PREDLOG
EVA: 2018-2030-0045
REDNI POSTOPEK

IPP 007-87/2019

ZAKON O VARSTVU OSEBNIH PODATKOV

(drugi krog strokovnega in medresorskega usklajevanja, 14. 8. 2019)

I. UVOD

1. OCENA STANJA IN RAZLOGI ZA SPREJEM PREDLOGA ZAKONA

Predlog zakona je pripravljen kot del novega razvoja zagotavljanja sistema in pravic s področja varstva osebnih podatkov v Republiki Sloveniji. Po letu 2004, ko je bil sprejet dosedaj že tretji slovenski Zakon o varstvu osebnih podatkov (ZVOP-1)[1], je namreč zaradi izjemnega razvoja informacijsko-komunikacijske tehnologije (IKT) prišlo do bistvenega povečanja v količini in tudi kakovosti obdelave osebnih podatkov. Osebni podatki so tako postali vedno bolj dostopni najprej državi in njenim organom, nato pa tudi zasebnemu sektorju, javnosti, ter posameznikom in posameznicam. Obdelava osebnih podatkov je postala del velike večine poslovnih procesov. Izvajati so se začele vedno bolj sistemske povezave med zbirkami osebnih podatkov. S tem so se tveganja zlorabe osebnih podatkov, kot so nepooblaščeni dostopi, množična razkritja, ter profiliranje posameznikov, močno povečala.

V odziv na te nove trende sta se najprej začela razvijati dodatna in okrepljena sodna praksa Sodišča Evropske unije in Evropskega sodišča za človekove pravice glede varstva osebnih podatkov, pri nas pa praksa Ustavnega sodišča Republike Slovenije, sčasoma pa je začelo prihajati tudi do sprememb na zakonodajnem področju. Tako je leta 2012 Evropska komisija predlagala sprejetje dveh novih pravnih aktov Evropske unije kot del 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, znana tudi po angleški kratici »GDPR«)«[2], ki naj bi **moderniziral pravno ureditev obdelave osebnih podatkov na splošno**, ter »Predlog Direktive Evropskega parlamenta in Sveta o varstvu posameznikov pri obdelavi osebnih podatkov, ki jih pristojni organi obdelujejo za namene preprečevanja, preiskovanja, odkrivanja ali pregona kaznivih dejanj ali izvrševanja kazenskih sankcij, in o prostem pretoku takih podatkov ter o razveljavitvi Okvirnega sklepa Sveta 2008/977/PNZ«[3], ki naj bi isto storil še **za ti. policijske oziroma kazensko pravosodne in podobne obdelave.**

[1] Prvi Zakon o varstvu osebnih podatkov Republike Slovenije je bil sprejet dne 7. 3. 1990 (Uradni list RS, št. 8/90, 19/91 in 59/99 - ZVOP), drugi Zakon o varstvu osebnih podatkov je bil sprejet dne 8. 7. 1999 (Uradni list RS, št. 59/99, 57/01, 59/01 – popr., 73/04 – ZUP-C in 86/04 – ZVOP-1), tretji Zakon o varstvu osebnih podatkov pa dne 15. 7. 2004 (Uradni list RS, št. 86/04, 113/05 – ZInfP, 51/07 – ZUstS-A, 67/07 in 94/07 – uradno prečiščeno besedilo 1).
[2] Št. 5853/12, 27.01.2012, Medinstitucionalna oznaka: 2012/0011(COD).
[3] Št. 5833/12, 27.01.2012, Medinstitucionalna oznaka: 2012/0010(COD).

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

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

1.1 Ocena stanja

V času vložitve predlogov navedenih pravnih aktov na ravni Evropske unije je imela Republika Slovenija sistem varstva osebnih podatkov urejen v skladu z določbami 38. člena Ustave Republike Slovenije[4] iz leta 1991, Direktive 95/46/ES[5] iz leta 1995, Okvirnega sklepa 2008/977/PNZ[6] iz leta 2008 in Konvencije o varstvu posameznikov glede na avtomatsko obdelavo osebnih podatkov[7] (Sveta Evrope) iz leta 1981.

Republika Slovenija je v obdobju od leta 2012 do začetka leta 2016 glede predlagane Splošne uredbe o varstvu podatkov in povezane Direktive iz načelnih sistemskih razlogov navedenima predlogoma pravnih aktov Evropske unije pretežno ali v celoti nasprotovala[8], ob tem pa navedla tudi vrsto posebej obrazloženih pridržkov. Razlogi nasprotovanja ozir. kritike so bili opozarjanje na poslabšano pravno varnost, možnost znižanja dosežene visoke ravni varstva osebnih podatkov, pretirane obveznosti za upravljavce osebnih podatkov in obdelovalce – tudi finančne, očitno pretirane globe za upravne kršitve določb Splošne uredbe o varstvu podatkov, nato pretirana pooblastila Evropski komisiji glede izdaje izvedbenih in delegiranih aktov, določeni ustavnopravni vidiki, izbira vrste pravnega akta v primeru predloga Splošne uredbe, ustreznost takratnega Okvirnega sklepa 2008/977/PNZ in torej nepotrebnost sprejetja predlagane Direktive ipd.

Glede takratnega Predloga Splošne uredbe o varstvu podatkov je bil bistveni zaključek iz stališča Republike Slovenije – poleg prej navedene želje za spremembo vrste pravnega akta iz uredbe v direktivo – da se mora Republika Slovenija v pogajanjih v okviru Sveta Evropske unije prizadevati, da »ne bi prišlo do neutemeljenega zniževanja standardov varstva osebnih podatkov, ki bi bili nižji glede na primerljivi kazalnik – »Direktivo 95/46/ES o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem pretoku takih podatkov««, glede predloga Direktive pa, da zadošča vsebina določb takrat veljavnega Okvirnega sklepa 2008/977/PNZ iz leta 2008 in da torej sprejetje predlagane Direktive ni potrebno.

---

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

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

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

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

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

Glede vsebine Predloga Splošne uredbe so se ob začetku njenega zakonodajnega obravnavanja pojavili ustavnopravni pomisleki tudi v Zvezni republiki Nemčiji, tako je leta 2012 nemški zvezni ustavni sodnik Johannes Masing objavil članek[9], v katerem je z vidika nemškega Temeljnega zakona (Ustava) in obširne in ustaljene ustavnosodne presoje nemškega Zveznega Ustavnega sodišča izredno kritično nastopil proti Osnutku Splošne uredbe o varstvu podatkov. V članku je med drugim navedeno, da gre za neustaven in nesmiseln odvzem pristojnosti, da se ne upošteva, da je pravica do varstva osebnih podatkov individualna človekova pravica, ki izhaja iz nacionalnih Ustav, da se po njenem morebitnem sprejetju ne bo dalo več z nacionalnimi zakoni sploh (kaj več kot minimalno) regulirati osebnih podatkov... - ter da bo dosedanja ustaljena ustavnosodna presoja nemškega Zveznega Ustavnega sodišča torej šla kar v «razrez« (v »makulaturo«).

V nadaljnjih pogajanjih v okviru Sveta Evropske unije se je vsebina določb obeh predlogov pravnih aktov razdelovala in doseženi so bili tudi določeni kompromisi, ki so na koncu privedli do sprejetja obeh navedenih pravnih aktov dne 27. aprila 2016. Tako sta bili navedenega dne sprejeti »**Uredba (EU) 2016/679 Evropskega parlamenta in Sveta z dne 27. aprila 2016 o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem pretoku takih podatkov ter o razveljavitvi Direktive 95/46/ES (Splošna uredba o varstvu podatkov)**«[10] - v nadaljnjem besedilu: Splošna uredba ter «**Direktiva (EU) 2016/680 Evropskega parlamenta in Sveta z dne 27. aprila 2016 o varstvu posameznikov pri obdelavi osebnih podatkov, ki jih pristojni organi obdelujejo za namene preprečevanja, preiskovanja, odkrivanja ali pregona kaznivih dejanj ali izvrševanja kazenskih sankcij, in o prostem pretoku takih podatkov ter o razveljavitvi Okvirnega sklepa Sveta 2008/977/PNZ**«[11] - v nadaljnjem besedilu: Direktiva.

Z vidika končnega rezultata je možno oceniti, da določbe v Splošni uredbi o obdelavi osebnih podatkov na podlagi zakonitih interesov, naknadni obdelavi osebnih podatkov v druge namene ter o pooblaščenih osebah, zlasti s ciljem unifikacije režimov varstva osebnih podatkov v posameznih državah članicah, morda pomenijo določeno stopnjo znižanja dosežene ravni varstva osebnih podatkov. Da bi se ta trend neutemeljenega zniževanja standardov varstva osebnih podatkov v čim večji meri ublažilo, se je predlagatelj odločil v najvišji možni meri nasloniti na ti. pooblastilne klavzule («opening clauses«), ki državam članicam glede določenih vprašanj omogočajo ohranitev njihove nacionalne ureditve (npr. glede pogojev obdelave osebnih podatkov zaradi izvajanja nalog v javnem interesu oziroma javnih oblasti, obdelave nekaterih posebnih vrst osebnih podatkov oziroma njim podobnih osebnih podatkov, osebnih podatkov umrlih oseb, ali obdelav v znanstvenoraziskovalne, zgodovinskoraziskovalne oz. arhivske namene). Te klavzule dajejo Splošni uredbi o varstvu osebnih podatkov v določenem delu značaj ti. »direktivnega akta«[12], kot da bi bila direktiva Evropske unije, zlasti z vidika možnosti nacionalnega zakonodajnega (področnega) urejanja. Kar pomeni, da je možno precej določb Splošne uredbe implementirati v slovenskih zakonih, z ozirom na konkretne okoliščine stanja ali razvoja varstva osebnih podatkov v Sloveniji. Delno podobno je glede sprejete Direktive, kar se tiče sistema določitve namenov obdelav osebnih podatkov (naknadna obdelava podatkov v druge namene, kot so bili prvotno zbrani) in tudi njene določbe je možno v zakonih Republike Slovenije izvesti glede na konkretne okoliščine stanja ali razvoja varstva osebnih podatkov v Sloveniji.

1.2 Razlogi za sprejem zakona

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

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

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

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

Zaradi navedenih pravnih aktov Evropske unije oz. Sveta Evrope so potrebne spremembe zakonodaje Republike Slovenije, torej zlasti sprejetje Zakona o varstvu osebnih podatkov kot sistemskega zakona Republike Slovenije za področje varstva osebnih podatkov.

Posledično je bilo pripravljeno besedilo predloga novega Zakona o varstvu osebnih podatkov, ki ustrezno upošteva tudi izkušnje in spoznanja glede uporabe dosedanjega ZVOP-1 iz leta 2004, določbe 38. člena Ustave Republike Slovenije o človekovi pravici do varstva osebnih podatkov[13], obstoječo ustavnosodno presojo Ustavnega sodišča Republike Slovenije glede človekove pravice do varstva osebnih podatkov od leta 1992[14] dalje ter tudi določbe še veljavne (Konvencije o varstvu posameznikov glede na avtomatsko obdelavo osebnih podatkov - Konvencija št. 108).

Koncept zakona je v obdobju 2017-2018 ter v medresorskem usklajevanju in strokovnem usklajevanju (6. 3. 2019) vključeval širšo vsebino, vseboval je namreč precej povezovalnih ali dopolnjevalnih določb v zvezi s Splošno uredbo. Glede na pripombe iz prvega kroga medresorskega in strokovnega usklajevanja (od 6. 3. 2019 dalje) je koncept zakona v tem delu spremenjen in sedaj premišljeno v I. delu zakona ureja splošne določbe (zakonitost, nediskriminacija, določene pravice ter postopek), v II. delu zakona pa ti. policijski pravosodni del. Predlog zakona izhaja iz vidika, da naj bo čimveč rešitev na enem mestu, nima pa predlog zakona več značaja ti. »zakonika«, saj upošteva neposredno uporabnost Splošne uredbe ter njene razlage, kot so se že razvile v praksi.

2. CILJI, NAČELA IN POGLAVITNE REŠITVE PREDLOGA ZAKONA

2.1 Cilji Predloga zakona

Cilji Predloga zakona so:

- zagotoviti izvrševanje določb Splošne uredbe, tako da se v mejah pooblastitvenih klavzul iz Splošne uredbe določi nacionalne posebnosti ureditve varstva osebnih podatkov, ter s tem v čim večji meri ohrani dosedanji visok nivo varstva osebnih podatkov v Republiki Sloveniji ter uresničevanje osebne človekove pravice do varstva osebnih podatkov (38. člen Ustave Republike Slovenije).
- zagotoviti prenos Direktive v pravni red Republike Slovenije, z istimi cilji.

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

Pri zakonodajni izvedbi določb Splošne uredbe se izhaja predvsem iz upoštevanja pooblastitvenih klavzul / direktivnih določb Splošne uredbe (tako določb členov kot tudi uvodnih navedb), ki določajo možnosti nacionalnih odstopanj od sicer neposredno uporabljive in enotne uredbene ureditve varstva osebnih podatkov. Splošna uredba tako npr. v uvodni navedbi št. 8 navaja, da »Kadar ta uredba določa natančnejše določitve ali omejitve svojih pravil s pravom držav članic, lahko države članice vključijo elemente te uredbe v svoje nacionalno pravo, kolikor je to potrebno zaradi skladnosti in razumljivosti nacionalnih določb za osebe, za katere se uporabljajo.«, v drugem odstavku člena 6 Splošne pa določa, da »lahko države članice Evropske unije ohranijo ali uvedejo podrobnejše določbe, da bi prilagodile uporabo pravil te uredbe v zvezi z obdelavo osebnih podatkov za zagotovitev skladnosti s točkama (c) in (e) prvega odstavka, tako da podrobneje opredelijo posebne zahteve v zvezi z obdelavo ter druge ukrepe za zagotovitev zakonite in poštene obdelave«. Še dalje pa posamezni členi Splošne uredbe določajo področja, kjer države članice niso uspele dogovoriti ali pa ne morejo vzpostaviti enotnih ali skupnih pravil varstva osebnih podatkov, in so zato ureditev teh področij prepustile nacionalni zakonodaji:

[13] Uradni list RS, št. 33/91-I, 42/97, 66/00, 24/03, 69/04, 68/06, 47/13 in 75/16.
[14] Začetna Odločba US, št. U-I-115/92, 24. 12. 1992; objava: OdlUS I, 105 in Uradni list RS, št. 3/93. Iz vmesnega obdobja sta morda vodilni odločbi: Odločba US, št. U-I-252/00, 8. 10. 2003; objava: Uradni list RS, št. 105/03 in OdlUS XII, 80 ter Odločba US, št. U-I-298/04, 27. 10. 2005; objava: Uradni list RS, št. 100/05 in OdlUS XIV, 77; iz obdobja po letu 2010 pa sta npr. pomembni: Odločba US, št. U-I-98/11, 26. 9. 2012: objava: Uradni list RS, št. 79/12 in Odločba US, št. U-I-70/12, 21. 3. 2014; objava: Uradni list RS, št. 24/14 in OdlUS XX, 23.

- pogoji za obdelavo osebnih podatkov v okviru dejavnosti zunaj področja uporabe prava Evropske unije ter obdelavo osebnih podatkov v strani Republike Slovenije, kadar deluje na področjih skupne varnostne in obrambne politike ter obveščevalno-varnostne dejavnosti (drugi odstavek 2. člena Splošne uredbe);
- pogoji za zagotovitev zakonitosti obdelave, ko gre za obdelave zaradi izpolnitve zakonske obveznosti oziroma izvajanja nalog v javnem interesu ali izvajanja javne oblasti, poverjene upravljavcu (drugi odstavek 6. člena Splošne uredbe);
- pogoji za preverjanje privolitve mladoletnih oseb v rabo storitev informacijske družbe (prvi odstavek 8. člena Splošne uredbe);
- pogoji za obdelavo osebnih podatkov umrlih oseb (uvodna navedba št. 27 k Splošni uredbi);
- pogoji za obdelave genskih podatkov, biometričnih ter zdravstvenih osebnih podatkov (drugi odstavek 9. člena Splošne uredbe);
- pogoji za obdelavo osebnih podatkov v kazenskih in prekrškovnih evidencah (10. člen Splošne uredbe);
- obveznost izbrisa osebnih podatkov po poteku določenega roka (točka e) prvega odstavek 17. člena Splošne uredbe) oziroma obveznost hrambe osebnih podatkov za določen rok (točki b) in e) tretjega odstavka 17. člena Splošne uredbe);
- obveznost priprave ocene učinkov oziroma izvedbe predhodnega usklajevanja z državnim nadzornim organom pri pripravi nekaterih zakonodajnih predlogov (peti odstavek 36. člena Splošne uredbe);
- pogoji za obvezno imenovanje pooblaščene osebe za varstvo osebnih podatkov, ter nalog pooblaščenih oseb (četrti odstavek 37. člena Splošne uredbe ter prvi odstavek 39. člena Splošne uredbe);
- pooblastila državnega nadzornega organa (prvi in šesti odstavek 58. člena);
- določitev ter postopek za izrekanje prekrškov zaradi kršitev določb Splošne uredbe (prvi odstavek 84. člena).

Zakonodajna izvedba Direktive, ki se načeloma nanaša na področje kaznovalnega delovanja države (kazensko pravosodje in policijsko delovanje) je predpisana v posebnem delu (II. del) predloga zakona, pri tem pa splošne določbe iz predloga zakona veljajo tudi za navedena področja iz tega posebnega dela predloga zakona – ob področnih določbah veljavne zakonodaje (npr. policijske, državnotožilske, kazensko procesne ipd.).

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

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

Delno primerljiv zakonodajni pristop, kot je predlagan v predlogu zakona, so dosedaj sprejele tudi tri primerljive države Evropske unije, namreč Zvezna republika Nemčija[15], Republika Avstrija[16] in Slovaška republika[17] (države s primerljivim pravnim redom in ustavnopravnim oziroma ustavnosodnim razumevanjem pravice do varstva osebnih podatkov). V njihovih novih zakonih o varstvu osebnih podatkov iz leta 2017 je zaslediti 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. Še bolj primerljiv slovenskim rešitvam iz predloga zakona je sicer bolj garantistični pristop Slovaške republike, ki je v njenem zakonu med drugim določila celo splošno uporabo (in istočasno neposredno uporabo) temeljnih definicij s področja varstva osebnih podatkov za vsa področja varstva osebnih podatkov iz njenega takratnega Predloga Zakona o varstvu osebnih podatkov in o spremembah in dopolnitvah določenih zakonov (št. UV-42294/2017, z dne 22. 9. 2017, sprejet dne 27. 11. 2017), natančno razdelala zakonska načela, ob tem da je dan poseben poudarek načelu zakonitosti, razdelala institut privolitve ter pravnosistemsko v zakonu izhajala iz celovite uporabe pristopa klasičnega mednarodnega zasebnega prava in postopka.

Predlog zakona delno sledi prenovljenemu izrazoslovju Splošne uredbe, npr. uporaba izrazov »zbirka« (dosedaj: zbirka osebnih podatkov), upravljavec (dosedaj: upravljavec zbirke osebnih podatkov), obdelovalec (dosedaj: pogodbeni obdelovalec), varnost osebnih podatkov (dosedaj: zavarovanje osebnih podatkov). Določene pojasnjevalne ali povezovalne spremembe glede teh izrazov so tudi v določenih delih predloga zakona (npr. posebne vrste osebnih podatkov v 12. členu).

Prav tako na dokončnejšo vsebino predloga zakona vpliva tudi dejstvo, da se je šele 23. maja 2018 izvedla objava popravkov uradne slovenske inačice besedil Splošne uredbe in Direktive, kar pa velja tudi za večino drugih jezikovnih inačic Splošne uredbe in Direktive.

Še dalje se, zlasti na pobudo predstavnikov gospodarstva ter združenja pooblaščenih oseb za varstvo osebnih podatkov, upošteva tudi dejstvo, da se v času vložitve predloga Splošna uredba neposredno uporablja že več kot eno leto, ter da morajo biti odstopanja od Splošne uredbe omejena zgolj na področja, kjer je to resnično potrebno za ohranitev visoke ravni varstva osebnih podatkov.

Glede na posebno kombinacijo in vsebino pravnih aktov Evropske unije, ki zahtevajo spremembe na področju sistemske ureditve varstva osebnih podatkov, delno prilagojeno »filozofijo« varstva osebnih podatkov glede na te pravne akte, relevantno Konvencijo Sveta Evrope, pomen zlasti določb 38. in 87. člena Ustave Republike Slovenije ter povezane ustaljene ustavnosodne presoje Ustavnega sodišča Republike Slovenije in tradicijo zakonodajnega urejanja varstva osebnih podatkov v Republiki Sloveniji predlagatelj ocenjuje, da je **edina možnost, da se pripravi nov Zakon o varstvu osebnih podatkov**, ki bi omogočal povezan in čimbolj koherenten pristop glede vseh teh vsebin in njihovih zahtev. Teh vsebin in zahtev ne bi bilo možno doseči le z novelo veljavnega ZVOP-1, ali s sprejemom ločenega zakona za ti. policijske oziroma kazensko pravosodne obdelave osebnih podatkov. Zlasti z vidika spoštovanja načela pravne varnosti je pristop skupnega urejanja sistema varstva osebnih podatkov na enem mestu (tradicionalen že od leta 1990[18]) – lahko edini upravičen.

2.3. O zakonodajni tehniki predloga zakona

Uporabljena je kombinacija več zakonodajnih tehnik:

1. tehnika indikacije (sklica), npr. na pravne podlage iz Splošne uredbe,
2. tehnika določanja posebnosti – pri pooblastilnih klavzulah,

[15] 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.
[16] 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.
[17] Zakon o varstvu osebnih podatkov in o spremembah in dopolnitvah določenih zakonov: objava: č. 704/2017 Z. z..
[18] Glejte: Zakon o varstvu osebnih podatkov iz leta 1990 (Uradni list RS, št. 8/90, 19/91 in 59/99 - ZVOP).

3. tehnika razčlenitve – npr. postopka z zahtevami posameznika,

4. tehnika prepisa – npr. ključnih obveznosti upravljavca in obdelovalca.

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

Za razliko od prejšnjih osnutkov oziroma predlogov zakona se tehnika prepisa zdaj uporablja v bistveno manjši meri.

2.4. Načela predloga zakona

Načelo spoštovanja osebnosti in pravic človeka

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

Načelo zakonitosti

Načelo zakonitosti v predlogu zakona izhaja iz drugega odstavka 38. člena Ustave Republike Slovenije (»Zbiranje, obdelovanje, namen uporabe, nadzor, in varstvo tajnosti osebnih podatkov določa zakon.«) ter iz 87. člena Ustave Republike Slovenije po katerem se pravice in obveznosti lahko urejajo le z zakonom. Navedeno načelo izhaja tudi iz temeljne uvodne navedbe št. 39 Splošne uredbe, (a) točke prvega odstavka 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[19]). Temu pristopu tako sledijo 9. točka tretjega odstavka 6. člena, nato a) točka prvega odstavka 7. člena, zlasti pa prvi odstavek 8. člena in delno prvi odstavek 9. člena predloga zakona. Za delovanje (odločanje, poseganje v pravice, določanje obveznosti) s strani javnega sektorja (javne oblasti) velja strogo načelo zakonitosti, za zasebni sektor pa je to načelo nekoliko omiljeno v smislu, da lahko splošne določbe Splošne uredbe ter predloga zakona določajo splošna pravila za posege v varstvo osebnih podatkov, ki se jih nato konkretno uporabi v praksi preko ocene učinkov na varstvo osebnih podatkov. Tako (delno) omiljeno spoštovanje načela zakonitosti za zasebni sektor (pogodbe, storitve) je zahteva iz točk (a), (b) (d) in (f) prvega odstavka 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 zakona, konkretneje, po ustavnosodni presoji z uporabo strogega testa sorazmernosti (predvsem odločba US, št. U-I-60/03, 4. 12. 2003[20], zlasti 30. točka v zvezi s 17. točko odločbe).

Načelo namenske obdelave osebnih podatkov

[19] Odločba US, št. U-I-115/92, 24. 12. 1992; objava: Uradni list RS, št. 3/93 in OdlUS I, 105.
[20] Objava: Uradni list RS, št. 131/03 in OdlUS XII, 93.

Določbe predloga zakona 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 zakona 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. Vendar pa je ta odstop dosledno uveljavljen le na področju, kjer je Splošna uredba primarna, torej glede obdelav za zasebne namene – in še tam ima ta rešitev zakonsko podlago (6. člen Splošne uredbe), medtem ko je za obdelave zaradi izvrševanja javnega interesa in javne oblasti, še zlasti pa za obdelave po ti. Policijski direktivi tako bližje določbam Ustave – izrecno določilo, da lahko to določa le (področni) zakon.

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«[21]. Za posege s strani zasebnega sektorja pa je navedeno načelo omejeno v skladu z določbami predloga zakona in točkami (a), (b) (d) in (f) prvega odstavka člena 6 Splošne uredbe.

2.5. Poglavitne zakonodajne rešitve iz predloga zakona

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

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

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

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

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

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

Za namene izkazovanja skladnosti obdelave osebnih podatkov sta kot obveznost za upravljavce in obdelovalce poleg izvedbe ocene učinkov določena tudi izvajanja ukrepa ti. notranje sledljivosti posredovanj osebnih podatkov ((e) točka drugega odstavka 34. člena predloga zakona) ter ukrepa ti. zunanje sledljivosti obdelav osebnih podatkov (sedmi odstavek 30. člena predloga zakona), precej podobno kot v dosedanjem tretjem odstavku 22. člena ZVOP-1.

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

Podrobneje je urejen tudi postopek uveljavljanja pravic posameznikov, na katere se nanašajo osebni podatki, tudi z delno uporabo določb Zakona o splošnem upravnem postopku, kadar gre za javnopravne subjekte pravnega reda Republike Slovenije.

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

Posebej je v predlogu zakona poudarjen pomen svobode izražanja v razmerju do varstva osebnih podatkov, tako da je omogočeno zadržanje dosedanje ravni uresničevanja svobode izražanja v okviru pravnega reda Republike Slovenije[22].

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

Področje pravosodja in policije ter izvrševanja kazenskih sankcij in delno obrambe ter varnosti države je urejeno v posebnem delu predloga zakona (II. del), kjer pa je tudi navedeno da Idoločene določbe iz I. dela zakona veljajo tudi za to področje (obravnavanje zahtev, sledljivost ipd.). Ustrezne specifike in izjeme, tako glede namenov obdelav osebnih podatkov, kot tudi obveščanja posameznikov o njihovih osebnih podatkih, so seveda urejene specifično, glede na določbe Direktive. V povezavi s tem delom zakona so urejene tudi specifike glede obdelav osebnih podatkov na področjih varnosti države in obrambe države, sicer še vedno v okviru sistema in pravic ter njihovih omejitev po tem zakonu.

[22] Gre za načelen in sistemski pristop Republike Slovenije, ki v obdobju zadnjih približno 7 let ni bil izražen samo pri sprejemanju Stališč Republike Slovenije glede predlogov Splošne uredbe in Direktive leta 2012, ampak tudi širše (mednarodno prepoznavno), npr. pisna in ustna intervencija Republike Slovenije leta 2014 v postopku v primeru *Maximillian Schrems* (ti. »*Facebook primer*«) - sodba SEU, C-362/14, 6. 10. 2015 ter v vzdržanosti pri glasovanju Republike Slovenije (kot ene od le štirih držav, ki so se vzdržale glasovanja iz načelnih razlogov) glede Ščita zasebnosti (»*Privacy Shield*«) dne 8. 7. 2016 (glejte npr.: https://www.theguardian.com/technology/2016/jul/08/privacy-shield-data-transfer-us-european-union) ter tudi glede garantistične in podrobnejše vsebine določenih bilateralnih mednarodnih pogodb (npr. s področja policijskega in pravosodnega sodelovanja).

V področnih ureditvah obdelav osebnih podatkov (III. del predloga zakona) so npr. delno prenovljeno razdelane določbe o videonadzoru (npr. uvedba videonadzora na javnih površinah) ter o biometriji. Dodana je tudi možnost objavljanja sodb v okviru razmerja med varstvom osebnih podatkov in dostopom do informacij javnega značaja, vključno s psevdonimiziranimi objavami sodb prvostopenjskih sodišč.

