za množične avtomatične obdelave osebnih podatkov, ne gre za redno, sistematično in obsežno spremljanje posameznikov ali njihovo profiliranje ter tudi za obdelavo posebnih vrst osebnih podatkov kot del primarne dejavnosti subjekta javnega sektorja. Pogoji so torej kumulativne narave. Izjema od te izjeme je določena v tretjem odstavku 47. člena Predloga ZVOP-2 – za ministrstva.

Po četrtem odstavku lahko zasebni sektor za pooblaščen osebno upravljavca ali obdelovalca s pogodbo v pisni obliki imenuje tudi posameznika ali posameznico, ki ni zaposlena pri upravljavcu ali obdelovalcu, ali pravno osebo, podano je torej splošno pooblastilo za zunanje izvajalce.

Po petem odstavku je obveznost, da morajo v primerih, kadar se v skladu s tretjim ali četrtem odstavkom 44. člena ZVOP-2 imenuje pravno osebo, vsi zaposleni in drugi sodelavci in pravne osebe, kateri bodo opravljali naloge pooblaščenih oseb, izpolnjevati pogoje za imenovanje v pooblaščen osebno. Prav tako mora biti v pogodbi s pravno osebo določen vodilni član (zaposleni) pravne osebe, ki odgovarja za delo pravne osebe in katerega kontaktne podatki bodo objavljeni v skladu določbami tretjega odstavka 43. člena tega zakona.

Predlagani šesti odstavek določa, da lahko pooblaščen osebno pri opravljanju njenih nalog pomagajo tudi druge osebe, ki so pri tem vezane na njena navodila. Te osebe morajo izpolnjevati pogoje za imenovanje za pooblaščen osebno. To pomeni, da je pooblaščen osebno funkcionalno in organizacijsko vedno le ena (ima lahko namestnika, ki jo v času odsotnosti polno nadomešča), je ti.



»vodilna oseba« in da torej tudi ni možno ustanoviti kolektivne pooblaščen osebe (kolegijski subjekt ali kolegijski »organ«). Ta vodilna oseba je hierarhično nadrejena ostalim članom skupine in odgovorna za delo. Seveda za pooblaščen osebo ne more biti imenovana oseba, ki ima konflikt interesov, tj. še zlasti, da v organizaciji, ki jo nadzira, opravlja druge naloge v zvezi z obdelavo osebnih podatkov. V teh primerih bi ta oseba namreč nadzirala samo sebe, kar bi izničilo namen instituta. Takšna oseba torej ne sme biti imenovana, seveda pa jo je treba tudi razrešiti, če ti pogoji nastopijo naknadno.

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

V osmem odstavku je prepoved iz sedmega odstavka podrobneje razdelana. Po njej se za javni sektor šteje, da ima določena oseba konflikt interesov, če ima položaj predstojnika ali drugega funkcionarja v subjektu javnega sektorja, če je član organov upravljanja ali nadzora pri upravljavcu ali obdelovalcu, če njene druge naloge vključujejo odločanje o obdelavi osebnih podatkov pri upravljavcu ali obdelovalcu, ali če zastopa upravljavca oziroma obdelovalca v sodnih ali arbitražnih postopkih v zvezi z vprašanji varstva osebnih podatkov. V primeru, da pooblaščen oseba izve za situacijo, ki predstavlja ali bi lahko predstavljala konflikt interesov, mora o tem takoj pisno obvestiti upravljavca oziroma obdelovalca. Upravljavec oziroma obdelovalec mora v tem primeru bodisi odpraviti konflikt bodisi pooblaščen osebo razrešiti ob upoštevanju določb tretjega in četrtega odstavka 48. člena ZVOP-2. Enako ravna v primeru, če se na drug način seznanijo z obstojem ali verjetnostjo obstoja konflikta interesov. Vse navedeno velja tudi za osebe, ki pooblaščen osebi pomagajo pri opravljanju njenih nalog.

#### **K 45. členu:**

V 45. členu je določena možnost imenovanja skupne pooblaščen osebe za varstvo podatkov. Več upravljavcev iz javnega sektorja ali več upravljavcev iz zasebnega sektorja lahko, upošteva njihovo delovno področje, organizacijsko strukturo in velikost, imenuje tudi skupno pooblaščen osebo (ne more pa del javnega sektorja skupaj z delom zasebnega sektorja imenovati skupne pooblaščen osebe). Pri tem morajo zagotoviti, da je pooblaščen oseba še vedno sposobna opravljati svoje naloge v zvezi z vsemi upravljavci ali obdelovalci, za katere je imenovana. Upoštevana je torej možnost, da zaradi strogosti pogojev in pa zahtevnosti nalog pooblaščen osebe obstaja skrb, da bodo morale pooblaščen osebo za polni delovni čas imenovati tudi takšni subjekti, ki je v resnici ne rabijo večino časa v letu. Zato se daje družbam v povezani družbi, državnim organom, ter društvom ipd. možnost, da določijo skupno pooblaščen besedo.

Zakon torej z vidikov ekonomičnosti (stroški) in racionalnosti (izkušnje) omogoča izbiro (imenovanje) zunanjih pooblaščenih oseb. Tako omogoča tudi fleksibilnost, da lahko zlasti skupine gospodarskih družb, društva ipd. določijo eno pooblaščen osebo, ki skrbi za notranje varstvo osebnih podatkov v več subjektih.

#### **K 46. členu:**

46. člen Predloga ZVOP-2 določa naloge pooblaščen osebe za varstvo podatkov. Po prvem odstavku pooblaščen oseba opravlja naloge iz člena 39 Splošne uredbe. Po drugem odstavku pooblaščen oseba opravlja navedene naloge iz člena 39 Splošne uredbe v zvezi z vsemi obdelavami osebnih podatkov, ki jih izvaja upravljavec oziroma obdelovalec, pri katerem je imenovana. Po tretjem odstavku pooblaščen oseba sodišča ali državnega tožilstva ne sme opravljati navedenih nalog v zvezi z obdelavami osebnih podatkov, izvršenih v okviru izvajanja neodvisnega sodniškega odločanja (125. člen, prvi odstavek 23. člena Ustave Republike Slovenije, prvi odstavek 6. člena Evropske konvencije o človekovih pravicah) ali samostojnega opravljanja državnotožilske funkcije odločanja

(135. člen Ustave Republike Slovenije), kot ju opredeljujeta Zakon o sodiščih in Zakon o državnem tožilstvu. Pooblaščen osebni sme opravljati te naloge samo glede zadev sodne uprave (npr. kadri, finance, poslovna razmerja) in državno tožilske uprave ter glede izvajanja varnosti osebnih podatkov.

Za Ustavno sodišče Republike Slovenije je primerljivo (kot za neodvisna sodišča) v četrtem odstavku določeno, da pooblaščen osebni Ustavnega sodišča Republike Slovenije ne sme opravljati navedenih nalog v zvezi z obdelavami osebnih podatkov, izvršenih v okviru odločanja Ustavnega sodišča Republike Slovenije, kot jih opredeljujejo Zakon o ustavnem sodišču ali drugi zakoni (npr. drugi odstavek 5.č člena Zakona o referendumu in ljudski iniciativi). Pooblaščen osebni sme opravljati te naloge samo glede zadev uprave Ustavnega sodišča (pretežno zadeve s področja odločanja upravne seje Ustavnega sodišča) ter glede izvajanja varnosti osebnih podatkov.

Po petem odstavku pooblaščen osebni Varuha človekovih pravic ne sme opravljati navedenih nalog v zvezi z obdelavami osebnih podatkov, izvršenih v okviru delovanja Varuha človekovih pravic, kot jih opredeljuje Zakon o varuhu človekovih pravic ali drug zakon, ki ureja pristojnosti ali naloge varuha človekovih pravic (npr. 5. člen izvedbenega dela Zakona o ratifikaciji Opcijskega protokola h Konvenciji proti mučenju in drugim krutim, nečloveškim ali poniževalnim kaznim ali ravnanju<sup>59</sup>). Varuh ima namreč položaj posebnega ustavnega organa (159. člen Ustave Republike Slovenije) ki kot *sui generis* ustavni organ izven trodelne veje oblasti neoblastno izvaja nadzor glede uresničevanja in varstva človekovih pravic ter temeljnih svoboščin v republiki Sloveniji in to neodvisno in samostojno (4. člen Zakona o varuhu človekovih pravic). Pooblaščen osebni za varstvo podatkov Varuha človekovih pravic sme opravljati te naloge samo glede zadev obdelav osebnih podatkov s področja zagovorništva otrok – 25.a-25.d člen Zakona o varuhu človekovih pravic (glede na posebno občutljivost področja ter dejstvo, da ne gre za nadzorno vlogo Varuha človekovih pravic, ampak za ti. »upravno pomožno delovanje« Varuha človekovih pravic) ter glede izvajanja varnosti osebnih podatkov.

#### **K 47. členu:**

V 47. členu Predloga ZVOP-2 je v prvem odstavku najprej določeno, da na Ustavnem sodišču Republike Slovenije Ustavno sodišče kot celota (plenarna seja) določi eno pooblaščen osebni, ki opravlja naloge v skladu s četrtem odstavkom 46. člena tega zakona. V drugem odstavku je določeno, da Varuh človekovih pravic (najvišji funkcionar) določi eno pooblaščen osebni, ki opravlja naloge v skladu s petim odstavkom 46. člena tega zakona. V tretjem odstavku je določeno strogo pravilo, po katerem mora vsak minister ali ministrica določiti svojo pooblaščen osebni, 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<sup>60</sup>).

Za področja obveščevalno-varnostne dejavnosti je v četrtem odstavku določeno, da predstojnik organizacije (Slovenska obveščevalno-varnostna agencija, Obveščevalno varnostna služba Ministrstva za obrambo) s tega področja določi eno pooblaščen osebni in njenega namestnika znotraj organizacije s tega področja, ki opravlja tiste naloge iz člena 39 Splošne uredbe, za katere tako določi predstojnik, med njih pa so obvezno vključene naloge glede izvajanja varnosti osebnih podatkov ter posredovanja osebnih podatkov Vladi Republike Slovenije, Predsedniku Republike Slovenije, policiji, državnim tožilstvom ali sodiščem ali pristojnemu delovnemu telesu Državnega zbora Republike Slovenije, čezmejne obdelave in prenosi.

#### **K 48. členu:**

Prvi odstavek določa, da morata upravljavec ali obdelovalec pooblaščen osebni zagotoviti pogoje za učinkovito in neodvisno opravljanje njenih nalog po 46. členu ZVOP-2, zlasti, da je pooblaščen osebni:

<sup>59</sup> Uradni list RS, št. 114/06 – Mednarodne pogodbe, št. 20/06.

<sup>60</sup> 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.

1. ustrezno in pravočasno vključena v vsa vprašanja in postopke, povezane z varstvom osebnih podatkov in ima možnost podati ustrezeni nasvet, mnenje ali predlog,
2. ima dostop do vseh osebnih podatkov ter dejanj obdelave,
3. ima na razpolago sredstva, potrebna za izvajanje njenih nalog in za ohranjanje njenega strokovnega znanja,
4. lahko posamezniki, na katere se nanašajo osebni podatki, z njo v slovenščini ali v drugem uradnem jeziku Republike Slovenije vstopijo v stik in se posvetujejo glede vseh vprašanj, povezanih z obdelavo njihovih osebnih podatkov in uresničevanje njihovih pravic po Splošni uredbi, ter
5. da ima neposredni dostop do vodstva upravljavca ali obdelovalca, če oceni, da je to zaradi pomembnosti določene obdelave osebnih podatkov nujno potrebno, zlasti kadar gre za tvegane obdelave, obdelave posebnih vrst osebnih podatkov, množične obdelave in vpliv na človekove pravice, temeljne svoboščine ali interese posameznikov, na katere se nanašajo osebni podatki ali za očitno neustreznost ukrepov zavarovanja osebnih podatkov, neposredni dostop vključuje možnost predstavitve stališč ali ocen o neustreznosti varstva osebnih podatkov.

Po drugem odstavku morata upravljavec ali obdelovalec zagotoviti, da pooblaščen osebni pri izvajanju svojih nalog ne prejema nobenih navodil. Pooblaščen osebni o svojem izvedenem delu neposredno in neodvisno poroča vodstvu upravljavca ali obdelovalca (omogočen torej neposreden neoviran pristop ter zagotovljen neodvisen način dela).

Po tretjem odstavku upravljavec oziroma obdelovalec pooblaščen osebni za varstvo podatkov zaradi izvajanja njenih nalog ne sme razrešiti, je kaznovati ali je zapostavljati (kar je del jamstva neodvisnosti iz drugega odstavka).

Po četrtem odstavku je odpoved delovnega razmerja pooblaščen osebni prepovedana za čas njenega imenovanja in še eno leto po prenehanju imenovanja, razen v primeru redne odpovedi iz razloga nesposobnosti ali krivdnega razloga, izredne odpovedi, odpovedi v postopku prenehanja delodajalca, oziroma če v primeru poslovnega razloga odkloni ponujeno ustrezno zaposlitev pri delodajalcu. V primeru statusne spremembe delodajalca, pooblaščen osebni ohrani svoj položaj pooblaščen osebni, če pri delodajalcu prevzemniku še naprej obstaja obveznost imenovanja v skladu s tem zakonom. Na ta način je ponovno zagotovljena neodvisnost pooblaščen osebni, njen položaj je urejen primerljivo določena podobna jamstva kot za sindikalnega zaupnika po določbah Zakona o delovnih razmerjih.

#### **K 49. členu:**

V 49. členu Predloga ZVOP-2 je v prvem in drugem odstavku posebej urejena dolžnost varovanja tajnosti osebnih podatkov (glede na drugi odstavek 1. člena ZVOP-2, ki izhaja iz drugega odstavka 38. člena Ustave Republike Slovenije), še posebej v razmerju do varovanja identitete posameznikov in posameznic, katerih pritožbe obravnava pooblaščen osebni.

Tretji odstavek predlaganega člena določa, da če ima pooblaščen osebni pri svoji dejavnosti vpogled v osebne podatke, v zvezi s katerimi ima osebni, ki je podvržena nadzoru pooblaščen osebni, pravico do molka, ta pravica velja tudi za pooblaščen osebni in za v njenem imenu delujoče osebni, in sicer do mere, v kateri je osebni, ki ima zakonsko pravico do molka, slednjo uveljavila. Gre za smiselni in delni element privilegija zoper samoobtožbo.

#### **K 50. členu:**

V 2. poglavju IV. dela Predloga ZVOP-2 so od 50. do 52. člena določena pravila glede samoregulacije (kodeksi ravnanja) na področju varstva osebnih podatkov, njihove veljavnosti, certifikacijskega postopka ter pristojnost certificiranja (Slovenska akreditacija).

Modernizacija pravil varstva osebnih podatkov ima za posledico tudi, da so postala ta pravila znatno številčnejša, obsežnejša in vse bolj zapletena. Temu primerno se povečuje tudi potreba po nadzoru nad izvrševanjem teh pravil, ki pa jih, glede na vseprisotnost in obsežnost obdelav osebnih podatkov v današnji družbi, ni v celoti več mogoče zagotoviti skozi delo državnega nadzornega organa (Informacijski pooblaščenec).

Posledično se po zgledu številnih drugih področjih državno regulacijo dopolnjuje z instrumenti samoregulacije, kot so prostovoljne zaveze podjetij, da bodo pri svojem poslovanju spoštovala določene kodekse ravnanja, oziroma, da bodo svoje poslovne procese predala v neodvisno zunanjo revizijo certifikacijski agenciji, ki jim bo v primeru skladnosti tudi izdaja ustreznih certifikat. Takšna potrdila imajo številne prednosti; poleg olajšanega izvajanja inšpekcijskega nadzora predvsem vzbujajo zaupanje posameznikov, na katere se nanašajo osebni podatki, da upravljavci oziroma obdelovalci njihove podatke obdelujejo v skladu s pravili, ter da temu posvečajo zadostna sredstva.