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

Glede na drugačne definicije iz Splošne uredbe in Direktive je prišlo do znatne spremembe dosedanjega tradicionalnega izrazoslovja s področja varstva osebnih podatkov (ustaljeno od leta 1984[23])..

Tako so sedanji novi temeljni izrazi zlasti:

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

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

- ukinitev Registra zbirk osebnih podatkov in dolžnosti notifikacije zbirk Informacijskemu pooblaščencu, kar je nadomeščeno z evidenco dejanj obdelav za upravljalce in obdelovalce osebnih podatkov;
- na predloge prakse je v predlogu zakona še vedno urejeno neposredno trženje, četudi je z vidika Splošne uredbe morda nekoliko sporno, koliko je neposredno trženje dopustno – izhaja se iz stališča, da je bolje regulirati, kot prepustiti nejasni praksi, ki lahko področje čisto odpre ali pa pride do (možnih) določenih prepovedi;
- določen je olajšan sistem izbire pooblaščene osebe za varstvo osebnih podatkov (pomembno za gospodarstvo, samoupravne lokalne skupnosti, pa tudi za državne organe- to so osebe, ki svetujejo znotraj upravljavcev osebnih podatkov glede skladnosti obdelave osebnih podatkov), tudi javni sektor lahko izbere osebo iz zasebnega sektorja, olajšani so tudi pogoji glede njihovih izkušenj, delovne dobe, usposobljenosti (v prehodnih določbah), za področje vzgoje in izobraževanja ter samoupravnih lokalnih skupnosti je tudi določen olajšan sistem določanja pooblaščenih oseb za varstvo osebnih podatkov;
- določena je definicija povezovanja zbirk osebnih podatkov – samo veliki sistemi s tveganimi obdelavami osebnih podatkov bodo potrebovali ureditev v področnem zakonu (sodni register, E-Sociala…) ter Informacijski pooblaščenec ne bo izdajal odločb o povezovanju.

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

2.6. Sprejetje zakona

Zakon bi moral biti uveljavljen že 6. 5. 2018, ko je potekel rok za zakonodajno izvedbo Direktive (EU) 2016/680 oziroma 25. 5. 2018 ko bi moral biti slovenski Zakon o varstvu osebnih podatkov usklajen s Splošno uredbo o varstvu podatkov in povezano Direktivo. Zato mora zakon biti čimprej sprejet in objavljen v Uradnem listu Republike Slovenije.

3. OCENA FINANČNIH POSLEDIC PREDLOGA ZAKONA ZA DRŽAVNI PRORAČUN IN DRUGA JAVNA FINANČNA SREDSTVA

3.1 Ocena finančnih sredstev za državni proračun:

Predlog zakona ne bo imel posledic za Proračun Republike Slovenije.

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

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

Ocena drugih javnih finančnih sredstev:

Predlog zakona ne bo imel posledic za druga javno finančna sredstva.

Predvideno povečanje ali zmanjšanje prihodkov državnega proračuna:

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

Predvideno povečanje ali zmanjšanje obveznosti za druga javna finančna sredstva:

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

Predvideni prihranki za državni proračun in druga javna finančna sredstva;

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

Sredstva bodo zagotovljena z zadolževanjem (poroštva):

Zaradi predloga zakona ni potrebno zadolževanje.

V naslednjem proračunskem obdobju bodo sredstva zagotovljena:

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

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

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

Za leto 2018 so bile zagotovljene naslednje proračunske postavke:

- proračunska postavka 1267 plače; na kateri so predvidena finančna sredstva za 10 novih državnih nadzornikov za varstvo osebnih podatkov (41. plačni razred in 10 let delovne dobe) - na letni ravni se za enega ocenjujejo finančna sredstva v višini 34.200,00 EUR, skupaj 342.000,00 EUR,
- proračunska postavka 1273 investicije; na kateri so zagotovljena finančna sredstva za osnovno opremo za 10 novo zaposlenih, skupaj 10.000,00 EUR
- proračunska postavka 1271; na kateri so predvidena finančna sredstva za materialne stroške, selitev, skupaj v znesku 20.000,00 EUR ter za najem poslovnih prostorov za obdobje 6 mesecev (15.300 EUR/mesec), skupaj 91.800,00 EUR.

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

Za sedanje proračunsko leto 2019 pa so zagotovljena naslednja finančna sredstva oziroma proračunske postavke:

- proračunska postavka 1267 plače; na kateri so predvidena finančna sredstva za 5 novih državnih nadzornikov za varstvo osebnih podatkov (41. plačni razred in 10 let delovne dobe) - na letni ravni za enega ocenjujejo finančna sredstva v višini 34.200,00 EUR, skupaj 171.000,00 EUR in
- proračunska postavka 1273 investicije; na kateri so zagotovljena finančna sredstva za osnovno opremo za 5 novo zaposlenih, skupaj 5.000,00 EUR, najem poslovnih prostorov za 12 mesecev (15.300 EUR/mesec), skupaj 183.600,00 EUR.

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

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

5. 1. Uvodno o primerjalnopravni ureditvi

V letu 2017 in do meseca maja 2018 so bili sprejeti le štirje izvedbeni zakoni držav članic Evropske unije – v Zvezni republiki Nemčiji, v Republiki Avstriji, v Slovaški republiki ter v Kraljevini Belgiji. Večina preostalih držav članic Evropske unije je šele po mesecu maju 2018 sprejela izvedbene zakone ali pa jih še pripravlja ali pa delno rešuje stanje glede nesprejete zakonodaje celo z uredbami z zakonsko močjo, če to njen ustavni red dopušča (npr. Kraljevina Španija). »Modeli« oziroma »smeri« zakonodajnega urejanja iz navedenih zakonov so si precej različne (načeloma je vsaka država razvila

zakonsko izvedbeno ureditev v njej lastno smer)[24], 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[25] ter naknadno glede njega ocenila, da bo treba zaradi vsebinske nepopolnosti oziroma vsebinskih problemov že sprejeti zakon razveljaviti (v delu, ki se nanaša na varstvo osebnih podatkov) ter pripraviti popolnoma nov Zakon o varstvu osebnih podatkov, ki je bil nato izdan leta 2018[26]. 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« oziroma »smeri« zakonodajnega urejanja s strani držav članic Evropske unije je tudi (možna) bodoča situacija, da bo treba v letu 2019 po proučitvi vseh sprejetih zakonskih rešitev večino izvedbenih zakonov držav članic Evropske unije dopolnjevati (kar velja tudi za predlog zakona). Države članice pri svojih zakonodajnih pristopih sicer štejejo, da ustrezno izvajajo določbe Splošne uredbe in Direktive.

V nadaljevanju so tako predstavljeni že sprejeti nemški, avstrijski, slovaški in belgijski zakon (torej štirje sprejeti zakoni držav članic Evropske unije), delno tudi na način, da se opozarja na motivacijo predlagateljev iz uradnih obrazložitev predlogov teh zakonov.

5.2. Zvezna republika Nemčija

Zvezna republika Nemčija je 27. aprila 2017 sprejela Zakon o prilagoditvi zakonodaje o varstvu osebnih podatkov Uredbi (EU) 2016/679 in izvajanju Direktive (EU) 2016/680 (Zakon o prilagoditvi in izvajanju zakonodaje o varstvu osebnih podatkov EU)[27]. 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[28] 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

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

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

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

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

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

obdelave osebnih podatkov. V 35. členu so določene omejitve pravice do izbrisa osebnih podatkov – če bi bil poseg nesorazmeren ali pa gre le za minimalno korist za posameznika.

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

To predstavitev nemške pravne ureditve glede novega sistema varstva osebnih podatkov še ni možno šteti za popolno predstavitev, saj še niso sprejeti zakoni vseh zveznih dežel Zvezne republike Nemčije, ki so pristojne za obdelavo osebnih podatkov v zasebnem sektorju ter za ureditev deželnih nadzornih organov za varstvo osebnih podatkov.

Znano je sicer tudi, da je sprejeti Zakon o prilagoditvi in izvajanju zakonodaje o varstvu osebnih podatkov EU deležen (sicer neupoštevanih) kritik iz dela zasebnega sektorja in dela javnosti[29], češ da ni dovolj v skladu z določbami Splošne uredbe - da naj bi bile občasno njegove določbe prestroge ali preširoke. Za domnevati je, da je Nemčija glede teh vprašanj (vidiki domnevne neskladnosti določb Zakona o prilagoditvi in izvajanju zakonodaje o varstvu osebnih podatkov EU v razmerju do določb Splošne uredbe) izhajala iz podlage varstva temeljnih pravic po Temeljnem zakonu (Ustavi) Zvezne republike Nemčije ter ustaljene ustavnosodne presoje Zveznega Ustavnega sodišča Zvezne republike Nemčije.

5.3. Republika Avstrija

Republika Avstrija je v letu 2017 sprejela Zvezni zakon, s katerim se spreminja Zakon o varstvu osebnih podatkov iz leta 2000 (Zakon o prilagoditvi varstva osebnih podatkov 2018)[30].

Sprejeti zakonski okvir precej sledi dosedanji ureditvi varstva osebnih podatkov v Republiki Avstriji, Avstrija je namreč izbrala način novelacije (spremembe in dopolnitve) veljavnega zakona. 1. člen veljavnega zakona, ki ureja varstvo osebnih podatkov kot osebno človekovo pravico in ima (uradni) pravni pomen ustavne norme, ni bil spremenjen zaradi neobstoja zahtevane dvotretjinske večine vseh poslancev in poslank Državnega zbora Republike Avstrije za ustavno revizijo, kar pomeni, da je Avstrija zadržala dosedanjo širšo opredelitev varstva osebnih podatkov kot temeljne pravice – kot nadrejeno glede vseh obdelav osebnih podatkov (tudi obdelav v druge namene). Prav tako je Avstrija zadržala dosedanjo tradicionalno ureditev (po sodni praksi od leta 1951 dalje) glede obravnavanja tudi (dela) podatkov o pravnih osebah, ki se tako varujejo kot (da so) osebni podatki. Za obdelavo osebnih podatkov otrok v zvezi storitvami informacijske družbe je določila mejna starost 14 let (v predlogu je bilo 16 let). Glede osebnih podatkov v zvezi s kazenskimi obsodbami je določeno (nekoliko drugače kot v členu 10 Splošne uredbe), da se lahko ti podatki obdelujejo tudi s strani upravljavca, če ima za to legitimen interes. Avstrija ni sprejela (ni jasno uveljavila) rešitev glede kritiziranih (spornih) visokih glob po Splošni uredbi, glede katerih se v Avstriji zatrjuje kršitev človekovih pravic ozir. neustavnost (tudi z vidika, da tako visokih glob ne bi smel izrekati nadzorni organ – ker ni sodišče), ampak bo počakala na odločitev Ustavnega sodišča Republike Avstrije v primerljivem primeru – presoja ustavnosti previsokih glob, katere lahko izreka avstrijski Urad za finančni trg. Poleg tega je naknadno glede navedenega kaznovanja z globami dne 20. aprila 2018 sprejela novelo navedenega zakona (sprememba Zakona o varstvu osebnih podatkov z zakonskim nazivom: Zakon o deregulaciji varstva osebnih podatkov - Datenschutz-Deregulierungs-Gesetz 2018, BGBl. I Nr. 24/2018) in v njej določila, da se v primeru predpisanih glob za kršitve po Splošni uredbi najprej izrekajo opozorilne sankcije, šele v primeru ponovljenih kršitev pa globe po Splošni uredbi (spremembe 11. člena), prav tako pa je v isti noveli

[29] 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/

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

določila, da nosilci javnih pooblastil niso odgovorni za prekrške po Splošni uredbi (spremembe 35. člena).

Glede razmerja varstvo osebnih podatkov – znanstveno raziskovanje je Avstrija določila le splošne določbe, obdelave pa bodo potekale po obstoječih področnih zakonih. V sprejetem zakonu tudi ni podana jasna rešitev glede dosedanjih pridobljenih privolitev za obdelavo osebnih podatkov, če namreč ostanejo veljavne (nespremenjene) po novi ureditvi po Splošni uredbi – le v obrazložitvi prehodnih določb je bilo v predlogu zakona v zvezi z omembo uvodne navedbe št. 171 Splošne uredbe nekoliko nejasno navedeno, da dosedanje privolitve za obdelavo osebnih podatkov ostanejo v veljavi, če ustrezajo pogojem iz Splošne uredbe.

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

V prihodnosti se bo v Avstriji tako kot 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 v razmerju do končno sprejetega zakona leta 2017 in njegove novele iz leta 2018) 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 pravne ureditve.

5.4. Slovaška republika

Vlada Slovaške republike je dne 20. 9. 2017 (vloženo v zakonodajni postopek dne 22. 9. 2017) sprejela besedilo Predloga Zakona o varstvu osebnih podatkov in o spremembah in dopolnitvah določenih zakonov, njen Ljudski svet (Parlament) pa ga je sprejel dne 27. 11. 2017[31]. Njegove bistvene nacionalne (sistemske) rešitve zlasti glede Splošne uredbe so predstavljene v nadaljevanju.

Tako je zelo bistvena sistemska rešitev v zakonu določitev splošne uporabe (in istočasno neposredne uporabe) temeljnih definicij s področja varstva osebnih podatkov iz člena 4 Splošne uredbe za vsa zakonska področja (5. člen), kot so to npr. obdelava osebnih podatkov, privolitev ipd.. Povezano s tem je v posebnem 2. členu iz 1. točke člena 4 Splošne uredbe prenesena tudi definicija pojma osebni podatek.[32] V 6. členu je vzpostavljeno strogo načelo zakonitosti, po katerem se lahko osebne podatke obdeluje le v skladu z zakonom in tako da niso prekršene temeljne pravice posameznikov, na katere se nanašajo osebni podatki. V tem členu Slovaška republika tudi primarno izhaja iz pristopa, da je varstvo osebnih podatkov osebna človekova pravica. V 7. členu je določena dokaj stroga namenska obdelava osebnih podatkov, po kateri se sme osebne podatke pridobiti le za specifično določene, izrecne in legitimne namene in se jih ne sme nadalje obdelovati na način, ki bi bil v neskladju s temi nameni, obdelavo v druge namene pa je dopuščena le glede arhivskih, statističnih, znanstvenih, zgodovinsko raziskovalnih namenov. V 17. členu je določeno, da je obdelava osebnih podatkov o kazenskih obsodbah možna le v primeru podlage v zakonitem predpisu ali na podlagi obvezujoče mednarodne pogodbe, te podatke pa lahko upravlja le državni organ. V 26. členu je npr. urejena pravica do prenosljivosti osebnih podatkov, s tem da je določeno, da ta pravica ne sme imeti škodljivega učinka na pravice drugih oseb. 28. člen ureja avtomatizirano obdelavo osebnih podatkov, vključno s profiliranjem in določa, da se ne sme izvajati avtomatizirana obdelava glede posebnih vrst osebnih podatkov. III. Poglavje II. Dela, III. Del in IV. Del zakona pa določajo zakonsko izvedbo določb Direktive (EU) 2016/680.

5.5. Kraljevina Belgija

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

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

Predosnutek Zakona o varstvu fizičnih oseb glede obdelave osebnih podatkov Kraljevine Belgije je bil objavljen 16. marca 2018 in vsebuje 287. členov. Zakonodajno smer takratnega Predosnutka je za oceniti kot garantistično (glede človekove pravice do varstva osebnih podatkov) in prepisovalno oziroma samostojno urejevalno. 1. člen predloga zakona določa posebno zakonodajno pristojnost s sklicem na Ustavo Kraljevine Belgije, 2. člen med drugim določa delno omejitev glede področja obrambe države – da se zakon ne nanaša na uporabo oboroženih sil ali na pripravo na uporabo oboroženih sil. V 3. členu je najprej določeno, da prosti pretok osebnih podatkov na ozemlju Evropske unije ali Kraljevine Belgije ne more biti omejen iz razlogov varstva osebnih podatkov, nato pa je ta pristop zamejen s strogo določbo, da to ne posega v pristojnosti nadzornega organa za varstvo osebnih podatkov. Nadalje 5. člen določa, da so definicije iz tega zakona iste kot v Splošni uredbi in da kadar predosnutek zakona navede definicijo, da to pomeni, da je mišljen le sklic na definicijo iz Splošne uredbe (s formulacijo: »brez posega v definicije v tem zakonu…«). V 7. členu je določeno, da je privolitvena starost za otroke glede uporabe storitev informacijske družbe 13 let. Sistem uvedbe pooblaščenih oseb za varstvo osebnih podatkov je dokaj podrobno razdelan, glede na vse njihove možne uporabe z vidika zagotavljanja skladnosti obdelave osebnih podatkov, s tem, da bo tudi Kraljevina Belgija samostojno določila pogoje za določitev pooblaščene osebe – vendar na način, da je za to dano pooblastilo v obliki delegirane zakonodaje za Kraljevo (dejansko: vladno) uredbo v zakonu (peti odstavek 65. člena – sedaj peti odstavek 63. člena)[33]. Področja iz Direktive 2016/680/EU so urejena v II. Delu Predosnutka zakona, delno pa tudi v III. Delu Predosnutka zakona. Področja arhiviranja, znanstvenega in zgodovinskega raziskovanja ter statističnega delovanja so urejena v 4. Delu Predosnutka zakona. V 233. členu so podrobneje določeni sodelovanje in kvalifikacije nevladnih organizacij za (pooblastilno) zastopanje posameznikov pred sodišči, kadar posamezniki zatrjujejo kršitev svojih pravic s področja varstva osebnih podatkov, s tem da je izrecno podano pooblastilo tudi za možnost zastopanja v kazenskem postopku. V 235. členu in naslednjih členih so določeni prekrški za kršitve zakona in za njih predpisane globe očitno odstopajo (in so sorazmerne) od upravnih sankcij po Splošni uredbi – npr. globe za upravljavce in obdelovalce (pravne osebe) so pretežno predpisane od 250 do 15.000 evrov (EUR) oziroma od 500 do 30.000 evrov.

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

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

6. DRUGE POSLEDICE, KI JIH BO IMELO SPREJETJE ZAKONA

6.1 Administrativne in druge posledice

a) V postopkih oziroma poslovanju javne uprave ali pravosodnih organov:
Vzpostavitev pooblaščenih oseb za varstvo osebnih podatkov, z zakonsko določenimi izjemami. Za postopke seznanitve z lastnimi osebnimi podatki se bodo delno (poenostavljeno) uporabljale določbe Zakona o splošnem upravnem postopku, kolikor gre za subjekte javnega sektorja, ki odločajo (delujejo) po pravilih splošnega upravnega postopka.

b) Pri obveznostih strank do javne uprave ali pravosodnih organov:
Predlog zakona nima tovrstnih posledic.

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

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

Predlog zakona ne bo imel tovrstnih posledic.

6.3 Presoja posledic za gospodarstvo

Predlog zakona nima tovrstnih posledic (glejte tudi obrazložitev zakonskih rešitev zgoraj o določenih poenostavitvah za gospodarstvo).

6.4 Presoja posledic za socialnem področju

Predlog zakona nima tovrstnih posledic.

6.5 Presoja posledic za dokumente razvojnega načrtovanja

Predlog zakona nima tovrstnih posledic.

6.6 Presoja posledic za druga področja

Predlog zakona nima tovrstnih posledic.

6.7 Izvajanje sprejetega predpisa

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

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

Druge tovrstne okoliščine niso podane.

7. PRIKAZ SODELOVANJA JAVNOSTI PRI PRIPRAVI PREDLOGA ZAKONA:

Javna razprava (prvi krog) glede prvotnega predloga zakona je bila izvedena od 3. 10. 2017 do 13. 11. 2017 ter ponovno (drugi krog) od 23. 1. 2018 do 2. 2. 2018. Precej pripomb je bilo upoštevanih, zlasti glede neposrednega trženja, pooblaščenih oseb, privolitve, obdelave v druge namene. Nato je bila glede prenovljenega predloga zakona izvedena nova Javna razprava od 7. 3. 2019 do 25. 3. 2019, glede na konceptualne spremembe v predlogu zakona pa je sedaj predlagan drug krog strokovnega in medresorskega usklajevanja – do 16. 8. 2019.

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

Zunanji strokovnjaki niso sodelovali pri pripravi predloga zakona.

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

- Andreja Katič, ministrica za pravosodje,
- dr. Dominika Švarc Pipan, državna sekretarka na Ministrstvu za pravosodje,
- Gregor Strojin, državni sekretar na Ministrstvu za pravosodje,
- mag. Nina Koželj, v.d. generalne direktorice Direktorata za kaznovalno pravo in človekove pravice
- Peter Pavlin, višji sekretar, Direktorat za kaznovalno pravo in človekove pravice

– Igor Kolar, višji svetovalec, kabinet ministrice

II. BESEDILO ČLENOV

I. DEL
TEMELJNE DOLOČBE

1. poglavje

Splošne določbe

1. člen

(vsebina)

(1) Ta zakon ureja pravice, obveznosti, upravičenja, načela, postopke in ukrepe, s katerimi se preprečujejo neustavni, nezakoniti ali neupravičeni posegi v zasebnost, dostojanstvo oziroma druge temeljne pravice posameznika pri obdelavi osebnih podatkov.

(2) S tem zakonom se izvaja Uredba (EU) 2016/679 Evropskega parlamenta in Sveta z dne 27. aprila 2016 o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem pretoku takih podatkov ter o razveljavitvi Direktive 95/46/ES (Splošna uredba o varstvu podatkov) (UL L št. 119 z dne 4. 5. 2016, str. 1), zadnjič popravljena s Popravkom (UL L št. 127 z dne 23. 5. 2018, str. 2; v nadaljnjem besedilu: Splošna uredba), katera ureja pravila glede prostega pretoka osebnih podatkov in varstvo osebnih podatkov kot temeljne pravice in prenaša Direktiva (EU) 2016/680 Evropskega parlamenta in Sveta z dne 27. aprila 2016 o varstvu posameznikov pri obdelavi osebnih podatkov, ki jih pristojni organi obdelujejo za namene preprečevanja, preiskovanja, odkrivanja ali pregona kaznivih dejanj ali izvrševanja kazenskih sankcij, in o prostem pretoku takih podatkov ter o razveljavitvi Okvirnega sklepa Sveta 2008/977/PNZ (UL L št. 119 z dne 4. 5. 2016, str. 89), zadnjič popravljena s Popravkom (UL L št. 127 z dne 23. 5. 2018, str. 20); v nadaljnjem besedilu: Direktiva), katera ureja delovanje državnih organov in drugih subjektov na področju obravnavanja kaznivih dejanj in njihovih storilcev ter pravice posameznikov, na katere se nanašajo osebni podatki.

2. člen

(človekova pravica do varstva osebnih podatkov)

(1) Za zagotavljanje zasebnosti in osebnega dostojanstva pripada vsaki posameznici in posamezniku (v nadaljnjem besedilu: posameznik) človekova pravica do varstva njegovih osebnih podatkov ob upoštevanju njegove podatkovne samoodločbe.

(2) Človekova pravica iz prejšnjega odstavka vsebuje tudi upravičenje, da se z zakonom ter pošteno in na pregleden način ureja obdelava posameznikovih osebnih podatkov, upravičenje do tajnosti njegovih osebnih podatkov ter druga upravičenja, določena z zakonom, v zvezi z obdelavo njegovih osebnih podatkov in uresničevanjem njegovih pravic s področja varstva osebnih podatkov.

3. člen

(prepoved diskriminacije glede obdelave osebnih podatkov)

Pri izvajanju obdelave osebnih podatkov je zagotovljeno vsakemu posamezniku, da se obdelave njegovih osebnih podatkov ne izvajajo na podlagi nedopustne diskriminacije, ne glede na narodnost, raso, barvo kože, veroizpoved, etnično pripadnost, spol, jezik, politično ali drugo prepričanje, spolno usmerjenost, spolno identiteto, premoženjsko stanje, kraj rojstva, izobrazbo, družbeni položaj, državljanstvo, kraj oziroma vrsto prebivališča, zdravstveno stanje, genske predispozicije ali katerokoli drugo osebno okoliščino teh posameznikov.

4. člen

(področje uporabe)

(1) Določbe tega zakona veljajo za obdelave osebnih podatkov, ki se v celoti ali delno izvajajo z avtomatiziranimi sredstvi, in za obdelave osebnih podatkov, ki so del zbirke ali so namenjeni oblikovanju dela zbirke, ki se ne izvaja z avtomatiziranimi sredstvi.

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

(3) Če II. del tega zakona ne določa drugače, določbe Splošne uredbe in določbe tega zakona veljajo tudi za obdelave osebnih podatkov s strani pristojnih državnih organov za namene iz 66. člena tega zakona.

5. člen

(ozemeljska veljavnost zakona)

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

(2) Ta zakon velja tudi za obdelavo osebnih podatkov, ki se izvaja v okviru dejavnosti sedeža, podružnice ali drugačne poslovne enote obdelovalca, ki je ustanovljen ali registriran v Republiki Sloveniji in opravlja dejavnosti obdelave za upravljavca, ki je ustanovljen ali registriran v drugi državi članici Evropske unije, če se te dejavnosti obdelave izvajajo v Republiki Sloveniji.

(3) 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, ne glede na to, ali je zanje potrebno plačilo, ali če so povezane s spremljanjem njihovega delovanja ali vedenja, če to poteka v Republiki Sloveniji.

6. člen

(pomen izrazov)

(1) Za uporabo tega zakona in drugih zakonov, ki urejajo obdelavo osebnih podatkov, veljajo pojmi iz 4. člena Splošne uredbe.

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

1. »pristojni organ« v II. delu tega zakona je katerikoli državni organ Republike Slovenije, ki je zakonsko določen kot pristojen za preprečevanje, preiskovanje, odkrivanje ali pregon kaznivih dejanj ali izvrševanje kazenskih sankcij, vključno s kaznivimi dejanji na področju preprečevanja pranja denarja ali financiranja terorizma, varnosti države in obrambe države, varovanja pred grožnjami javni varnosti in njihovim preprečevanjem, v delu, ko izvrševanje njihovih pristojnosti vključuje preprečevanje, preiskovanje ali odkrivanje kaznivih dejanj, izvrševanje kazenskih sankcij ali varnost države ter katerikoli drug organ ali drug subjekt, ki v skladu z zakonom lahko opravlja javne funkcije ali

izvaja javna pooblastila na prej navedenih zakonsko določenih področjih glede preprečevanja, preiskovanja, odkrivanja ali pregona kaznivih dejanj.

2. »nadzorni organ« pomeni Informacijskega pooblaščenca, določenega z zakonom, ki ureja Informacijskega pooblaščenca;

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

4. »državni organ« pomeni organ, kot je določen v zakonu, ki ureja javne uslužbence;

5. »javni organ« pomeni subjekte iz 2. in 3. točke tega člena;

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

7. »povezovalni znak« pomeni osebno identifikacijsko številko in druge z zakonom opredeljene enolične identifikacijske številke posameznika, z uporabo katerih je mogoče zbrati oziroma priklicati osebne podatke iz zbirk osebnih podatkov, v katerih so enolične identifikacijske številke obdelovane ter druge podobne znake v javnem sektorju, ki se redno ali sistematično uporabljajo za povezovanje zbirk med različnimi upravljavci ali dveh ali več zbirk znotraj enega upravljavca;

8. »zakon« pomeni ta zakon, druge zakone Republike Slovenije, obvezujoče mednarodne pogodbe, ki zavezujejo Republiko Slovenijo, ter pravne akte ali odločitve Evropske unije, katerih določbe so enakovredne zakonom in neposredno uporabljive ali neposredno učinkovite;

9. »varnost države« pomeni izvajanje nalog ali pooblastil v skladu z zakoni, ki urejajo izvajanje obveščevalnih in protiobveščevalnih dejavnosti države;

10. »kazenske evidence« pomenijo evidence, ki se upravljajo na podlagi določb zakona, ki ureja izvrševanje kazenskih sankcij, zakona, ki ureja kazenski postopek in kazenskega zakonika;

11. »prekrškovne evidence« pomenijo evidence, ki se upravljajo na podlagi določb zakona, ki ureja prekrške.

7. člen

(pravne podlage za obdelavo osebnih podatkov)

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

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

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

(4) V javnemu sektorju se lahko obdelujejo tisti osebni podatki, ki so nujno potrebni za izvrševanje zakonskih pristojnosti, nalog ali obveznosti javnega sektorja, če se s to obdelavo ne poseže v

upravičen interes posameznika, na katerega se osebni podatki nanašajo.(5) V javnem sektorju se lahko obdelujejo osebni podatki, ki so potrebni za uresničevanje zakonitih interesov javnega sektorja, če pri tem ne gre za izvajanje zakonskih pristojnosti, nalog ali obveznosti javnega sektorja ter če nad temi interesi ne prevladajo človekove pravice in temeljne svoboščine ali interesi posameznika, na katerega se nanašajo osebni podatki.

(5) Če obdelavo osebnih podatkov v zasebnem sektorju v skladu s prvim odstavkom tega člena določa zakon, mora ta določati namen obdelave osebnih podatkov in vrste osebnih podatkov, ki se obdelujejo, kategorije posameznikov, na katere se nanašajo osebni podatki, uporabnike osebnih podatkov oziroma namene, za katere se jim lahko posreduje osebne podatke, posamezna dejanja obdelave in postopke obdelave ter druge ukrepe za zagotovitev zakonite, poštene in pregledne obdelave.

(6) Obdelava osebnih podatkov za drug namen kot za tistega, za katerega so bili zbrani, je v javnem sektorju in v zasebnem sektorju dopustna, če je to v skladu z določbami iz četrtega odstavka 6. člena Splošne uredbe. Če gre za obdelavo, ki jo izvajajo upravljavci v okviru svojih nalog v javnem interesu ali pri izvajanju javne oblasti pa mora takšno obdelavo tudi določati zakon v skladu z drugim odstavkom tega člena.

8. člen

(privolitev mladoletne osebe za uporabo storitev informacijske družbe)

(1) Privolitev mladoletne osebe za uporabo storitev informacijske družbe, ki se jih ponuja neposredno mladoletnim osebam oziroma za katere se lahko verjetno domneva, da jih bodo uporabljale mladoletne osebe, je lahko veljavna, če je mladoletna oseba, stara 15 let ali več. Če je mladoletna oseba mlajša od 15 let, je privolitev veljavna le, če jo da ali odobri eden od staršev mladoletne osebe ali njen rejnik ali skrbnik. V primerih, ko pogoji poslovanja izvajalca storitev informacijske družbe predpisujejo višjo starost mladoletne osebe za uporabo storitev informacijske družbe, pa se upošteva ta starost.

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

9. člen

(posebno varstvo osebnih podatkov umrlih posameznikov)

(1) Osebni podatki umrlih posameznikov se varujejo v skladu s tem zakonom in drugimi zakoni.

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

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

(4) Če zakon ne določa drugače, lahko upravljavec podatke o umrlem posamezniku posreduje tudi drugi osebi, ki namerava te podatke uporabljati za zgodovinskoraziskovalne, znanstvenoraziskovalne, statistične ali arhivske namene.

(5) V zgodovinskih in drugih izobraževalnih publikacijah se lahko objavljajo zakonito pridobljeni osebni podatki umrlih posameznikov, če tako določa zakon, če je privolitev pred smrtjo dal posameznik sam ali če je za takšno objavo v času po smrti posameznika podana pisna privolitev naslednjih oseb v izključujočem vrstnem redu: zakonec ali partner iz zunajzakonske skupnosti ali partner v z njima z zakonom izenačeni skupnosti, otroci ali starši umrlega posameznika.

10. člen

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

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

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

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

(4) Za izvedbo povezovanje iz prejšnjega odstavka se za državljana Republike Slovenije ali osebo s prebivališčem v Republiki Sloveniji kot identifikacijska znaka uporabita osebno ime in njihova enotna matična številka, za tujca pa njegovo osebno ime in njegova enotna matična številka ali drug ustrezen identifikacijski znak iz kazenske ali prekrškovne evidence.

(5) Povezovanje iz tretjega odstavka tega člena se izvede tako, da je mogoče avtomatično posodabljanje podatkov v kazenskih evidencah in prekrškovnih evidencah oziroma tako, da povezovanje omogoča vsaj, da se v evidencah pri osebnih podatkih določenega ali določljivega posameznika pojavi samodejno opozorilo, da je pri njegovih podatkih v drugi zbirki osebnih podatkov prišlo do spremembe.

2. Poglavje

Postopek odločanja o pravicah posameznikov

11. člen

(uvodno)

(1) Zahtevo za uveljavljanje svojih pravic v skladu s 15. do 22. členom Splošne uredbe in 2. poglavja II. dela tega zakona vloži posameznik, na katerega se nanašajo osebni podatki, pisno ali ustno, na izkazljiv način, pri upravljavcu osebnih podatkov. Kot pisna zahteva se šteje tudi zahteva v elektronski obliki.

(2) Za obravnavo zahtev s strani upravljavcev iz javnega sektorja, ki so dolžni delovati po določbah zakona, ki ureja splošni upravni postopek, se glede vprašanj, ki niso urejena v tem zakonu, subsidiarno uporabljajo določbe zakona, ki ureja splošni upravni postopek.

12. člen

(zahteva)

(1) Zahteva mora biti razumljiva in mora obsegati vse, kar je treba, da se lahko obravnava. Vsebuje lahko le najmanjši možen obseg osebnih podatkov, ki je nujen za iskanje oziroma za določitev osebnih podatkov oziroma za rešitev zahteve ali odgovor posamezniku, kar so lahko: osebno ime posameznika, na katerega se nanašajo osebni podatki, morebitni naslov elektronske pošte oziroma naslov prebivališča, izjemoma poleg kakšnega od navedenih osebnih podatkov tudi povezovalni znak, po potrebi pa tudi druge njegove podobne nujne podatke ter morebitne podatke o pooblaščencu ali zastopniku posameznika, opredelitev oblike, v kateri želi prejeti odgovor, ter opredelitev obsega zahtevanih osebnih podatkov.

(2) Če je zahteva nepopolna ali nerazumljiva, upravljavec v roku desetih delovnih dni zahteva, da se pomanjkljivosti odpravijo, in določi posamezniku rok za odpravo pomanjkljivosti. Če posameznik, na katerega se nanašajo osebni podatki, v roku, ki ne more biti krajši od desetih delovnih dni, pomanjkljivosti ne odpravi, upravljavec v javnem sektorju zavrže njegovo zahtevo, v zasebnem sektorju pa pisno sporoči, da je ne bo obravnaval.

13. člen

(preverjanje identitete vlagatelja zahteve)

(1) Kadar ima upravljavec upravičen dvom v zvezi z identiteto vlagatelja zahteve ali pristnostjo podpisa, lahko od vlagatelja zahteva dodatne potrebne informacije za potrditev njegove identitete.

(2) Preverjanje identitete vlagatelja pri zahtevi, prejeti v elektronski obliki, se lahko izvaja tudi z uporabo sredstev elektronske identifikacije. Upravljavec glede na okoliščine samostojno odloča, katero raven zanesljivosti sredstev elektronske identifikacije bo štel kot zadostno za izkaz identitete vlagatelja, pri čemer pa ne sme nesorazmerno posegati v njegovo obveznost, da posamezniku olajša uveljavljanje pravic po tem zakonu.

14. člen

(odločitev o zahtevi)

Upravljavec o zahtevi posameznika, na katerega se nanašajo osebni podatki, odloči brez nepotrebnega odlašanja, najpozneje pa v enem mesecu po prejemu popolne zahteve. Ta rok se lahko po potrebi podaljša za največ dva dodatna meseca ob upoštevanju zapletenosti in števila zahtev. Upravljavec obvesti posameznika, na katerega se nanašajo osebni podatki, o vsakem takem podaljšanju v enem mesecu po prejemu zahteve skupaj z razlogi za zamudo in informacijo o možnosti pritožbe v skladu s tem zakonom.

15. člen

(oblika odločitve)

(1) Če upravljavec iz javnega sektorja ugodi zahtevi posameznika, na katerega se nanašajo osebni podatki, mu pošlje zahtevane podatke v obliki pisnega obvestila. Če njegovo zahtevo zavrne ali delno zavrne, o tem odloči z upravno odločbo, če je dolžan uporabljati zakon, ki ureja splošni upravni postopek, v drugih primerih pa po določbah naslednjega odstavka.

(2) Upravljavec iz zasebnega sektorja o zahtevi posameznika, na katerega se nanašajo osebni podatki, odloči v obliki pisnega obvestila, ki vsebuje obrazložitev razlogov za odločitev in informacijo o možnosti pritožbe v skladu s tem zakonom.

(3) V primerih iz prvega in drugega odstavka tega člena se v zvezi z zahtevo, ki je bila vložena po elektronski poti, odgovor poda v elektronski obliki.

16. člen

(ugovor)

(1) Če posameznik, na katerega se nanašajo osebni podatki, po prejeti odločitvi upravljavca meni, da upravljavec ni v celoti odločil o njegovi zahtevi, ali če meni, da osebni podatki, ki jih je prejel, niso osebni podatki, ki jih je zahteval, ali da ni prejel vseh zahtevanih osebnih podatkov, lahko pred vložitvijo pritožbe pri upravljavcu vloži obrazložen ugovor v osmih dneh od prejema odločitve upravljavca.

(2) Upravljavec o ugovoru odloči v desetih delovnih dneh, o ugovoru glede osebnih podatkov s področij v skladu s 66. členom tega zakona pa v petnajstih delovnih dneh.

(3) Rok za pritožbo začne v primeru vložitve ugovora teči po preteku roka za odločitev.

17. člen

(pritožba)

(1) Če upravljavec ne odloči o zahtevi posameznika, na katerega se nanašajo osebni podatki, v roku iz 14. člena tega zakona oziroma o ugovoru v roku iz prejšnjega člena, lahko posameznik pri nadzornem organu vloži pritožbo zaradi molka upravljavca. Če upravljavec zahtevo oziroma ugovor zavrne, lahko posameznik pri upravljavcu, če gre za javni sektor, oziroma pri nadzornem organu, če gre za zasebni sektor, vloži pritožbo v 15 dneh od prejema obvestila oziroma odločbe upravljavca.

(2) Pravica strank in stranskih udeležencev do pregledovanja dokumentov v zadevah odločanja o posameznikovi pritožbi v skladu z zakonom, ki ureja splošni upravni postopek, do dokončnosti odločbe nadzornega organa ne vključuje pregledovanja upravne zadeve v delu, ki se nanaša na dokumente, ki so predmet zahteve, in drugih dokumentov zadeve, iz katerih bi se dalo razbrati ali sklepati na vsebino zahtevanih osebnih podatkov.

(3) Po dokončnosti odločbe nadzornega organa o pritožbi pravica oseb iz prejšnjega odstavka vključuje pregled zadeve v obsegu, dovoljenem z dokončno odločbo Informacijskega pooblaščenca ali odločitvijo upravljavca.

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

18. člen

(postopek obravnave pritožbe)

V postopku obravnavanja pritožbe po prejšnjem členu, pritožbe zoper odločitev upravljavca o podaljšanju roka za obravnavo zahtevkov posameznika iz 14. člena tega zakona in pritožbe glede stroškov postopka po 21. členu tega zakona odloča nadzorni organ v skladu s subsidiarno uporabo zakona, ki ureja splošni upravni postopek, razen če je v tem delu zakona določeno drugače.

19. člen

(pooblastila nadzornega organa v pritožbenem postopku)

(1) V pritožbenem postopku iz prejšnjega člena ima pooblaščena uradna oseba nadzornega organa, ki mora izpolnjevati pogoje za državnega nadzornika za varstvo osebnih podatkov, poleg preiskovalnih pooblastil iz prvega odstavka 58. člena Splošne uredbe oziroma 53. člena tega zakona tudi pooblastila iz zakona, ki ureja inšpekcijski nadzor. Druga postopkovna dejanja v upravnem postopku, vključno z dejanji iz drugega in tretjega odstavka tega člena, lahko opravlja in v njih dokončno odloči tudi pooblaščena uradna oseba, ki ne izpolnjuje pogojev za državnega nadzornika osebnih podatkov.

(2) V pritožbenem postopku iz prejšnjega člena lahko pooblaščena uradna oseba nadzornega organa opravlja ogled prostorov, osebnih podatkov in dokumentarnega gradiva ter zaslišuje osebe pri upravljavcu in priče brez prisotnosti pritožnika ter morebitnih stranskih udeležencev. Če zadostuje za odločitev o pritožbi posameznika, lahko pooblaščena uradna oseba nadzornega organa pridobi le pisne izjave o dejstvih ter pisna pojasnila od upravljavca, prič ter drugih oseb. Pri dajanju pisnih ali ustnih izjav odgovornih oseb upravljavca ali pooblaščenih oseb morajo te osebe govoriti resnico in ne smejo ničesar zamolčati, njihove izjave pa se lahko štejejo kot izjave strank. Določbe prejšnjega stavka ne vplivajo na odločanje v prekrškovnem postopku.

(3) V pritožbenem postopku iz prejšnjega člena lahko pooblaščena uradna oseba nadzornega organa namesto izdaje upravne odločbe upravljavcu z ureditvenim predlogom predlaga prostovoljno rešitev posameznikove pritožbe v postavljenem roku, ki ne sme biti daljši od enega meseca, če se z ureditvenim predlogom predhodno strinja posameznik, na katerega se nanašajo osebni podatki in je to smiselno zaradi učinkovitega uresničevanja njegovih pravic. Po izpolnitvi ureditvenega predloga nadzorni organ pritožbeni postopek zaključi s sklepom o ustavitvi postopka. Zoper sklep ni dovoljena pritožba, je pa dopusten upravni spor.

(4) Če tako narekuje učinkovitost odločanja v postopku, lahko nadzorni organ o pritožbi odloči z odločbo s skrajšano obrazložitvijo, v kateri poleg izreka navede le pravno podlago in temeljne razloge odločitve ter pravni pouk. Če po prejemu odločbe s skrajšano obrazložitvijo posameznik, organ ali stranka najpozneje v 8 dneh neobvezujoče napove upravni spor zoper odločitev nadzornega organa, ta izda odločbo s polno obrazložitvijo v 15 dneh, s katero tudi razveljavi odločbo s skrajšano obrazložitvijo.

(5) Nadzorni organ v primerih, ki jih ni mogoče rešiti v skladu s prejšnjim odstavkom, o pritožbi odloči z odločbo. Zoper odločbo ni dovoljena pritožba, je pa dopusten upravni spor.

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

20. člen

(upravna izvršba)

(1) Za izvedbo upravne izvršbe, je pristojen nadzorni organ.

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

21. člen

(zaračunavanje stroškov)

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

(2) Kadar so zahteve posameznika, na katerega se nanašajo osebni podatki, očitno neutemeljene ali pretirane, zlasti ker se zahteve pogosto ponavljajo, lahko upravljavec s posebno obrazloženo odločitvijo:

– zavrne ukrepanje v zvezi z zahtevo, ali

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

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

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

(5) Stroške priprave podatkov za seznanitev in stroške dokazovanja tehnične izvedljivosti prenosljivosti osebnih podatkov nosi upravljavec.

22. člen

(omejitve pravic posameznikov)

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

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

23. člen

(sodno varstvo pravic posameznika)

(1) Posameznik, ki ugotovi, da so kršene njegove pravice, določene s Splošno uredbo ali z zakonom, lahko zahteva sodno varstvo njegovih pravic 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 po prvem in drugem odstavku tega člena odloča pristojno sodišče po določbah zakona, ki ureja upravni spor, kolikor ta zakon ne določa drugače.

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

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

(6) Postopek pred sodiščem je nujen in prednosten.

24. člen

(posebna pravila glede načina uveljavljanja pravic na določenih področjih)

(1) Pravice posameznikov, na katere se nanašajo osebni podatki, iz I. dela tega zakona se na področjih iz 100. do 105. člena tega zakona ne izvršujejo v postopkih pred nadzornim organom po določbah tega zakona ali po določbah Splošne uredbe.

(2) Pravice zasebnosti in pravice iz Splošne uredbe v zvezi s področji iz 100. do 105. člena tega zakona se izvršujejo v skladu z zakoni, ki urejajo ta področja, ter določbami 100. do 105. člena tega zakona.

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

25. člen

(izjema glede uveljavljanja pravic posameznika preko zakonitega zastopnika glede zdravstvene dokumentacije)

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

3. poglavje

Varnost osebnih podatkov in ocena učinka

26. člen

(varnost osebnih podatkov v javnem sektorju)

(1) Upravljavec in obdelovalec iz javnega sektorja z ustreznimi tehničnimi in organizacijskimi ukrepi, s katerimi se varujejo osebni podatki ter preprečuje njihovo naključno, namerno ali drugače nezakonito uničenje, spremembo, izgubo, nepooblaščeno razkritje, dostop ali drugo nepooblaščeno obdelavo, zagotavljata ustrezno raven varnosti osebnih podatkov ob upoštevanju vseh tveganj pri obdelavi osebnih podatkov.

(2) Ukrepi iz prejšnjega odstavka morajo biti primerni glede na stanje najnovejšega tehnološkega razvoja na področju varstva osebnih podatkov, ob upoštevanju narave, obsega, okoliščin in namenov obdelave ter resnosti in verjetnosti tveganj za človekove pravice in temeljne svoboščine posameznikov, ki nastajajo pri obdelavi, lahko pa se upošteva tudi stroške njihovega izvajanja. Ob upoštevanju teh okoliščin morajo ukrepi zagotavljati zlasti:

1. psevdonimizacijo in šifriranje osebnih podatkov;

2. stalno zaupnost, celovitost, dostopnost in odpornost sistemov in storitev za obdelavo;

3. pravočasno povrnitev razpoložljivosti osebnih podatkov v primeru incidenta informacijske varnosti, ki je fizično ali tehnološko onemogočil ali omejil razpoložljivost osebnih podatkov;

4. preprečitev posredovanja, razširjanja ali drugačnega omogočanja dostopa do osebnih podatkov, ki so predmet incidenta informacijske varnosti;

5. obveznosti in omejitve, ki veljajo za zaposlene pri upravljavcu oziroma obdelovalcu na področju varovanja osebnih podatkov ter postopke in ravnanje ob incidentih informacijske varnosti, kadar so ti postopki in ravnanja namenjeni zagotavljanju varnosti omrežja in informacij ter pomenijo spoštovanje zakonitega interesa upravljavca;

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

7. možnost poznejšega ugotavljanja, kdaj so bili posamezni osebni podatki vneseni v zbirko osebnih podatkov, uporabljeni ali drugače obdelani in kdo je to storil, in sicer za obdobje petih let od zaključka leta, v katerem je potekala obdelava, razen če za obdelave posameznih vrst osebnih podatkov drug zakon določa drugače;

8. možnost rednega testiranja, ocenjevanja in vrednotenja učinkovitosti tehničnih in organizacijskih ukrepov.

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

(4) Upravljavec oziroma obdelovalec v notranjem aktu določita ukrepe iz drugega odstavka tega člena in osebe, ki so odgovorne za določene zbirke osebnih podatkov ter osebe, ki lahko zaradi narave svojega dela obdelujejo osebne podatke iz posamezne zbirke osebnih podatkov. Določitev oseb ni obvezna, če njihova pravica do obdelave izhaja iz zakona.

(5) Če upravljavec oziroma obdelovalec sprejmeta potrjen kodeks ravnanja iz 40. člena Splošne uredbe, se kodeks lahko uporabi za dokazovanje izpolnjevanja zahtev iz drugega odstavka tega člena.

(6) Nadzorni organ vzpostavi sistem, ki omogoča, da prejeta sporočila o kršitvah določb tega zakona, zlasti glede varnosti osebnih podatkov, obravnava zaupno, razen če mora razkriti prijavitelje v odločbah po tem zakonu ali pa na podlagi sodne odločbe.

(7) Nadzorni organ izda smernice za izvajanje obveznosti iz tega člena, pri čemer upošteva tudi smernice Odbora glede tega vprašanja.

27. člen

(ocena učinka glede obdelav osebnih podatkov v javnem sektorju)

(1) Kadar bi lahko obdelava osebnih podatkov v javnem sektorju, ki se določa z zakonom, zlasti kadar gre za uporabo novih tehnologij in upoštevaje naravo, obseg, okoliščine in namen te obdelave, vsebovala obdelavo osebnih podatkov večjega števila posameznikov, na katere se nanašajo osebni podatki ali pa veliko tveganje za človekove pravice in temeljne svoboščine posameznikov, mora upravljavec pred začetkom obdelave opraviti oceno učinka predvidenih dejanj obdelave na varstvo osebnih podatkov v skladu s 35. členom Splošne uredbe.

(2) Predlagatelj zakona mora pripraviti predhodno oceno učinka iz prejšnjega odstavka, še preden je predlog zakona dostopen javnosti.

3. poglavje
Posebne določbe

28. člen

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

(1) Posredovanje osebnih podatkov, ki ga izvedejo osebe javnega sektorja drugim osebam javnega sektorja ali tretjim osebam, je dovoljeno, če je potrebno za izvajanje nalog v pristojnosti osebe javnega sektorja, ki posreduje podatke, ali obveznosti ali nalog tretje osebe, ki se ji podatki posredujejo, ali so izpolnjeni pogoji, ki bi dopuščali obdelavo v skladu s 7. členom tega zakona. Oseba javnega sektorja ali tretja oseba, ki se ji podatki posredujejo, sme osebne podatke obdelovati samo za namen, za uresničevanje katerega se ji posredujejo.

(2) Posredovanje osebnih podatkov, ki ga izvedejo osebe javnega sektorja pravnim ali fizičnim osebam zasebnega sektorja, je dovoljeno, če je to potrebno za uveljavljanje, izvajanje ali obrambo pravnih zahtevkov in se je pravna ali fizična oseba zasebnega sektorja do osebe javnega sektorja, ki posreduje podatke, obvezala, da bo podatke obdelovala samo za namen, za uresničevanje katerega se ji posredujejo.

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

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

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

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

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

29. člen

(posredovanje podatkov, ki ga izvajajo osebe zasebnega sektorja)

(1) Osebe zasebnega sektorja posredujejo osebne podatke drugim fizičnim ali pravnim osebam ali osebam javnega sektorja samo na podlagi zahteve iz drugega odstavka 30. člena tega zakona, iz katere izhaja veljavna pravna podlaga za pridobitev podatkov ter utemeljenost zahteve.

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

30. člen

(postopek posredovanja osebnih podatkov)

(1) Zahteva za posredovanje osebnih podatkov vsebuje:

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

2. pravno podlago za pridobitev zahtevanih osebnih podatkov;

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

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

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

6. obliko in način pridobitve zahtevanih osebnih podatkov.

(2) Upravljavec osebnih podatkov vlagatelju zahteve, če zakon ne določa drugačnega načina, zahtevane osebne podatke posreduje najpozneje v 15 dneh od prejema popolne zahteve, ali pa ga v tem roku pisno obvesti o razlogih, zaradi katerih mu zahtevanih osebnih podatkov ne bo posredoval.

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

(4) Če je zahteva za posredovanje osebnih podatkov delno ali v celoti zavrnjena, lahko vlagatelj v primeru, ko se zahteva nanaša na posredovanje osebnih podatkov iz uradnih evidenc ali javnih knjig, zahteva, da o njegovi vlogi najprej odloči organ druge stopnje, če tega ni ali če tudi organ druge stopnje zavrne njegovo zahtevo, pa lahko zahteva sodno varstvo, o katerem odloča pristojno sodišče v skladu z zakonom, ki ureja upravni spor. V primeru zavrnitve zahteve za posredovanje osebnih podatkov iz zbirk, ki niso uradne evidence ali javne knjige, lahko vlagatelj zahteva sodno varstvo, o katerem odloča sodišče s splošno pristojnostjo v skladu z zakonom, ki ureja nepravdni postopek.

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

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

(7) Informacije iz prejšnjega odstavka upravljavec hrani pet let, razen če zakon za posredovanje posameznih vrst podatkov določa drugačni rok.

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

31. člen

(pravica do vpogleda v osebni dokument)

Upravljavec osebnih podatkov lahko pred vnosom osebnih podatkov v zbirko ali njihovo spremembo ali dopolnitvijo v zbirki preveri točnost osebnih podatkov posameznika, na katerega se nanašajo, z vpogledom v njegovo osebno izkaznico, potni list ali vozniško dovoljenje, ki vsebuje tudi njegovo fotografijo, lahko pa poleg tega tudi z vpogledom v drugo javno listino. Ta člen ne posega v določbe drugih zakonov, ki urejajo posamezne osebne dokumente, glede preverjanja točnosti osebnih podatkov posameznika ali dopustnosti kopiranja osebnega dokumenta.

32. člen

(uporaba povezovalnih znakov)

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

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

(3) Na področjih varnosti države se povezovalni znak lahko uporablja tako, da se za pridobitev določenega osebnega podatka uporabi izključno ta znak, v skladu z notranjim aktom o varnosti osebnih podatkov ter ob upoštevanju sledljivosti obdelav osebnih podatkov iz šestega in sedmega odstavka 30. člena tega zakona.

(4) Prvi odstavek tega člena se ne uporablja za povezovanje v skladu s 118. členom tega zakona ter za zemljiško knjigo, sodni register in poslovni register, če tako določa drug zakon.

33. člen

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

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

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

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

5. poglavje

Pooblaščene osebe za varstvo osebnih podatkov

34. člen

(pooblaščena oseba)

Pooblaščena oseba za varstvo osebnih podatkov (v nadaljnjem besedilu: pooblaščena oseba) je oseba, ki upravljavcu ali obdelovalcu v skladu z 39. členom Splošne uredbe na neodvisen način pomaga pri zagotovitvi skladnosti obdelave s Splošno uredbo, tem zakonom, drugimi zakoni ali predpisi, ki urejajo obdelavo in varstvo osebnih podatkov.

35. člen

(obveznost določitve pooblaščene osebe)

(1) Pooblaščeno osebo določijo:

1. upravljavci in obdelovalci v javnem sektorju,

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

3. upravljavci ali obdelovalci v zasebnem sektorju, katerih temeljne dejavnosti ali naloge zajemajo obsežne obdelave posebnih vrst osebnih podatkov ali osebnih podatkov iz 10. člena tega zakona.

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

(3) Vsak upravljavec ali obdelovalec, ki je določil pooblaščeno osebo, lahko imenuje njenega namestnika za čas njene zadržanosti ali odsotnosti. Namestnik opravlja za ta čas naloge pooblaščene osebe in ima vsa pooblastila in upravičenja v skladu z 38. in 39. členom Splošne uredbe in tem zakonom.

(4) Upravljavec ali obdelovalec v osmih dneh od določitve pooblaščene osebe vpiše njene kontaktne podatke v skladu s 30. členom Splošne uredbe v svojo evidenco dejavnosti obdelav in kontakt javno objavi na primeren način, zlasti na spletni strani. V istem roku kontaktne podatke pooblaščene osebe (osebno ime, naziv upravljavca ali obdelovalca, telefonska številka, lahko pa tudi naslov elektronske pošte ter morebitni strokovni ali znanstveni naslov) sporoči nadzornemu organu, ki jih vključi v seznam pooblaščenih oseb. Seznam ni dostopen javnosti.

36. člen

(pogoji za določitev pooblaščene osebe)

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

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

2. je poslovno sposoben,

3. ima najmanj izobrazbo, pridobljeno po študijskem programu druge stopnje, oziroma izobrazbo, ki ustreza ravni izobrazbe, pridobljene po študijskem programu druge stopnje, in je v skladu z zakonom, ki ureja slovensko ogrodje kvalifikacij, uvrščena na 7. raven,

4. znanje in usposobljenost s področja varstva osebnih podatkov,

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

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

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

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

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

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

(7) Namestnik iz tretjega odstavka 35. člena tega zakona in druge osebe, ki pooblaščeni osebi pomagajo pri izvajanju nalog, morajo izpolnjevati pogoje za pooblaščeno osebo v skladu s prvim odstavkom tega člena, razen pogojev iz 1. in 4. točke prvega odstavka tega člena. Namestniki in druge osebe so pri svojem delu vezane na navodila pooblaščene osebe.