Ta razdelek Predloga ZVOP-2 ureja obe pojavniki obliki takšne samoregulacije, in sicer tako kodekse ravnanja kot tudi certifikacijo. Pri kodeksih ravnanja sicer ne implementira možnosti zunanjega nadzora s strani pooblaščenih organizacij. Pri certifikaciji to prepušča tako Informacijskemu pooblaščenec kot morebitnim zunanjim certifikacijskim organizacijam, ki jih za to pooblasti nacionalni akreditacijski organ (Slovenska akreditacija). Za vsebine certifikacij (standarde) se v veliki meri zanaša na standarde, sprejete na evropski ravni, in odobrene s strani Informacijskega pooblaščenca.

V predlaganem 50. členu se tako ureja kodekse ravnanja - podana je pravna podlaga, ki omogoča uporabo kodeksov ravnanja, tj. pravil dobre prakse na področju posameznih vrst obdelav osebnih podatkov, ki jih pripravijo relevantna domača ali tuja združenja podjetij v določenem sektorju, in so že prilagojena posebnostim manjših, srednjih oziroma večjih podjetij. Člen predvideva uporabo kodeksov, ki so potrjeni na različnih nivojih nadzornih organov; tako s strani posameznega državnega nadzornega organa, kot tudi širše, s strani Evropskega Odbora za varstvo osebnih podatkov po členu 68 Splošne uredbe kot s strani Evropske komisije. Pri tem Evropska komisija potrjuje tiste kodekse, ki se nanašajo na obdelave, ki potekajo v več državah članicah, pri čemer mora predhodno pridobiti tudi mnenje Odbora.

Člen hkrati omogoča, da lahko Informacijski pooblaščenec razveljavi uporabo določenega kodeksa, če oceni, da ni oziroma da ni več ustrezen. Navedeno izhaja iz sodbe Sodišča Evropske unije v primeru *Maximilian Schrems* (ozir. ti. *Facebook primer*)<sup>61</sup>, 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:**

V 51. členu Predloga ZVOP-2 se ureja certificiranje obdelav osebnih podatkov. V prvem odstavku je tako določena definicija certificiranja, ki za potrebe tega zakona pomeni prostovoljni postopek ugotavljanja, ali so dejanja obdelave osebnih podatkov s strani upravljavcev in obdelovalcev skladna z merili iz določenega mehanizma certificiranja (vsebinski kriterij) ter da se o ugotovitvi takšne skladnosti se upravljavcu ali obdelovalcu izda certifikat (oblastveni kriterij). Predmet certificiranja je lahko zbirka, njena delovanja obdelave ter informacijski sistem - Klub zvestobe trgovinske gospodarske družbe, sistem SISBON, eAsistent informacijski sistem za šole, informacijski sistem za bolnišnico.

Po drugem odstavku merila posameznega certifikacijskega mehanizma pripravi upravljavec ali obdelovalec. Odobri jih z odločbo Informacijski pooblaščenec v skladu s petim odstavkom člena 42 Splošne uredbe ali Evropski Odbor za varstvo osebnih podatkov v skladu s petim odstavkom člena 42 Splošne uredbe ter v zvezi s členom 63 Splošne uredbe. Zoper odločbo Informacijskega pooblaščenca iz prejšnjega stavka pritožba ni dopustna, je pa dopusten upravni spor pred Upravnim sodiščem Republike Slovenije.

<sup>61</sup> Sodba SEU, C-362/14, 6. 10.2015.

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 njihovih delovanj obdelave osebnih podatkov s Splošno uredbo in ne posega v naloge in pristojnosti Informacijskega pooblaščenca za ugotavljanje te skladnosti.

Po predlaganem četrtem odstavku se certifikat izda upravljavcu ali obdelovalcu za obdobje največ treh let in se pod enakimi pogoji lahko tudi podaljša, če so zahtevani pogoji certifikacijskega mehanizma še naprej izpolnjeni.

Po petem odstavku mora upravljavec ali obdelovalec, ki svoje obdelave osebnih podatkov predloži v mehanizmu certifikacije, telesu, ki izvaja certifikacijo, zagotoviti dostop do vseh informacij oziroma dostope do svojih dejanj obdelave, ki so potrebne za izvedbo postopka certifikacije.

Po šestem odstavku lahko Informacijski pooblaščenec z odločbo po uradni dolžnosti razveljavi certifikat, če ugotovi, da zahteve v zvezi z njim niso bile ali niso več izpolnjene. Zoper to odločbo pritožba ni dopustna, je pa dopusten upravni spor.

Po sedmem odstavku Informacijski pooblaščenec pripravlja in upravlja seznam pravnomočnih certifikacijskih mehanizmov, ki jih je odobril in ta seznam sprotno objavlja na svoji spletni strani.

#### **K 52. členu:**

V predlaganem 52. členu se glede na 121. člen Ustave Republike Slovenije smiselno predaja javno pooblastilo za izvajanje certificiranja telesom, ki jih na podlagi njihove vloge za to akreditira (ne pa izrecno pooblasti) nacionalni akreditacijski organ – to je Javni zavod Slovenska akreditacija, v skladu z določbami točke b prvega odstavka člena 43 Splošne uredbe in Zakona o akreditaciji<sup>62</sup> (torej tudi pooblastilo na podlagi zakona). Dodatne zahteve glede certifikacije v skladu s točko b prvega odstavka in tretjim odstavkom člena 43 Splošne uredbe določi Informacijski pooblaščenec.

Po drugem odstavku pred izdajo pooblastila zunanjemu certifikacijskemu telesu Slovenska akreditacija v skladu s prvim odstavkom člena 43 Splošne uredbe o vlogi zainteresiranega subjekta obvesti Informacijskega pooblaščenca, ki preveri izpolnjevanje dodatnih zahtev v skladu s točko b prvega odstavka in tretjim odstavkom člena 43 Splošne uredbe in o tem izda odločbo. Zoper to odločbo pritožba ni dopustna, je pa dopusten upravni spor pred Upravnim sodiščem Republike Slovenije.

Po tretjem odstavku Slovenska akreditacija na lastno pobudo ali na predlog Informacijskega pooblaščenca prekliče pooblastilo za certificiranje zunanjemu certifikacijskemu telesu, če je ugotovljeno, da pogoji za pooblastilo niso ali niso več izpolnjeni, ali, da so bili ukrepi, ki jih je v postopku certifikacije izvedlo pooblaščenec certifikacijsko telo, v neskladju s Splošno uredbo.

Predlagan je torej spodbujevalni mehanizem za varstvo osebnih podatkov, ki je le na razpolago in katerega je šteti, da utegne trajati daljše obdobje, preden bo v Republiki Sloveniji dejansko uporaben.

#### **5. K V. delu Predloga ZVOP-2:**

V. del Predloga ZVOP-2 je povezan (le) z IX. delom Predloga ZVOP-2, namreč potrebe (nameni) obdelave osebnih podatkov s strani pristojnih državnih organov ali organov samoupravnih lokalnih skupnosti ali nosilcev javnih pooblastil za namene preprečevanja, preiskovanja, odkrivanja ali pregona kaznivih dejanj ali prekrškov, izvrševanja nalog in pooblastil policije, varnosti države, obrambe države ter izvrševanja kazenskih sankcij, v skladu z določbami Direktive. Za druga področja prenosov ali čezmejnih obdelav veljajo neposredno določbe Splošne uredbe (členi 44. do 49.).

#### **K 53. členu:**

---

<sup>62</sup> Uradni list RS, št. 59/99.

V predlaganem 53. členu ZVOP-2 so določena splošna pravila za prenos osebnih podatkov ter glede čezmejne obdelave (za posredovanja osebnih podatkov med državami članicami Evropske unije). Po prvem odstavku določbe tega dela ZVOP-2 veljajo za primere, ko osebne podatke obdelujejo pristojni državni organi ali organi samoupravnih lokalnih skupnosti ali nosilci javnih pooblastil za namene preprečevanja, preiskovanja, odkrivanja ali pregona kaznivih dejanj ali prekrškov, izvrševanja nalog in pooblastil policije, varnosti države, obrambe države ter izvrševanja kazenskih sankcij, v skladu z določbami Direktive ter v zvezi z IX. delom tega zakona. Po drugem odstavku sme pristojni organ osebne podatke, ki so že obdelani ali naj bi se obdelali po prenosu tretji državi oziroma mednarodni organizaciji ali naj bi se čezmejno obdelovali, posredovati le, če so upoštevane določbe tega dela zakona in:

1. je prenos potreben za namene iz 82. člena tega zakona;
2. se osebni podatki posredujejo upravljavcu v tretji državi ali mednarodni organizaciji, ki je pristojni organ za izpolnitev enega od namenov iz 82. člena tega zakona;
3. je pristojna država članica v primerih, ko se osebni podatki posredujejo iz druge države članice Evropske unije ali tej dajo na razpolago, prenos vnaprej odobrila;
4. je Evropska komisija v skladu s 54. členom tega zakona sprejela sklep o ustreznosti ali, če tak sklep ne obstaja, so bili predloženi oziroma obstajajo ustrezni ukrepi v smislu 55. člena tega zakona ali je, če ne obstaja sklep o ustreznosti v skladu s 54. členom tega zakona in niso predložena ustrezna zagotovila v smislu 55. člena tega zakona, možno v skladu s 56. členom tega zakona uporabiti izjeme za določene primere in
5. je zagotovljeno, da je nadaljnji prenos tretji državi ali drugi mednarodni organizaciji dovoljen le na podlagi predhodne odobritve pristojnega organa, ki je izvedel prvotni prenos podatkov, in ob primernem upoštevanju vseh tehničnih meril, vključno z naravo ali težo kaznivega dejanja ali prekrška, namenom prvotnega prenosa osebnih podatkov in stopnjo varstva osebnih podatkov v tretji državi ali mednarodni organizaciji, ki se ji posredujejo osebni podatki oziroma jih posreduje naprej.

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

#### **K 54. členu:**

V 54. členu je urejen sistem prenosa osebnih podatkov na podlagi sklepa o ustreznosti varstva osebnih podatkov, ki ga izda Evropska komisija na podlagi tretjega odstavka člena 36 Direktive (izvedbeni akt), če pač odloči, da zadevna tretja država, njena regija oziroma eden ali več specifičnih sektorjev (javni sektor, zasebni sektor, deli zasebnega sektorja, deli javnega sektorja) v tej tretji državi ali zadevna mednarodna organizacija nudi ustrezno stopnjo varstva osebnih podatkov. Za tak prenos podatkov ni potrebna posebna odobritev nobenega drugega organa (ni potrebna naknadna odobritev). Ta Sklep Evropske komisije, sprejet v skladu s petim odstavkom člena 36 Direktive, ki se nanaša na preklic, spremembo ali odložitev izvajanja že izdanega sklepa po tretjem odstavku člena 36 Direktive ne vpliva na prenose osebnih podatkov tretji državi, regiji oziroma enemu ali več specifičnim sektorjem v tretji državi oziroma mednarodni organizaciji v skladu z 55. in 56. členom tega zakona.

#### **K 55. členu:**

Po 55. členu se lahko izvaja tudi prenos osebnih podatkov z uveljavljanjem ustreznih ukrepov varstva osebnih podatkov, namreč če ne obstaja sklep Evropske komisije v skladu s prvim odstavkom 54. člena tega zakona, je prenos osebnih podatkov v tretjo državo ali mednarodno organizacijo dopusten, če:

1. so v ustreznem pravnem aktu, ki je pravno obvezujoč, določeni ustrezni ukrepi za varstvo osebnih podatkov ali
2. je upravljavec po oceni vseh okoliščin, ki so pri prenosu pomembne, ugotovil, da dejansko obstajajo ustrezni ukrepi za varstvo osebnih podatkov.

V predlaganem drugem odstavku je določeno, da če v skladu z 2. točko prvega odstavka obstajajo ustrezni ukrepi za določene vrste prenosov, mora upravljavec o teh kategorijah prenosov obvestiti Informacijskega pooblaščenca, ki lahko odredi prepoved prenosa osebnih podatkov. Po tretjem odstavku je treba prenose v skladu z 2. točko prvega odstavka dokumentirati, dokumentacijo, ki vključuje datum in čas prenosa, informacije o pristojnemu organu prejemniku, utemeljitev prenosa in prenešene osebne podatke, pa je treba na zahtevo dati na razpolago Informacijskemu pooblaščenca.

#### **K 56. členu:**

V 56. členu so določene izjeme, ki urejajo dodatne možnosti prenosa osebnih podatkov, če ne obstajajo podlage po 54. in 55. členu ZVOP-2. Po prvem odstavku je prenos osebnih podatkov tretji državi ali mednarodni organizaciji dopusten le, če je prenos potreben:

1. za zaščito življenjsko pomembnih interesov posameznika (življenje in telo);
2. če je to predvideno zaradi varovanja zakonitih interesov posameznikov, na katere se nanašajo osebni podatki (obramba pred tožbo);
3. za odvrnitev neposredne in resne nevarnosti za javno varnost države članice Evropske unije ali tretje države (ne gre samo za varnost države);
4. v posameznem primeru za namene, navedene v 82. členu ZVOP-2, ali
5. v posameznem primeru za uveljavljanje, izvajanje ali obrambo pravnih zahtevkov v povezavi z nameni, navedenimi v 82. členu ZVOP-2.

Po drugem odstavku je v primerih iz 4. in 5. točke prvega odstavka prenos osebnih podatkov dovoljen le, če ni kršena nobena od nad javnim interesom prevladujočih temeljnih pravic in svoboščin posameznikov, na katere se osebni podatki nanašajo. Po tretjem odstavku za prenose v skladu s prvim odstavkom veljajo določbe tretjega odstavka 55. člena tega zakona (obveznost dokumentiranja).

#### **6. K VI. delu Predloga ZVOP-2:**

1. poglavje VI. dela Predloga ZVOP-2 ureja položaj in temeljne pristojnosti in naloge Informacijskega pooblaščenca kot nadzornega organa za varstvo osebnih podatkov Republike Slovenije.

#### **K 57. členu:**

Predlagani 57. člen ZVOP-2 ponovno potrjuje obstoječe in ustrezno stanje, da je nadzorni organ za varstvo osebnih podatkov Republike Slovenije Informacijski pooblaščenec, kot ga določa Zakon o informacijskem pooblaščenca<sup>63</sup>. Nato ponovi iz obstoječe ureditve, da je Informacijski pooblaščenec (javnopravno) samostojni in neodvisni državni organ (ki pa nima funkcije tribunala, saj o njegovih odločitvah razsojajo Upravno sodišče Republike Slovenije ali prekrškovni oddelki okrajnih sodišč). Nadalje je v tretjem odstavku določeno, da pri Informacijskem pooblaščenca delujejo poleg informacijskega pooblaščenca in namestnikov tudi državne nadzornice oziroma državni nadzorniki za varstvo osebnih podatkov, ki opravljajo pristojnosti inšpekcijskega nadzora in druge naloge glede varstva osebnih podatkov po določbah Splošne uredbe, ZVOP-2 in drugih zakonov ali predpisov. V četrtem odstavku je določeno, da imajo informacijski pooblaščenec (funkcionar, predstojnik tega

<sup>63</sup> Uradni list RS, št. 113/05 in 51/07 – ZUstS-A.

državnega organa) in njegovi namestniki enaka pooblastila in pristojnosti, kot velja za nadzornike iz prejšnjega odstavka – torej vsi lahko izvajajo nadzore glede varstva osebnih podatkov. Po petem odstavku informacijskemu pooblaščenca, namestnikom informacijskega pooblaščenca in državnim nadzornikom lahko pri izvajanju pristojnosti iz tretjega odstavka, zlasti ugotavljanju dejstev in okoliščin, pomembnih za odločanje, ter opravljanju strokovnih oziroma administrativnih opravil, po pooblastilu informacijskega pooblaščenca pomagajo drugi zaposleni pri Informacijskem pooblaščenca.

#### **K 58. členu:**

V 58. členu ZVOP-2 so določene temeljne pristojnosti Informacijskega pooblaščenca. V prvem odstavku je določeno, da Informacijski pooblaščenec samostojno in neodvisno izvaja inšpekcijski nadzor nad izvajanjem določb Splošne uredbe, ZVOP-2 in drugih zakonov, ki urejajo varstvo, obdelavo ali prenos osebnih podatkov oziroma prenos osebnih podatkov iz Republike Slovenije, ter opravlja druge naloge ali pooblastila, ki jih določajo ti predpisi. Po drugem odstavku Informacijski pooblaščenec pri inšpekcijskem nadzoru iz prvega odstavka izvaja tudi nadzor glede uporabe podzakonskih predpisov, ki so izdani na podlagi predpisov iz prejšnjega odstavka (ki pa ne smejo glede na drugi odstavek 38. člena in 87. člen Ustave Republike Slovenije originarno urejati obdelave konkretnih osebnih podatkov). Po tretjem odstavku je Informacijski pooblaščenec pristojen za izvajanje inšpekcijskih nadzorov nad vsemi obdelavami osebnih podatkov v Republiki Sloveniji (torej tudi področja varstva osebnih podatkov umrlih oseb, obveščevalno-varnostne dejavnosti, obrambe države ipd.), razen glede obdelav, za katere je po določbah Splošne uredbe pristojen nadzorni organ druge države članice Evropske unije. V četrtem odstavku je uvodno določeno, da je Informacijski pooblaščenec prekrškovni organ, ki je pristojen za nadzor glede izvajanja določb ZVOP-2, drugih zakonov, ki urejajo varstvo osebnih podatkov ter je kot prekrškovni organ pristojen za nadzor glede izvajanja določb Splošne uredbe v zvezi s prekrški iz člena 83 Splošne uredbe. Navedeni odstavek je povezan s 108. členom ZVOP-2.

#### **K 59. členu:**

V predlaganem 59. členu so določene izjeme glede pristojnosti Informacijskega pooblaščenca glede dometa inšpekcijskih nadzorov na določenih sistemskih področjih. Namreč glede tistih obdelav osebnih podatkov, izvršenih v okviru izvajanja neodvisnega sodniškega odločanja, kot to opredeljuje Zakon o sodiščih (3. člen), obdelav osebnih podatkov, izvršenih v okviru opravljanja samostojne državnotožilske funkcije delovanja po Zakonu o državnem tožilstvu (19. člen v zvezi s 3. členom), obdelav osebnih podatkov, izvršenih v okviru odločanja Ustavnega sodišča Republike Slovenije, kot jih opredeljujejo Zakon o ustavnem sodišču (21. člen) ter obdelav osebnih podatkov, izvršenih v okviru delovanja Varuha človekovih pravic, kot jih opredeljuje Zakon o varuhu človekovih pravic (zlasti v zvezi s 6.a členom) ali drug zakon, ki ureja pristojnosti ali naloge varuha človekovih pravic, razen področja zagovornišva otrok ter glede obdelav osebnih podatkov na področjih predkazenskega postopka ali obveščevalno-varnostne dejavnost, iz katerih bi bilo lahko razvidno, da v postopku delujejo ali sodelujejo tajni delavci oziroma sodelavci po določbah Zakona o kazenskem postopku, Zakona o obrambi ali Zakona o Slovenski obveščevalno-varnostni agenciji oziroma bi bila lahko razkrita identiteta teh posameznikov<sup>64</sup> ter podobno tudi glede tistih obdelav osebnih podatkov na področju zaščiteneh prič po določbah Zakona za zaščito prič, iz katerih bi bila lahko razkrita identiteta teh posameznikov.

Glede sodne oblasti nadzor glede varstva osebnih podatkov v zvezi s sodnim odločanjem preprečujejo ustavne določbe, konvencijske določbe ter določbe Splošne uredbe – namreč neodvisno odločanje sodstva (prvi odstavek 23. člena in 125. člen Ustave Republike Slovenije, prvi odstavek 6. člena

<sup>64</sup> Primerljiva omejitev parlamentarnega nadzora glede tajnih delavcev in tajnih sodelavcev je že od leta 2007 določena v drugem odstavku 25. člena Zakona o parlamentarnem nadzoru obveščevalnih in varnostnih služb (Uradni list RS, št. 93/07 – uradno prečiščeno besedilo), namreč: »(2) Ne glede na določbe prejšnjega odstavka pooblaščenca skupina ne sme vpogledati v tisti del dokumentacije nadzorovane službe, iz katerega bi bilo lahko razvidno, da v postopku delujejo ali sodelujejo tajni delavci oziroma sodelavci po določbah ZKP, ZObr in ZSOVA oziroma bi bila lahko razkrita identiteta teh tajnih delavcev ali sodelavcev.«



Evropske konvencije o človekovih pravicah ter tretji odstavek člena 55 Splošne uredbe). Podobno (primerljivo) velja za državna tožilstva glede na samostojnost državnih tožilcev po 135. členu Ustave Republike Slovenije, saj gre po ustavnosodni presoji za delno primerljiv (funkcionalno) samostojni sistem<sup>65</sup> napram sistemu neodvisnega sodnega odločanja – zlasti v delu, ki se nanaša na kazenski pregon.

Pri izjemah glede nadzora v zvezi z varstvom osebnih podatkov v razmerju do Varuha človekovih pravic se izhaja iz *sui generis* ustavnega položaja Varuha človekovih pravic po 159. členu Ustave Republike Slovenije in njegove neoblastne nadzorne funkcije.

Po drugem odstavku je Informacijski pooblaščenec ne glede na prvi odstavek tega člena pristojen za opravljanje inšpekcijskega nadzora zvezi z zadevami sodne uprave, državnotožilske uprave, uprave Ustavnega sodišča Republike Slovenije, uprave Varuha človekovih pravic ter glede izvajanja ukrepov in postopkov s področja varnosti osebnih podatkov ter sledljivosti obdelav in posredovanj osebnih podatkov po sedmem odstavku 38. člena tega zakona glede vseh državnih organov iz prvega odstavka tega člena. Navedena področja ne spadajo med temeljna delovna področja navedenih državnih organov oziroma so nekoliko bolj tehnične narave in je ta zakonodajni pristop (polna nadzorna pristojnost Informacijskega pooblaščenca) upravičen. Prav tako ni za področja, ki so izločena po prvem odstavku, predlagan kakšen poseben (*sui generis*) nadomestni nadzorni sistem (mehanizem) glede varstva osebnih podatkov, saj se npr. za sodstvo šteje, da je presoja zakonitosti obdelave določenih osebnih podatkov v sodnih postopkih del običajne postopkovne zakonodaje v zvezi z uporabo pravnih sredstev oziroma vprašanje dokaznega prava.

#### **K 60. členu:**

V predlaganem 60. členu so določene naloge Informacijskega pooblaščenca glede posvetovanj o uvedbah obdelav osebnih podatkov. Po prvem odstavku Informacijski pooblaščenec daje predhodna mnenja ministrstvu Vlade Republike Slovenije, Državnemu zboru Republike Slovenije ter Državnemu svetu Republike Slovenije, nato organom samoupravnih lokalnih skupnosti, drugim državnim organom ter nosilcem javnih pooblastil o usklajenosti določb predlogov zakonov, podzakonskih aktov ter drugih predpisov z ZVOP-2, Splošno uredbo in drugimi zakoni ter predpisi, ki urejajo osebne podatke. Po drugem odstavku so se organi in nosilci javnih pooblastil iz prvega odstavka dolžni pravočasno, v skladu z določbami o rokih iz drugega odstavka člena 36 Splošne uredbe, predhodno posvetovati z Informacijskim pooblaščencom po določbah prejšnjega odstavka, kadar je v predlaganem predpisu določena vzpostavitev nove zbirke, njena sprememba ali prenos osebnih podatkov iz obstoječe zbirke. Kadar se vrste obdelav, ki jih ureja predlagani predpis, nanašajo na situacije iz 41. člena ZVOP-2, mora predlagatelj predpisa v okviru posvetovanja Informacijskemu pooblaščenecu predložiti oceno učinka iz sedmega odstavka člena 25. člena Splošne uredbe. V tretjem odstavku je določeno, da kadar zakon določa, da Informacijski pooblaščenec poda soglasje k predlogu predpisa, se smiselno uporabljajo določbe drugega odstavka. V četrtem odstavku je z vidikov načel transparentnosti in legitimnosti določeno, da mora biti Mnenje Informacijskega pooblaščenca del javno dostopnega gradiva predloga predpisa iz prvega odstavka tega člena, skupaj z odzivom organa ali nosilca javnega pooblastila. V petem odstavku je določeno, da lahko Informacijski pooblaščenec samostojno odloči, da posreduje tudi naknadno mnenje organu ali nosilcu javnega pooblastila iz prvega odstavka tega člena, če oceni, da je bilo njegovo mnenje neutemeljeno neupoštevano (npr. v postopku obravnave predloga zakona v Državnem zboru Republike Slovenije). V šestem odstavku je določeno, da so se drugi upravljavci dolžni predhodno posvetovati z Informacijskim pooblaščencom, s smiselno uporabo določb prvega do četrtega odstavka tega člena, kadar je iz ocene učinka na varstvo osebnih podatkov iz 41. člena ZVOP-2 razvidno, da bi obdelava osebnih podatkov povzročila veliko tveganje za posameznike, na katere se nanašajo osebni podatki, če upravljavec ne bi sprejel ukrepov za ublažitev tveganja.

#### **K 61. členu:**

---

<sup>65</sup> Odločba US, št. U-I-42/12, 7. 2. 2013; objava: Uradni list RS, št. 17/13 in OdlUS XX, 1.

Predlagani 61. člen določa sistem sodelovanja Informacijskega pooblaščenca z drugimi nadzornimi in podobnimi organi, nevladnimi organizacijami ipd. Po prvem odstavku ima Informacijski pooblaščenec možnost, da pri svojem delu sodeluje z državnimi organi, Evropskim odborom za varstvo podatkov, drugimi pristojnimi organi Evropske unije za varstvo posameznikov pri obdelavi osebnih podatkov ter podobnimi organi Sveta Evrope, drugimi mednarodnimi organizacijami, tujimi nadzornimi organi za varstvo osebnih podatkov, zavodi, združenji, nevladnimi organizacijami s področja varstva osebnih podatkov ali zasebnosti ter drugimi organizacijami in organi glede vseh vprašanj, ki so pomembna za varstvo osebnih podatkov.

Po drugem odstavku je Informacijski pooblaščenec je pristojen tudi za skupno ukrepanje ali preiskovanje z drugimi nadzornimi organi držav članic po členu 62 Splošne uredbe, torej za izvajanje skupnega nadzora glede varstva osebnih podatkov.

V tretjem odstavku sta določena ti. kriterij »vrhovne oblasti« ter stroškovno pravilo, namreč če se skupni nadzor izvaja na ozemlju Republike Slovenije ali v okviru pristojnosti Informacijskega pooblaščenca po tretjem odstavku 4. člena ZVOP-2. Tako so člani (vodstvo, funkcionarji) ali strokovno osebje (javni uslužbenci) nadzornega organa druge države članice Evropske unije dolžni izvajati nadzor tako, da nadzor vodi Informacijski pooblaščenec (so začasno del njegove »ekipe«). Člani ali osebje drugega nadzornega organa krijejo svoje stroške.

V četrtem odstavku je urejena nasprotna situacija, če Informacijski pooblaščenec (funkcionar, namestniki ali državni nadzorniki) izvajajo skupni nadzor na ozemlju druge države članice Evropske unije ali v okviru njenih pristojnosti (pristojnosti njenega nadzornega organa za varstvo osebnih podatkov). Tudi v tem primeru vodi nadzor nadzorni organ druge (pristojne) države članice. In predstavniki Informacijskega pooblaščenca krijejo svoje stroške.

V 2. poglavju VI. dela ZVOP-2 sta urejeni področji sistema inšpekcijskega nadzora glede varstva osebnih podatkov ter tudi javnost delovanja nadzornega organa.

#### **K 62. členu:**

Predlagani 62. člen ureja uporabo predpisov, ki urejajo opravljanje inšpekcijskega nadzora, tako določa, da se za opravljanje inšpekcijskega nadzora in drugih nalog po določbah ZVOP-2 in po določbah Splošne uredbe uporabljajo določbe Splošne uredbe, ZVOP-2, Zakona o inšpekcijskem nadzoru ter Zakona o splošnem upravnem postopku. V primeru neskladnosti med določbami Zakona o inšpekcijskem nadzoru ter Zakona o splošnem upravnem postopku v razmerju do določb ZVOP-2 ter določb Splošne uredbe veljajo določbe ZVOP-2 ter določbe Splošne uredbe.

#### **K 63. členu:**

V 63. členu je določen obseg inšpekcijskega nadzora, po katerem v njegovem okviru nadzorni organ Informacijski pooblaščenec (torej informacijski pooblaščenec, njegovi namestniki in državni nadzorniki za varstvo osebnih podatkov – glejte tudi prvi odstavek 64. člena ZVOP-2):

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

#### **K 64. členu:**

V 64. členu je določeno neposredno opravljanje inšpekcijskega nadzora s strani državnih nadzornikov, informacijski pooblaščenec in namestniki informacijskega pooblaščenca v mejah pristojnosti Informacijskega pooblaščenca (kot državnega nadzornega organa po tem zakonu, Zakonu o Informacijskem pooblaščenču in drugih zakonov). Po drugem odstavku državni nadzornik, informacijski pooblaščenec in namestnik informacijskega pooblaščenca izkazujejo pooblastilo (namen obdelave osebnih podatkov) za opravljanje nalog inšpekcijskega nadzora s službeno izkaznico in značko, ki vsebuje fotografijo nadzornika, informacijskega pooblaščenca ali namestnika informacijskega pooblaščenca, njegovo osebno ime, strokovni ali znanstveni naslov ter navedbo organa in pooblastil. Obliko in vsebino službene izkaznice in značke podrobneje predpiše Informacijski pooblaščenec v podzakonskem predpisu.

#### **K 65. členu:**

V 65. členu so glede na 62. člen ZVOP-2 podrobneje urejena preiskovalna pooblastila Informacijskega pooblaščenca. Po prvem odstavku so državni nadzornik, namestniki informacijskega pooblaščenca ter informacijski pooblaščenec upravičeni:

1. pregledovati vsebino zbirk ne glede na tajnost ali drugo vrsto zaupnosti;
2. pregledovati dokumentacijo, ki se nanaša na obdelavo osebnih podatkov, ne glede na njeno zaupnost ali tajnost, ter na prenos osebnih podatkov v tretjo državo in posredovanje uporabnikom osebnih podatkov iz tretjih držav, ne glede na njeno tajnost ali drugo vrsto zaupnosti;
3. brez predhodne najave in brez navzočnosti zavezanca, njegovega zakonitega zastopnika oziroma pooblaščenca opraviti pregled vsebine in preveriti način delovanja zavezančevih spletnih strani in drugih elektronsko dostopnih storitev;
4. preverjati postopke in ukrepe ter pregledovati dokumentacijo in akte, ki se nanašajo na varnost osebnih podatkov oziroma na njeno izvajanje;
5. pregledovati prostore, v katerih se obdelujejo osebni podatki, računalniško in drugo opremo ter tehnično dokumentacijo;
6. izvajati druga pooblastila, določene z zakonom, ki ureja inšpekcijski nadzor, ter zakonom, ki ureja splošni upravni postopek;
7. opravljati druga preiskovalna pooblastila, določena z zakonom.