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

(9) V javnem sektorju se šteje, da je določena oseba v konfliktu interesov, če ima položaj predstojnika v osebi javnega sektorja, če je član organov upravljanja ali nadzora pri upravljavcu ali obdelovalcu, če njene druge naloge vključujejo sistemsko odločanje o obdelavi osebnih podatkov pri upravljavcu ali obdelovalcu ali če zastopa upravljavca oziroma obdelovalca v sodnih ali arbitražnih postopkih v zvezi z vprašanji varstva osebnih podatkov. Če pooblaščena oseba izve za situacijo, ki predstavlja ali bi lahko predstavljala konflikt interesov, o tem takoj pisno obvesti upravljavca oziroma obdelovalca. Upravljavec oziroma obdelovalec v tem primeru odpravi konflikt ali pooblaščeno osebo razreši od

opravljanja določene naloge kot pooblaščene osebe. Enako velja tudi za namestnika pooblaščene osebe. Določbe tega odstavka se smiselno uporabljajo za zasebni sektor.

37. člen

(skupna določitev pooblaščene osebe)

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

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

(3) Javni zavodi lahko v dogovoru s samoupravnimi lokalnimi skupnostmi kot ustanoviteljicami določijo skupno pooblaščeno osebo v skladu s prejšnjim odstavkom ali določijo, da bo naloge pooblaščene osebe za javni zavod opravljala pooblaščena oseba samoupravne lokalne skupnosti kot ustanoviteljice.

(4) Odvetniki lahko v dogovoru z Odvetniško zbornico Slovenije določijo skupno pooblaščeno osebo.

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

38. člen

(naloge pooblaščene osebe)

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

(2) Pooblaščena oseba sodišča ali državnega tožilstva ne sme opravljati nalog iz prejšnjega odstavka v zvezi z obdelavami osebnih podatkov v konkretnih zadevah, izvršenimi v okviru izvajanja neodvisnega sodniškega odločanja oziroma za izvajanje neodvisnega sodnega postopka ali odločanja strokovnih sodelavcev ali sodniških pomočnikov po odredbi sodnika ali samostojnega opravljanja državnotožilske funkcije ali opravljanja nalog strokovnih sodelavcev po odredbi državnega tožilca v okviru državnotožilske funkcije, kot jih opredeljujejo zakon, ki ureja sodišča, zakon, ki ureja državna tožilstva, ter zakoni, ki urejajo sodne postopke. Pooblaščena oseba lahko opravlja naloge iz prejšnjega odstavka samo glede zadev sodne uprave in državnotožilske uprave, zagotavljanja varnosti osebnih podatkov ter z dajanjem sistemskih stališč glede varstva osebnih podatkov. Kadar za izvrševanje neodvisnega sodniškega odločanja oziroma za izvajanje neodvisnega sodnega postopka ali po odredbi sodišča izvršitelji in stečajni upravitelji opravljajo določena dejanja kot del izvrševanja teh namenov, ne določijo pooblaščene osebe za obdelave osebnih podatkov za te zadeve.

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

(4) Pooblaščena oseba Varuha oziroma Varuhinje človekovih pravic (v nadaljnjem besedilu: Varuh človekovih pravic) ne sme opravljati nalog iz prvega odstavka tega člena v zvezi z obdelavami osebnih podatkov, izvršenimi v okviru delovanja Varuha človekovih pravic, kot jih opredeljujejo zakoni, ki določajo njegove pristojnosti ali pooblastila. Pooblaščena oseba Varuha človekovih pravic lahko

opravlja naloge iz prvega odstavka tega člena samo glede zadev obdelav osebnih podatkov s področja zagovorništva otrok ter glede izvajanja varnosti osebnih podatkov.

39. člen

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

(1 Ustavno sodišče Republike Slovenije določi pooblaščeno osebo, ki opravlja naloge v skladu s tretjim odstavkom prejšnjega člena.

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

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

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

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

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

40. člen

(dolžnost varstva tajnosti osebnih podatkov)

(1) Pooblaščena oseba, namestnik in osebe, ki izvajajo pomoč pri opravljanju njenih nalog, so pri opravljanju nalog zavezane k varstvu tajnosti obdelovanih osebnih podatkov. Pridobljene informacije smejo uporabljati izključno za opravljanje nalog in so tudi po zaključku dejavnosti zavezane k varstvu tajnosti osebnih podatkov.

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

(3) Kadar ima oseba, ki je nadrejena pooblaščeni osebi, pravico do molka v zakonsko določenem postopku, ta pravica velja za postopek o prekršku tudi za pooblaščeno osebo, namestnika in osebe, ki izvajajo pomoč pri opravljanju njenih nalog, in sicer do mere, v kateri je nadrejena oseba, ki ima zakonsko pravico do molka, to pravico uveljavila.

6. poglavje

Kodeksi ravnanja in certificiranje

41. člen

(kodeksi ravnanja)

(1) Kodeksi ravnanja so podrobnejša pravila za uporabo Splošne uredbe na posameznih delovnih področjih, ki jih na prostovoljni podlagi razvijajo in pripravljajo združenja ali drugi predstavniki upravljavcev ali obdelovalcev na določenem področju, tudi ob upoštevanju posebnosti mikro, majhnih in srednjih gospodarskih družb. Kodekse potrjujejo nadzorni organ, Odbor oziroma Evropska komisija.

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

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

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

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

(6) Upravljavec je ob predložitvi osnutka kodeksa nadzornemu organu dolžan izkazati, da se vsebina kodeksa nanaša na več držav članic Evropske unije. Če nadzorni organ v ugotovitvenem postopku iz tretjega odstavka tega člena ugotovi, da je osnutek kodeksa skladen s Splošno uredbo, pred izdajo ugotovitvene odločbe preveri, ali se kodeks nanaša na dejavnosti obdelave v več državah članicah Evropske unije. Če ugotovi, da se osnutek ne nanaša na takšno obdelavo, z ugotovitveno odločbo potrdi kodeks, ga po ugotovitvi pravnomočnosti odločbe vpiše v seznam potrjenih kodeksov, ki ga upravlja na svoji spletni strani, in objavi v Uradnem listu Republike Slovenije. Če ugotovi, da se osnutek nanaša na takšno obdelavo, pa v skladu s sedmim odstavkom 40. člena Splošne uredbe postopek prekine in osnutek kodeksa s sklepom predloži v mnenje Odboru iz 68. člena Splošne uredbe. Če Odbor osnutka kodeksa v svojem mnenju ne potrdi, nadzorni organ nadaljuje postopek in z odločbo zavrne osnutek kodeksa. Če Odbor osnutek kodeksa potrdi, nadzorni organ nadaljuje postopek, z odločbo potrdi kodeks, ga po ugotovitvi pravnomočnosti odločbe vpiše v seznam potrjenih kodeksov na svoji spletni strani in objavi v Uradnem listu Republike Slovenije.

42. člen

(certificiranje)

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

(2) Za certificiranje se uporabljajo merila, ki jih v skladu s petim odstavkom 42. člena Splošne uredbe odobri nadzorni organ ali Odbor.

(3) Certifikat se lahko uporablja za izkazovanje, da so dejanja obdelave osebnih podatkov s strani upravljavca ali obdelovalca skladna s Splošno uredbo, tem zakonom ali drugim zakonom, pri čemer pa posedovanje certifikata ne posega v odgovornosti upravljavca ali obdelovalca za skladnost njunih dejanj obdelave osebnih podatkov s Splošno uredbo, tem zakonom in drugimi zakoni in ne posega v nadzorne pristojnosti nadzornega organa v skladu z določbami tega zakona ali Splošne uredbe.

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

43. člen

(postopek akreditiranja teles za certificiranje)

(1) Certificiranje izvajajo telesa, ki jih na podlagi njihove vloge za to akreditira nacionalni akreditacijski organ (v nadaljnjem besedilu: Slovenska akreditacija), v skladu z b) točko prvega odstavka 43. člena Splošne uredbe in zakonom, ki ureja akreditacijo. Dodatne zahteve v skladu z b) točko prvega odstavka in tretjim odstavkom 43. člena Splošne uredbe določi nadzorni organ, skladno z njimi pa v okviru postopka akreditacije preverja Slovenska akreditacija.

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

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

7. poglavje

Nadzorni organ za varstvo osebnih podatkov Republike Slovenije

44. člen

(nadzorni organ za varstvo osebnih podatkov Republike Slovenije)

(1) Nadzorni organ za varstvo osebnih podatkov v Republiki Sloveniji v skladu s Splošno uredbo in tem zakonom je nadzorni organ iz 2. točke drugega odstavka 6. člena tega zakona.

(2) Pri nadzornem organu delujejo državne nadzornice oziroma državni nadzorniki za varstvo osebnih podatkov (v nadaljnjem besedilu: državni nadzornik), ki imajo pooblastila in pristojnosti izvajanja inšpekcijskega nadzora in drugih nalog glede varstva osebnih podatkov v skladu s Splošno uredbo, tem zakonom in drugimi zakoni ali predpisi.

(3) Informacijski pooblaščenec in njegovi namestniki imajo enaka pooblastila in pristojnosti, kot državni nadzornik.

(4) Informacijski pooblaščenec lahko za določeno osebo strokovnega osebja, ki izpolnjuje pogoje za državnega nadzornika, posamično določi, da izvaja določena pooblastila in pristojnosti državnih nadzornikov v zadevah nadzora.

(5) Informacijski pooblaščenec, njegovi namestniki, državni nadzorniki ter strokovno osebje iz prejšnjega odstavka so uradne osebe, kadar izvršujejo nadzorne pristojnosti in pooblastila po tem zakonu (v nadaljnjem besedilu: nadzorne osebe).

45. člen

(pristojnosti Informacijskega pooblaščenca)

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

(2) Nadzorni organ pri inšpekcijskem nadzoru iz prejšnjega odstavka izvaja tudi nadzor glede uporabe podzakonskih predpisov, ki so izdani na podlagi in v mejah predpisov iz prejšnjega odstavka.

(3) Nadzorni organ je pristojen za izvajanje inšpekcijskih nadzorov nad vsemi obdelavami osebnih podatkov v Republiki Sloveniji, v skladu s 5. členom tega zakona.

(4) Nadzorni organ je pristojen tudi za izvajanje inšpekcijskih nadzorov ali čezmejno sodelovanje v inšpekcijskih nadzorih glede obdelave osebnih podatkov, ki se izvajajo v okviru 6. in 7. poglavja Splošne uredbe, če se obdelava nanaša na sedež v njegovi državi članici ali znatno vpliva zgolj na posameznike v Republiki Sloveniji.

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

46. člen

(izjeme glede pristojnosti nadzornega organa)

(1) Ne glede na tretji in četrti odstavek prejšnjega člena nadzorne osebe niso pristojne za inšpekcijski in prekrškovni nadzor glede:

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

2. obdelav osebnih podatkov, izvršenih v okviru samostojnega opravljanja državnotožilske funkcije ali opravljanja nalog strokovnih sodelavcev po odredbi državnega tožilca v okviru državnotožilske funkcije, kot to opredeljuje zakon, ki ureja državno tožilstvo,

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

(2) Nadzorne osebe lahko vpogledajo v vso dokumentacijo Varuha človekovih pravic, predkazenskega postopka ali obveščevalno-varnostne dejavnosti, zaščitenih prič, prijaviteljev korupcije ter varnostnega preverjanja. Ne glede na tretji in četrti odstavek prejšnjega člena pa nadzorne osebe pri opravljanju inšpekcijskega in prekrškovnega nadzora na področjih iz prejšnjega stavka ne smejo zabeležiti identifikacijskih osebnih podatkov oziroma kopirati nobene dokumentacije glede:

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

2. obdelav osebnih podatkov na področjih predkazenskega postopka ali obveščevalno-varnostne dejavnost, samo v delu, kjer je izvedena identifikacija tajnih delavcev oziroma sodelavcev v skladu z zakonom, ki ureja kazenski postopek, zakonom, ki ureja obrambo, ali zakonom, ki ureja Slovensko obveščevalno-varnostno agencijo,

3. obdelav osebnih podatkov na področju zaščitenih prič v skladu z zakonom, ki ureja zaščito prič, samo v delu, kjer je izvedena identifikacija zaščitene priče, ali prijaviteljev korupcije po zakonu, ki ureja integriteto in preprečevanje korupcije,

4. obdelav osebnih podatkov varnostno preverjanih oseb v skladu z zakonom, ki ureja tajne podatke, samo v delu, kjer je izvedena identifikacija virov ugotavljanja oziroma preverjanja prejetih osebnih podatkov, ki jih organom, pristojnim za varnostno preverjanje, posredujejo pristojni organi v skladu z zakonom, ki ureja obrambo, ali zakonom, ki ureja Slovensko obveščevalno-varnostno agencijo.

(3) Nadzorne osebe so ne glede na prvi odstavek pristojne za opravljanje inšpekcijskega nadzora na vseh ostalih delovnih področjih državnih organov ali odločanj ali delovanj funkcionarjev, ki niso določena v prvem odstavku, zlasti v zvezi z zadevami sodne uprave, državnotožilske uprave, sodne uprave Ustavnega sodišča Republike Slovenije ter glede izvajanja ukrepov in postopkov s področja varnosti osebnih podatkov, razen kadar gre za posredovanje osebnih podatkov med sodišči za potrebe sodnega odločanja v sodnih postopkih ali med državnimi tožilstvi za potrebe državnotožilskega odločanja.

47. člen

(posvetovanja o uvedbah obdelav osebnih podatkov)

(1) Nadzorni organ daje predhodna mnenja vladi, ministrstvom, državnemu zboru in državnemu svetu o usklajenosti določb predlogov zakonov s tem zakonom, Splošno uredbo, drugimi zakoni in drugimi predpisi, ki urejajo osebne podatke.

(2) Nadzorni organ lahko daje predhodna mnenja organom samoupravnih lokalnih skupnosti, drugim državnim organom ter nosilcem javnih pooblastil v postopku priprave podzakonskih predpisov ter drugih splošnih aktov o skladnosti teh pravnih aktov s tem zakonom, Splošno uredbo, drugimi zakoni in drugimi predpisi, ki urejajo osebne podatke.

(3) Kadar predlagani pravni akt iz prvega ali drugega odstavka tega člena predvideva tudi obdelave osebnih podatkov, glede katerih je treba v skladu s 27. členom tega zakona opraviti oceno učinka na varstvo osebnih podatkov, predlagatelj pravnega akta nadzornemu organu predloži tudi oceno učinka.

(4) Kadar zakon določa, da nadzorni organ da soglasje ali predhodno mnenje k predlogu podzakonskega predpisa ali drugega splošnega akta, se smiselno uporabljajo določbe prvega odstavka.

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

(6) Nadzorni organ lahko posreduje tudi ponovno mnenje organu ali nosilcu javnega pooblastila iz prvega ali drugega odstavka tega člena, če oceni, da je bilo njegovo mnenje neutemeljeno neupoštevano.

48. člen

(sodelovanje z drugimi organi)

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

(2) Nadzorni organ je pristojen tudi za skupno ukrepanje ali preiskovanje z drugimi nadzornimi organi držav članic v skladu s 60., 61. in 62. členom Splošne uredbe.

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

(4) Kadar skupno ukrepanje ali preiskovanje iz drugega odstavka tega člena poteka v drugi državi članici Evropske unije, nadzor vodi pristojni nadzorni organ druge države članice. Nadzorni organ v okviru tega nadzora krije stroške predstavnikov ali nadzornega osebja nadzornega organa.

49. člen

(uporaba predpisov, ki urejajo opravljanje inšpekcijskega nadzora)

Za opravljanje inšpekcijskega nadzora v skladu s tem zakonom in Splošno uredbo se uporabljajo določbe Splošne uredbe in tega zakona ter določbe zakona, ki ureja inšpekcijski nadzor, in določbe zakona, ki ureja splošni upravni postopek, če Splošna uredba ali ta zakon ne določata drugače.

50. člen

(obseg inšpekcijskega nadzora)

V okviru inšpekcijskega nadzora nadzorna oseba nadzoruje skladnost obdelave osebnih podatkov s Splošno uredbo, tem zakonom in drugimi predpisi, ki urejajo obdelavo osebnih podatkov.

51. člen

(načini opravljanja inšpekcijskega nadzora)

(1) Nadzorne osebe neposredno opravljajo inšpekcijski nadzor.

(2) Inšpekcijski nadzor se lahko opravlja na oddaljeni način samo v primerih in v skladu s pogoji, katere določa ta zakon.

52. člen

(službena izkaznica)

(1) Nadzorna oseba izkazuje pooblastilo za opravljanje nalog inšpekcijskega in prekrškovnega nadzora ter njihovo identiteto s službeno izkaznico, ki vsebuje fotografijo nadzorne osebe, njegovo osebno ime, naziv nadzorne osebe, strokovni ali znanstveni naslov, navedbo organa in pooblaščenost za izvajanje nadzora.

(2) Obliko in vsebino službene izkaznice podrobneje določi minister, pristojen za pravosodje.

53. člen

(preiskovalna pooblastila)

(1) Nadzorna oseba lahko pri opravljanju inšpekcijskega nadzora poleg uporabe preiskovalnih pooblastil iz prvega odstavka 58. člena Splošne uredbe oziroma pooblastil po zakonih, ki urejata inšpekcijski postopek ter splošni upravni postopek, tudi:

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

2. pregleduje poslovne knjige, pogodbe, listine, poslovno korespondenco, poslovne evidence in druge podatke, ki se nanašajo na obdelavo osebnih podatkov s strani upravljavca ali obdelovalca ali druge pravne ali fizične osebe po njunem pooblastilu, oziroma na prenos osebnih podatkov v tretjo državo ali posredovanje uporabnikom osebnih podatkov iz tretjih držav s strani upravljavca ali obdelovalca oziroma druge pravne ali fizične osebe po njunem pooblastilu (v nadaljnjem besedilu: poslovne knjige in druga dokumentacija), ne glede na njihovo tajnost ali drugo vrsto zaupnosti ter ne glede na nosilec, na katerem so zapisani ali shranjeni;

3. vstopi in pregleda prostore, zemljišča, prevozna sredstva ter opremo in sredstva za obdelavo osebnih podatkov (v nadaljnjem besedilu: prostori in oprema), v oziroma s katerimi upravljavec ali obdelovalec sam ali drugo podjetje ali posameznik po njunem pooblastilu opravlja obdelavo osebnih podatkov, za katero izhaja verjetnost kršitve določb tega zakona, Splošne uredbe oziroma drugih predpisov, ki urejajo varstvo osebnih podatkov;

4. zavarujejo in pregledujejo elektronske in z njimi povezane naprave ter nosilce elektronskih podatkov, vključno s preko omrežja dosegljivimi informacijskimi sistemi, na katerih so shranjeni podatki (v nadaljnjem besedilu: elektronska naprava), za katere je verjetno, da se na njih nahajajo podatki, glede katerih izhaja verjetnost kršitve določb tega zakona, Splošne uredbe oziroma drugih zakonov ali predpisov, ki urejajo varstvo osebnih podatkov;

5. odvzame ali pridobi ustrezne kopije, forenzične kopije ali izvlečke iz poslovnih knjig in druge dokumentacije v kakršni koli obliki z uporabo fotokopirnih sredstev ali računalniške opreme upravljavca ali obdelovalca oziroma nadzornega organa. Če zaradi tehničnih ali časovnih razlogov ni

mogoče narediti kopij na kraju samem, lahko odnese poslovne knjige in drugo dokumentacijo za čas, potreben, da se naredijo kopije. O tem naredi uradni zaznamek;

6. zapečati poslovne prostore ter poslovne knjige in drugo dokumentacijo za čas trajanja postopka in v obsegu, potrebnem za njegovo izvedbo. O tem se naredi uradni zaznamek.

7. zaseže predmete ter poslovne knjige in drugo dokumentacijo za največ 20 delovnih dni, če je to potrebno za izvedbo postopka. O tem naredi potrdilo o zasegu, v katerem mora biti navedeno, kateri predmeti so bili zaseženi, njihov opis, navedba kraja, kjer so bili najdeni, ter razlog za zaseg.

8. brez predhodne najave in brez navzočnosti upravljavca ali obdelovalca, njegovega zakonitega zastopnika oziroma pooblaščenca pregleduje vsebine in preveri način delovanja zavezančevih spletnih strani in drugih javno dostopnih storitev informacijske družbe, če je to nujno zaradi varovanja človekovih pravic, temeljnih svoboščin ali interesov posameznikov, na katere se nanašajo osebni podatki in obstaja utemeljena bojazen, da teh pooblastil ali dejanj pozneje ne bo mogoče izvesti ali da bo njihova izvedba pozneje otežena;

9. izvaja druga pooblastila, določena z zakonom.

(2) Izvedba ukrepov pregleda skritih predelov prostorov oziroma opreme iz 3. točke prejšnjega odstavka oziroma zavarovanje in pregled elektronskih naprav in nosilcev iz 4. točke prejšnjega odstavka je dopustna le na podlagi soglasja upravljavca ali obdelovalca oziroma obrazložene pisne odredbe sodišča. Odredbo iz prejšnjega stavka izda preiskovalni sodnik pri Okrožnem sodišču v Ljubljani najpozneje v 48 urah od prejema predloga nadzorne osebe.

(3) V primerih iz prejšnjega odstavka nadzorne osebe najprej upravljavca ali obdelovalca pozovejo, da poda soglasje za izvedbo navedenega pregleda, ki se zabeleži. Če soglasje ni podano, nadzorna oseba odredi začasno zapečatenje oziroma blokiranje ustreznega predela prostorov oziroma opreme ali elektronske naprave ali nosilca, tako da se lahko ohranijo možni dokazi in le za čas, dokler ni izdana ustrezna sodna odredba oziroma do poteka roka za njeno izdajo. Upravljavec ali obdelovalec sta dolžna v primeru, če ni podano soglasje, navesti, da obstaja očitna verjetnost, da bi lahko prišlo do posega v pravice do njune prostorske ali komunikacijske zasebnosti, ali da bi lahko prišlo do posega v dolžnost varovanje odvetniške zaupnosti. Prav tako v primeru, če nadzorna oseba še pred začetkom izvajanja ukrepa oceni, da bi lahko prišlo do možnosti posega iz prejšnjega stavka v zasebnost oziroma zaupnost, to navede v predlogu za izdajo pisne sodne odredbe, v primeru iz prejšnjega stavka pa v predlogu za izdajo pisne sodne odredbe navede stališče upravljavca in obdelovalca ter poda svoje stališče.

(4) Preiskovalni sodnik z odredbo odloči, da se pregled izvede, če obstajajo utemeljeni razlogi za sum, da je upravljavec ali obdelovalec huje kršil ali krši določbe Splošne uredbe, tega zakona ali drugih zakonov ali predpisov, in je verjetno, da se bodo pri pregledu prostorov ali opreme oziroma elektronskih naprav našli dokazi, ki so pomembni za odločanje v postopku inšpekcijskega nadzora ali v povezanem prekrškovnem postopku. Odredba vsebuje:

1. opredelitev skritih predelov prostorov ali opreme, ki jih je treba pregledati, oziroma elektronskih naprav, ki jih je treba zavarovati in pregledati,

2. opredelitev razlogov za pregled,

3. opredelitev dokazov oziroma vsebine podatkov, ki se iščejo,

4. navedbo razlogov, ki utemeljujejo uporabo preiskovalnega pooblastila in način njegove izvršitve in

5. kadar gre za preiskavo gradiva, ki bi lahko bilo zajeto z odvetniško zaupnostjo, tudi določitev izvedenca, ki bo pregledal zaseženo dokumentacijo oziroma elektronske naprave, nosilce oziroma podatke ter odločil, katere dele se lahko razkrije nadzorni osebi.

(5) Pregled se opravi v skladu z odredbo preiskovalnega sodnika in na način, s katerim se v najmanjši možni meri posega v pravice oseb, ki niso zavezanci za nadzor in varuje tajnost oziroma zaupnost podatkov ter ne povzroča nesorazmerna škoda. Za zavarovanje podatkov na elektronskih napravah se smiselno uporabljajo določbe zakona, ki ureja kazenski postopek glede zavarovanja podatkov v

elektronski obliki. Upravljavec ali obdelovalec imata pravico biti navzoča pri zavarovanju in pregledu elektronske naprave. Če določeno elektronsko napravo uporablja oseba, ki upravičeno pričakuje zasebnost na njej, ima pravico biti navzoča ob zavarovanju in pregledu elektronske naprave.

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

(7) Kadar gre za pregled dokumentacije ali podatkov, ki so zajete z odvetniško zaupnostjo, nadzorna oseba še pred pregledom zadevnega gradiva le-to ob prisotnosti dveh prič oziroma predstavnika upravljavca ali obdelovalca ali Odvetniške zbornice Slovenije, če so prisotni, popiše in zapečati, nato pa posreduje s strani sodišča imenovanemu izvedencu, ki ga pregleda in določi, katere dele gradiva se lahko razkrije nadzorni osebi (neprivilegirano gradivo), katere pa je treba zaradi varovanja opisanih zaupnih razmerij izločiti (privilegirano gradivo). Izvedenec tako razdeljeno gradivo posreduje preiskovalnemu sodniku, ki po pregledu s sklepom (odredba o posredovanju gradiva) posreduje kopijo neprivilegiranega gradiva nadzorni osebi, privilegirano gradivo pa vrne upravljavcu oziroma obdelovalcu. Če je to zaradi izvedbe ločitve gradiv po tem odstavku potrebno, lahko preiskovalni sodnik na predlog izvedenca ali upravljavca oziroma obdelovalca zaradi izvedbe ločitve razpiše tudi posebni narok, na katerega se vabi izvedenca ter upravljavca oziroma obdelovalca.

(8) Zoper odredbo preiskovalnega sodnika o posredovanju gradiva ni pritožbe.

54. člen

(popravljalna pooblastila in ukrepi ter njihove omejitve)

(1) Nadzorna oseba, ki pri opravljanju inšpekcijskega nadzora ugotovi kršitev določb Splošne uredbe, tega zakona ali drugega zakona ali predpisa, ki ureja varstvo osebnih podatkov, lahko poleg uporabe popravljalnih pooblastil iz drugega odstavka 58. člena Splošne uredbe, odredi da se nepravilnosti ali pomanjkljivosti odpravijo na način in v roku, ki ga sama določi, zlasti:

1. prepoved obdelave osebnih podatkov ali anonimiziranje, omejitev obdelave, psevdonimizacijo, brisanje ali uničenje osebnih podatkov;

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

3. druge ukrepe, določene z zakonom, ki ureja inšpekcijski nadzor, zakonom, ki ureja splošni upravni postopek, s Splošno uredbo ali drugim zakonom.

(2) Ukrepov iz prejšnjega odstavka ni mogoče odrediti zoper:

1. ponudnika izključnega prenosa podatkov v komunikacijskem omrežju, če ta ne sproža prenosa, ne izbira naslovnika in prenesenih podatkov ne izbira ali spreminja;

2. ponudnika shranjevanja podatkov v predpomnilniku, če ta ne spreminja posredovanih podatkov in brez odlašanja odstrani ali onemogoči dostop do podatka, ki ga hrani, takoj ko je obveščen, da je bil vir podatka odstranjen iz omrežja ali da je bil dostop do njega onemogočen;

3. ponudnika gostovanja v zvezi s podatki, ki jih je zagotovil prejemnik storitve, ki ne deluje v okviru pooblastil ali pod nadzorom ponudnika gostovanja, dokler ni seznanjen s protipravnostjo oziroma mu niso znana dejstva ali okoliščine, iz katerih izhaja protipravnost tako hranjenih podatkov.

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

55. člen

(odločitev, da se postopek ne uvede)

(1) Kadar iz podatkov iz prijave ali iz drugih podatkov ni mogoče sklepati na kršitev varstva osebnih podatkov po Splošni uredbi, tem zakonu ali drugem zakonu oziroma predpisu, ki ureja obdelavo in varstvo osebnih podatkov, nadzorna oseba odloči, da se inšpekcijski postopek ne uvede.

(2) Odločitev iz prejšnjega odstavka s kratko navedbo razlogov se zaznamuje v spisu. V primeru, ko je prijavitelj znan, se s takšno odločitvijo pisno seznani prijavitelja.

(3) Kadar prijavo iz prvega odstavka tega člena poda posameznik, na katerega se nanašajo osebni podatki in prijava izpolnjuje formalne zahteve po določbah zakona, ki ureja splošni upravni postopek, nadzorna oseba s sklepom odloči, da se inšpekcijski postopek ne uvede. V obrazložitvi sklepa se navedejo razlogi za neuvedbo postopka ter pravni pouk. Sklep se vroči prijavitelju.

56. člen

(pravice prijavitelja)

(1) Nadzorna oseba po opravljenem nadzoru in sprejetem zadnjem ukrepu oziroma ustavitvi postopka obvesti prijavitelja o vseh pomembnejših ugotovitvah in dejanjih v postopku inšpekcijskega nadzora.