Po drugem odstavku se o opravljenem inšpekcijskem ogledu sestavi zapisnik, ki se lahko ne glede na določbe zakonov, ki urejata upravni in inšpekcijski postopek, v primeru, ko ne gre za nujne in neodložljive ukrepe, sestavi v roku 15 dni od dneva opravljenega nadzora ter se vroči zavezancu. Zapisnik vsebuje ugotovljeno dejansko stanje, ki vključuje dejstva in okoliščine, pomembne za odločbo, vključno s posnetki in izpisi podatkov iz spletnih strani ter drugimi pridobljenimi podatki. Zavezanec lahko na zapisnik poda pripombe ter se o ugotovljenih dejstvih in okoliščinah pisno ali ustno izjavi v roku, ki ga določi nadzornik in ne sme biti krajši od 2 delovnih dni po vročitvi zapisnika, o čemer mora biti zavezanec v zapisniku izrecno poučen<sup>66</sup>.

#### **K 66. členu:**

<sup>66</sup> Glejte: odločba US, št. U-I-252/00, 8. 10. 2003, 15. točka; objava: Uradni list RS, št. 105/03 in OdlUS XII, 80,

V 66. členu so urejena popravljalna pooblastila in ukrepi državnega nadzornika za varstvo osebnih podatkov. V prvem odstavku je urejeno, da nadzornik, ki pri opravljanju inšpekcijskega nadzora ugotovi kršitev določb Splošne uredbe, tega zakona ali drugega zakona ali predpisa, ki ureja varstvo osebnih podatkov, ima pristojnost, poleg uporabe popravljalnih pooblastil iz Splošne uredbe, takoj:

1. odrediti, da se nepravilnosti ali pomanjkljivosti, ki jih ugotovi, odpravijo na način in v roku, ki ga nadzornik sam določi;
2. odrediti prepoved obdelave osebnih podatkov osebam javnega ali zasebnega sektorja, ki niso zagotovile ali ne izvajajo ukrepov in postopkov za varnost osebnih podatkov;
3. odrediti prepoved obdelave osebnih podatkov ter anonimiziranje, omejitve obdelave, psevdonimizacijo, brisanje ali uničenje osebnih podatkov, kadar ugotovi, da se osebni podatki obdelujejo v nasprotju z določbami Splošne uredbe, tega zakona in drugih zakonov;
4. odrediti prepoved prenosa osebnih podatkov v tretjo državo ali njihovega prenosa uporabnikom osebnih podatkov v tretji državi, če se posredujejo v nasprotju z določbami Splošne uredbe ali zakona;
5. odrediti druge ukrepe, določene z zakonom, ki ureja inšpekcijski nadzor, ter zakonom, ki ureja splošni upravni postopek.

Ukrepov po prvem odstavku ni mogoče odrediti zoper osebo, ki v elektronskem komunikacijskem omrežju opravlja storitev izključnega prenosa podatkov, vključno z začasnim shranjevanjem podatkov in drugimi delovanji v zvezi s podatki, ki so izključno v funkciji opravljanja ali olajšanja prenosa podatkov po omrežjih, če ta oseba sama nima interesa, povezanega z vsebino teh podatkov, in ne gre za osebo, ki lahko sama ali skupaj z omejenim krogom z njo povezanih oseb učinkovito nadzoruje dostop do teh podatkov, kot je bilo že dosedaj določeno v drugem odstavku 54. člena ZVOP-1<sup>67</sup>. Ta varovalni ukrep je tudi nekoliko povezan z 9. in 10. členom Zakona o elektronskem poslovanju na trgu<sup>68</sup> - sodni »take down« sistem ter tudi novejša praksa na ravni Evropske unije na področjih odgovornosti ponudnikov družbenih omrežij za lažne novice (»fake news«) in prirejanje volitev preko njih (»election rigging«), tako, da se dosedanja varovalna sistemska določba proti možnosti sistemske cenzure ne spremeni.

#### **K 67. členu:**

V 67. členu je določen postopek odločitve, da se postopek nadzora ne uvede. Nadzornik v primerih, kadar je iz prijave posameznika, na katerega se nanašajo osebni podatki očitno, da glede na podatke iz prijave ni možno sklepati na kršitev varstva osebnih podatkov po Splošni uredbi, tem zakonu ali drugem zakonu oziroma predpisu, ki ureja obdelavo in varstvo osebnih podatkov, s sklepom odloči, da se inšpekcijski postopek ne uvede. Nadzornik v obrazložitvi sklepa navede razloge za neuvedbo postopka.

#### **K 68. členu:**

Glede obveščanje prijavitelja je v 68. členu ZVOP-2 določeno, da mora nadzornik prijavitelja po opravljenem nadzoru in sprejetem zadnjem ukrepu oziroma ustavitvi postopka obvestiti o vseh pomembnejših ugotovitvah in dejanjih v postopku inšpekcijskega nadzora.

#### **K 69. členu:**

---

<sup>67</sup> Kot reakcija na »afero udba.net« iz leta 2003 - ukrep preprečevanja vzpostavljanja cenzure (posega v svobodo izražanja in svobodo komuniciranja). Glejte tudi: Makarovic, Bostjan, *Foreign Internet content restriction in the Republic of Slovenia: Artificial borders within the Internet to protect personal data?*, Journal of Computer, Media and Telecommunications Law, Volume 8, Number 5, 2003, str. 371-374.

<sup>68</sup> Uradni list RS, št. 96/09 – uradno prečiščeno besedilo in 19/15.

V 69. členu je določeno splošno pravno sredstvo zoper odločitve Informacijskega pooblaščenca, da namreč zoper odločbo ali sklep Informacijskega pooblaščenca ni dovoljena pritožba, dovoljen pa je upravni spor. Informacijski pooblaščenec kot samostojni in neodvisni državni organ za varstvo osebnih podatkov torej ne sme imeti (nad seboj) drugostopenjskega upravnega organa, torej pritožbenega organa<sup>69</sup>.

#### **K 70. členu:**

V 70. členu ZVOP-2 je urejeno ukrepanje ob zaznavi kaznivih dejanj ali prekrškov. V prvem odstavku je določeno, da če nadzornik pri izvrševanju svojih pristojnosti ugotovi, da obstaja sum storitve prekrška, ki je v pristojnosti Informacijskega pooblaščenca, izvede postopek po zakonu, ki ureja prekrške, po določbah Splošne uredbe ter v skladu z določbami IX. dela tega zakona. V drugem odstavku je določeno, da če nadzornik pri izvrševanju svojih pristojnosti ugotovi, da obstaja sum storitve kaznivega dejanja ali prekrška iz pristojnosti drugega prekrškovnega organa, poda kazensko ovadbo v skladu z Zakonom o kazenskem postopku oziroma izvede ustrezne postopke v skladu z Zakonom o prekrških.

#### **K 71. členu:**

V 71. členu je določeno varovanje tajnosti osebnih podatkov, v okviru nadzornih postopkov Informacijskega pooblaščenca. Po prvem odstavku so dolžni državni nadzornik za varstvo osebnih podatkov, informacijski pooblaščenec in namestnik informacijskega pooblaščenca dolžni varovati tajnost osebnih podatkov, s katerimi se seznanijo pri opravljanju inšpekcijskega nadzora, preiskovalnih pooblastil, popravljalnih ali prekrškovnih pooblastil tudi po prenehanju delovnega razmerja ali funkcije. Po drugem odstavku dolžnost iz prvega odstavka velja tudi za vse javne uslužbence pri Informacijskem pooblaščenču ali druge osebe, ki sodelujejo pri postopkih po tem zakonu.

#### **K 72. členu:**

V predlaganem 72. členu so določeni javnost dela Informacijskega pooblaščenca, informiranje javnosti ter dodatna svetovanja. Po prvem odstavku Informacijski pooblaščenec lahko:

1. izdaja notranje glasilo ter strokovno literaturo;
2. na spletni strani ali na drug primeren način pravočasno objavlja mnenja iz 44. člena tega zakona;
3. na spletni strani oziroma na drug primeren način objavlja odločbe in sklepe Ustavnega sodišča Republike Slovenije o zahtevah ocene ustavnosti, ki jih je vložil Informacijski pooblaščenec ter odločitve Ustavnega sodišča Republike Slovenije o njih;
4. na spletni strani oziroma na drug primeren način objavlja odločbe in sklepe sodišč s splošno pristojnostjo in upravnega sodišča, ki se nanašajo na varstvo osebnih podatkov, tako da iz njih ni možno razbrati osebnih podatkov strank, oškodovancev, prič ali izvedencev z uporabo psevdonimizacije;
5. daje mnenja o skladnosti kodeksov poklicne etike, splošnih pogojev poslovanja oziroma njihovih predlogov s predpisi s področja varstva osebnih podatkov;
6. daje neobvezna mnenja, pojasnila in stališča o vprašanih s področja varstva osebnih podatkov in jih objavlja na spletni strani ali na drug primeren način;
7. pripravlja in daje neobvezne smernice in priporočila glede varstva osebnih podatkov na posameznem področju;

---

<sup>69</sup> Glejte: odločba US, št. P-5/11, 2. 6. 2011; objava: Uradni list RS, št. 52/11.

8. po potrebi daje izjave za javnost o izvedbi posamičnih zadev po tem zakonu;
9. izvaja konference za medije v zvezi z delom Informacijskega pooblaščenca ter prepise izjav ali posnetke izjav s konferenc za medije objavi na spletni strani;
10. obdeluje kontaktne podatke za izvajanje izobraževanj, posvetovanj, javnih dogodkov;
11. na spletni strani objavlja druga pomembna obvestila.

Po drugem odstavku lahko Informacijski pooblaščenec za opravljanje pristojnosti iz 5., 6., in 7. točke prvega odstavka pozove k sodelovanju tudi predstavnike društev in drugih nevladnih organizacij s področja varstva osebnih podatkov, zasebnosti ter potrošnikov.

V 3. poglavju VI. dela ZVOP-2 so urejeni kontrolni mehanizmi (poročanje ipd.) glede delovanja Informacijskega pooblaščenca.

#### **K 73. členu:**

Po prvem odstavku Informacijski pooblaščenec v svojem letnem poročilu poroča Državnemu zboru Republike Slovenije o stanju na področju varstva osebnih podatkov ter povezanih ugotovitvah, predlogih in priporočilih. Poročilo iz prejšnjega stavka je del skupnega letnega poročila po določbah zakona, ki ureja Informacijskega pooblaščenca. Po drugem odstavku se poročilo posreduje tudi Evropski komisiji, Odboru ter je dostopno javnosti. To je prvi zunanji kontrolni mehanizem parlamentarne vrste, nekako analogno zgodovinskemu izvoru »ombudsmanov«, ki so nastali kot parlamentarni organ (Informacijski pooblaščenec je v manjšem delu primerljiv s klasičnim ombudsmanom).

#### **K 74. členu:**

Dodatni kontrolni mehanizem določa pristojnosti Varuha človekovih pravic. Določeno je da Varuh človekovih pravic opravlja svoje naloge na področju varstva osebnih podatkov v razmerju do državnih organov, organov samoupravnih lokalnih skupnosti in nosilcev javnih pooblastil v skladu z Zakonom o varuhu človekovih pravic – torej gre za rezervni (generalni) kontrolni mehanizem, ki deluje neoblastno z lastnimi nadzori na področju varstva osebnih podatkov kot ene od človekovih pravic iz Ustave Republike Slovenije. V drugem odstavku je določeno, da je varstvo osebnih podatkov posebno delovno področje varuha, za katerega je zadolžen eden od namestnikov varuha (glede na zgodovino urejanja področja iz leta 2001).

#### **K 75. členu:**

Kot dodatna izpeljava kontrolnega mehanizma je določeno glede pristojnosti zakonodajne oblasti, da stanje na področju varstva osebnih podatkov in izvrševanje določb tega zakona, v skladu s 73. členom tega zakona, spremlja pristojno delovno telo državnega zbora.

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

### **7. K VII. delu Predloga ZVOP-2:**

## K 76. členu:

Predlagani 76. člen ureja obdelava osebnih podatkov v znanstvene raziskovalne, zgodovinske raziskovalne in statistične namene. Ta področja so načeloma z vidika varstva osebnih podatkov dobro urejena v področni zakonodaji – v Zakonu o varstvu dokumentarnega in arhivskega gradiva ter arhivih<sup>70</sup>, v Zakonu o državni statistiki<sup>71</sup> (kjer bi morda vseeno bilo potrebno urediti področno povezovanje zbirk) ter v Zakonu o raziskovalni in razvojni dejavnosti<sup>72</sup> (ki pa bi ga bilo treba širše spremeniti ozir. dopolniti z vidika urejanja varstva osebnih podatkov).

Po prvem odstavku lahko upravljavec ne glede na prvotni namen zbiranja osebne podatke nadalje obdeluje za znanstvene raziskovalne, zgodovinske raziskovalne in statistične namene, drug uporabnik osebnih podatkov pa za iste namene. Urejena je torej obdelava v druge namene glede na določbe (b) točke prvega odstavka člena 5 in člena 89 Splošne uredbe. Obdelava za te druge namene, ki so v posebnem javnem interesu, je dopustna v okviru naslednjih pravnih podlag:

- če je posameznik, na katerega se osebni podatki nanašajo za takšno obdelavo podal predhodno pisno privolitve (torej posebna vrsta privolitve, določena na sistemski način v ZVOP-2),
- če jih pridobi in nadalje obdeluje v anonimizirani obliki (tako da torej ne veljajo več za osebne podatke) ali
- če tako določa področni zakon (torej posebna zakonska podlaga).

V drugem odstavku je določen strog sistem, kdo lahko izvaja delovanja za namene iz prvega odstavka, namreč registrirane znanstveno-raziskovalne organizacije ali registrirani raziskovalci po zakonu, ki ureja raziskovalno in razvojno dejavnost. Nato je določeno da lahko za namen obdelave iz prvega odstavka tega člena pri upravljavcu osebnih podatkov vpogledajo oziroma pridobijo posebne vrste osebnih podatkov ali druge osebne podatke praviloma v psevdonimizirani obliki, če predložijo predstavitveni elaborat raziskave, s katerim izkažejo:

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

Predlagani so torej kumulativni strogi pogoji, kdaj lahko pridobijo osebne podatke brez privolitve, posebnega (področnega) zakona, brez anonimizacije.

Po tretjem odstavku se uporabniku (organizaciji ali raziskovalcu) iz drugega odstavka praviloma omogoči vpogled, lahko pa tudi pridobitev podatkov s kopiranjem, prepisom ali izpisom, če se z vpogledom ne da doseči namena raziskave ali bi bila izvedba vpogleda povezana z nesorazmernim naporom ali stroški.

Četrty odstavek določa stroge pogoje za vsebino elaborata ter nujnost (priložene) izvedbe ocene učinka v zvezi z varstvom osebnih podatkov po 35. členu ZVOP-2. Po petem odstavku se osebne podatke po opravljeni raziskavi praviloma uniči, so pa možne izjeme, namreč osebni podatki, ki jih je uporabnik pridobil v skladu s 1. in 3. točko prvega odstavka in drugim odstavkom tega člena, se ob

<sup>70</sup> Uradni list RS, št. 30/06 in 51/14.

<sup>71</sup> Uradni list RS, št. 45/95 in 9/01.

<sup>72</sup> Uradni list RS, št. 22/06 – uradno prečiščeno besedilo, 61/06 – ZDru-1, 112/07, 9/11 in 57/12 – ZPOP-1A.

zaključku raziskave uničijo ali nepovratno anonimizirajo, če zakon ne določa drugače, če posameznik ni privolil v nadaljnjo hrambo osebnih podatkov ali če to ni pomembno za izvršitev namena raziskave. Uporabnik osebnih podatkov pa mora upravljavca, ki mu je posredoval osebne podatke, brez odlašanja po njihovem uničenju pisno obvestiti, kdaj in na kakšen način jih je uničil.

Šesti odstavek je en od najpomembnejših odstavkov tega člena, določa namreč objave rezultatov raziskav praviloma v anonimizirani obliki (uporabljeno načelo sorazmernosti). Določeno je, da se rezultati obdelave objavijo v anonimizirani obliki, razen če ZVOP-2 ali drug zakon določa drugače ali če je posameznik, na katerega se nanašajo osebni podatki, za objavo v neanonimizirani obliki podal pisno privolitev ali če je za takšno objavo v času po smrti posameznika podana pisna privolitev določenih oseb v izključujočem vrstnem redu (zakonec, zunajzakonski partner oziroma partner iz istospolne partnerske skupnosti, otroci ali starši umrlega posameznika). Upravljavec pa ne sme objaviti neanonimiziranih osebnih podatkov, če je to v nasprotju z interesom varovanja tajnosti ali zaupnosti postopkov odločanja, ali pa ti postopki še niso končani. V sedmem odstavku je določeno, da določbe 76. člena ZVOP-2 ne posegajo v (področne) določbe Zakona o varstvu dokumentarnega in arhivskega gradiva ter arhivih<sup>73</sup>,

#### **K 77. členu:**

V 77. členu je določena obdelava naslovov za kontaktiranje posameznikov v znanstvene raziskovalne, zgodovinske raziskovalne in statistične namene. Po prvem odstavku se v okviru obdelave osebnih podatkov za namene znanstvenega raziskovanja, zgodovinskega raziskovanja ali statističnega raziskovanja upravljavcu izjemoma dovoljuje tudi obdelovati osebne podatke ciljnih skupine posameznikov za potrebe pridobitve privolitve za obdelavo njihovih osebnih podatkov ali zaradi pridobitve dodatnih podatkov ali pojasnil za prej navedene namene.

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

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

Gre torej za primere, ko uporabnik želi pridobiti privolitev, pa nima osebnih podatkov, zato kontaktiranje posameznika, na katerega se nanašajo osebni podatki, za njega izvede upravljavec iz javnega sektorja in to proti plačilu stroškov ter le za namene iz prvega in drugega odstavka.

Po tretjem odstavku se v okviru obdelave iz prvega in drugega odstavka lahko za namen kontaktiranja obdelujejo samo osebno ime, naslov stalnega ali začasnega prebivališča, kontaktna telefonska številka ali kontaktni naslov elektronske pošte (uporabljeno načelo sorazmernosti ter določen namen obdelave).

Po četrtem odstavku se posredovani ali obdelani osebni podatki lahko obdelajo izključno za namen raziskave in jih je treba izbrisati takoj, ko niso več potrebni (namenska obdelava osebnih podatkov ter definicija izbrisa iz 6. točke tretjega odstavka 6. člena ZVOP-2).

V petem odstavku je določeno, da določbe 77. člena ZVOP-2 ne posegajo v (področne) določbe Zakona o varstvu dokumentarnega in arhivskega gradiva ter arhivih<sup>74</sup> (podobno kot to velja za določbe

---

<sup>73</sup> Uradni list RS, št. 30/06 in 51/14.

<sup>74</sup> Uradni list RS, št. 30/06 in 51/14.



76. člena ZVOP-1), za področje arhivov namreč tudi veljajo (podrejeno) možnosti npr. znanstvenega raziskovanja ter zgodovinskega raziskovanja.

#### **K 78. členu:**

V predlaganem 78. členu je določena obdelava podatkov za namene arhiviranja v javnem interesu. Po prvem odstavku je obdelava osebnih podatkov za namene arhivskega delovanja je dovoljena, če je v javnem interesu in določeno z zakonom. Upravljavca mora v skladu z zakonom določiti ukrepe za varnost osebnih podatkov ter primerne in posebne ukrepe za varstvo interesov posameznika, na katerega se nanašajo osebni podatki, zlasti glede posebnih vrst osebnih podatkov.

Po drugem odstavku posameznik, na katerega se nanašajo osebni podatki, nima pravice do seznanitve z lastnimi osebnimi podatki v arhivskem gradivu po členu 15 Splošne uredbe le, če bi dajanje informacij ali kopij njegovih osebnih podatkov zahtevalo očitno nesorazmeren napor, niti ne sme zahtevati popravka osebnih podatkov zaradi netočnosti ali neposodobljenosti v skladu s členom 16 Splošne uredbe<sup>75</sup>. Posameznik, na katerega se nanašajo osebni podatki nima pravice zahtevati izvedbe izbrisa v skladu s pravico do pozabe iz člena 17 Splošne uredbe.

Po tretjem odstavku se ne glede na določbe drugega stavka prejšnjega odstavka v primeru, kadar posameznik, na katerega se nanašajo osebni podatki in le-ta navaja netočnost in neposodobljenosti svojih osebnih podatkov, posamezniku dati na razpolago možnost za nasprotni prikaz dejstev. Pristojni arhiv mora nasprotni prikaz dejstev priložiti dokumentom ali ustrezno označiti na njih, kje se ta prikaz nahaja (posebna vrsta uradnega zaznamka).

Po četrtem odstavku posameznik, na katerega se nanašajo osebni podatki, nima pravice zahtevati omejitev obdelave po členu 18, pravice do prenosljivosti osebnih podatkov po členu 20 ter izvajati pravice do ugovora po členu 21 Splošne uredbe.

### **8. K VIII. delu Predloga ZVOP-2:**

#### **K 79. členu:**

V 79. členu Predloga ZVOP-2 je primarno poudarjen pomen svobode izražanja v razmerju do varstva osebnih podatkov, tako da je omogočeno zadržanje dosedanje visoke ravni uresničevanja svobode izražanja v okviru pravnega reda Republike Slovenije<sup>76</sup>. Treba je upoštevati, da je področje svobode izražanja eno od tistih, ki ni najbolj primerno za podrobno regulacijo (za razliko od varstva pravice do osebnih podatkov) in je torej z vidika varovanih ustavnih vrednot (npr. prvi odstavek 39. člena Ustave Republike Slovenije, 10. člen Evropske konvencije o človekovih pravicah<sup>77</sup>) področje, ki ga je treba nekoliko bolj varovati pred posegi države.

<sup>75</sup> Glejte: Sklep Višjega sodišča v Ljubljani, opr. št. I Cp 490/2000, 11. 4. 2001.

<sup>76</sup> Ko se je leta 2012 začelo obravnavanje takratnega Predloga Splošne uredbe, je Republika Slovenija navedla znatno število sistemskih pomislekov (Stališče Državnega zbora Republike Slovenije z dne 23. 3. 2012, št. EPA 191-VI, EU U 393), med drugim tudi z vidika varstva svobode izražanja v razmerju do varstva osebnih podatkov, zlasti:

»Republika Slovenija se načeloma strinja z določbami člena 80 glede razmerja med varstvom osebnih podatkov in svobodo izražanja. Bo pa v zakonodajnem postopku podrobneje proučila navedene določbe z vidika, če niso morda z vidika ostalih določb predloga pravnega akta preskope in je morda treba bolj aplikativno razmišljati o varstvu svobode izražanja, tudi z vidika razmerja do nove pravice "biti pozabljen" iz člena 17 predloga pravnega akta....«.

<sup>77</sup> 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

V prvem odstavku je glede na določbe prvega odstavka 39. člena Ustave Republike Slovenije zagotovljeno uresničevanje svobode izražanja, kar vključuje svobodo izražanja misli, govora in javnega nastopanja, tiska in drugih oblik javnega obveščanja in izražanja v okvirih pravnega reda Republike Slovenije. Vsakdo lahko svobodno zbira, sprejema in širi vesti in mnenja ter v njih vsebovane osebne podatke, ki so v ta namen potrebni in upravičeno obdelovani. Prvi odstavek (ozir. določbe celotnega člena) so formulirane tako, da se ne nanašajo samo na registrirane medije ali npr. akreditirane novinarje, ampak na celotno skupnost, ki izvaja svobodo izražanja (npr. tudi delovanje blogerjev, pisma bralcev, pisanje knjig...), torej ni mišljeno samo izvajanje svobode izražanja po določbah Zakona o medijih<sup>78</sup>. Posredno (posledično) pa pokriva predlagani člen tudi področje svobode komuniciranja<sup>79</sup> po 37. členu Ustave Republike Slovenije.

V drugem odstavku je natančneje določena varstvo svobode izražanja v razmerju do varstva osebnih podatkov za namene obveščanja javnosti s strani medijev, književnega, umetniškega ali znanstvenega ustvarjanja, zaradi resne kritike, obrambe kakšne pravice ali varstva upravičene koristi ter izobraževanja, ki ga izvajajo izobraževalne organizacije ali izobraževanja preko javno dostopnih publikacij, kar vključuje pravice medijev in drugih, da se osebni podatki uporabijo, objavijo ali drugače razkrijejo za namene uresničevanja svobode izražanja pod naslednjimi pogoji:

1. če je posameznik za uporabo, objavo ali razkritje podal privolitev (ki se dokazuje po določbah ZVOP-2 o dokumentiranju delovanj obdelave),
2. če je posameznik osebne podatke že javno objavil (uporaba pravice do informacijske samoodločbe),
3. če so osebni podatki na zakonit način že bili dostopni javnosti (npr. starejše objave v okviru izvrševanja svobode izražanja),
4. če so bili osebni podatki pridobljeni na podlagi prisotnosti posameznika na javno dostopnih krajih (npr. javno zbiranje) ali dogodkih, kjer posameznik glede na vse okoliščine ne more razumno pričakovati varstva zasebnosti ter na način, ki ne pomeni občutnega posega v razumno pričakovano zasebnost (koncept utemeljenega pričakovanja zasebnosti),
5. če gre za zakonito objavo mnenja ali vrednostne ocene, kjer je objava osebnih podatkov v njunem okviru nujna za utemeljitev mnenja ali vrednostne ocene<sup>80</sup> (ta določba ne posega nujno v pravico do pozabe – če gre za zelo staro objavo),
6. če so bili osebni podatki pridobljeni na drug zakonit način (jih npr. nekdo drug zakonito objavil, raziskovalno novinarstvo, povzetek objave iz čezmejne obdelave ipd.),
7. če javni interes po obveščanju javnosti, pravica do obveščeniosti 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<sup>81</sup>).

---

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.

<sup>78</sup> 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.

<sup>79</sup> 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.

<sup>80</sup> Glede pomembnosti osebnih podatkov, ki so vsebovani v mnenjih v okviru svobode izražanja ter načelni neprimernosti uporabe pravic izbriša 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..

<sup>81</sup> Uradni list RS, št. 58/11, 21/12 – ZDU-1F, 47/12, 15/13 – ZODPol, 47/13 – ZDU-1G, 48/13 – ZSKZDČEU-1, 19/15 in 23/17 – ZSSve.

Po tretjem odstavku uveljavljanje pravic v zvezi z določbami 79. člena ZVOP-2 zagotavlja samo sodna oblast (sodišča) v skladu z določbami zakonov, ki urejajo sodne postopke ali urejajo sodno varstvo (po splošnih določbah Zakona o pravnem postopku, Zakona o kazenskem postopku, delno tudi Zakona o upravnem sporu – ne gre pa več za posebno upravnosodno varstvo kot je to v 34. členu ZVOP-1).

Le v četrtem odstavku je zadržana pristojnost Informacijskega pooblaščenca – da nadzor nad zakonitostjo posredovanja, razkritja ali omogočanja nepooblaščenega dostopa do osebnih podatkov iz zbirke za namene iz uvodnega dela besedila drugega odstavka tega člena izvaja Informacijski pooblaščenec.

#### **K 80. členu:**

Podobno kot za varstvo svobode izražanja v 79. členu Predloga ZVOP-2 je določeno tudi za varstvo druge človekove pravice, namreč dostopa do informacij javnega značaja (drugi odstavek 39. člena Ustave Republike Slovenije) v razmerju do človekove pravice do varstva osebnih podatkov, povzeto: obveljajo dosedanja pravila iz Zakona o dostopu do informacij javnega značaja<sup>82</sup>.

Po prvem odstavku 80. člena ZVOP-2 lahko zavezanci po Zakonu o dostopu do informacij javnega značaja javnosti posredujejo osebne podatke, če so ti po zakonu javni ali če je za njihovo razkritje podan prevladujoč javni interes po določbah Zakonu o dostopu do informacij javnega značaja, Zakona o medijih ali drugega zakona (npr. drugi odstavek 178. člena Zakona o državnem tožilstvu).

Po drugem odstavku za namene uresničevanja javnega interesa na področju sodelovanja javnosti, zagotavljanja transparentnosti dela ali spremljanja njihove prakse, zavezanci iz prvega odstavka po postopku iz Zakona o dostopu do informacij javnega značaja zakona, lahko proaktivno javno objavijo tudi dokumente, ki niso zajeti v prvem odstavku tega člena, in predstavljajo informacijo javnega značaja, na način delnega dostopa praviloma v anonimizirani obliki. V primerih, kjer zasledovanje navedenih ciljev na ta način ni mogoče, pa jih objavijo v psevdonimizirani obliki v skladu s Splošno uredbo upoštevaloč druge zakonske izjeme v skladu z določbami Zakona o dostopu do informacij javnega značaja zakona, Zakona o medijih ali drugega zakona.

Po predlaganem tretjem odstavku uveljavljanje pravic v zvezi z določbami 80. člena ZVOP-2 zagotavljajo najprej Informacijski pooblaščenec v skladu z določbami Zakona o dostopu do informacij javnega značaja, Zakona o medijih, nato pa sodišča (zlasti po določbah Zakona o upravnem sporu, lahko pa tudi po določbah Zakona o pravnem postopku, Zakona o kazenskem postopku).

#### **K 81. členu:**

V predlaganem 81. členu ZVOP-2 je za upravljavce in obdelovalce določeno, da če so osebni podatki javni na podlagi zakona (npr. po določbah ZVOP-2, Zakona o medijih, Zakona o nalogah in pooblastilih policije, Zakona o sistemu plač v javnem sektorju ipd.), posameznika, na katerega se nanašajo osebni podatki, ni treba obveščati po členih 13. ali 14. Splošne uredbe, po 15. do 17. členu ZVOP in po določbah Zakona o splošnem upravnem postopku<sup>83</sup> (npr. šesti odstavek 143. člena o vabljenju k stranski udeležbi).

### **9. K IX. delu Predloga ZVOP-2:**

Posebni IX. del ZVOP-2 pomeni izvrševanje določb Direktive za namene preprečevanja, preiskovanja, odkrivanja ali pregona kaznivih dejanj ali prekrškov, izvrševanja nalog in pooblastil policije, varnosti države, obrambe države ter izvrševanja kazenskih sankcij. Zakonodajni pristop, da se področje ureja v posebnem delu systemskega Zakona o varstvu osebnih podatkov, je podoben pristopom Nemčije,

<sup>82</sup> Uradni list RS, št. 51/06 – uradno prečiščeno besedilo, 117/06 – ZDavP-2, 23/14, 50/14, 19/15 – odl. US in 102/15.

<sup>83</sup> Uradni list RS, št. 24/06 – uradno prečiščeno besedilo, 105/06 – ZUS-1, 126/07, 65/08, 8/10 in 82/13.

Avstrije, Slovaške, izhaja pa tudi iz pristopa Republike Slovenije iz časa priprave Predloga Direktive. Vsebinski pristop, da se v tem »policijsko ter kazensko pravosodnem« delu zakona izhaja iz uporabe določenih standardov (določb) Splošne uredbe sledi pristopu Zvezne republike Nemčije, ki je v Zakonu o prilagoditvi in izvajanju zakonodaje o varstvu osebnih podatkov EU (iz leta 2017) izvedla razširitev določb Splošne uredbe na določena vprašanja, ki jih ureja sicer Direktiva (zaradi pravne varnosti in enakosti), v III. Delu zakona je namreč določena izvedba določb Direktive (EU) 2016/680 in določbe v njem, ki so enake ali podobne istim, ki so v Splošni uredbi ali v predhodnih delih zakona izhajajo iz pristopa, po katerem je nacionalnemu zakonodajalcu prepuščeno, kako bo izvedel določbe navedene Direktive in lahko tako tudi uporabi (z vidika pravne varnosti) splošni sistem (splošno sistemsko raven) urejanja varstva osebnih podatkov po (nekoliko prilagojenih) določbah iz Splošne uredbe. To je tudi pristop predlagatelja ZVOP-2. K temu delu spada tudi V. del Predloga ZVOP-2 o prenosu osebnih podatkov tretjim državam ali mednarodnim organizacijam ter glede čezmejne obdelave.