(2) Prijavitelj, ki meni, da obstaja kršitev varstva njegovih osebnih podatkov, lahko v skladu s prvim odstavkom 80. člena Splošne uredbe pisno pooblasti nevladno organizacijo s področja varstva osebnih podatkov ali zasebnosti, ki ima status nevladne organizacije v javnem interesu, da v njegovem imenu vloži prijavo pri nadzornem organu.

57. člen

(pravno sredstvo zoper odločitve nadzornega organa)

(1) Zoper odločbo ali sklep nadzornega organa ni dovoljena pritožba. Zoper odločbo ali sklep o ustavitvi postopka ali sklep o neuvedbi postopka je dopusten upravni spor.

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

58. člen

(ukrepanje ob zaznavi kaznivih dejanj ali prekrškov)

(1) Če nadzorna oseba pri izvrševanju svojih pristojnosti ugotovi, da obstaja sum storitve prekrška, ki je v pristojnosti nadzornega organa, izvede postopek v skladu z zakonom, ki ureja prekrške, v skladu s Splošno uredbo in v skladu s tem zakonom.

(2) Če nadzorna oseba 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 postopek v skladu z zakonom, ki ureja prekrške.

(3) Postopka po prvem odstavku tega člena ni mogoče izvajati zoper ponudnike iz drugega odstavka 54. člena tega zakona.

(4) Če gre za sum obstoja velikega tveganja za človekove pravice ali temeljne svoboščine posameznika, na katerega se nanašajo osebni podatki in torej za možnost hude kršitve določb tega

zakona ali določb Splošne uredbe in je za izvedbo prekrškovnega postopka nujno potrebno pridobiti podatke o uporabniku storitev ponudnikov iz drugega odstavka 54. člena tega zakona, pri tem pa je mogoče utemeljeno sklepati, da prekrška z drugimi ukrepi ne bi bilo mogoče odkriti ali dokazati oziroma bi bilo to povezano z nesorazmernimi težavami, lahko sodišče, pristojno za prekrške, na obrazložen predlog nadzorne osebe odredi ponudniku iz drugega odstavka 54. člena tega zakona, da nadzorni osebi sporoči podatke, na podlagi katerih je mogoče identificirati tega uporabnika (osebno ime, naslov prebivališča, firma, naslov elektronske pošte).

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

59. člen

(varovanje tajnosti)

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

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

60. člen

(javnost dela)

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

1. izdaja notranje glasilo ter strokovno literaturo;

2. na spletni strani ali na drug primeren način objavlja mnenja iz 47. 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 nadzorni organ 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, upravnega sodišča, Vrhovnega sodišča ter dokončne odločbe in sklepe nadzornega organa, ki se nanašajo na varstvo osebnih podatkov, tako da iz njih ni mogoče razbrati osebnih podatkov strank, oškodovancev, prič ali izvedencev - z uporabo psevdonimizacije;

5. daje mnenja o skladnosti splošnih pogojev poslovanja oziroma njihovih predlogov s predpisi s področja varstva osebnih podatkov;

6. daje neobvezna mnenja, pojasnila in stališča o vprašanjih s področja varstva osebnih podatkov in jih objavlja na spletni strani ali na drug primeren način;

7. pripravlja in daje neobvezne smernice in priporočila glede varstva osebnih podatkov na posameznem področju;

8. daje izjave za javnost o izvedbi posamičnih zadev v skladu s tem zakonom;

9. izvaja konference za medije v zvezi z delom nadzornega organa ter prepise izjav ali posnetke izjav s konferenc za medije objavi na spletni strani;10. na spletni strani objavlja druga pomembna obvestila.

(2) Nadzorni organ lahko za opravljanje nalog iz 5., 6., in 7. točke prejšnjega odstavka pozove k sodelovanju tudi predstavnike društev in drugih nevladnih organizacij s področja varstva osebnih podatkov, zasebnosti, človekovih pravic in temeljnih svoboščin, potrošnikov ter strokovnjake določenih strok, povezanih s prej navedenimi področji.

8. poglavje

Zunanji nadzor delovanja nadzornega organa

61. člen

(letno poročilo nadzornega organa)

(1) Nadzorni organ v svojem letnem poročilu poroča Državnemu zboru Republike Slovenije o stanju na področju varstva osebnih podatkov ter povezanih ugotovitvah, predlogih in priporočilih. To poročilo je del skupnega letnega poročila v skladu z zakonom, ki ureja Informacijskega pooblaščenca.

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

62. člen

(pristojnosti Varuha človekovih pravic)

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

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

63. člen

(pristojnosti državnega zbora)

(1) Stanje na področju varstva osebnih podatkov in izvrševanje določb tega zakona spremlja pristojno delovno telo državnega zbora.

(2) Pristojno delovno telo državnega zbora za nadzor obveščevalnih in varnostnih služb lahko sodeluje z nadzornim organom, na lasten predlog ali na pobudo nadzornega organa glede sprememb zakonov ali drugih predpisov ali pa kadar je v določenih primerih potrebna zaupna izmenjava informacij o ugotovitvah nadzornih postopkov.

9. poglavje

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

64. člen

(splošna določba)

Osebni podatki iz 9. in 10. člena tega zakona ter osebni podatki zunaj področja uporabe prava Evropske unije, se posredujejo državam članicam Evropske unije, tretjim državam ali mednarodnim organizacijam le po določbah tega poglavja ali če to določa zakon.

65. člen

(odstopanja v posebnih primerih)

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

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

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

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

4. če je prenos potreben zaradi pomembnih razlogov javnega interesa, določenih z zakonom;

5. če je prenos potreben za uveljavljanje, izvajanje ali obrambo pravnih zahtevkov;

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

7. če se prenos opravi iz uradne evidence, javne knjige ali drugega registra, ki je namenjen zagotavljanju informacij javnosti in je na voljo za vpogled bodisi javnosti na splošno bodisi katerikoli osebi, ki lahko izkaže zakonit interes, vendar le, če so v posameznem primeru izpolnjeni pogoji za tak vpogled, določeni s pravnim redom Republike Slovenije ter če gre za posamično pridobivanje osebnih podatkov.

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

(3) Kadar ne obstaja druga pravna podlaga za posredovanje osebnih podatkov v tretjo državo ali mednarodno organizacijo, se lahko prenos v tretjo državo ali mednarodno organizacijo izjemoma izvede, če prenos ni ponovljiv, zadeva le omejeno število posameznikov, na katere se nanašajo osebni podatki, je potreben zaradi nujnih zakonitih interesov, za katere si prizadeva upravljavec in nad katerimi ne prevladajo človekove pravice ali temeljne svoboščine ali interesi posameznika, na katerega se nanašajo osebni podatki, in pod pogojem, da je upravljavec ocenil vse okoliščine v zvezi s prenosom podatkov in na podlagi te ocene predvidel ustrezne zaščitne ukrepe v zvezi z varstvom osebnih podatkov. Upravljavec o takem prenosu naknadno najpozneje v roku 3 delovnih dni obvesti nadzorni organ. Upravljavec posreduje posamezniku, na katerega se nanašajo osebni podatki informacije iz 13. in 14. člena Splošne uredbe ter bistvene informacije o izvedenem prenosu in opis nujnih zakonitih interesov iz prejšnjega stavka.

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

1. poglavje
Splošne določbe

66. člen
(področje uporabe tega dela zakona)

Določbe II. dela zakona se uporablja za primere, ko osebne podatke obdelujejo pristojni državni organi, ki so zakonsko določeni kot pristojni za preprečevanje, preiskovanje, odkrivanje ali pregon kaznivih dejanj ali izvrševanje kazenskih sankcij, vključno s kaznivimi dejanji na področju preprečevanja pranja denarja ali financiranja terorizma, varnosti države in obrambe države, varovanja pred grožnjami javni varnosti in njihovim preprečevanjem, v delu, ko izvrševanje njihovih pristojnosti vključuje preprečevanje, preiskovanje ali odkrivanje kaznivih dejanj, izvrševanje kazenskih sankcij ali varnost države ter katerikoli drug organ ali drug subjekt, ki v skladu z zakonom lahko opravlja javne funkcije ali izvaja javna pooblastila na prej navedenih zakonsko določenih področjih glede preprečevanja, preiskovanja, odkrivanja ali pregona kaznivih dejanj.

67. člen

(uporaba splošne ureditve)

Če ta del zakona ne določa drugače, veljajo za primere obdelav iz prejšnjega člena tega zakona določbe I. dela tega zakona, razen 5. in 41.-43. člena.

68. člen

(ozemeljska veljavnost tega dela zakona)

(1) Določbe II. dela tega zakona se uporabljajo za obdelave osebnih podatkov, ki po določbah 66. člena tega zakona potekajo na ozemlju Republike Slovenije.

(2) Določbe II. dela tega zakona se uporabljajo tudi v primerih, ko organi in subjekti iz 66. člena tega zakona izvajajo svoja pooblastila, pristojnosti ali naloge na misijah v tujini, če po določbah mednarodnega javnega prava za njihovo delovanje velja pravni red Republike Slovenije.

69. člen

(pomen izrazov)

Izrazi, uporabljeni v tem delu zakona, pomenijo:

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

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

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

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

5. »psevdonimizacija« pomeni obdelavo osebnih podatkov na tak način, da osebnih podatkov brez dodatnih informacij ni več mogoče pripisati specifičnemu posamezniku, na katerega se nanašajo

osebni podatki, če se take dodatne informacije hranijo ločeno ter zanje veljajo tehnični in organizacijski ukrepi za zagotavljanje, da se osebni podatki ne pripišejo določenemu ali določljivemu posamezniku;

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

7. »pristojni organ« pomeni organe in subjekte iz 66. člena tega zakona;

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

9. »obdelovalec« pomeni fizično ali pravno osebo, javni organ, agencijo ali drugo telo, ki obdeluje osebne podatke v imenu upravljavca;

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

11. »privolitev« posameznika, na katerega se nanašajo osebni podatki, pomeni vsako prostovoljno, konkretno, informirano in nedvoumno ravnanje v obliki izjave ali jasnega pritrdilnega dejanja, iz katerega je mogoče sklepati na želje posameznika, na katerega se nanašajo osebni podatki, s katerim izrazi strinjanje z obdelavo osebnih podatkov, ki se nanašajo nanj;

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

13. »posebne vrste osebnih podatkov« pomenijo osebne podatke, ki razkrivajo rasno ali etnično poreklo, politično mnenje, versko ali filozofsko prepričanje ali članstvo v sindikatu, obdelavo genskih podatkov, biometričnih podatkov za namene edinstvene identifikacije posameznika, podatke v zvezi z zdravjem posameznikov in podatke v zvezi s posameznikovim spolnim življenjem ali spolno usmerjenostjo;

14. »podatki o zdravstvenem stanju« pomenijo osebne podatke, ki se nanašajo na telesno ali duševno zdravje posameznika, vključno z zagotavljanjem zdravstvenih storitev, in razkrivajo informacije o njegovem zdravstvenem stanju;

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

16. »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;

17. »nadzorni organ« pomeni Informacijskega pooblaščenca iz 2. točke drugega odstavka 6. člena tega zakona;

18. »mednarodna organizacija« pomeni organizacijo in njena podrejena telesa, ki jih ureja mednarodno javno pravo, ali katera koli druga telesa, ustanovljena z mednarodno pogodbo med dvema ali več državami ali na podlagi take mednarodne pogodbe;

19. »izbris« pomeni trajno odstranitev ali uničenje osebnega podatka, tako da ga ni več mogoče obnoviti; pri tem je zaradi zagotavljanja sledljivosti obdelave osebnih podatkov v skladu s sedmim odstavkom 30. člena tega zakona dopustno tudi zabeležiti zaznamek, da je bil v zvezi z osebnimi podatki določenega posameznika izveden izbris, pri čemer pa zaznamek ne sme vsebovati podatkov, ki bi omogočali obnovo izbrisanega osebnega podatka;

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

70. člen

(načela varstva osebnih podatkov)

(1) Osebni podatki:

1. se obdelujejo zakonito, pošteno in na pregleden način v zvezi s posameznikom, na katerega se nanašajo osebni podatki (zakonitost, poštenost in preglednost);

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

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

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

5. se hranijo v obliki, ki dopušča identifikacijo posameznikov, na katere se nanašajo osebni podatki, le toliko časa, kolikor je potrebno za izpolnitev namena, za katerega se osebni podatki obdelujejo, razen če je z zakonom ali drugim predpisom določen drug rok hrambe (omejitev roka hrambe);

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

(2) Upravljavec je odgovoren in mora biti vedno zmožen dokazati skladnost svojih obdelav osebnih podatkov z določbami prejšnjega odstavka (skladnost obdelave).

71. člen

(razlikovanje med osebnimi podatki in različnimi položaji posameznikov, na katere se nanašajo osebni podatki)

(1) Pri obdelavi osebnih podatkov se v največji možni meri, z uporabo vseh razumnih ukrepov, razlikuje zlasti med različnimi položaji posameznikov, katerih osebni podatki se obdelujejo, tudi z vidika, ali temeljijo na dejstvu ali temeljijo na osebni oceni. Razlikuje se zlasti med naslednjimi položaji:

1. osumljenci storitve kaznivega dejanja;

2. osebe, zoper katere na podlagi določenih dejstev in v zvezi z uporabo prikritih preiskovalnih ukrepov obstaja utemeljen sum, da bodo storile kaznivo dejanje;

3. obsojeni storilci kaznivih dejanj;

4. pravnomočno obsojeni storilci kaznivih dejanj

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

6. druge osebe, povezane s kaznivim dejanjem, zlasti osebe, ki bi lahko nastopale kot priče, osebe, ki lahko podajo informacije o kaznivem dejanju, ali osebe, ki so v stiku ali povezane z osebami iz prejšnjih točk tega odstavka.

(2) Osebne podatke, ki vsebujejo navedbo osebne ocene ali temeljijo na njej, se ustrezno označi ter, če je to možno in dopustno, utemelji na način, ki omogoča naknadno preverjanje te ocene. Upravljavec izvaja redno notranje preverjanje skladnosti obdelav z določbami prejšnjega odstavka in to ustrezno dokumentira.

72. člen

(točnost, popolnost, posodobljenost in zanesljivost osebnih podatkov)

(1) Osebni podatki, ki so netočni, nepopolni, neposodobljeni ali nezanesljivi ali jih je treba izbrisati, se ne smejo posredovati, dajati na razpolago ali pripraviti za avtomatiziran priklic iz zbirk. Upravljavci morajo pred posredovanjem z uporabo vseh razumnih ukrepov ustrezno preveriti kakovost podatkov. Glede osebnih podatkov, ki so že na razpolago za avtomatiziran priklic, se stalno izvajajo ustrezna prizadevanja za zagotavljanje njihove točnosti, popolnosti, posodobljenosti in zanesljivosti.

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

(3) Kadar se izkaže, da so bili posredovani osebni podatki, ki ne ustrezajo zahtevam iz prvega odstavka tega člena, pošiljatelj to nemudoma sporoči vsem uporabnikom. Uporabniki nemudoma popravijo, omejijo obdelavo ali izbrišejo nezakonito posredovane, netočne, neposodobljene ali nezanesljive podatke.

(4) Če imata upravljavec ali uporabnik verjeten razlog za domnevo, da so bili posredovani ali čezmejno obdelani osebni podatki netočni, nepopolni, neposodobljeni ali nezanesljivi in da jih je treba popraviti, omejiti njihovo obdelavo ali jih izbrisati, se nemudoma izvede medsebojno obveščanje. Pošiljatelj nemudoma popravi, omeji obdelavo ali izbriše osebne podatke, če so dejstva o netočnosti, nepopolnosti, neposodobljenosti ali nezanesljivosti osebnih podatkov potrjena. Uporabnik je na to odločitev vezan, lahko pa označi svoje morebitno stališče v svoji zbirki.

(5) Posameznika, na katerega se nanašajo osebni podatki, upravljavec seznani z dejstvom, katerim uporabnikom so bili posredovani netočni, nepopolni, neposodobljeni ali nezanesljivi osebni podatki ter kdaj je bil uporabnik obveščen o tem dejstvu. Z zakonom se lahko začasno omeji pravico posameznika iz prejšnjega stavka, če je to sorazmerno z zastavljenim ciljem, spoštuje bistvo pravice do varstva osebnih podatkov ter so zagotovljeni dodatni in posebni ukrepi za varstvo človekovih pravic in temeljnih svoboščin ali interesov posameznika, na katerega se nanašajo osebni podatki.

73. člen

(zakonitost obdelave osebnih podatkov)

(1) Obdelave, posredovanja, prenosi in čezmejne obdelave osebnih podatkov za namene iz 66. člena tega zakona so zakoniti le, če so potrebni za opravljanje nalog iz 66. člena tega zakona in če takšne obdelave osebnih podatkov, vrste osebnih podatkov, ki naj se obdelujejo, namen njihove obdelave, kategorije posameznikov, na katere se ti osebni podatki nanašajo ter, kadar je to potrebno, rok hrambe osebnih podatkov, določajo zakoni, ki urejajo naloge, pooblastila oziroma pristojnosti organov in subjektov iz 66. člena tega zakona. Če je mogoče, zakoni določijo tudi uporabnike osebnih podatkov, posamezna dejanja obdelave in postopke obdelave ter druge ukrepe za zagotovitev zakonite, poštene in pregledne obdelave. Obdelava je zakonita le v obsegu, v katerem je potrebna za opravljanje teh zakonskih nalog, pooblastil oziroma pristojnosti.

(2) V skladu s prvim odstavkom tega člena je obdelava posebnih vrst osebnih podatkov zakonita le, če je to nujno potrebno in je zagotovljeno ustrezno varstvo človekovih pravic ali temeljnih svoboščin posameznika, na katerega se nanašajo osebni podatki, v naslednjih primerih:

1. je nujno potrebna za varovanje življenjskih interesov posameznika, zlasti življenja ali telesa ali zdravja posameznika, na katerega se osebni podatki nanašajo, ali druge osebe, kadar posameznik, na katerega se osebni podatki nanašajo, fizično ali poslovno ni sposoben dati svoje privolitve,

2. je posameznik, na katerega se nanašajo posebne vrste osebnih podatkov, te javno objavil, brez očitnega ali izrecnega namena, da omeji namen njihove obdelave,

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

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

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

74. člen

(zakonitost obdelave javno dostopnih posebnih vrst osebnih podatkov)

Če posameznik, na katerega se nanašajo osebni podatki, javno objavi svoje osebne podatke, ki spadajo med posebno vrsto osebnih podatkov, brez očitnega ali izrecnega namena, da omeji namen njihove obdelave, je njihova obdelava zakonita, če je v skladu z nameni iz 66. člena tega zakona.

75. člen

(obdelava osebnih podatkov za druge namene)

Obdelava osebnih podatkov v skladu s tem delom zakona s strani istega ali drugega upravljavca za drug namen obdelave od tistega, za katerega so bili podatki pridobljeni, je dovoljena le, če ta drug namen obdelave spada med namene iz 66. člena tega zakona ter izpolnjuje pogoje iz 66. člena tega zakona in če tako določa zakon.

76. člen

(posredovanje osebnih podatkov drugim državam članicam Evropske unije)

Če za obdelavo osebnih podatkov v skladu z zakonom veljajo posebni pogoji, pošiljatelj iz Republike Slovenije uporabnika obvesti o teh pogojih in o tem, da jih je treba upoštevati. Pri posredovanju osebnih podatkov iz Republike Slovenije uporabnikom v druge države članice Evropske unije ali v ustanove in druge organe, vzpostavljene skladno s 4. in 5. poglavjem V. naslova Pogodbe o delovanju Evropske unije, se ne smejo uveljavljati pogoji, ki za ustrezno posredovanje osebnih podatkov ne veljajo tudi v Republiki Sloveniji.

77. člen

(avtomatizirano odločanje in avtomatizirana obdelava osebnih podatkov v posameznih primerih)

(1) Odločanje, ki temelji izključno na avtomatizirani obdelavi osebnih podatkov, ki imajo lahko negativen pravni učinek na posameznika, na katerega se nanašajo osebni podatki, ali ga lahko bistveno prizadenejo, je prepovedano, razen če to določa zakon ter če so izvedena naknadna preverjanja rezultatov avtomatizirane obdelave in drugi ukrepi za zagotavljanje ustreznega varstva človekovih pravic in temeljnih svoboščin.

(2) Odločitve iz prejšnjega odstavka ne smejo izhajati iz obdelav posebnih vrst podatkov, razen če zakon določa ustrezne ukrepe za varstvo človekovih pravic in temeljnih svoboščin ter zakonitih interesov posameznika, na katerega se nanašajo osebni podatki.

(3) Pred sprejetjem zakona, ki določa dejanja obdelave glede avtomatiziranega odločanja, mora pristojni predlagatelj zakona ali upravljavec izvesti oceno učinkov 27. člena tega zakona .

(4) Izvajanje profiliranja v okviru avtomatizirane obdelave osebnih podatkov, ki ima lahko za posledico diskriminacijo posameznikov, na katere se nanašajo osebni podatki, je prepovedano.

78. člen

(dnevniki obdelav osebnih podatkov)

(1) Upravljavci in obdelovalci iz 66. člena tega zakona, ki izvajajo obdelavo v avtomatiziranih sistemih obdelave osebnih podatkov, morajo vzpostaviti učinkovite sisteme dnevnikov obdelav osebnih podatkov. Dnevniki vpogleda in razkritja morajo omogočati utemeljitev, opredelitev datuma in časa takih dejanj obdelave osebnih podatkov ter tudi identifikacijo osebe, ki je vpogledala v osebne podatke ali jih razkrila ali spremenila ter identiteto uporabnikov takih osebnih podatkov, tako da so zagotovljeni sledljivost posegov v osebne podatke in varnost osebnih podatkov.

(2) Sistemi dnevnikov obdelav morajo omogočati beleženje vsaj naslednjih dejanj obdelave osebnih podatkov v avtomatiziranih sistemih obdelave osebnih podatkov:

1. zbiranje,
2. predelava,
3. vpogled,
4. razkritje, vključno s prenosi,
5. kombiniranje,
6. izbris.

(3) Dnevniki obdelav po tem delu zakona se uporabljajo zgolj za preverjanje zakonitosti obdelave, notranje spremljanje obdelave osebnih podatkov, zagotavljanje neoporečnosti in varnosti osebnih podatkov, v predkazenskih postopkih, kazenskih postopkih ter na področju obveščevalno-varnostne dejavnosti.

(4) Upravljavec in obdelovalec omogočita dostop do vsebine dnevnikov obdelav nadzornemu organu, Varuhu človekovih pravic, pooblaščenim osebam pri upravljavcu, drugim notranjim nadzornim organom ter državnim organom v skladu z zakonom.

(5) Vsebino dnevnikov obdelav se hrani pet let od zaključka koledarskega leta v katerem so bila v njih zabeležena dejanja obdelave iz drugega odstavka tega člena, če drug zakon ne določa drugačnega roka hrambe.

79. člen

(ocena učinka)

(1) Kadar bi lahko obdelava, zlasti z uporabo novih tehnologij in ob upoštevanju narave, obsega, okoliščin oziroma namena obdelave, povzročila veliko tveganje za človekove pravice in temeljne svoboščine posameznikov, mora upravljavec iz 66. člena tega zakona pred začetkom obdelave opraviti oceno učinka predvidenih dejanj obdelave na varstvo osebnih podatkov v skladu s sedmim in devetim odstavkom 35. člena Splošne uredbe.

(2) Oceno učinka 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 osebnih podatkov ali osebnih podatkov v zvezi s kazenskimi obsodbami in prekrški v velikem obsegu,

3. sistematičnega nadzora javno dostopnega območja v velikem obsegu.

(3) Ocene učinkov ni treba opraviti glede obdelav, ki jih izvajajo upravljavci iz 66. člena tega zakona in imajo pravno podlago v zakonu, pa je bila ocena učinka izvedena že med sprejemanjem zakona v skladu z drugim odstavkom 27. člena tega zakona, vendar le, če se narava, obseg, okoliščine ali namen obdelave niso v ničemer bistvenem spremenili po izdelavi ocene.

(4) Ob upoštevanju pogojev iz prvega odstavka tega člena upravljavec v primerih nastanka novih tveganj glede obdelave izvede podrobno preverjanje, ali obdelava poteka v skladu z oceno učinka.

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

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

80. člen

(predhodno posvetovanje)

(1) Upravljavec in obdelovalec iz 66. člena tega zakona morata pred začetkom obdelave osebnih podatkov, ki bo del nove zbirke, izvesti posvetovanje z nadzornim organom, kadar:

1. iz ocene učinka na varstvo podatkov iz 27. člena tega zakona izhaja, da bi obdelava osebnih podatkov povzročila znatno tveganje za človekove pravice ali temeljne svoboščine ali zakonsko zaščitene interese posameznikov, na katere se osebni podatki nanašajo, če upravljavec ne sprejme ukrepov za ublažitev tveganja; ali

2. vrsta obdelave osebnih podatkov, zlasti kadar vključuje uporabo novih tehnologij, mehanizmov ali postopkov, predstavlja znatno tveganje za človekove pravice ali temeljne svoboščine ali zakonsko zaščitene interese posameznikov, na katere se osebni podatki nanašajo.

(2) Nadzorni organ lahko določi seznam dejanj obdelave, ki so del obveznega predhodnega posvetovanja iz prejšnjega odstavka.

(3) Nadzornemu organu upravljavec in obdelovalec zagotovita dostop do vsebine ocene učinkov ter druge dokumentacije v zvezi z obdelavo iz prvega odstavka tega člena.

(4) Kadar nadzorni organ meni, da načrtovana obdelava osebnih podatkov lahko pomeni kršitev zakona, zlasti ker upravljavec ni ustrezno opredelil tveganja ali ni sprejel ustreznih ukrepov za ublažitev tveganja, lahko v roku šestih tednov po prejetju zahteve za posvetovanje, pisno svetuje upravljavcu in, kadar je to primerno, obdelovalcu, katere dodatne ukrepe je treba sprejeti. Nadzorni organ lahko rok podaljša za največ šest mesecev, če je načrtovana obdelava posebej zapletena z vidika vpliva na osebne podatke večjega števila ljudi, poseganja v njihove človekove pravice ali temeljne svoboščine ali zakonsko zaščitene interese.

81. člen

(preiskave prostorov in posvetovanja)

(1) Nadzorni organ izvaja preiskave uradnih prostorov organov ali subjektov iz 66. člena tega zakona v skladu s 53. členom tega zakona ter brez sodne odredbe za preiskavo.

(2) Organi in subjekti iz 66. člena tega zakona ter obdelovalci skrbijo, da se posvetovanja z nadzornim organom izvedejo pravočasno.

82. člen

(splošne obveznosti upravljavca)

(1) Upravljavec iz 66. člena tega zakona ob upoštevanju narave, obsega, okoliščin in namenov obdelave, pa tudi tveganj za človekove pravice in temeljne svoboščine posameznikov, na katere se nanašajo osebni podatki, izvede ustrezne tehnične in organizacijske ukrepe, ki zagotavljajo zakonitost obdelave osebnih podatkov.

(2) Ukrepi iz prejšnjega odstavka morajo upoštevati verjetnost in resnost tveganj za človekove pravice in temeljne svoboščine posameznikov in morajo omogočiti dokazovanje, da obdelava osebnih podatkov poteka v skladu s tem zakonom ali drugimi zakoni. Ti ukrepi se po potrebi pregledajo in dopolnijo, kadar se spremenijo okoliščine obdelave osebnih podatkov. Kadar je to sorazmerno glede na dejavnosti obdelave osebnih podatkov, ti ukrepi vključujejo tudi izvajanje ustreznih politik za varstvo podatkov s strani upravljavca.

83. člen

(vgrajeno in privzeto varstvo osebnih podatkov)

(1) Upravljavec iz 66. člena tega zakona ob upoštevanju najnovejšega tehnološkega razvoja in stroškov izvajanja ter narave, obsega, okoliščin in namenov obdelave, pa tudi tveganj za človekove pravice in temeljne svoboščine posameznikov, ki so povezana z obdelavo in se razlikujejo po verjetnosti in resnosti, tako v času določanja sredstev obdelave kot tudi v času same obdelave, izvede ustrezne tehnične in organizacijske ukrepe, kot je zlasti psevdonimizacija, ki so oblikovani za učinkovito izvajanje načel varstva osebnih podatkov iz 70. člena tega zakona, kot je načelo najmanjšega obsega podatkov, ter v obdelavo vključi potrebne zaščitne ukrepe, zaščitijo pravice posameznikov, na katere se nanašajo osebni podatki.

(2) Upravljavec izvede ustrezne tehnične in organizacijske ukrepe, s katerimi zagotovi, da se samodejno obdelajo samo osebni podatki, ki so potrebni za vsak poseben namen obdelave. Ta obveznost velja ne glede na količino zbranih osebnih podatkov, obseg njihove obdelave, rok njihove hrambe in njihovo dostopnost. S takšnimi ukrepi se zagotovi zlasti, da osebni podatki niso samodejno dostopni nedoločenemu številu oseb brez posredovanja pristojne uradne osebe upravljavca.

84. člen

(skupni upravljavci)

(1) V primerih, ko dva ali več upravljavcev iz 66. člena tega zakona skupaj določijo namene in načine obdelave, veljajo za skupne upravljavce. Skupni upravljavci na pregleden način z medsebojnim pisnim dogovorom ali dogovorom na podlagi zakona določijo dolžnosti vsakega od njih za izpolnjevanje

obveznosti iz tega zakona, zlasti v zvezi z uresničevanjem pravic posameznika, na katerega se nanašajo osebni podatki po tem zakonu ter naloge vsakega od njih glede zagotavljanja informacij, razen če in kolikor so te dolžnosti vsakega od upravljavcev določene z zakonom. Z dogovorom se določi kontaktna točka za posameznike, na katere se nanašajo osebni podatki. Z zakonom se lahko določi, kateri od skupnih upravljavcev lahko deluje kot enotna kontaktna točka za uresničevanje pravic posameznikov, na katere se nanašajo osebni podatki.

(2) Posameznik, na katerega se nanašajo osebni podatki, uresničuje pravice, ki jih ima na podlagi tega in drugih zakonov glede varstva njegovih pravic s področja osebnih podatkov, glede vsakega od upravljavcev in proti vsakemu od njih.

85. člen

(obdelovalec)

(1) Kadar se obdelava izvaja v imenu upravljavca iz 66. člena tega zakona, mora ta sodelovati le s tistimi obdelovalci, ki zagotovijo zadostna jamstva za izvedbo ustreznih tehničnih in organizacijskih ukrepov na tak način, da obdelava izpolnjuje zahteve iz II. dela tega zakona in zagotavlja varstvo pravic posameznika, na katerega se nanašajo osebni podatki. Zahteva po ustreznih tehničnih in organizacijskih ukrepih lahko vsebuje tudi zahtevo po stalni dosegljivosti ustreznega osebja obdelovalca, da se zagotovi zakonita in čimbolj neprekinjena obdelava osebnih podatkov.

(2) Obdelovalec lahko zaposli drugega obdelovalca, ki opravlja naloge za upravljavca, le na podlagi predhodnega posebnega pisnega dovoljenja upravljavca.

(3) Izvajanje obdelave s strani obdelovalca ureja pisna pogodba ali drug pisni dogovor ali določa zakon, ki mora določiti obveznosti obdelovalca do upravljavca ter v katerem so določeni vsebina in trajanje obdelave, narava in namen obdelave, vrsta osebnih podatkov, kategorije posameznikov, na katere se nanašajo osebni podatki, ter obveznosti in pravice upravljavca. Pogodba ali drug dogovor ali zakon določa zlasti, da obdelovalec:

1. deluje samo po navodilih upravljavca;

2. zagotovi, da so osebe, ki so pooblaščene za obdelavo osebnih podatkov, zavezane k zaupnosti ali jih k zaupnosti zavezuje ustrezen zakon;

3. pomaga upravljavcu na kakršen koli primeren način, da se zagotovi skladnost z določbami o pravicah posameznika, na katerega se nanašajo osebni podatki;

4. v skladu z odločitvijo upravljavca izbriše ali vrne vse osebne podatke upravljavcu po zaključku storitev obdelave podatkov ter uniči obstoječe kopije, razen če zakon določa posebno hrambo osebnih podatkov;

5. da upravljavcu na razpolago vse informacije, potrebne za dokazovanje skladnosti delovanja s tem členom;

6. pri izbiri drugega obdelovalca zagotovi izpolnjevanje pogojev iz prejšnjega in tega odstavka.

(4) Če obdelovalec za obdelavo podatkov določi druge namene in način obdelave, ki niso v skladu s pogodbo, dogovorom ali zakonom iz prvega odstavka tega člena, se obdelovalec šteje za upravljavca v zvezi s to obdelavo in je odgovoren za nezakonito obdelavo osebnih podatkov.

(5) Obdelovalec in katera koli oseba, ki deluje ali dela pod vodstvom upravljavca ali obdelovalca in ima dostop do osebnih podatkov, teh podatkov ne sme obdelati brez navodil upravljavca, razen če to določa zakon ali sodna odločba, izdana na podlagi zakona.

86. člen

(evidenca dejavnosti obdelav)

(1) Upravljavec iz 66. člena tega zakona upravlja evidenco vseh vrst dejavnosti obdelav osebnih podatkov in skrbi za njeno točnost in posodobljenost.

(2) Evidenca dejavnosti obdelav vsebuje naslednje informacije:

1. naziv in kontaktne podatke upravljavca, in kadar obstaja, tudi enako za skupnega upravljavca ter osebno ime in kontaktne podatke pooblaščene osebe;

2. namene obdelave;

3. navedbo pravne podlage za dejanja obdelave, vključno s prenosi, za katere so osebni podatki namenjeni;

4. kategorije uporabnikov, ki so jim bili ali jim bodo razkriti osebni podatki, vključno z uporabniki v tretjih državah ali mednarodnih organizacijah;

5. opis kategorij posameznikov, na katere se nanašajo osebni podatki, in vrst osebnih podatkov;

6. informacijo ali se izvaja profiliranje;

7. kategorije prenosov osebnih podatkov v tretjo državo ali mednarodno organizacijo;

8. kadar je to možno, predvidene roke za izbris različnih vrst osebnih podatkov;

9. kadar je to možno, splošni opis tehničnih in organizacijskih ukrepov.

(2) Obdelovalec vodi evidenco vseh vrst dejavnosti obdelave, ki jih izvaja v imenu upravljavca, evidenca pa vsebuje:

1. naziv in kontaktne podatke obdelovalca ali obdelovalcev, posameznih upravljavcev, v imenu katerih deluje obdelovalec, in kadar je določena, tudi osebno ime in kontaktne podatke pooblaščene osebe;

2. vrste obdelave, ki se izvaja v imenu posameznega upravljavca;

3. kadar je ustrezno, prenose osebnih podatkov v tretjo državo ali mednarodno organizacijo in identifikacijo te tretje države ali mednarodne organizacije, kadar to izrecno naroči upravljavec;

4. kadar je to možno, splošni opis tehničnih in organizacijskih ukrepov.

(3) Evidenca dejavnosti obdelav mora biti pisna, kar vključuje tudi elektronsko obliko.

(4) Upravljavec in obdelovalec omogočita nadzornemu organu dostop do evidence dejavnosti obdelav, kadar to nadzorni organ zahteva.

2. poglavje

Pravice posameznika, na katerega se nanašajo osebni podatki

87. člen

(pritožba pri nadzornem organu)

Prijave in opozorila nadzornemu organu glede kršitev določb II. dela tega zakona, ki jih podajo posamezniki, na katere se nanašajo osebni podatki, ali druge osebe, se rešujejo kot pritožbe pri nadzornem organu po tem zakonu. Zoper odločitve nadzornega organa v postopku pritožbe je dopusten upravni spor.

88. člen

(dajanje splošnih informacij)

(1) Upravljavec iz 66. člena tega zakona posamezniku, na katerega se nanašajo osebni podatki, zagotovi najmanj naslednje splošne informacije:

1. naziv in kontaktne podatke upravljavca;

2. kontaktne podatke pooblaščene osebe;

3. navedbo namenov obdelave osebnih podatkov;

4. obstoj pravice do vložitve prijave pri nadzornemu organu in njegove kontaktne podatke;

5. obstoj pravice dostopa do vsebine osebnih podatkov in obveznosti upravljavca, da na zahtevo posameznika izvaja posameznikove pravice do popravka, izbrisa ali omejitve obdelave njegovih osebnih podatkov.

(2) Poleg informacij iz prejšnjega odstavka upravljavec posamezniku, na katerega se nanašajo osebni podatki, ob upoštevanju možnega posebnega položaja posameznika ali kadar je to glede na konkretne okoliščine zadeve ali obdelave potrebno zaradi zagotovitve poštenosti obdelave, zagotovi naslednje dodatne informacije, da s tem omogoči učinkovitejše uresničevanje njegovih pravic:

1. pravno podlago obdelave;

2. rok hrambe osebnih podatkov ali, če to izjemoma ni mogoče, merila za določitev tega roka v skladu s 33. členom tega zakona;

3. če je možno, kategorije uporabnikov osebnih podatkov, tudi uporabnikov v tretjih državah in mednarodnih organizacijah;

4. če je možno, druge informacije, zlasti če so bili osebni podatki pridobljeni brez vednosti posameznika, na katerega se nanašajo.

(3) Obveščanje posameznika, na katerega se osebni podatki nanašajo, v skladu z drugim odstavkom tega člena se lahko opusti ali delno ali začasno omeji v skladu s prvim odstavkom 91. člena tega zakona.

89. člen

(pravica do pridobitve informacij o obdelanih podatkih)

(1) Posameznik, na katerega se nanašajo osebni podatki, ima pravico od upravljavca iz 66. člena tega zakona na svojo zahtevo prejeti potrdilo o tem, ali so v obdelavi osebni podatki, ki se nanašajo nanj ali ustrezno kopijo teh podatkov. Če so v obdelavi osebni podatki, ki se nanašajo nanj, ima pravico pridobiti informacije o:

1. namenih obdelave in njihovi pravni podlagi;

2. vrstah osebnih podatkov, ki se obdelujejo;

3. uporabnikih ali kategorijah uporabnikov, ki so jim bili podatki razkriti, zlasti če gre za uporabnike v tretjih državah ali mednarodnih organizacijah, v primerih omejitev iz prvega odstavka 91. člena tega zakona pa se lahko navede le okvirni opis uporabnikov;

4. če je mogoče, predvidenem roku hrambe osebnih podatkov ali, če to izjemoma ni mogoče, o merilih za določitev tega roka v skladu s 33. 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 nadzornem organu 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) Upravljavec sporoči informacije iz prejšnjega odstavka v roku enega meseca. Omejitve pravice do pridobitve informacij so dovoljene le pod pogoji iz prvega odstavka 91. člena tega zakona.

(3) V primeru nerazkritja informacij iz prvega odstavka tega člena upravljavec posameznika, na katerega se nanašajo osebni podatki, brez nepotrebnega odlašanja, najpozneje pa v treh delovnih dneh, pisno obvesti o zavrnitvi ali omejitvi informacij in razlogih za takšno odločitev. Ta odstavek se ne uporablja, če je zagotovitev teh informacij v nasprotju z enim od namenov iz prvega odstavka 91. člena tega zakona. Upravljavec posameznika, na katerega se nanašajo osebni podatki, obvesti o možnosti vložitve prijave nadzornemu organu.

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

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

90. člen

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

(1) Posameznik, na katerega se nanašajo osebni podatki, ima pravico od upravljavca iz 66. člena tega zakona zahtevati takojšnji popravek svojih netočnih osebnih podatkov oziroma dopolnitev nepopolnih ali neposodobljenih osebnih podatkov. Popravek ali dopolnitev se lahko po potrebi izvede z dodatno priloženo izjavo ali zaznamkom, če je naknadna sprememba nezdružljiva z namenom dokumentiranja glede na fazo določenega postopka. Upravljavec mora dokazati točnost ali posodobljenost osebnih podatkov, če osebni podatki niso bili pridobljeni izključno na podlagi navedb posameznika, na katerega se podatki nanašajo. Za postopek po tem členu se smiselno uporabljajo določbe prejšnji člen.

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

1. obdelava določenih osebnih podatkov ni več potrebna za namene, za katere so bili pridobljeni ali drugače obdelani;

2. so bili osebni podatki obdelani nezakonito ali

3. je izbris osebnih podatkov potreben zaradi izpolnitve druge obveznosti po zakonu ali po pravnomočni sodni odločbi.

(3) Upravljavec namesto izbrisa osebnih podatkov njihovo obdelavo omeji, če:

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

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

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

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

(6) Glede vprašanj rokov za odločanje, dokazovanja, odplačnosti ter zaračunavanja razumne pristojbine se smiselno uporablja 12. člen Splošne uredbe.

91. člen

(omejitve pravice do dostopa do lastnih osebnih podatkov)

(1) Pravice posameznika, na katerega se nanašajo osebni podatki, glede dostopa do njegovih osebnih podatkov po tem delu zakona je mogoče izjemoma in začasno omejiti če in dokler je to v posameznem primeru nujno in očitno sorazmerno in določeno z zakonom ali določeno v zakonu za določene primere posameznikov, na katere se nanašajo osebni podatki:

1. da se onemogoči oviranja ali vplivanja na postopke, katerih nameni so določeni v 66. členu tega zakona, vključno s pridobivanjem ali prenosi osebnih podatkov za še nedokončane uradne postopke za te namene;

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

3. zaradi varnosti države;

4. zaradi varstva obrambe države;

5. zaradi varstva človekovih pravic in temeljnih svoboščin tretjih oseb.

(2) Upravljavec iz 66. člena tega zakona mora posameznika, na katerega se nanašajo osebni podatki, brez nepotrebnega odlašanja pisno obvestiti o vsaki zavrnitvi ali omejitvi dostopa in razlogih za to. Informacij se ne poda, če bi njihovo dajanje ogrozilo izvrševanje namena iz prejšnjega odstavka. Upravljavec posameznika, na katerega se nanašajo osebni podatki, obvesti o možnosti za vložitev pritožbe pri nadzornem organu ali mu poda pravni pouk o možni uporabi pravnega sredstva. Za postopek po tem členu se smiselno uporabljajo določbe 89. člena tega zakona.

(3) Upravljavec z zaznamkom zabeleži dejansko stanje ali pravne razloge, na katerih temelji odločitev iz prvega odstavka tega člena. Zaznamek je dostopen nadzornemu organu in Varuhu človekovih pravic.

92. člen

(zagotavljanje varnosti osebnih podatkov)

(1) Upravljavec iz 66. člena tega zakona in obdelovalec morata ob upoštevanju tehnološkega razvoja, stroškov izvajanja in narave, obsega, okoliščin in namenov obdelave, pa tudi tveganj za človekove pravice in temeljne svoboščine posameznikov, ki se razlikujejo po verjetnosti in resnosti, z ustreznimi tehničnimi in organizacijskimi ukrepi zagotoviti ustrezno raven varnosti obdelave osebnih podatkov glede na tveganje, zlasti kar zadeva obdelavo posebnih vrst osebnih podatkov.

(2) Kadar se izvaja avtomatizirana obdelava osebnih podatkov morata upravljavec ali obdelovalec po izvedeni oceni tveganja izvesti dodatne ukrepe, kateri:

1. onemogočajo dostop nepooblaščenih oseb do opreme, ki se uporablja za obdelavo (nadzor dostopa do opreme);

2. preprečujejo nepooblaščeno branje, prepisovanje, spreminjanje ali odnašanje nosilcev podatkov (nadzor nosilcev podatkov);

3. preprečujejo nepooblaščeno vnašanje osebnih podatkov v podatkovne zbirke in nepooblaščeno pregledovanje, spreminjanje ali brisanje shranjenih osebnih podatkov (nadzor shranjevanja);

4. preprečujejo nepooblaščenim osebam, ki uporabljajo opremo za prenos podatkov, uporabo sistemov za avtomatizirano obdelavo (nadzor uporabnikov);

5. zagotavljajo, da imajo osebe, pooblaščene za uporabo sistema za avtomatizirano obdelavo, dostop samo do podatkov, ki jih zajema njihovo pooblastilo za dostop (nadzor dostopa do podatkov);

6. zagotavljajo, da je mogoče preveriti in ugotoviti, katerim upravljavcem ali uporabnikom iz 66. člena tega zakona so osebni podatki bili ali bi lahko bili poslani oziroma jim je bil ali bi jim lahko bil omogočen dostop do njih prek opreme za prenos podatkov (nadzor prenosa);

7. zagotavljajo, da je mogoče naknadno preveriti in ugotoviti, kateri osebni podatki so bili vneseni v sisteme za avtomatizirano obdelavo ter kdaj in kdo jih je vnesel (nadzor vnosa);

8. preprečujejo nepooblaščeno branje, prepisovanje, spreminjanje ali izbris osebnih podatkov med pošiljanjem osebnih podatkov ali med premeščanjem nosilcev podatkov (nadzor premeščanja);

9. zagotavljajo, da je mogoče nameščene sisteme v primeru prekinitve ponovno vzpostaviti (obnova);

10. zagotavljajo, da funkcije sistema delujejo, da se pojavljanje napak v funkcijah sporoči (zanesljivost) in da shranjeni osebni podatki ne morejo postati neuporabni zaradi okvare sistema (neoporečnost).

93. člen

(uradno obvestilo o kršitvi varnosti osebnih podatkov)

(1) Upravljavec iz 66. člena tega zakona ali obdelovalec morata v primeru kršitve varnosti osebnih podatkov brez nepotrebnega odlašanja, najpozneje v 72 urah po seznanitvi s kršitvijo, o njej uradno obvestiti nadzorni organ, razen če ni verjetno, da bi bilo s kršitvijo varstva osebnih podatkov povzročeno tveganje za pravice in svoboščine posameznikov. Kadar uradno obvestilo nadzornemu organu ni podano v 72 urah, mu morata upravljavec ali obdelovalec priložiti razloge za zamudo.

(2) Obdelovalec ob seznanitvi s kršitvijo varnosti osebnih podatkov brez nepotrebnega odlašanja o tem uradno obvesti upravljavca, najpozneje v 24 urah po seznanitvi s kršitvijo.

(3) Uradno obvestilo iz prvega in drugega odstavka tega člena vsebuje vsaj:

1. opis vrste kršitve varnosti osebnih podatkov, po možnosti tudi kategorije in približno število zadevnih posameznikov, na katere se nanašajo osebni podatki, ter vrste in približno število zadevnih zbirk, kjer so se zgodile kršitve;

2. sporočilo o imenu in kontaktnih podatkih pooblaščene osebe ali druge kontaktne točke, pri kateri je mogoče pridobiti več informacij;

3. opis verjetnih posledic kršitve varnosti osebnih podatkov;

4. opis ukrepov, ki jih upravljavec ali obdelovalec sprejmeta ali katerih sprejetje načrtujeta za obravnavanje kršitve varnosti osebnih podatkov, vključno z če je to primerno - ukrepi za ublažitev morebitnih škodljivih učinkov kršitve.

(4) Kadar informacij ni mogoče zagotoviti istočasno, se informacije lahko zagotovijo postopoma brez nepotrebnega dodatnega odlašanja.

(5) Upravljavec dokumentira vsako kršitev varnosti osebnih podatkov iz prvega odstavka tega člena, vključno z dejstvi v zvezi s kršitvijo varstva osebnih podatkov, njene učinke in sprejete popravne ukrepe. Dokumentacija iz prejšnjega stavka je na razpolago nadzornemu organu, kadar preverja skladnost delovanja upravljavca z določbami tega člena.

(6) Kadar kršitev varnosti osebnih podatkov vključuje osebne podatke, ki jih je upravljavec druge države članice poslal ali so mu bili poslani, mora organ ali subjekt iz 66. člena tega zakona informacije iz tretjega odstavka sporočiti brez nepotrebnega odlašanja upravljavcu navedene države članice.

94. člen

(sporočilo posamezniku o kršitvi varnosti osebnih podatkov)

(1) V primerih, ko je verjetno, da bi kršitev varnosti osebnih podatkov lahko povzročila veliko tveganje za človekove pravice in temeljne svoboščine posameznikov, upravljavec brez nepotrebnega odlašanja sporoči posamezniku, na katerega se nanašajo osebni podatki, da je prišlo do kršitve varnosti osebnih podatkov.

(2) V sporočilu posamezniku, na katerega se nanašajo osebni podatki, po prvem odstavku tega člena je treba v jasnem in preprostem jeziku opisati vrsto kršitve varnosti osebnih podatkov, v njem morajo biti vključene vsaj informacije in opis ukrepov iz 2., 3. in 4. točke tretjega odstavka 93. člena tega zakona.

(3) Sporočilo posamezniku, na katerega se nanašajo osebni podatki, ni potrebno, če je izpolnjen kateri izmed naslednjih pogojev:

1. upravljavec je izvedel ustrezne tehnološke in organizacijske zaščitne ukrepe in so bili ti ukrepi uporabljeni za osebne podatke, v zvezi s katerimi je bila storjena kršitev varstva, zlasti ukrepe, na podlagi katerih postanejo osebni podatki nerazumljivi vsem, ki niso pooblaščeni za dostop do njih, kot je šifriranje,

2. upravljavec je sprejel naknadne ukrepe za zagotovitev, da se veliko tveganje za človekove pravice in temeljne svoboščine posameznikov, na katere se nanašajo osebni podatki, verjetno ne bo ponovilo,

3. bi to zahtevalo nesorazmeren napor. V takšnem primeru se namesto tega objavi javno sporočilo ali izvede podoben ukrep, s katerim so posamezniki, na katere se nanašajo osebni podatki, enako učinkovito obveščeni.

(4) Če upravljavec posameznika, na katerega se nanašajo osebni podatki, še ni obvestil o kršitvi varnosti osebnih podatkov, lahko nadzorni organ to od njega lahko zahteva po preučitvi verjetnosti, da bi kršitev varnosti osebnih podatkov povzročila veliko tveganje, ali pa odloči, da je izpolnjen kateri od pogojev iz prejšnjega odstavka.

(5) Sporočilo posamezniku, na katerega se nanašajo osebni podatki, iz prvega odstavka tega člena se lahko pod pogoji in iz razlogov iz prvega odstavka 91. člena tega zakona zadrži, omeji ali opusti.

3. poglavje

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

95. člen

(splošna pravila za prenos osebnih podatkov ter čezmejno obdelavo)

(1) To poglavje se uporablja za primere, ko osebne podatke obdelujejo organi in subjekti iz 66. člena tega zakona za namene iz 66. člena tega zakona.

(2) Organ ali subjekt iz 66. člena tega zakona sme osebne podatke, ki so že obdelani ali naj bi se obdelali po prenosu tretji državi oziroma mednarodni organizaciji ali naj bi se čezmejno obdelovali, prenesti le, če so upoštevane določbe tega dela zakona in:

1. je prenos potreben za namene iz 66. člena tega zakona;

2. se osebni podatki posredujejo upravljavcu v tretji državi ali mednarodni organizaciji, ki je pristojni organ ali subjekt za izpolnitev enega od namenov iz 66. člena tega zakona;

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

4. je Evropska komisija sprejela sklep o ustreznosti ravni varstva osebnih podatkov ali, če tak sklep ne obstaja, obstajajo ustrezni ukrepi v skladu s 96. členom tega zakona, ali je, če ne obstaja sklep o ustreznosti in ne obstajajo ustrezni ukrepi in niso predložena ustrezna zagotovila, možno v skladu z 98. členom tega zakona uporabiti izjeme za določene primere in

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

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

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

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

(6) Nadzorni organ lahko po uradni dolžnosti odloči, ne glede na obstoj pravnih podlag za prenos po II. delu zakona, da za določeno obdobje izjemoma ustavi prenose določenih vrst osebnih podatkov tretji državi ali mednarodni organizaciji, če obstaja dejansko in resno tveganje, da bi prenos osebnih podatkov iz Republike Slovenije tretji državi ali mednarodni organizaciji ali državi članici Evropske unije ali Sveta Evrope ali nadaljnji prenosi osebnih podatkov s strani tretje države ali mednarodne organizacije omogočali kršitev določb zakona. Pred uvedbo teh ukrepov nadzorni organ pridobi mnenje ministrstva, pristojnega za zunanje zadeve.

(7) Zoper odločbo iz prejšnjega odstavka nista dovoljena pritožba ali začasna odredba, dopusten pa je upravni spor.

(8) Nadzorni organ Informacijski pooblaščenec odločitev objavi v Uradnem listu Republike Slovenije ter o tem obvesti Evropsko komisijo.

96. člen

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

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

(2) Sklep Evropske komisije, sprejet v skladu s petim odstavkom 36. člena Direktive o razveljavitvi, spremembi ali začasni odložitvi izvajanja sklepa iz tretjega odstavka 36. člena Direktive ne vpliva na prenose osebnih podatkov v skladu s 97. in 98. členom tega zakona.

(3) Upravljavci v Republiki Sloveniji so vezani na sklepe Evropske komisije iz prvega in drugega odstavka tega člena od datuma njihove objave v Uradnem listu Evropske unije.

97. člen

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

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

1. so v zakonu določeni ustrezni ukrepi za varstvo osebnih podatkov ali

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

(2) Če v skladu z 2. točko prejšnjega odstavka obstajajo ustrezni ukrepi za določene vrste prenosov, upravljavec o njih obvesti nadzorni organ, ki lahko odredi prepoved prenosa osebnih podatkov, če ugotovi neskladnosti z II. delom zakona. Upravljavec mora izpolnjevanje pogojev iz 2. točke prejšnjega odstavka ustrezno dokumentirati, pri čemer mora biti dokumentacija vedno na razpolago nadzornemu organu, vključno z datumom in uro prenosa, podatki o pristojnem prejemniku, navedbo pravne podlage, utemeljitev prenosa ter navedbo, kateri osebni podatki so bili preneseni.

(3) Upravljavec mora izvajati redno notranje preverjanje skladnosti obdelav z določbami prvega odstavka tega člena ter to preverjanje in prenose dokumentirati. Dokumentacija vsebuje datum in čas prenosa, informacije o pristojnemu organu ali uporabniku, pravno podlago, razloge prenosa in opis prenešenih osebnih podatkov, lahko pa tudi druge informacije.

98. člen

(izjeme za posamezne primere)

(1) Če ne obstaja sklep o ustreznosti v skladu s tretjim odstavkom 36. člena Direktive ali ustrezen ukrep v skladu s prejšnjim členom, je prenos osebnih podatkov tretji državi ali mednarodni organizaciji dopusten, kadar gre:

1. za zaščito življenjskih interesov posameznika, na katerega se nanašajo osebni podatki ali druge osebe;

2. če je to predvideno zaradi varovanja zakonitih interesov posameznikov, na katere se nanašajo osebni podatki, in je to določeno v zakonu države članice, ki prenaša osebne podatke, ali v enakovrednem predpisu mednarodne organizacije;

3. za preprečitev neposredne in resne nevarnosti za javno varnost države članice ali tretje države;

4. v posameznem primeru za namene iz 66. člena tega zakona ali

5. v posameznem primeru za uveljavljanje, izvajanje ali obrambo pravnih zahtevkov v povezavi z nameni iz 66. člena tega zakona.

(2) V primerih iz 4. in 5. točke prejšnjega odstavka je prenos dovoljen le, če človekove pravice in temeljne svoboščine posameznika, na katerega se nanašajo osebni podatki, ne prevladajo nad javnim interesom.

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

99. člen

(posebni prenosi določenim uporabnikom v tretjih državah)

(1) Ne glede na drugi odstavek 95. člena tega zakona smejo upravljavci in uporabniki iz 66. člena tega zakona izvesti prenos osebnih podatkov v tretjo državo v posebnem posameznem primeru, tako da jih prenesejo neposredno upravljavcu ali uporabniku javnega ali zasebnega sektorja v tretji državi ali mednarodni organizaciji, če je prenos nujno potreben za opravljanje konkretnih zakonskih nalog, če so izpolnjene zahteve iz tega zakona in so izpolnjeni vsi naslednji pogoji:

1. je prenos nujno potreben za izvajanje naloge pristojnega organa ali subjekta, ki podatke prenese v skladu z zakonom za namene iz 66. člena tega zakona in namena ne more izpolniti brez prenosa osebnih podatkov,

2. v konkretnem primeru pristojni organ ali subjekt, ki podatke prenese, ugotovi, da človekove pravice in temeljne svoboščine posameznika, na katerega se nanašajo osebni podatki, ne prevladujejo nad javnim interesom za prenos,

3. bi bil prenos v skladu z drugimi določbami tega dela zakona neučinkovit ali neprimeren, zlasti ker ga ni mogoče izvesti pravočasno,

4. je pristojni organ tretje države o tem obveščen brez odlašanja, razen če to ni učinkovito ali primerno in

5. pristojni organ ali subjekt, ki podatke prenese, uporabniku sporoči določene in dopustne namene obdelave, za katere naj bi uporabnik izključno obdelal osebne podatke, in se uporabnik zaveže, da bo te osebne podatke obdeloval samo za te namene in v obsegu, v katerem je obdelava za te namene potrebna.