#### **K 82. členu:**

V 82. členu je določeno področje uporabe IX. dela zakona. Po njem določbe tega dela zakona veljajo za primere, ko osebne podatke obdelujejo pristojni državni organi ali organi samoupravnih lokalnih skupnosti ali nosilci javnih pooblastil za namene preprečevanja, preiskovanja, odkrivanja ali pregona kaznivih dejanj ali prekrškov, izvrševanja nalog in pooblastil policije, varnosti države, obrambe države ter izvrševanja kazenskih sankcij, v skladu z določbami Direktive. Dodano je sistemsko napotilo (ne sistemska varovalka) glede določb področnih zakonov, da če ta del zakona ne določa drugače, veljajo za konkretne vrste osebnih podatkov, konkretne zbirke, obdelave osebnih podatkov ter njihova posredovanja, prenose in čezmejne obdelave določbe zakonov, ki urejajo naloge in pooblastila policije, kazenski postopek, državno tožilstvo, sodišča, sodniško službo, obrambo, obveščevalno-varnostno dejavnost ter izvrševanje kazenskih sankcij.

#### **K 83. členu:**

V 83. členu so podarjeno določena temeljna načela obdelave osebnih podatkov za področja (namene) iz 82. člena ZVOP-2, najprej na način sistemskega sklica na I. del ZVOP-2, ki velja »nadrejeno« (1. točka), v nadaljevanju pa je dan poudarek, da morajo biti osebni podatki (še posebej) točni in po potrebi posodobljeni ter da je pri tem je treba sprejeti vse primerne ukrepe, da se osebni podatki, ki glede na namene njihove obdelave niso ustrezni (ni uporabljen izraz: točni), takoj izbrišejo ali popravijo ali ustrezno označijo. Nato je določeno, da se smejo osebni podatki hraniti v obliki, ki dopušča identifikacijo posameznikov, na katere se nanašajo osebni podatki, le toliko časa, kot je potrebno za namene, za katere se obdelujejo ter da se morajo obdelovati na način, ki zagotavlja ustrezno varnost osebnih podatkov, vključno z ustreznimi tehničnimi in organizacijskimi ukrepi za zagotavljanje zaščite pred nedovoljeno ali nezakonito obdelavo, nenamerno izgubo, nedovoljenim uničenjem ali nedovoljenim poškodovanjem osebnih podatkov.

#### **K 84. členu:**

Predlagani 84. člen ZVOP-2 določa razvrščanje osebnih podatkov po vrstah ter kakovost osebnih podatkov, ob upoštevanju realnih (tudi tehničnih zmožnosti), kakovosti virov podatkov ipd.. V bistvu gre za razlikovanje med različnimi postopkovnimi položaji posameznikov (faza postopka, oznaka kakovosti podatkov glede na zgodnjo ali poznejšo fazo), kar ne vključuje samo osumljencev, tudi žrtve kaznivih dejanj, udeležence prekrška ipd. Drugi odstavek podrobneje določa, da če je to možno, je treba razlikovati podatke, ki temeljijo na dejstvih, od tistih, ki temeljijo na osebni oceni, nato da je osebne podatke, ki temeljijo na osebni oceni, je treba ustrezno označiti ter, če je to možno in dopustno, utemeljiti na način, ki omogoča naknadno preverjanje te ocene ter zaključno je določeno, da je za izvajanje tega preverjanja je odgovoren upravljavec. Po tretjem odstavku se osebni podatki, ki so netočni, nepopolni, ki niso posodobljeni ali jih je treba izbrisati, se ne smejo ne prenašati ne pripraviti za avtomatiziran priklic iz zbirk, upravljavci pa morajo v ta namen pred prenosom v skladu z

razločljivimi možnostmi ustrezno preveriti kakovost podatkov. Glede osebnih podatkov, ki so že na razpolago za avtomatiziran priklic, se je treba neprestano prizadevati za ohranjanje njihove točnosti in posodobljenosti. Po četrtem odstavku je pri vsakem posredovanju, čezmejni obdelavi ali prenosu osebnih podatkov treba po možnosti osebnim podatkom priložiti informacije, na podlagi katerih lahko prejemnik oceni oceno aktualnost, pravilnost, popolnost in zanesljivost. V petem odstavku je določeno, da če prejemnik, Informacijski pooblaščenec ali pooblaščen osebna za varstvo osebnih podatkov na podlagi sporočila posameznika, na katerega se nanašajo osebni podatki, ugotovijo (katerikoli od njih), da so bili posredovani osebni podatki, ki ne ustrezajo zahtevam iz tretjega odstavka tega člena, mora pošiljatelj to nemudoma sporočiti prejemniku. Ta pa mora nemudoma izvesti izbris nezakonito posredovanih podatkov, popravek netočnih podatkov, dopolnitev nepopolnih podatkov ali omejitev obdelave. Po šestem odstavku velja, da če imata pošiljatelj ali prejemnik verjeten razlog za domnevo (nadpolovična verjetnost), da so posredovani osebni podatki netočni ali da niso bili posodobljeni, da bi jih bilo treba izbrisati ali omejiti njihovo obdelavo, je treba nemudoma izvesti medsebojno obveščanje. Pošiljatelj pa mora nemudoma sprejeti ustrezne ukrepe popravka ali izbriša če so dejstva o neustreznih osebnih podatkih potrjena, prejemnik je na to odločitev vezan, je pa dolžan označiti morebitno nestrinjanje v svoji zbirki.

#### **K 85. členu:**

V predlaganem 85. členu je določena zakonitost obdelave osebnih podatkov, po kateri je obdelava osebnih podatkov po IX. delu ZVOP-2 zakonita le - če je določena z zakonom, ali če je potrebna zaradi varstva življenja ali telesa posameznika ter je potrebna in sorazmerna za izpolnitev določenih nalog, ki jih pristojni subjekt izvaja v skladu z nameni iz 82. člena tega zakona.

#### **K 86. členu:**

V 86. členu ZVOP-2 so določene posebne določbe o obdelavi osebnih podatkov za druge namene ter prenos osebnih podatkov. Po prvem odstavku je obdelava osebnih podatkov po določbah tega dela zakona s strani istega ali drugega upravljavca in za drug namen obdelave od tistega, za katerega so bili podatki pridobljeni, je dovoljena le, če ta drug namen spada na področje iz 82. člena ZVOP-2 ter izpolnjuje pogoje iz 84. in 85. člena ZVOP-2. Prenos, posredovanje ali čezmejna obdelava osebnih podatkov, obdelanih skladno z določbami tega dela, za namen, ki ni naveden v 82. členu tega zakona, je dovoljeno le, če je to izrecno določeno v zakonu (zakon, obvezujoča mednarodna pogodba ali pravni akt ali odločitev Evropske unije, ki sta enakovredna zakonu in se v Republiki Sloveniji uporabljata neposredno) ter je prejemnik po svojih predpisih pooblaščen za obdelavo teh osebnih podatkov za ta drug namen.

Po tretjem odstavku mora v primeru, če za obdelavo osebnih podatkov veljajo posebni pogoji, mora pristojni pošiljatelj prejemnika osebnih podatkov obvestiti o teh pogojih in o tem, da jih je treba upoštevati. Pri čezmejni obdelavi prejemnikom v druge države članice Evropske unije ali v ustanove in druge organe, vzpostavljene skladno s 4. in 5. poglavjem V. naslova Pogodbe o delovanju Evropske unije, se ne smejo uveljavljati pogoji, ki za ustrezni prenos podatkov ne veljajo tudi v Republiki Sloveniji.

#### **K 87. členu:**

Predlagani 87. člen ZVOP-2 določa posebne pogoje za avtomatizirano odločanje v posameznem primeru. Po prvem odstavku so odločitve, ki temeljijo izključno na avtomatizirani obdelavi, vključno z oblikovanjem profilov (obdelava osebnih podatkov z uporabo profiliranja), ki imajo negativne pravne posledice za posameznika, na katerega se podatki nanašajo, oziroma lahko v večji meri vplivajo nanj, dovoljene le, če so izrecno določeno v zakonski podlagi (zakon, obvezujoča mednarodna pogodba ali pravni akt ali odločitev Evropske unije, ki sta enakovredna zakonu in se v Republiki Sloveniji uporabljata neposredno). Po drugem odstavku odločitve iz prvega odstavka lahko v skladu z 82. členom ZVOP-2 izjemoma temeljijo na posebnih vrstah osebnih podatkov samo, če so bili sprejeti

posebni ustrezni ukrepi za varstvo človekovih pravic in temeljnih svoboščin ter upravičenih interesov posameznika, na katerega se nanašajo osebni podatki. Odločitve, ki bi lahko vodile do diskriminacije posameznika, na katerega se nanašajo osebni podatki, ali njemu bližnjih oseb, so prepovedane.

#### **K 88. členu:**

V 88. členu se urejajo splošna pravila glede pravic posameznika, na katerega se nanašajo osebni podatki. Po prvem odstavku mora upravljavec posamezniku, na katerega se nanašajo osebni podatki, posredovati informacije in sporočila, v skladu s 89. do 91. členom ZVOP-2, ki se nanašajo na obdelavo osebnih podatkov, podajati v čim bolj točni, razumljivi in lahko dostopni obliki ter v jasnem in preprostem jeziku, če to posameznik zahteva. Informacije in sporočila se posredujejo v posamezniku ustrezni obliki. Po drugem odstavku mora upravljavec posamezniku, na katerega se nanašajo osebni podatki, olajšati uveljavljanje njegovih pravic iz 89. do 91. člena ZVOP-2 (pač vzpostaviti ustrezno prakso glede na zahteve prvega odstavka tega člena). Po tretjem odstavku mora upravljavec posameznika, na katerega se nanašajo osebni podatki, v roku petih delovnih dni po prejemu zahtevka, pisno obvestiti o stanju obravnave zahtevka (npr. da ga preučuje pooblaščenca oseba, da bo zahtevek odstopljen, da bo predvidoma odločeno v roku... dni). Po četrtem odstavku mora upravljavec posamezniku, na katerega se nanašajo podatki, informacije o ukrepih, ki so bili na podlagi zahtevka sprejeti, zagotoviti čimprej, najpozneje pa v enem mesecu od vložitve zahtevka. Ta rok se lahko podaljša za dva meseca, če je to potrebno zaradi zapletenosti zahtevka ali števila zahtevkov. Upravljavec mora posameznika, na katerega se nanašajo podatki, v enem mesecu od vložitve zahtevka obvestiti o podaljšanju roka in ob tem navesti razloge za zamudo. Če posameznik, na katerega se podatki nanašajo, zahtevo predloži elektronsko, mora biti po možnosti obveščen po isti elektronski poti, če ne navede drugega kontaktnega naslova. Po petem odstavku v primeru, če upravljavec ne odgovori na zahtevo posameznika, na katerega se podatki nanašajo ali ne ukrepa drugače in o tem obvesti posameznika, mora posameznika, na katerega se podatki nanašajo, brez zavlačevanja, najpozneje pa v enem mesecu od vložitve zahtevka obvestiti o razlogih za to ter o možnosti vložitve pritožbe pri Informacijskem pooblaščenca, navesti kontaktne podatke Informacijskega pooblaščenca ter navesti možnosti za uveljavljanje pravice do pravnega sredstva. Po šestem odstavku morajo biti informacije iz 89. člena ZVOP-2 ter vsa sporočila in ukrepi v skladu s 90. in 91. členom ZVOP-2 zagotovljeni brezplačno. Pri očitno neutemeljenih ali pretiranih zahtevah posameznika, na katerega se podatki nanašajo, zlasti če se zahteve pogosto ponavljajo (elementi šikanoznosti), lahko upravljavec s posebno obrazložitvijo odkloni ukrepanje na podlagi zahtevka, obrazložitev pa mora vsebovati vsaj povzetek razlogov glede očitne neutemeljenosti ali pretirano narave zahtevka. Po sedmem odstavku lahko upravljavec zaradi potrditve identitete posameznika, na katerega se nanašajo osebni podatki, ki je v skladu z 90. ali 91. členom tega zakona vložil zahtevek, zahteva tudi dodatne potrebne informacije (če posameznika npr. ne pozna glede na stalnost obravnavanja/sodelovanja) od posameznika, kar vključuje glede na konkretne okoliščine zadeve poleg osebnega imena tudi navedbo datuma rojstva oziroma navedbo enotne matične številke občana, zahtevek pa mora biti podpisan lastnoročno (če je v papirnati obliki) ali v elektronski obliki z ustreznim digitalnim potrdilom (uporabljen splošna formulacija glede na to, da še niso v celoti sprejete odločitve glede ustrezne izvedbe E-IDAS Uredbe). Po osmem odstavku se v primerih iz četrtega odstavka 89. člena, tretjega odstavka 90. člena in četrtega odstavka 91. člena ZVOP-2 posluje tako, da ima posameznik, na katerega se podatki nanašajo, pravico, da zahteva preverjanje zakonitosti zadevne omejitve njegovih pravic s strani Informacijskega pooblaščenca. Upravljavec pa mora posameznika, na katerega se nanašajo osebni podatki, izrecno poučiti o tej pravici. Po devetem odstavku mora v primeru, če se uveljavlja pravica, navedena v osmem odstavku, Informacijski pooblaščenec posameznika, na katerega se osebni podatki nanašajo, ne glede na določbe 91. člena tega zakona, obvestiti vsaj o tem, da so bila izvedena vsa potrebna preverjanja ali da je preverjanje izvedel Informacijski pooblaščenec. Poleg tega mora Informacijski pooblaščenec posameznika, na katerega se nanašajo osebni podatki, obvestiti o njegovi pravici do uporabe sodnega varstva po 28. členu tega zakona.

#### **K 89. členu:**

V 89. členu ZVOP-2 je urejeno področje dajanja informacij posamezniku, na katerega se nanašajo osebni podatki. Uvodno besedilo prvega odstavka določa, da se informacije zagotovi na zahtevo posameznika. Zagotoviti je treba najmanj:

1. naziv in kontaktne podatke upravljavca;
2. po potrebi tudi kontaktne podatke pooblaščenih oseb (glede na konkretne okoliščine zadeve ali zahtevka);
3. navedbo namenov, v katere bodo osebni podatki obdelani;
4. obstoj pravice do vložitve prijave pri Informacijskem pooblaščenca ter kontaktne podatke Informacijskega pooblaščenca;
5. navesti obstoj pravice dostopa do vsebine osebnih podatkov in do tega, da upravljavec popravi ali izbriše podatke ali omeji obdelavo podatkov posameznika, na katerega se osebni podatki nanašajo.

Po drugem odstavku mora poleg informacij iz prvega odstavka upravljavec posamezniku, na katerega se nanašajo podatki, v posebnih primerih na njegovo zahtevo po prvem odstavku zagotoviti tudi določene (navedene) dodatne informacije, da lahko s tem omogoči izvajanje pravic tega posameznika:

1. pravno podlago obdelave;
2. rok hrambe osebnih podatkov ali, če to izjemoma ni možno, merila za določitev tega roka v skladu z 41. členom tega zakona;
3. po potrebi navesti kategorije prejemnikov osebnih podatkov, tudi prejemnikov v tretjih državah in mednarodnih organizacijah;
4. po potrebi druge informacije, zlasti če so bili osebni podatki pridobljeni brez vednosti posameznika, na katerega se nanašajo.