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

(3) Ne glede na prvi in drugi odstavek tega člena se prenosi osebnih podatkov pristojnim organom in drugim organom tretje države iz 1. točke drugega odstavka 6. člena tega zakona lahko izvedejo v skladu z obvezujočimi mednarodnimi pogodbami s področja pravosodnega sodelovanja v kazenskih zadevah in policijskega sodelovanja.

III. DEL
PODROČNE UREDITVE OBDELAVE OSEBNIH PODATKOV

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

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

(1) Ne glede na prvotni namen obdelave lahko upravljavec osebne podatke, vključno s posebnimi vrstami osebnih podatkov, nadalje obdeluje za znanstvenoraziskovalne, zgodovinskoraziskovalne in statistične namene če:

1. je posameznik, na katerega se osebni podatki nanašajo, za takšno obdelavo podal predhodno pisno privolitev, pri obdelavah za znanstvenoraziskovalne namene pa tudi, če je podal prehodno pisno privolitev za obdelavo njegovih osebnih podatkov na določenem znanstvenoraziskovalnem področju, ki vključuje tudi namene zadevne raziskave;

2. če nameni takšne nadaljnje obdelave niso nezdružljivi s prvotnim namenom obdelave, ali

3. tako dovoljuje drug zakon.

(2) Raziskovalne organizacije ter raziskovalci, vpisani v zbirko podatkov o izvajalcih raziskovalne in razvojne dejavnosti pri Agenciji za raziskovalno dejavnost Republike Slovenije, lahko za namene iz prejšnjega odstavka in v soglasju z upravljavcem od njega vpogledajo pridobijo osebne podatke,

vključno s posebnimi vrstami osebnih podatkov, če predložijo predstavitveni elaborat raziskave (v nadaljnjem besedilu: elaborat), s katerim izkažejo:

1. dejanski obstoj raziskave, naslov ter navedbo nosilcev raziskave,

2. podatke o neposrednih izvajalcih raziskave (osebno ime, naziv, prebivališče, razmerje do nosilca raziskave in šifra raziskovalca);

3. podatke o znanstveno raziskovalnem področju (opisno in po klasifikaciji Agencije za raziskovalno dejavnost Republike Slovenije);

4. namene oziroma cilje raziskave;

5. metode dela v zvezi z osebnimi podatki,

6. vrste osebnih podatkov, ki bi jih želeli pridobiti od upravljavca, ter kategorije posameznikov, na katere se nanašajo ti podatki;

7. obliko, v kateri želijo prejeti osebne podatke (predvsem izvorni osebni podatki, psevdonimizirani osebni podatki, osebni podatki v obliki, ki ne zahteva identifikacije, anonimizirani podatki);

8. da namenov oziroma ciljev raziskave ni mogoče doseči brez obdelave zaprošenih osebnih podatkov, z že anonimiziranimi osebnimi podatki oziroma z osebnimi podatki v manj izvirni obliki, ali da bi bilo to povezano z nesorazmernim naporom ali stroški (primernost in nujnost obdelave),

9. da bi predvidene koristi od raziskave bistveno pretehtale nad posledicami, ki bi lahko nastale posameznikom, na katere se nanašajo osebni podatki (sorazmernost obdelave),

10. način objave rezultatov raziskave,

11. navedbo morebitnih specifičnih etičnih pravil znanstvenoraziskovalnega, zgodovinskoraziskovalnega ali statističnega področja ter

12. način objave raziskave oziroma njene bodoče dostopnosti oziroma navedbo kroga oseb ali subjektov, ki bodo imeli dostop do nje.

(3) Elaboratu iz prejšnjega odstavka se priloži oceno učinkov v zvezi z varstvom osebnih podatkov iz 35. člena Splošne uredbe, ki mora vključevati tudi zaščitne ukrepa za zavarovanje pravic posameznikov, na katere se nanašajo osebni podatki, pod pogoji iz 36. člena Splošne uredbe pa tudi zaključke posvetovanja z nadzornim organom. Upravljavec ima pravico biti udeležen pri pripravi ocene učinkov oziroma posvetovanja.

(4) Upravljavec zavrne posredovanje osebnih podatkov, če oceni, da ti osebni podatki niso primerni ali nujni za izvedbo raziskave, oziroma če oceni, da nameni oziroma cilji raziskave ne upravičujejo posega v pravice posameznikov, na katere se nanašajo podatki. Upravljavec lahko pri tem prosilcu predlaga tudi potrebne dopolnitve elaborata oziroma ocene učinkov, pod katerimi bi posredovanje lahko bilo dopustno.

(5) Upravljavec, v primeru iz drugega odstavka pa tudi izvajalec raziskave, pred začetkom raziskave pisno obvestita posameznike o nameravani obdelavi osebnih podatkov pod pogoji iz 12. do 14. člena Splošne uredbe.

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

(7) Rezultati raziskave iz prejšnjih odstavkov se objavijo v anonimizirani obliki, razen če ta ali drug zakon določa drugače ali če je posameznik, na katerega se nanašajo osebni podatki, za objavo v neanonimizirani obliki podal pisno privolitev ali če je za takšno objavo v času po smrti posameznika podana pisna privolitev naslednjih oseb v izključujočem vrstnem redu: zakonec ali zunajzakonski

partner ali partner z njima z zakonom izenačene skupnosti, otroci ali starši umrlega posameznika. Upravljavec ne sme objaviti neanonimiziranih osebnih podatkov, če je to v nasprotju z interesom varovanja tajnosti ali zaupnosti postopkov odločanja, ali pa ti postopki še niso končani.

(8) Posameznik, na katerega se nanašajo osebni podatki, ima v razmerju do izvajalca raziskave pravico dostopa do vsebine svojih osebnih podatkov, v primerih izvajanja raziskave na podlagi združljivosti namenov pa tudi pravico do ugovora. Pravico do izbrisa ima le v primeru, da izkaže, da so bili njegovi osebni podatki pridobljeni oziroma obdelani nezakonito, oziroma da niso več potrebni za namene raziskave.

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

101. člen

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

(1) V okviru obdelave osebnih podatkov za znanstvenoraziskovalne, zgodovinskoraziskovalne ali statistične namene upravljavec izjemoma lahko obdeluje tudi osebne podatke ciljne skupine posameznikov zaradi pridobitve privolitev za obdelavo njihovih osebnih podatkov ali zaradi pridobitve dodatnih podatkov ali pojasnil za prej navedene namene.

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

1. za obdelavo osebnih podatkov nima podlage v zakonu ali privolitvi in

2. z elaboratom izkaže, da bo osebne podatke po pridobitvi privolitve obdeloval na znanstvenoraziskovalnem, zgodovinskoraziskovalnem ali statističnem področju.

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

(4) Osebni podatki se v skladu s tem členom lahko obdelajo izključno za namene iz prvega odstavka prejšnjega člena in jih je treba izbrisati takoj, ko niso več potrebni, razen če drug zakon določa drugače.

(5) Ta člen se ne uporablja za obdelavo osebnih podatkov v skladu z določbami zakona, ki ureja varstvo dokumentarnega in arhivskega gradiva ter arhive.

102. člen

(obdelava podatkov za namene arhivskega delovanja)

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

(2) Posameznik, na katerega se nanašajo osebni podatki, nima pravice do dostopa do lastnih osebnih podatkov v arhivskem gradivu v skladu s 15. členom Splošne uredbe, če bi dajanje informacij ali kopij njegovih osebnih podatkov zahtevalo očitno nesorazmeren napor. Posameznik, na katerega se nanašajo osebni podatki, nima pravice zahtevati:

1. popravka osebnih podatkov zaradi netočnosti ali neposodobljenosti v skladu s 16. členom Splošne uredbe,

2. izbrisa v skladu s 17. členom Splošne uredbe,

3. omejitve obdelave v skladu z 18. členom Splošne uredbe,

4. prenosljivosti osebnih podatkov v skladu z 20. členom Splošne uredbe ter

5. izvršitve pravice do ugovora v skladu z 21. členom Splošne uredbe.

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

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

2. poglavje

Varstvo svobode izražanja ter dostopa do informacij v razmerju do varstva osebnih podatkov

103. člen

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

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

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

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

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

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

4. so bili osebni podatki pridobljeni na podlagi prisotnosti posameznika na javno dostopnih krajih ali dogodkih, kjer posameznik glede na vse okoliščine ne more razumno pričakovati varstva zasebnosti, ter na način, ki ne pomeni občutnega posega v razumno pričakovano zasebnost,

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

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

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

8. tako določa drug zakon.

(3) Uveljavljanje pravic posameznika, na katerega se nanašajo osebni podatki, v zvezi s tem členom zagotavljajo sodišča v skladu z določbami drugih zakonov, ki urejajo svobodo izražanja in sodno varstvo.

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

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

104. člen

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

(1) Zavezanci po zakonu, ki ureja dostop do informacij javnega značaja, javnosti posredujejo osebne podatke, če so ti po zakonu javni ali če je za njihovo razkritje podan prevladujoč javni interes v skladu z zakonom, ki ureja dostop do informacij javnega značaja.

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

105. člen

(izjema glede obveščanja posameznika)

Če so osebni podatki javni na podlagi zakona, posameznika, na katerega se nanašajo osebni podatki, ni treba obveščati v skladu z 12. do 14. členom Splošne uredbe in določbami zakona, ki ureja splošni upravni postopek.

3. poglavje

Neposredno trženje

106. člen

(pravice in dolžnosti upravljavca na področju neposrednega trženja)

(1) Upravljavec lahko obdeluje kontaktne podatke posameznika, na katerega se nanašajo osebni podatki, kateri so: osebno ime, naslov stalnega ali začasnega prebivališča, telefonska številka oziroma naslov elektronske pošte, ki jih je zbral v okviru zakonitega opravljanja dejavnosti oziroma iz javno dostopnih virov. Osebne podatke iz prejšnjega stavka lahko obdeluje za namene ponujanja blaga, storitev, obveščanja o svojih dejavnostih, ponujanja zaposlitev ali začasnega opravljanja del temu posamezniku in to z uporabo poštnih storitev, telefonskih klicev, elektronske pošte ali drugih elektronskih komunikacijskih sredstev v skladu z določbami tega poglavja, če drug zakon ne določa drugače. Obdelava osebnih podatkov za namene iz prvega stavka pomeni izvajanje neposrednega trženja.

(2) Ne glede na določbe prejšnjega odstavka lahko upravljavec obdeluje kontaktne oziroma druge osebne podatke za namene neposrednega trženja tudi na podlagi 6. člena Splošne uredbe.

(3) Upravljavec neposredno trženje iz prvega in drugega odstavka izvaja tako, da posamezniku skupaj z vsakim trženjskim sporočilom zagotovi vsaj naslednje informacije:

1. informacijo, da gre za trženjsko sporočilo;

2. identiteto in kontaktne podatke upravljavca in njegovega predstavnika, kadar ta obstaja;

3. od kje izvirajo osebni podatki, na podlagi katerih je bilo trženjsko sporočilo pripravljeno oziroma poslano, in če ti podatki izvirajo iz javno dostopnih virov, opis teh virov;

4. na kakšen način lahko posameznik uveljavlja pravico zahtevati prenehanje obdelave njegovih osebnih podatkov za namene neposrednega trženja iz 107. člena tega zakona.

(4) Upravljavcu podatkov iz prejšnjega odstavka ni potrebno zagotavljati, če jih posameznik že ima, razen informacije o tem, da gre za trženjsko sporočilo, ki mora biti v vsakem primeru jasno navedena oziroma drugače jasno razpoznavna.

(5) Naknadna obdelava osebnih podatkov, ki so bili obdelani za namene iz prvega in drugega odstavka tega člena, je prepovedana za namene izvajanja političnega trženja, kar vključuje kontaktiranje ali prepričevanje morebitnih volivcev ali njihovo profiliranje.

(6) Prodaja osebnih podatkov, ki so bili obdelani za namene iz prvega in drugega odstavka tega člena, je prepovedana za namene izvajanja političnega trženja iz prejšnjega odstavka.

(7) Glede uporabe osebnih podatkov s področja elektronskih komunikacijskih sredstev za izvajanje neposrednega trženja se uporabljajo tudi določbe zakona, ki ureja elektronske komunikacije.

107. člen

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

(1) Posameznik, na katerega se nanašajo osebni podatki, lahko kadarkoli pisno ali na drug dogovorjen način brezplačno zahteva, da upravljavec trajno ali začasno preneha uporabljati ali drugače obdelovati njegove osebne podatke za namen neposrednega trženja. Upravljavec v primeru iz prejšnjega stavka najpozneje v 15 dneh preneha obdelovati osebne podatke za namen neposrednega trženja ter o tem v nadaljnjih petih dneh pisno ali na drug dogovorjen način obvesti posameznika, ki je vložil zahtevo.

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

4. poglavje
Videonadzor

108. člen

(splošne določbe o videonadzoru in varstvu osebnih podatkov)

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

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

(3) Obvestilo iz prejšnjega odstavka vsebuje naslednje informacije:

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

2. naziv osebe javnega ali zasebnega sektorja, ki ga izvaja;

3. telefonsko številko za pridobitev informacije, kje in koliko časa se shranjujejo posnetki videonadzornega sistema.

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

(5) Če ni z zakonom drugače določeno, zbirka posnetkov videonadzornega sistema vsebuje posnetek posameznika (slika), datum in čas posnetka. Zbirka posnetkov lahko vsebuje poleg osebnih podatkov iz prejšnjega stavka tudi zvok, če je v tem ali drugem zakonu tako določeno.

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

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

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

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

109. člen

(videonadzor dostopa v uradne službene oziroma poslovne prostore)

(1) V javnem in zasebnem sektorju se lahko izvaja videonadzor dostopa v njihove uradne službene oziroma poslovne prostore, če je to potrebno za varnost ljudi ali premoženja, zaradi zagotavljanja nadzora vstopa ali izstopa v ali iz uradnih službenih oziroma poslovnih prostorov ali če zaradi narave dela obstaja možnost ogrožanja zaposlenih. Vpogled, uporaba ali posredovanje posnetkov je dopustno le za te namene, če drug zakon ne določa drugače.

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

(3) O izvajanju videonadzora se pisno obvesti vse zaposlene, 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.

110. člen

(videonadzor v večstanovanjskih stavbah)

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

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

(3) Strinjanje iz prejšnjega odstavka mora biti pisno, pri čemer se na listini izrecno navede, kateri lastniki so se strinjali z uvedbo videonadzora.

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

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

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

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

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

111. člen

(videonadzor znotraj delovnih prostorov)

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

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

(3) Spremljanje neposrednega dogajanja pred kamerami je pod pogoji iz prvega in drugega odstavka tega člena dopustno le, če ga izvaja pooblaščeno varnostno osebje ali na področju iger na srečo drugo posebej pooblaščeno in usposobljeno osebje upravljavca.

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

(5) Pred uvedbo videonadzora v osebi javnega ali zasebnega sektorja se mora delodajalec posvetovati z reprezentativnimi sindikati pri delodajalcu ter svetom delavcev oziroma delavskim zaupnikom, če obstajajo. Posvetovanje se izvede v roku 30 dni oziroma v drugem daljšem roku, ki ga določi delodajalec. Po prejetju morebitnega mnenja delodajalec dokončno odloči o uvedbi ali neuvedbi videonadzora.

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

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

112. člen

(videonadzor na javnih površinah)

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

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

(3) Videonadzor na javnih površinah lahko izvaja oseba javnega ali zasebnega sektorja, ki upravlja z javno površino ali na njej zakonito opravlja dejavnost. Videonadzor smejo za javni sektor izvajati le uradne osebe ali pooblaščeno varnostno osebje, za zasebni sektor pa pooblaščeno varnostno osebje.

5. poglavje

Obdelava osebnih podatkov z uporabo biometrije

113. člen

(biometrični ukrepi v javnem sektorju)

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

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

(3) Ne glede na določbe prvega in drugega odstavka tega člena se v javnem sektorju lahko uvedejo biometrični ukrepi v zvezi z vstopom v stavbo ali dele stavbe, ki se izvedejo ob smiselni uporabi 114. člena tega zakona.

114. člen

(biometrični ukrepi v zasebnem sektorju)

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

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

(3) Oseba zasebnega sektorja lahko izvaja biometrične ukrepe tudi v zvezi s svojimi strankami, kadar se na ta način zagotavlja varstvo točnosti njihove identitete in pod pogojem, da to za namene varovanja interesov iz prvega odstavka tega člena določa drug zakon ali pogodba ali so stranke podale izrecno pisno privolitev, ki je določena v drugem zakonu.

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

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

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

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

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

115. člen

(prepoved pridobivanja biometričnih osebnih podatkov v zvezi s trženjem)

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

6. poglavje

Evidentiranje vstopov in izstopov

116. člen

(evidentiranje vstopov in izstopov iz službenih prostorov)

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

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

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

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

7. poglavje

Javne knjige in varstvo osebnih podatkov

117. člen

(zakoniti namen javne knjige)

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

8. poglavje

Povezovanje zbirk osebnih podatkov

118. člen

(povezovanje uradnih evidenc in javnih knjig)

(1) Uradne evidence in javne knjige, v katerih se obdelujejo posebne vrste osebnih podatkov, osebni podatki v zvezi s kazenskimi obsodbami in prekrški, podatki o dohodkih v skladu z zakonom, ki ureja dohodnino, podatki o premoženju posameznika v skladu z zakonom, ki ureja uveljavljanje pravic iz javnih sredstev, podatki o nepremičninah v lasti posameznika v skladu z drugimi zakoni, podatki oziroma informacije o kreditni sposobnosti v skladu z zakonom, ki ureja centralni kreditni re*gister, in uradne evidence v skladu z zakonom, ki ureja naloge in pooblastila policije, in zakonom, ki ureja preprečevanje pranja denarja in financiranja terorizma, se lahko povezuje med seboj ali z drugimi zbirkami samo, če takšno povezovanja izrecno določa zakon.

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

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

(4) Najpozneje 30 dni pred začetkom povezovanja zbirk iz prvega odstavka tega člena mora upravljavec oziroma obdelovalec poslati obvestilo nadzornemu organu, v katerem navede, da namerava izvesti povezovanje v skladu s tem členom ter ga podrobno opiše zlasti z navedbo pravnih podlag, tehničnih rešitev in zaščitnih ukrepov.

9. poglavje

Strokovni nadzor

119. člen

(strokovni nadzor)

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

120. člen

(splošne določbe)

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

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

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

121. člen

(obveščanje posameznika in pridobivanje podatkov)

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

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

122. člen

(posebne vrste osebnih podatkov)

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

10. poglavje

Javni kontaktni podatki in podatki za organiziranje dogodkov v javnem sektorju

123. člen

(javni kontaktni podatki)

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

124. člen

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

(1) Oseba iz javnega sektorja lahko uporablja kontaktne podatke posameznikov, ki jih je zbrala iz javno dostopnih virov ali v okviru izvrševanja svojih javnih nalog ali so ji jih posamezniki, na katere se

nanašajo, prostovoljno razkrili ali podali za to privolitev, za namene organiziranja uradnih srečanj in dogodkov, določanja sestav komisij, delegacij in drugih podobnih delovanj javnega sektorja, dajanja izjav za javnost oziroma druge aktivnosti obveščanja zainteresirane javnosti o svojem delovanju. Zbirke osebnih podatkov, ki nastanejo na tej podlagi, morajo biti ločene od drugih zbirk osebnih podatkov, ki nastanejo pri izvrševanju zakonitih pristojnosti, nalog ali obveznosti.

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

IV. DEL
KAZENSKE DOLOČBE

125. člen
(uporaba določb Splošne uredbe glede upravnih kazni in glob ter odločanje o prekrških po tem zakonu)

(1) Nadzorni organ odloča o predpisanih kršitvah in upravnih globah iz 83. člena Splošne uredbe kot o prekrških v okviru pristojnosti prekrškovnega organa po določbah zakona, ki ureja prekrške, ne glede na določbe o določanju razponov glob iz 17. člena zakona, ki ureja prekrške.

(2) Poleg splošnih pravil za odmero sankcije iz zakona, ki ureja prekrške, se pri odločanju nadzornega organa o višini izrečene globe za kršitve, predpisane v četrtem do šestem odstavku 83. člena Splošne uredbe, v skladu z določbami prvega odstavka 83. člena Splošne uredbe in zakona, ki ureja prekrške, ob obravnavanju konkretnih okoliščin posameznega primera tudi upošteva, da globa ne sme biti nesorazmerno breme ali neprimerljivo breme za upravljavce ali obdelovalce glede na druge primerljive kršitve človekovih pravic in temeljnih svoboščin, ki se kaznujejo za prekrške, ali je obstajal namen koristoljubnosti ali namen škodovanja posameznikom, na katere se nanašajo osebni podatki, v primeru izvajanja popravljalnih ukrepov s strani upravljavca ali obdelovalca njihovo učinkovitost ali samostojno ukrepanje še pred uvedbo nadzora, glede fizičnih oseb pa se zlasti upošteva splošna raven dohodkov v Republiki Sloveniji ter njihov ekonomski položaj. Prav tako je treba upoštevati pri tem odločanju za vse obdelovalce ali upravljavce ali gre za ponavljajoče kršitve ter pomen, ki bi ga za odvračanje teh kršitev imela višine globe. (3) Nadzorni organ odloča kot prekrškovni organ tudi o predpisanih prekrških po tem delu zakona in po določbah Splošne uredbe.

(4) Za prekrške po določbah Splošne uredbe in po določbah tega zakona sme nadzorni organ v hitrem postopku izreči globo tudi v znesku, ki je nižji ali višji od najnižje predpisane globe.

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

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

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

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

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

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

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

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

127. člen

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

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

1. krši temeljna načela za obdelavo, vključno s pogoji za privolitev, kot so določena v 5., 6., 7. in 9. členu Splošne uredbe;

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

3. krši določbe v zvezi s prenosi osebnih podatkov uporabniku v tretji državi ali mednarodni organizaciji, kot so določene v 44. do 49. členu Splošne uredbe;

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

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

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

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

128. člen

(kršitve I. dela tega zakona)

(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 uniči, spremeni ali odsvoji zahtevane osebne podatke v nasprotju s četrtim odstavkom 17. člena tega zakona,

2. če ne uvede ukrepov za zagotavljanje sledljivosti obdelave osebnih podatkov v nasprotju s 7. točko drugega odstavka 26. člena tega zakona,

3. če ne določi odgovornih oseb v nasprotju s četrtim odstavkom 26. člena tega zakona,

4. če ne uvede ukrepov sledljivosti posredovanja osebnih podatkov v nasprotju s šestim odstavkom 30. člena tega zakona.

(2) Z globo od 2.000 do 4.000 eurov se kaznuje za prekršek iz prejšnjega odstavka odgovorna oseba pravne osebe, samostojnega podjetnika posameznika ali posameznika, ki samostojno opravlja dejavnost.

(3) Z globo od 600 do 2.000 eurov se kaznuje za prekršek iz prvega odstavka tega člena posameznik.

129. člen

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

(1) Z globo od 4.000 do 12.000 eurov se kaznuje za prekršek pravna oseba, samostojni podjetnik posameznik ali posameznik, ki samostojno opravlja dejavnost, če kot upravljavec ali obdelovalec nezakonito razkrije ali nezakonito omogoči dostop do osebnih podatkov v zvezi s svobodo izražanja (četrti odstavek 103. člena tega zakona).

(2) Z globo od 1.000 do 8.000 eurov se kaznuje za prekršek iz prejšnjega odstavka odgovorna oseba pravne osebe, samostojnega podjetnika posameznika ali posameznika, ki samostojno opravlja dejavnost ter odgovorna oseba v državnem organu ali v samoupravni lokalni skupnosti.

(3) Z globo od 1.000 do 4.000 eurov se kaznuje za prekršek iz prvega odstavka posameznik.

130. člen

(kršitve določb o uporabi povezovalnega znaka in avtomatiziranem odločanju)

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

če uporablja povezovalni znak v nasprotju s prvim ali drugim ali tretjim odstavkom 32. člena tega zakona,

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

131. člen

(kršitve iz II. dela tega zakona)

(1) Z globo od 1.000 do 8.000 eurov se kaznuje za prekršek odgovorna oseba državnega organa ali odgovorne osebe organa samoupravne lokalne skupnosti ali odgovorne osebe pravne osebe, če:

1. obdeluje osebne podatke za namen iz 66. člena tega zakona, ne da bi za to imela podlago v zakonu (73. člen), pa ne gre za primer, ko je obdelava nujno potrebna za varovanje življenja in telesa;

2. obdeluje osebne podatke, ki so bili pridobljeni za namen iz 66. člena tega zakona, za drug namen kot je to določeno v 66. členu, pa pri tem krši splošna pravila o varstvu osebnih podatkov (67. člen) oziroma za takšno obdelavo za dodatni namen nima podlage v drugem zakonu (75. člen);

3. prenese, posreduje ali pošlje v čezmejno obdelavo osebne podatke, ki so bili pridobljeni za namen iz 66. člena tega zakona, ne da bi bilo to izrecno določeno v zakonu, nujno potrebno za dosego namena prenosa, posredovanja ali čezmejne obdelave, ali če uporabnik prejetih, posredovanih ali

poslanih osebnih podatkov ni bil zakonito pooblaščen za obdelavo teh podatkov (drugi in tretji odstavek 95. člena);

4. osebne podatke, ki temeljijo zlasti na osebni oceni, ne označi kot takšnih, pa zaradi tega posamezniku, na katerega se nanašajo ti osebni podatki, nastane večja premoženjska škoda (drugi odstavek 71. člena tega zakona);

5. če v največji možni meri in še zlasti, če bi bilo to mogoče zagotoviti s pregledovanjem več lastnih evidenc, ne izvede potrebnih ukrepov za zagotovitev točnosti, popolnosti, podrobljenosti oziroma zanesljivosti podatkov, pa zaradi tega posamezniku, na katerega se nanašajo ti osebni podatki, nastane večja premoženjska škoda, nepremoženjska škoda ali fizična škoda (prvi odstavek 90. člena tega zakona);

6. ne vodi dnevnikov o posameznih dejanjih obdelave na način, da bi bilo mogoče ugotoviti utemeljitev, datum in čas, ter identifikacijo oseb, ki so razkrile določene osebne podatke, pa zaradi tega ni mogoče ugotoviti, katera oseba je izvedla nezakonito razkritje osebnih podatkov, zaradi katerega je posamezniku, na katerega se ti podatki nanašajo, nastala večja premoženjska škoda (78. člen tega zakona);

7. sprejme odločitev, ki temelji izključno na avtomatizirani obdelavi osebnih podatkov in ima lahko negativni pravni učinek na posameznika ali ga lahko bistveno prizadane ne da bi za to imel zakonsko podlago ali brez da bi izvajal naknadno preverjanje rezultatov avtomatizirane obdelave in drugih ukrepov zagotavljanja človekovih pravic in temeljnih svoboščin (prvi odstavek 77. člena) oziroma z ali brez zakonske podlage na isti način obdeluje posebne vrste osebnih podatkov brez uporabe ustreznih zaščitnih ukrepov (drugi odstavek 77. člena tega zakona);

8. krši pravice posameznika, na katerega se nanašajo osebni podatki, kot so določene v 88. do 91. členu tega zakona;

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

132. člen

(kršitev določb o neposrednem trženju)

(1) Z globo od 2.000 do 12.000 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 v nasprotju s 106. ali 107. členom tega zakona.