Po tretjem odstavku se v primeru, če so bili osebni podatki pridobljeni neposredno od posameznika, na katerega se nanašajo, je treba temu posamezniku, ob poizvedbi predložiti informacije v skladu z določbami prvega in drugega odstavka tega člena. Informacije iz prvega in drugega odstavka se ne podajo, če so bili osebni podatki pridobljeni s prenosom podatkov iz drugih področij nalog istega upravljavca ali iz uporabe zbirk drugega upravljavca in je ta obdelava podatkov zakonsko določena. Po četrtem odstavku se lahko obveščanje posameznika, na katerega se osebni podatki nanašajo, v skladu s tretjim odstavkom opusti ali delno ali začasno omeji, če in dokler je to v posameznem primeru očitno sorazmerno ali posebej določeno v drugem zakonu, za te primere (namene):

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

#### **K 90. členu:**

V 90. členu so določene posebne seznanitvene pravice posameznika, na katerega se nanašajo osebni podatki, do pridobitve posebnih informacij o vsebini teh podatkov. Po drugem odstavku za pridobitev informacij iz prvega odstavka veljajo roki po določbah člena 12 Splošne uredbe. Omejitve pravice do pridobitve informacij so dovoljene le pod pogoji, navedenimi v četrtem odstavku 89. člena ZVOP-2.

Nato je v tretjem odstavku določeno, da v primeru neizdaje informacij v skladu z drugim odstavkom mora upravljavec posameznika, na katerega se nanašajo podatki, nemudoma pisno obvestiti o zavrnitvi ali omejitvi informacij in razlogih, na katerih to temelji. Ta določba se ne uporablja, če je zagotovitev teh informacij v nasprotju z enim od namenov iz četrtega odstavka 89. člena tega zakona. Upravljavec mora posameznika, na katerega se nanašajo podatki, obvestiti o možnosti vložiti pritožbo na organ za varstvo podatkov. Po četrtem odstavku mora upravljavec dokumentirati razloge za odločitev o neizdaji informacij v skladu z drugim odstavkom. Ti podatki morajo biti dostopni Informacijskemu pooblaščenču in pooblašчени osebi. Po petem odstavku se v obsegu, v katerem ima posameznik, na katerega se nanašajo osebni podatki, v drugem zakonu določeno zakonsko pravico do vpogleda v njegove osebne podatke, ki se obdelujejo, pravico pridobiti informacije v skladu z določbami tega drugega zakona, ki urejajo pravico do vpogleda (navedeni drugi področni zakon torej prevlada – npr. Zakon o nalogah in pooblastilih policije).

#### **K 91. členu:**

V 91. členu je ločeno (področno) urejena pravica do popravka ali izbrisa osebnih podatkov in do omejitve obdelave. Po prvem odstavku ima vsak posameznik, na katerega se nanašajo osebni podatki, pravico, da od upravljavca zahteva takojšnji popravek svojih netočnih osebnih podatkov in dopolnitev nepopolnih ali neposodobljenih osebnih podatkov. Popravek ali dopolnitev se lahko po potrebi izvede z dodatno priloženo izjavo ali posebnim uradnim zaznamkom, če je naknadna sprememba nezdružljiva z namenom dokumentiranja glede na fazo določenega postopka (podatkov se torej ne spremeni, ampak se jim le priloži uradni zaznamek o izjavi). Upravljavec je dolžan dokazati točnost ali posodobljenost osebnih podatkov, če osebni podatki niso bili pridobljeni izključno na podlagi navedb posameznika, na katerega se podatki nanašajo. Po drugem odstavku mora upravljavec osebne podatke nemudoma izbrisati na lastno pobudo ali na podlagi zahtevka posameznika, na katerega se podatki nanašajo, če:

1. osebni podatki niso več potrebni za namene, za katere so bili pridobljeni ali drugače obdelani;
2. so bili osebni podatki obdelani nezakonito ali
3. je izbris osebnih podatkov potreben zaradi izpolnitve druge obveznosti po zakonu ali po pravnomočni sodni odločbi (npr. pravnomočna oprostilna kazenska sodba). Po tretjem odstavku lahko namesto izbrisa osebnih podatkov upravljavec njihovo obdelavo omeji, če:
  1. posameznik, na katerega se podatki nanašajo, izpodbija točnost ali posodobljenost osebnih podatkov in pravilnosti ali nepravilnosti ni mogoče ugotoviti, vendar mora posameznika, na katerega se nanašajo osebni podatki, obvestiti pred razveljavitvijo omejitve, ali
  2. je treba osebne podatke še nadalje hraniti za dokazne namene v okviru izvajanja zakonsko določene naloge.

Po četrtem odstavku mora upravljavec posameznika, na katerega se nanašajo osebni podatki, pisno obvestiti o zavrnitvi popravka ali izbrisa osebnih podatkov ali o omejitvi obdelave in o razlogih za zavrnitev. Upravljavec mora posameznika, na katerega se nanašajo podatki, obvestiti o možnosti vložiti prijavo Informacijskemu pooblaščenču in o njegovih kontaktnih podatkih. Po petem odstavku mora upravljavec morebitni popravek nepravilnih osebnih podatkov sporočiti pristojnemu organu, ki mu je prenesel ali drugače poslal (čezmejna obdelava, posredovanje) te osebne podatke. Po šestem odstavku se v primerih popravka, izbrisa podatkov ali omejitve obdelave po prvem do tretjem odstavku mora upravljavec o tem obvestiti vse prejemnike osebnih podatkov. Prejemniki so zavezani osebne podatke, ki so v njihovi pristojnosti, nemudoma popraviti, izbrisati, ustrezno označiti ali omejiti njihovo obdelavo. Po sedmem odstavku se za druga vprašanja smiselno uporablja člen 12 Splošne uredbe (Pregledne informacije, sporočila in načini za uresničevanje pravic posameznika, na katerega se nanašajo osebni podatki), npr. zaračunavanje razumne pristojbine pod pogoji iz tega člena.

#### **10. K X. delu Predloga ZVOP-2:**



**K 92. členu:**

Predlagani 92. člen ZVOP-2 ureja pravice in dolžnosti upravljavca na področju neposrednega trženja, kar je posebna (področna obdelava v druge namene v zvezi z upravičenimi interesi upravljavca) - glede na možnosti iz zadnjega stavka uvodne navedbe št. 47, ki je načeloma opsijska («Obdelava osebnih podatkov za neposredno trženje se lahko šteje za opravljeno v zakonitem interesu.»). Drugi odstavek pa ne vsebuje (ne omogoča obdelave) osebnih podatkov s področja kazenskih obsodb in kaznovanj za prekrške (glejte 13. člen ZVOP-2). Predlagani člen je načeloma enak kot določbe dosedanjega 72. člena ZVOP-1 (z navedeno izjemo osebnih podatkov iz 13. člena ZVOP-2), s tem da so določeni izrazi usklajeni z izrazoslovjem Splošne uredbe.

**K 93. členu:**

Predlagani 93. člen določa posebno pravico do ugovora ozir. prekinitve dogovorjenega dela od upravljavca glede njegovih osebnih podatkov, ki se obdelujejo za namene neposrednega trženja. Enak člen je vsebovan v določbah dosedanjega 73. člena ZVOP-1.

**K 94. členu:**

S 94. členom se začne posebno (drugo) poglavje X. dela Predloga ZVOP-2. V njem se urejajo splošne določbe o videonadzoru in obdelavi osebnih podatkov. Člen je pretežno enak določbam dosedanjega 74. člena ZVOP-1, z določenimi dodatnimi rešitvami (trimesečni rok v sedmem odstavku).

**K 95. členu:**

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

**K 96. členu:**

V 96. členu je urejen videonadzor v zvezi z večstanovanjskimi stavbami, podrobno kot je to v dosedanjem 76. členu ZVOP-1. Tretji odstavek posebej poudarja pomen (pisne) privolitve, četrti in peti odstavek definirata za ta kontekst posebej kdo je upravljavec, osmi odstavek pa določa, da je izjemoma dovoljeno omogočiti združitev videonadzornega sistema z napravami, ki jih uporabljajo lastniki za potrebe vstopa v večstanovanjsko stavbo, kot sta na primer domofon ali video domofon, razen če te naprave omogočajo snemanje ali spremljanje dogajanja v območju izvajanja videonadzora na posamezni napravi. Spremljanje dogajanja v območju izvajanja videonadzora mora onemogočiti upravljavec videonadzora.

**K 97. členu:**

V predlaganem 97. členu ZVOP-2 je urejen videonadzor glede delovnih prostorov, gre za nekoliko drugačno ureditev glede vstopov v uradne službene oziroma poslovne prostore v 95. členu predloga ZVOP-2, tukaj gre namreč za snemanje znotraj delovnih prostorov. Člen je pretežno enak 77. členu dosedanjega ZVOP-1, s tem da je tretji odstavek dodal, da je spremljanje neposrednega dogajanja pred kamerami pod pogoji iz prvega in drugega odstavka 97. člena ZVOP-2 dopustno le, če ga izvaja pooblaščen varnostno osebje. Posebna dodana vrednost je v petem odstavku, kjer je določeno, da se mora pred uvedbo videonadzora v osebi javnega ali zasebnega sektorja delodajalec posvetovati z reprezentativnimi sindikati pri delodajalcu ter svetom delavcev ali delavskim zaupnikom (dosedaj je bilo to določeno le glede reprezentativnih sindikatov pri delodajalcu), kar je »jamstveni« prispevek k dodatnemu spoštovanju človeškega dostojanstva z uporabo mehanizmov participacije s področja socialne države (2. člen Ustave Republike Slovenije).

**K 98. členu:**

V 98. členu je urejena nova vrsta videonadzora, namreč izvajanje videonadzora na javnih površinah, kar dosedaj ni bilo urejeno v ZVOP-1. Določbe so načeloma previdno in sorazmerno napisane, upoštevajo delno dejansko stanje, njihov namen pa ni podpiranje ali promocija ali razvoj ti. »totalne nadzorovalne družbe«. Po prvem odstavku je videonadzor na javnih površinah dovoljen le v izjemnih primerih, kadar je to nujno potrebno, ker obstaja resna in utemeljena nevarnost za življenje ali zdravje ljudi, varnost premoženja ali varovanje tajnih podatkov in tega namena ni mogoče doseči z milejšimi sredstvi (prvi strogi kriterij/skupek pogojev kumulativne narave). Prav tako je dovoljen za potrebe varovanja prostorov, zgradb ali območij, ki jih je potrebno varovati na podlagi zakona in sicer samo v obsegu in trajanju, ki je za dosego teh namenov nujno potreben (drugi in nekoliko milejši kumulativni kriterij). Po drugem odstavku se videonadzor lahko izvaja le glede tistih delov javne površine in v obsegu, kjer je potrebno varovati interese iz prvega odstavka 98. člena ZVOP-2. V tretjem odstavku je podana še organizacijska omejitev, po kateri lahko videonadzor na javnih površinah izvaja le oseba javnega ali zasebnega sektorja, ki upravlja z javno površino ali na njej zakonito opravlja dejavnost.

**K 99. členu:**

V 99. členu se začne 3. poglavje X. dela Predloga ZVOP-2 – urejanje biometrije oziroma biometričnih ukrepov. Kot že v ZVOP-1, je zakonodajni pristop glede biometrije dokaj zadržan in garantističen, kar pomeni – načeloma nenaklonjen uporabi biometrije. Ne glede na navedeno predlagane rešitve nekoliko omogočajo širšo uporabo biometrije (za zasebni sektor), kot je to dosedaj bila urejena v ZVOP-1.

99. člen ureja biometrične ukrepe v javnem sektorju. Biometrične ukrepe v javnem sektorju se lahko določi le z zakonom, če je to nujno potrebno za varnost ljudi ali premoženja ali za (dodatno) identifikacijo pogrešanih ali umrlih posameznikov ter poslovne skrivnosti, tega namena pa ni možno doseči z milejšimi sredstvi (načelo sorazmernosti). Po izjemi v drugem odstavku se ne glede na prejšnji odstavek biometrične ukrepe lahko določi z zakonom, če gre za izpolnjevanje obveznosti iz obvezujoče mednarodne pogodbe ali za identifikacijo posameznikov pri prehajanju državnih meja. Predlagani člen ima določen tudi prekršek za kršitve v 116. členu ZVOP-2.

**K 100. členu:**

V predlaganem 100. členu se urejajo biometrični ukrepi v zasebnem sektorju. Po prvem odstavku lahko zasebni sektor izvaja biometrične ukrepe le, če so nujno potrebni za opravljanje dejavnosti, za varnost ljudi ali premoženja ali za varovanje tajnih podatkov ali poslovne skrivnosti v skladu z določbami tega člena. Po drugem odstavku sme biometrične ukrepe izvajati nad svojimi zaposlenimi ter nad tistimi osebami, ki so zaposlene pri pogodbenih partnerjih upravljavca, če je to potrebno za namene varovanja interesov iz prvega odstavka in so bili te osebe o tem predhodno pisno obveščene. Po tretjem odstavku zasebni sektor lahko izvaja biometrične ukrepe tudi nad svojimi strankami pod naslednjimi pogoji: da tako za namene varovanja interesov iz prvega odstavka določa zakon in so stranke podale pisno privolitev ter se na ta način preprečuje nastanek hude škode, kar je pomembna izjema od strogega pristopa k dovoljeni uporabi biometrije. V četrtem odstavku je kot varovalni organizacijski ukrep določeno da mora upravljavec osebnih podatkov, ki namerava izvajati biometrične ukrepe, še pred uvedbo ukrepov posredovati Informacijskemu pooblaščenцу opis nameravanih ukrepov in razloge za njihovo uvedbo. V petem odstavku je določeno, da je Informacijski pooblaščenec dolžan po prejemu posredovanih informacij iz četrtega odstavka dolžan v dveh mesecih odločiti, ali je nameravana uvedba biometričnih ukrepov v skladu s tem zakonom, predvsem s pogoji iz prvega stavka prvega odstavka tega člena. Rok se ob upoštevanju zapletenosti predvidene obdelave lahko podaljša za največ dva meseca. Po šestem odstavku sme upravljavec osebnih podatkov izvajati biometrične ukrepe šele po prejemu odločbe iz petega odstavka, s katero je izvajanje biometričnih ukrepov dovoljeno. Po sedmem odstavku zoper odločbo Informacijskega pooblaščenca iz petega

odstavka tega člena ni pritožbe, dovoljen pa je upravni spor. V osmem odstavku je določena večja izjema, po kateri upravljavcu izjemoma ni treba pridobiti odločbe iz petega odstavka tega člena, če pri izvajanju biometričnih ukrepov ne nastaja zbirka biometričnih značilnosti ali matematičnih pretvorb biometričnih značilnosti in so te vedno pod nadzorom posameznika. Po devetem odstavku mora upravljavec pred začetkom uporabe biometričnih ukrepov posamezniku, nad katerim se bodo izvajali ti ukrepi, predložiti splošno obvestilo o zakonski ureditvi izvajanja biometričnih ukrepov, ki ga izdela in na svoji spletni strani objavi Informacijski pooblaščenec.

Predlagani člen ima določen tudi prekršek za kršitve v 117. členu ZVOP-2.

#### **K 101. členu:**

V 101. členu Predloga ZVOP-2 je določena obdelava osebnih podatkov v okviru evidentiranja vstopov in izstopov iz službenih prostorov, podobno kot je to že urejeno v 82. členu ZVOP-1. Po prvem odstavku oseba javnega ali zasebnega sektorja lahko za zagotavljanje varnosti ljudi in premoženja, ter reda v njenih prostorih ali v prostorih, ki jih ima v uporabi od posameznika, ki namerava vstopiti ali izstopiti iz tega prostora, zahteva, da navede vse ali nekatere osebne podatke iz drugega odstavka tega člena ter razlog vstopa ali izstopa. Po potrebi pa lahko osebne podatke preveri tudi z vpogledom v osebni dokument posameznika. Po drugem odstavku se v zbirki o vstopih in izstopih iz službenih prostorov lahko o posamezniku vodijo samo naslednji osebni podatki, kadar je to potrebno: osebno ime, številka in vrsta osebnega dokumenta, naslov prebivališča, zaposlitev, vrsta in registrska številka vozila ter datum, ura in razlog vstopa ali izstopa v ali iz prostorov. Po tretjem odstavku evidenca iz prejšnjega odstavka velja za uradno evidenco v skladu z Zakonom o splošnem upravnem postopku (drugi odstavek 179. člena), če je potrebno pridobiti podatke iz nje z vidika koristi mladoletnika ali za izvrševanje pristojnosti policije ter obveščevalno-varnostne dejavnosti. Po četrtem odstavku se osebni podatki iz evidence iz drugega odstavka tega člena se lahko hranijo največ tri leta (rok hrambe) od vpisa, nato se zbršejo ali na drug način uničijo, če zakon ne določa drugače.

Predlagani člen ima določen tudi prekršek za kršitve v 118. členu ZVOP-2.

#### **K 102. členu:**

V 102. členu je določeno, da se lahko osebni podatki iz javne knjige, urejene z zakonom (npr. zemljiška knjiga), uporabljajo le v skladu z namenom<sup>84</sup>, za katerega so bili zbrani ali se obdelujejo, če je zakoniti namen njihovega zbiranja ali obdelave določen ali določljiv (se da na njega iz vsebine zakona sklepati tako, da je določljiv – npr. varnost pravnega prometa, izkazovanje pravnih ali osebnih stanj ipd.). S tem členom je povezana tudi prekrškovna določba v 119. členu ZVOP-2.

#### **K 103. členu:**

Predlagani 103. člen določa pretežno podobno, kot je to že v 84. členu ZVOP-1, urejeno povezovanje vsebine uradnih evidenc in javnih knjig. Javne knjige so omenjene že v 102. členu in v njegovi obrazložitvi, uradne evidence pa so tiste evidence, ki so določene (opisane) v drugem odstavku 179. člena Zakona o splošnem upravnem postopku<sup>85</sup>. Definicija povezovanja je določena v 4. točki tretjega odstavka 6. člena ZVOP-2. Razlika napram določbam prvega odstavka 84. členu ZVOP-1 glede na predlagane določbe v sedanjem prvem odstavku 103. člena ZVOP-2 je v tem, da so podane morda potrebne pojasnilne določbe, povezovanja med katerimi zbirkami so mišljena (»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«). Po drugem

<sup>84</sup> 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.

<sup>85</sup> Uradni list RS, št. 24/06 – uradno prečiščeno besedilo, 105/06 – ZUS-1, 126/07, 65/08, 8/10 in 82/13.

odstavku so upravljavci ali upravljavec, ki povezuje dve ali več zbirk iz prvega odstavka, dolžni o tem predhodno pisno obvestiti Informacijskega pooblaščenca. Po tretjem odstavku v primeru, da če vsaj ena zbirka iz prvega odstavka, ki naj bi se jo povežalo, vsebuje osebne podatke iz 17. (posebne vrste osebnih podatkov) ali 18. člena (podatki o kazenskih obsodbah ali kaznovanjih za prekrške) ZVOP-2, ali če bi povezovanje imelo za posledico njihovo razkritje ali je za izvedbo povezovanja potrebna uporaba povezovalnega znaka, povezovanje ni dovoljeno brez predhodnega dovoljenja Informacijskega pooblaščenca. Informacijski pooblaščenec dovoli povezavo po tretjem odstavku na podlagi pisne vloge upravljavca, če ugotovi, da upravljavci zagotavljajo ustrezno varnost osebnih podatkov. Po petem odstavku pa zoper odločbo iz četrtega odstavka ni pritožbe, dovoljen pa je upravni spor. S tem členom so povezane prekrškovne določbe v 120. členu ZVOP-2.

**K 104. členu:**

V 104. členu je določena uvodna določba za posebno poglavje (7. poglavje) X. dela Predloga ZVOP-2 o strokovnem nadzoru in obdelavi osebnih podatkov.

**K 105. členu:**

V 105. členu so ponovljene dosedanje konkretne določbe o obdelavi osebnih podatkov v okviru strokovnega nadzora, kot je to določeno že v 88. členu ZVOP-1.

**K 106. členu:**

V 106. členu je določeno obveščanje posameznika in dodatna obdelava osebnih podatkov, kot je to določeno v 89. členu ZVOP-1. S tem členom so povezane prekrškovne določbe v 121. členu ZVOP-2.

**K 107. členu:**

V 107. členu so določeni strokovni nadzor in obdelava posebnih vrst osebnih podatkov, kot je to določeno v 90. členu ZVOP-2. S tem členom so povezane prekrškovne določbe v 121. členu ZVOP-2.

**11. K XI. delu Predloga ZVOP-2:**

**K 108. členu:**

Predlagani 108. člen določa načine uporabe določb Splošne uredbe glede upravnih kazni in glob ter odločanje o prekrških po tem delu zakona. Predlagani člen je pomemben z vidika določitve nadzornega in prekrškovnega organa, prenosa (pretvorbe) upravnih glob v prekrške ter glede odločanja o (pre)visokih upravnih globah po Splošni uredbi. Preko njegove vsebine se zagotavlja pravna varnost na področju prekrškov kot dela kaznovalnega prava.

Po prvem odstavku mora Informacijski pooblaščenec (glede na prvi odstavek 70. člena ZVOP-2) odločati o predpisanih kršitvah in upravnih globah iz člena 83 Splošne uredbe kot o prekrških v okviru pristojnosti prekrškovnega organa po določbah Zakona o prekrških, kolikor ta zakon ne določa drugače (pomeni: prilagojeno, npr. glede na drugi odstavek 108. člena ZVOP-2). Zakon o prekrških torej predpisane (opise; znake) kršitev iz Splošne uredbe opredeli kot prekrške, njihove sankcije pa kot sankcije za prekrške (slovensko kaznovalno pravo pozna v okviru kaznivih dejanj le kazniva dejanja in prekrške).

V drugem odstavku je sistemsko določeno, da se pri odločanju Informacijskega pooblaščenca o višini izrečene globe za kršitve, predpisane v členu 83 Splošne uredbe, v skladu z določbami prvega odstavka člena 83 Splošne uredbe in Zakona o prekrških, ob obravnavanju konkretnih okoliščin

posameznega primera tudi upošteva, da globa ne sme biti nesorazmerno breme ali neprimerljivo breme za upravljavce ali obdelovalce glede na druge primerljive kršitve človekovih pravic in temeljnih svoboščin, ki se kaznujejo za prekrške, ali je obstajal namen koristoljubnosti ali namen škodovanja posameznikom, na katere se nanašajo osebni podatki, v primeru izvajanja popravljivih ukrepov s strani upravljavca ali obdelovalca njihovo učinkovitost ali samostojno ukrepanje še pred uvedbo nadzora, glede fizičnih oseb pa se zlasti upošteva splošna raven dohodkov v Republiki Sloveniji ter njihov ekonomski položaj. Prav tako je treba upoštevati pri tem odločanju za vse obdelovalce ali upravljavce ali gre za ponavljajoče kršitve in pomen, ki bi ga za odvratanje teh kršitev imela izbira vrste ali višine globe. Pri tem se upošteva pooblastilo iz uvodnega dela besedila drugega odstavka člena 83 Splošne uredbe ter zlasti (c) in (k) točke navedenega odstavka. Na ta način se onemogoča, da bi bile v neskladju s temeljnim ustavnim načelom sorazmernosti (2. v zvezi s tretjim odstavkom 15. člena Ustave Republike Slovenije) izrečene nesorazmerno visoke globe (kot že navedeno, je delno primerljiva ureditev zaradi pretiranosti glob v ustavnosodni presoji pred Ustavnim sodiščem Republike Avstrije).

V predlaganem tretjem odstavku je določeno, da višine in razponi upravnih glob, ki so za pravne osebe, samostojne podjetnike posameznike in posameznike, ki samostojno opravljajo dejavnost, za kršitve, predpisane v členu 83 Splošne uredbe ter določene v 109. in 110. členu ZVOP-2, se uporabljajo ne glede na določbe o razponih glob iz 17. člena Zakona o prekrških.

V predlaganem četrtem odstavku je ponovno določeno, da Informacijski pooblaščenec odloča kot prekrškovni organ tudi o predpisanih prekrških po tem delu ZVOP-2 in po določbah Splošne uredbe.

V predlaganem petem odstavku je določeno, da Informacijski pooblaščenec lahko za prekrške po določbah Splošne uredbe in iz ZVOP-2 v hitrem postopku izreče globo v kateri koli višini v razponu, kot je določena v določbah Splošne uredbe in ZVOP-2.

#### **K 109. členu:**

V predlaganem 109. členu so zaradi pravne varnosti in pravne jasnosti (uporaba s strani prekrškovnega organa) z vidika prava prekrškov določene kršitve iz četrtega odstavka člena 83 Splošne uredbe.

#### **K 110. členu:**

V predlaganem 110. členu so tudi zaradi pravne varnosti in pravne jasnosti (uporaba s strani prekrškovnega organa) z vidika prava prekrškov določene kršitve iz petega odstavka člena 83 Splošne uredbe.

#### **K 111. členu:**

V 111. členu so določeni prekrški glede kršitve splošnih določb prve področne ureditve po ZVOP-2, namreč splošnih določb o videonadzoru, katere med drugim vključujejo ne-objavo obvestila o izvajanju videonadzora ipd. Globe so razumno (sorazmerno) predpisane.

#### **K 112. členu:**

V predlaganem 112. členu so določeni prekrški glede kršitev določb o videonadzoru glede dostopa v uradne službene oziroma poslovne prostore. Tudi v tem primeru so globe razumno (sorazmerno) predpisane.

#### **K 113. členu:**

V predlaganem 113. členu so določeni prekrški glede kršitev določb o videonadzoru pri večstanovanjskih stavbah. Tudi v tem primeru so globe razumno (sorazmerno) predpisane, so nekoliko nižje kot v primerih po 111. in 112. členu ZVOP-2, ker se upošteva pomembnejši zasebnopravni kontekst stanovanjskih razmerij.

**K 114. členu:**

V 114. členu so določeni prekrški glede kršitev določb o videonadzoru v delovnih prostorih. Tudi v tem primeru so globe razumno (sorazmerno) predpisane, so pretežno enake kot v primerih po 111. in 112. členu ZVOP-2, ker se upošteva pomembnejši kontekst varstva delavcev v delovnih prostorih.

**K 115. členu:**

V 115. členu so določeni prekrški glede kršitev določb o videonadzoru na javnih površinah (nov prekršek). Glede na kontekst (javne površine; javni prostor), kjer je večja nevarnost nastanka nadzorovalne države ozir. družbe je višina prekrškov nekoliko višja, vseeno pa primerljiva globam po 111. in 112. členu ZVOP-2.

**K 116. členu:**

V predlaganem 116. členu je določen prvi prekršek s področja druge področne – biometrije. Globe so razumno (sorazmerno) predpisane za kršitve določb glede biometrije v javnem sektorju.

**K 117. členu:**

V predlaganem 117. členu je določen drugi prekršek s področja druge področne – biometrije. Globe so razumno (sorazmerno) predpisane za kršitve določb glede biometrije v zasebnem sektorju.

**K 118. členu:**

V predlaganem 118. členu je določen prekršek s področja tretje področne ureditve, namreč kršitev določb o evidenci vstopov in izstopov. Glede na kontekst (običajni vstopi in izstopi v prostore) so globe razumno (sorazmerno) predpisane – nižje kot npr. v 111. in 112. členu ZVOP-2.

**K 119. členu:**

V predlaganem 119. členu je določen prekršek s področja četrte področne ureditve, namreč kršitev določb o javnih knjigah (njihovi namenski uporabi). Globe so razumno (sorazmerno) predpisane za kršitve določb.

**K 120. členu:**

V predlaganem 119. členu so določeni prekrški s področja pete področne ureditve glede povezovanj uradnih evidenc in javnih knjig (glede na prvi odstavek, drugi odstavek in tretji odstavek 103. člena ZVOP-2). Globe so glede na kontekst predpisane v nekoliko večji višini (glede na 119. člen).

**K 121. členu:**

V 121. členu so predpisani prekrški glede na 105. in 107. člen ZVOP-2, katera urejata področje strokovnega nadzora in obdelavo osebnih podatkov (torej zadnja - šesta področna ureditev). Globe so razumno (sorazmerno) predpisane za kršitve navedenih določb.

## **12. K XII. delu Predloga ZVOP-2:**

### **K 122. členu:**

V predlaganem 122. členu se urejajo prehodne določbe ZVOP-2, upoštevajoč zlasti načelo pravne varnosti in »pod-načelo« zaupanja v pravo. Prvi odstavek določa splošno pravilo, da z dnem uveljavitve ZVOP-2 (123. člen ZVOP-2) preneha veljati Zakon o varstvu osebnih podatkov iz leta 2004 (s spremembami do leta 2007 – ZVOP-1).

Predlagani drugi odstavek določa, da so upravljavci (dosedanji upravljavci osebnih podatkov) in obdelovalci (dosedanji pogodbeni obdelovalci) dolžni v roku enega leta od začetka uporabe tega zakona (120. člen ZVOP-2) izvesti ustrezne ukrepe prilagoditve glede uporabe privolitve kot pravne podlage za obdelavo osebnih podatkov. Za navedeno obdobje velja, da če obdelovalec in upravljavec izvajata ustrezne ukrepe prilagoditve (na novi sistem privolitve) in je bila dosedaj podana privolitev v skladu z dosedanjimi pravili iz ZVOP-1, da izvajata ustrezne popravljalne ukrepe, ki za obdobje iz prvega stavka preprečujejo nastanek kaznivosti za prekršek po Zakonu o prekrških. Z vidika spoštovanja pravne in ekonomske varnosti je torej določeno enoletno prehodno obdobje za pridobivanje novih privolitev za obdelavo osebnih podatkov po novem ZVOP-2.

Predlagani tretji odstavek določa, da se v Zakonu o spremembah in dopolnitvah Zakona o izvrševanju kazenskih sankcij (ZIKS-1F)<sup>86</sup> se z dnem uporabe ZVOP-2 črta 88. člen iz ZIKS-1F, namreč črtanje dosedanje prehodne (začasne) določbe glede uporabe istega povezovalnega znaka iz ZIKS-1F, saj so rešitve iz njega vsebovane v tretjem do petem odstavku 13. člena ZVOP-2.

Predlagani četrti odstavek določa, da se postopki odločanja ali obdelave osebnih podatkov, ki so se pred začetkom uporabe ZVOP-2 začeli pri Informacijskem pooblaščenca, na sodiščih in drugih državnih organih ter pri upravljavcih osebnih podatkov in pogodbenih obdelovalcih, nadaljujejo in končajo po določbah ZVOP-1 – v roku enega leta po uveljavitvi ZVOP-2. To pomeni, da sta zagotovljena pravna in ekonomska varnost.

Predlagani peti odstavek določa ukinitve dosedanjega Registra zbirk osebnih podatkov iz 28. člena ZVOP-1, ki po Splošni uredbi ne sme več obvezujoče obstajati. Nato je določeno, da Informacijski pooblaščenec njegovo vsebino v roku enega meseca arhivira in nato v roku enega leta preda Arhivu Republike Slovenije, ki vsebino Registra hrani kot trajno arhivsko gradivo (pomembno za zgodovino pravne države ter delno tudi za pravno varnost).

Predlagani šesti odstavek določa za potrebe izvrševanja osmega odstavka 18. člena ZVOP-2 (Pravica do popravka ali izbrisa osebnih podatkov, do omejitve obdelave ter posebni ukrepi varnosti osebnih podatkov) prehodno dobo, po kateri so upravljavci ali obdelovalci, ki za izvajanje svojega delovanja pridobivajo osebne podatke iz registrov ali evidenc upravnih notranjih zadev, dolžni v roku dveh let po začetku uporabe tega zakona vzpostaviti ustrezne varnostne mehanizme po predhodnem soglasju Ministrstva za notranje zadeve.

### **K 123. členu:**

V končni določbi je v 123. členu predlagano, da ZVOP-2 začne veljati naslednji dan po objavi v Uradnem listu Republike Slovenije, uporabljati pa se začne 25. maja 2018.

---

<sup>86</sup> Uradni list RS, št. 54/15.