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

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

133. člen

(kršitev splošnih določb o videonadzoru)

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

1. se izvaja videonadzor brez pisne odločitve po prvem odstavku 108. člena tega zakona;

2. ne objavi obvestila na način iz drugega odstavka 108. člena tega zakona;

3. obvestilo ne vsebuje informacij iz tretjega odstavka 108. člena tega zakona;

4. ne zavaruje videonadzornega sistema, s katerim izvaja videonadzor, na način iz šestega odstavka 108. člena tega zakona.

(2) Z globo od 1.000 do 2.000 eurov se kaznuje za prekršek iz prejšnjega odstavka odgovorna oseba pravne osebe, samostojnega podjetnika posameznika ali posameznika, ki samostojno opravlja dejavnost, državnega organa ali organa samoupravne lokalne skupnosti.

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

(4) Z globo od 6.000 do 20.000 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 108. člena tega zakona.

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

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

134. člen

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

(1) Z globo od 4.000 do 12.000 eurov se kaznuje za prekršek pravna oseba:

1. če izvaja videonadzor brez pravne podlage ali obdeluje posnetke v nasprotju z namenom iz prvega odstavka 109. 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 109. člena);

3. če pisno ne obvesti zaposlenih (tretji odstavek 109. člena).

(2) Z globo od 2.000 do 6.000 eurov se kaznuje za prekršek iz prejšnjega odstavka samostojni podjetnik posameznik ali posameznik, ki samostojno opravlja dejavnost

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

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

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

135. člen

(kršitev določb o videonadzoru pri večstanovanjskih stavbah)

(1) Z globo od 2.000 do 8.000 eurov se kaznuje za prekršek pravna oseba, samostojni podjetnik posameznik ali posameznik, ki samostojno opravlja dejavnost, ki izvaja videonadzor ali obdeluje posnetke v nasprotju z namenom iz prvega odstavka 110. člena tega zakona.

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

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

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

136. člen

(kršitev določb o videonadzoru znotraj delovnih prostorov)

(1) Z globo od 4.000 do 12.000 eurov se kaznuje za prekršek pravna oseba, samostojni podjetnik posameznik ali posameznik, ki samostojno opravlja dejavnost, ki izvaja videonadzor v delovnih prostorih ali obdeluje posnetke v nasprotju z namenom iz prvega in drugega odstavka 111. člena tega zakona.

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

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

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

137. člen

(kršitev določb o videonadzoru na javnih površinah)

(1) Z globo od 4.000 do 12.000 eurov se kaznuje za prekršek pravna oseba, samostojni podjetnik posameznik ali posameznik, ki samostojno opravlja dejavnost, ki izvaja videonadzor na javnih površinah v nasprotju s 112. členom tega zakona.

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

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

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

138. člen

(kršitev določb o biometriji v javnem sektorju)

(1) Z globo od 1.200 do 2.000 eurov se kaznuje za prekršek odgovorna oseba pravne osebe javnega sektorja, ki izvaja biometrične ukrepe v nasprotju s 113. členom tega zakona.

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

139. člen

(kršitev določb o biometriji v zasebnem sektorju)

(1) Z globo od 4.000 do 12.000 eurov se kaznuje za prekršek pravna oseba, samostojni podjetnik posameznik ali posameznik, ki samostojno opravlja dejavnost, ki izvaja biometrične ukrepe v nasprotju s 114. členom tega zakona.

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

140. člen

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

(1) Z globo od 8.000 do 20.000 eurov se kaznuje za prekršek pravna oseba, samostojni podjetnik posameznik ali posameznik, ki samostojno opravlja dejavnost, ki izvaja biometrične ukrepe v nasprotju s 115. členom tega zakona.

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

141. člen

(kršitev določb o evidentiranju vstopov in izstopov)

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

1. ki uporablja evidenco vstopov in izstopov kot uradno evidenco v nasprotju s tretjim odstavkom 116. člena tega zakona;

2. ki ravna v nasprotju s četrtim odstavkom 116. člena tega zakona.

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

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

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

142. člen

(kršitev določb o javnih knjigah)

(1) Z globo od 2.000 do 4.000 eurov se kaznuje za prekršek pravna oseba, samostojni podjetnik posameznik ali posameznik, ki samostojno opravlja dejavnost, ki uporablja osebne podatke v nasprotju z zakonskim namenom iz 117. člena tega zakona.

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

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

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

143. 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 izvede povezovanje uradnih evidenc ali javnih knjig v nasprotju s prvim in drugim odstavkom 118. člena tega zakona.

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

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

144. člen

(kršitev določb o strokovnem nadzoru)

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

1. izvaja strokovni nadzor v nasprotju z drugim odstavkom 120. člena tega zakona;

2. ne naredi uradnega zaznamka ali drugega uradnega zapisa iz 122. člena tega zakona.

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

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

V. DEL
PREHODNE IN KONČNE DOLOČBE

145. člen

(prehodne določbe glede pooblaščenih oseb)

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

(2) Ne glede na določbe prejšnjega odstavka samoupravne lokalne skupnosti in javni vzgojno-izobraževalni zavodi v devetih mesecih od uveljavitve tega zakona določijo pooblaščene osebe. Do poteka tega obdobja lahko njihove naloge zagotavljanja skladnosti obdelave osebnih podatkov po tem zakonu opravljajo druge osebe iz občinske uprave oziroma zavoda, ki so pristojne za izvajanje notranjih nadzorov ali revizij ali podobnih delovanj.

(3) Ne glede na pogoja izobrazbe iz 3. točke in vsebine in trajanja delovnih izkušenj iz 4. točke prvega odstavka 36. člena tega zakona se do 25. maja 2021 za pooblaščeno osebo lahko določi osebo, ki ima najmanj eno leto delovnih izkušenj s primerljivih področij informacijske varnosti, varstva poslovne skrivnosti po zakonu, ki ureja gospodarske družbe, ali varstva zaupnih podatkov po zakonu, ki ureja bančništvo.

146. člen

(prehodne določbe glede delovanja nadzornega organa)

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

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

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

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

147. člen

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

(1) Za izvrševanje šestega odstavka 28. člena tega zakona upravljavci ali obdelovalci, ki za izvajanje svojega delovanja pridobivajo osebne podatke iz registrov ali evidenc s področja upravnih notranjih zadev, v dveh letih od uveljavitve tega zakona vzpostavijo ustrezne varnostne mehanizme.

(2) Povezovanja uradnih evidenc in javnih knjig se uskladijo s 118. členom tega zakona v štirih letih od uveljavitve tega zakona.

148. člen

(prehodne določbe glede certificiranja)

Slovenska akreditacija začne izvajati postopke akreditacije 1. januarja 2022.

149. člen

(upoštevanje obvestil o določitvi pooblaščenih oseb)

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

150. člen

(podzakonski predpis iz 52. člena tega zakona)

Do izdaje novega Pravilnika o službeni izkaznici državnega nadzornika za varstvo osebnih podatkov se uporablja dosedanji Pravilnik o službeni izkaznici državnega nadzornika za varstvo osebnih podatkov (Uradni list RS, št. 35/13) ter službene izkaznice, izdane na njegovi podlagi ter službene izkaznice, ki bodo izdane na njegovi podlagi po uveljavitvi tega zakona.

151. člen

(razveljavitev in uporaba podzakonskih predpisov)

(1) Z dnem uveljavitve tega zakona prenehajo veljati:

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

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

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

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

(2) Predpis iz četrte alineje prejšnjega odstavka pa se uporablja do uveljavitve predpisa iz četrtega odstavka 21. člena tega zakona, kolikor ni v nasprotju s tem zakonom.

152. člen

(izdaja aktov)

Minister izda akte iz četrtega odstavka 21. člena tega zakona v treh mesecih od uveljavitve tega zakona.

153. člen

(prenehanje veljavnosti zakona)

Z dnem uveljavitve tega zakona preneha veljati Zakon o varstvu osebnih podatkov (Uradni list RS, št. 86/04, 113/05 – ZInfP, 51/07 – ZUstS-A, 67/07, 94/07 – uradno prečiščeno besedilo in UL L št. 119 z dne 4. 5. 2016, str. 1 in UL L št. 127 z dne 23. 5. 2018, str. 2 – popr.).

154. člen

(končna določba)

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

III. OBRAZLOŽITEV ČLENOV

Besedilo Predloga ZVOP-2 že ustrezno upošteva popravke v besedilu določb slovenskih inačic Splošne uredbe in Direktive, kot so bile objavljene v Uradnem listu Evropske unije (pretežno privolitev in varnost osebnih podatkov).

K I. delu predloga zakona: TEMELJNE DOLOČBE

K 1. poglavju – Splošne določbe

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

K 1. členu:

Prvi odstavek predlaganega člena navaja, da je vsebina zakona najprej določanje pravic, obveznosti, upravičenj, načel, postopkov in ukrepov, s katerimi se preprečujejo neustavni, nezakoniti ali neupravičeni posegi v zasebnost oziroma dostojanstvo oziroma druge temeljne pravice posameznika oziroma posameznice pri obdelavi osebnih podatkov, tako da se varuje ali uresničuje pravico do varstva osebnih podatkov iz 2. člena predloga zakona. Gre torej za nadaljevanje sistemskega pristopa regulacije v smeri priznavanja in spoštovanja osebne človekove pravice, kot je le-ta nadalje opredeljena v 2. členu predloga zakona. Na ta način je v določbi podana povezava oziroma interpretacija, da zakon predstavlja načine uresničevanja oziroma varstva pravic iz 38. (varstvo osebnih podatkov), 35. (varstvo pravic zasebnosti in osebnostnih pravic) in 34. (pravica do osebnega dostojanstva in varnosti) člena Ustave Republike Slovenije.

V drugem odstavku predlaganega člena je določeno, da se s tem zakonom (glede na zahtevo zakonskega urejanja iz drugega odstavka 38. člena[34] in 87. člena Ustave Republike Slovenije) v pravnem redu Republike Slovenije zagotavlja izvajanje določb Uredbe (EU) 2016/679 Evropskega parlamenta in Sveta z dne 27. aprila 2016 o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem pretoku takih podatkov ter o razveljavitvi Direktive 95/46/ES (Splošna uredba o varstvu podatkov) ter prenašajo določbe Direktive (EU) 2016/680 Evropskega parlamenta in Sveta z dne 27. aprila 2016 o varstvu posameznikov pri obdelavi osebnih podatkov, ki jih pristojni organi obdelujejo za namene preprečevanja, preiskovanja, odkrivanja ali pregona kaznivih dejanj ali izvrševanja kazenskih sankcij, in o prostem pretoku takih podatkov ter o razveljavitvi Okvirnega sklepa Sveta 2008/977/PNZ – vključno z navedbami Uradnih listov Evropske unije, kjer so objavljeni popravki njunih inačic v slovenskem jeziku. Določbe navedene Direktive se izvršuje z zakonom, delno podobno velja glede določb Splošne uredbe, ki se lahko izvršijo ali morajo izvršiti z zakonom Republike Slovenije. Glede obeh pravnih aktov Evropske unije je tudi okvirno zapisana njuna vsebina v določbi drugega odstavka.

K 2. členu:

Predlagani 2. člen v prvem odstavku določa bistvo človekove pravice do varstva osebnih podatkov. Pravico oziroma skupek pravic s področja podatkovne zasebnosti iz 38. člena Ustave Republike Slovenije (varstvo osebnih podatkov) določa kot človekovo pravico posameznika ali posameznice do varstva njegovih ali njenih osebnih podatkov. Pri tem določba izhaja iz ti. »subjektivnega pristopa« in ne iz pristopa regulacije (zakonske oziroma upravne obveznosti), v središču te ene od najbolj bistvenih

[34] Za najnovejšo precedenčno (garantistično) odločbo Ustavnega sodišča RS glejte: Odločba US, št. U-I-152/17, 4. 7. 2019; objava: Uradni list RS, št. 46/19.

pravic je namreč človek. To izhaja tudi iz prvega dela določbe, po kateri se posameznikom zagotavljajo zasebnost (38. in 35. člen Ustave Republike Slovenije) oziroma (torej: in/ali) dostojanstvo (34. člen Ustave Republike Slovenije) ob upoštevanju podatkovne samoodločbe (38. člen Ustave Republike Slovenije). Izraz podatkovna zasebnost ni nov, gre samo za določeno posodobljenje izraza »informacijska zasebnost«[35].

V primeru omenjene podatkovne samoodločbe[36] (ki dodatno kaže, da gre za človekovo posebej poudarjeno osebno pravico razpolaganja svojimi osebnimi podatki) gre za to, da je (in ima) vsak posameznik »oblast« nad svojimi osebnimi podatki, da torej primarno sam odloča ali želi ali ne želi, da se njegove osebne podatke obdela, posreduje (npr. za izpolnitev pogodbe), izjeme pa so dopustne (ob spoštovanju strogega testa sorazmernosti), da se namreč določene podatke obdeluje proti njegovi volji – npr. če to določi zakon, ki prestane navedene pogoje presoje. Torej tudi ne gre za lastninski koncept zasebnosti, ampak za strogo osebni koncept zasebnosti.

Predlagani drugi odstavek določa, da se v okviru človekove pravice po prvem odstavku zagotavlja, da ima vsaka posameznica ali posameznik upravičenje, da se z zakonom ter pošteno in na pregleden način ureja in zagotavlja obdelava njenih ali njegovih osebnih podatkov, tajnost njenih ali njegovih osebnih podatkov, ter njene ali njegove pravice do seznanitve z lastnimi osebnimi podatki, do popravka lastnih podatkov oziroma do uresničevanja drugih pravic iz tega ali drugega zakona. Podlaga za del določbe o tajnosti osebnih podatkov je v drugem odstavku 38. člena Ustave Republike Slovenije, po katerem »varstvo tajnosti osebnih podatkov določa zakon«, kar je v letu 2019 posebej izpostavila tudi nova ustavnosodna presoja Ustavnega sodišča Republike Slovenije[37].

Predlagani drugi odstavek 2. člena 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)[38]. Z navedenim zakonom namreč ni bil izveden poseg v 1. člen veljavnega zakona, ki temeljno ureja človekovo pravico od varstva osebnih podatkov – zaradi neobstoja dvotretjinske ustavne večine za revizijo, kar pomeni, da je tudi Avstrija zadržala dosedanjo širšo opredelitev varstva osebnih podatkov kot temeljne in osebne človekove pravice (na ustavni ravni).

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

2. člen ima pomen za razlago vseh določb tega predloga zakona, področne zakonodaje glede varstva osebnih podatkov ter za uporabo določb Splošne uredbe, tako da mora osredotočeni naslovnik pravic biti posameznik, na katerega se nanašajo osebni podatki (subjekt varstva pravice do tajnosti osebnih podatkov).

Glede na dosedanji 1. člen ZVOP-1 novi 2. člen ZVOP-2 torej vsebuje posodobljene formulacije, s posebnim pomenom za interpretacijo ZVOP-2, kot je opisan zgoraj.

K 3. členu:

Predlagani 3. člen ureja prepoved nedopustne diskriminacije glede varstva osebnih podatkov – natančneje: prepoved nedopustne diskriminacije, kadar se izvaja obdelava osebnih podatkov. Pri tem je pomembna povezava z 2. členom, da gre za človekovo pravico, da je osredotočeni naslovnik pravic posameznik, na katerega se nanašajo osebni podatki ter glede razlagalne »moči« glede drugih zakonov ipd.. V 3. členu so glede na 14. člen Ustave Republike Slovenije ter glede na druge ustaljene formulacije pravnega reda Republike Slovenije (npr. prvi odstavek 131. člena Kazenskega zakonika[39] ter prvi odstavek 1. člena Zakona o varstvu pred diskriminacijo[40]) navedene prepovedane okoliščine

[35] Odločba US, št. U-I-92/01, 28. 2. 2002, 27. točka odločbe; objava: Uradni list RS, št. 22/02 in OdlUS XI, 25.
[36] Odločba US, št. U-I-98/11, 26. 9. 2012, opomba št. 2; objava: Uradni list RS, št. 79/12.
[37] Glejte: Odločba US, št. U-I-152/17, 4. 7. 2019, zlasti 20. točka in opomba št. 10; objava: Uradni list RS, št. 46/19.
[38] Objava: Bundesgesetzblatt I Nr. 120/2017, Teil I.
[39] Uradni list RS, št. 50/12 – uradno prečiščeno besedilo, 6/16 – popr., 54/15, 38/16 in 27/17.
[40] Uradni list RS, št. 33/16.

diskriminacije. Določbe so nekoliko posodobljene – dodana je spolna identiteta po prvem odstavku 1. člena Zakona o varstvu pred diskriminacijo, dodana je genska (ne genetska) predispozicija, beseda »barva« iz dosedanjega 4. člena ZVOP-1 je spremenjena v »barvo kože«, omenjeno je tudi zdravstveno stanje.

Predlagani člen pomeni, da se nikogar ne sme nedopustno diskriminirati glede varstva osebnih podatkov, kar med drugim vključuje tudi prebivališče. Natančneje – med prepovedanimi kriteriji diskriminacije (razlikovanja) sta v praksi zlasti najbolj pomembna kriterija državljanstva in prebivališča, tudi glede na 1. člen Konvencije o varstvu posameznikov glede na avtomatsko obdelavo osebnih podatkov[41] (Sveta Evrope), ki se v tem delu v okviru reforme varstva osebnih podatkov v okviru Sveta Evrope ne spreminja.

Predlagani člen pa dopušča pod zakonsko določenimi pogoji možnost izvajanja profiliranja glede obdelave osebnih podatkov, avtomatiziranega odločanja pod zakonsko določenimi pogoji in jamstvi (npr. pravica do ugovora).

K 4. členu:

V navedenem členu je določena materialna veljava tega zakona, tj. za katere obdelave velja in za katere ne velja.

V prvem odstavku je tako določeno (glede na prvi odstavek člena 2 Splošne uredbe), da določbe ZVOP-2 veljajo za popolnoma ali delno avtomatizirano obdelavo osebnih podatkov ter za drugačne obdelave (ti. ročne ozir. papirnate obdelave) osebnih podatkov, ki so vključeni ali so namenjeni vključitvi v zbirko osebnih podatkov.

V drugem odstavku je določena splošna izjema od veljave zakona, namreč obdelava osebnih podatkov za domače potrebe, kar vključuje zlasti obdelave osebnih podatkov, ki jih izvajajo posamezniki izključno za osebno uporabo, družinsko življenje. Pri uporabi tega člena je treba biti pazljiv v dve smeri – sicer široko tolmačiti domače potrebe, vendar v okviru besede »izključno« - da ne pride do kombinacije med domačo potrebo (uporabo) in poslovnim namenom. V trenutno vodilni literaturi s področja razlage Splošne uredbe je npr. podana takšna razlaga:

»Najbolj pomembna izjema z vidika ekonomičnosti je določena v c. točki, po kateri se »uredba ne uporablja za obdelavo osebnih podatkov s strani fizične osebe v okviru *izključno osebne ali domače dejavnosti*«. Ta koncept se mora razlagati na podlagi splošnega družbenega mnenja in vključuje osebne podatke, ki se obdelujejo za prostočasovne aktivnosti, hobije, počitnice ali aktivnosti zabave, za uporabo družbenih omrežij ali podatkov, ki so del osebne zbirke naslovov, rojstnih dnevov ali drugih podobnih datumov, kot so obletnice.

Pomembno je, da v primerih, kadar obdelava zadeva tako zasebne kot poslovne informacije, se izjema ne uporabi. Beseda »izključno« nakazuje na *ozko interpretacijo* te določbe in poslovna aktivnost bi morala vključevati kakršnokoli aktivnost ne glede na to, ali je odplačna, kot tudi pripravljalna delovanja za njo, kot so npr. ukrepi trženja ali trgovanje z osebnimi podatki za to, da se dobi storitev.«[42]

V tretjem odstavku je določeno, da če II. del tega zakona ne določa drugače, določbe tega dela zakona veljajo tudi na področjih preprečevanja, preiskovanja, odkrivanja ali pregona kaznivih dejanj ali izvrševanja kazenskih sankcij ter varnosti države in obrambe države (področje izvrševanja določb »Direktive (EU) 2016/680 Evropskega parlamenta in Sveta z dne 27. aprila 2016 o varstvu posameznikov pri obdelavi osebnih podatkov, ki jih pristojni organi obdelujejo za namene preprečevanja, preiskovanja, odkrivanja ali pregona kaznivih dejanj ali izvrševanja kazenskih sankcij, in o prostem pretoku takih podatkov ter o razveljavitvi Okvirnega sklepa Sveta 2008/977/PNZ«). Navedena določba je povezana z določbami 67. člena predloga zakona glede veljavnosti prejšnjih delov predloga zakona za določbe iz II. dela predloga zakona.

[41] Uradni list RS, št. 11/94 – Mednarodne pogodbe, št. 3/94 in 86/04 – ZVOP-1.
[42] 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.

K 5. členu:

5. člen je eden od najpomembnejših členov predloga zakona, glede na to, da preko določanja jurisdikcije pravnega reda Republike Slovenije (prvi in drugi odstavek), njenega nadzornega organa (Informacijski pooblaščenec) ter posredno tudi (jurisdikcije) sodnega varstva pred sodišči Republike Slovenije določa raven varstva pravic posameznikov glede njihovih osebnih podatkov.

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 z njenim 3. členom tako velja za tiste obdelave, ki jih izvajajo upravljavci in obdelovalci iz Evropske unije, ter v določenem delu tudi obdelave tujih upravljavcev in obdelovalcev, če imajo ti namen obdelovati osebne podatke prebivalcev Evropske unije. Predlog zakona svojo veljavnost določa v teh okvirih.

Prvenstveno ta zakon v skladu s prvim odstavkom predlaganega člena tako kot dosedaj velja za tiste obdelave osebnih podatkov, ki potekajo v okviru opravljanja dejavnosti upravljavca ali obdelovalca, ki ima sedež, hčerinsko družbo, podružnico ali drugačno poslovno enoto na ozemlju Republike Slovenije, in to ne glede na to, ali sama dejanja obdelave dejansko potekajo na ozemlju Republike Slovenije ali ne[43].

Gre za že obstoječe kriterije iz (a) točke prvega odstavka člena 4 Direktive o varstvu osebnih podatkov oziroma prvega odstavka 5. člena dosedanjega ZVOP-1. Pri tem pri ugotavljanju, ali se neka obdelava izvaja v okviru dejavnosti določene poslovne enote, v skladu z sodno prakso Sodišča Evropske unije[44] ni nujno, da ta poslovna enota tudi dejansko izvaja zadevno obdelavo (tj. zlasti, da je namesto nje ne opravlja druga, z njo lastniško ali drugače povezana poslovna enota), ampak zadostuje že, da so dejavnosti poslovne enote na bistven način povezane z obdelavo. Pri ugotavljanju tega, ali se določen subjekt šteje za takšnega, ki ima sedež, hčerinsko družbo, podružnico ali drugačno poslovno enoto na ozemlju Republike Slovenije, pa prav tako ni nujno, da je ta subjekt vpisan v poslovni register Republike Slovenije in organiziran v obliki katere od ustaljenih organizacijskih oblik (npr. s.p., d.o.o., d.d., o.p., idr. – za te je veljava tega zakona nesporna), ampak štejejo tudi drugi subjekti, vključno s fizičnimi osebami, ki dejavnosti obdelave izvajajo dejansko in učinkovito ter prek ustaljenih ustanovitev[45], oziroma ki na ozemlju Republike Slovenije opravljajo dejansko in resnično, čeprav majhno, dejavnost, v okviru katere se izvaja ta obdelava[46].

Upravljavci in obdelovalci, ki so del javnega sektorja Republike Slovenije, so vključeni že po samem zakonu, brez potrebe po ugotavljanju njihovega sedeža. S tem so vključena tudi veleposlaništva, konzulati, stalna predstavništva in druge misije, za katere se slovensko pravo uporablja na podlagi mednarodnega prava (tretji odstavek 3. člena Splošne uredbe oziroma dosedaj tudi četrti odstavek 5. člena ZVOP-1).

Pravila za razmejevanje veljave zakonov posameznih držav članic so sicer podrobneje pojasnjena v mnenju Delovne skupine po členu 29 Direktive 95/46/ES št. 8/2010 o pravu, ki se uporablja[47] , upoštevaje okoliščino, da se kriterij opreme za obdelavo ((c) točka prvega odstavka člena 4 Direktive oziroma drugi odstavek 5. člena ZVOP-1) z začetkom uporabe Splošne uredbe več ne uporablja.

Dodatno predlog tega zakona v drugem odstavku tega člena določa, da ta zakon velja tudi za obdelavo osebnih podatkov, ki se izvaja v okviru dejavnosti sedeža, podružnice ali drugačne poslovne enote obdelovalca, ki je ustanovljen ali registriran v Republiki Sloveniji in opravlja dejavnosti obdelave za upravljavca, ki je ustanovljen ali registriran v drugi državi članici Evropske unije, če se te dejavnosti obdelave izvajajo v Republiki Sloveniji. Rešitev je predlagana po vzorcu tretjega odstavka 4. člena Zakona o varstvu fizičnih oseb glede obdelave osebnih podatkov Kraljevine Belgije iz leta 2018.

[43] Uvodna navedba št. 22 Splošne uredbe.
[44] Sodba Sodišča EU v zadevi C-131/12, tč. 52, 56 in 67.
[45] Uvodna navedba št. 22 Splošne uredbe.
[46] 1. točka izreka sodbe Sodišča Evropske unije v zadevi C-230/14 z dne 1. 10. 2015, *Weltimmo s. r. o. proti Nemzeti Adatvédelmi és Információszabadság Hatóság*.
[47] http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2010/wp179_en.pdf

Tretji odstavek določa, da predlog zakona velja tudi za obdelave osebnih podatkov prebivalcev Republike Slovenije, ki potekajo v okviru upravljavca s sedežem zunaj Evropske unije (izvaja jih upravljavec iz tretje države), vendar se ponujajo uporabnikom iz Republike Slovenije, oziroma zadevajo profiliranje slovenskih uporabnikov. Navedena določba temelji na drugem odstavku člena 3 Splošne uredbe in cilja na to, da prebivalci Republike Slovenije ne bi bili prikrajšani za varstvo svojih osebnih podatkov samo zato, ker upravljavec ali obdelovalec osebnih podatkov nista ustanovljena znotraj Evropske unije[48] (in torej za nadzor nad njim ni že tako v skladu s prvim odstavkom člena 3 Splošne uredbe pristojen kateri od državnih nadzornih organov držav članic Evropske unije). Pri tem pa sama dostopnost spletne strani upravljavca, obdelovalca ali njunega posrednika za prebivalce Republike Slovenije še ne zadostuje za vzpostavitev veljave zakona; za to mora biti izkazano, da namerava upravljavec oziroma obdelovalec tudi dejansko nuditi storitve posameznikom iz Republike Slovenije, še zlasti tako, da pri tem uporablja slovenski jezik[49] oziroma da namerava slediti obnašanju prebivalcev Republike Slovenije na internetu, še zlasti tako, da oblikuje profile njihovega obnašanja, oziroma drugače zbira podatke o tem z namenom sprejemanja odločitev o njem oziroma za analiziranje ali predvidevanje njegovega osebnega okusa in vedenja[50]. V takšnih primerih bo Informacijski pooblaščenec pristojen za nadzor skladnosti obdelave tujega upravljavca ozir. obdelovalca s tem zakonom, ter za obravnavo pritožb posameznikov v zvezi s tem.

K 6. členu:

V 6. členu je v prvem odstavku najprej določeno, da za varstvo osebnih podatkov veljajo bistveni izrazi (»pojmi« po Splošni uredbi), torej definicije privolitve, obdelave osebnih podatkov, zbirke ipd.

V drugem odstavku so določeni bistveni izrazi, ki veljajo tako za I. del (uredbeni del) kot II. del in ostale dele predloga zakona, npr. nadzorni organ, zakon, varnost države, kazenske evidence, javni in zasebni sektor. Gre za izraze, katere se lahko glede na specifičnosti pravnega reda Republike 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.

Izraz »zakon« pomeni glede na člen 6 Splošne uredbe, člen 4 Direktive ter za izvrševanje a) in b) točke 5. člena Konvencije o varstvu posameznikov glede na avtomatsko obdelavo osebnih podatkov (Sveta Evrope) - ta zakon, druge zakone Republike Slovenije, obvezujoče (in torej ratificirane) mednarodne pogodbe, ki zavezujejo Republiko Slovenijo ter pravne akte ali odločitve Evropske unije, katerih določbe so enakovredne zakonom in neposredno uporabljive ali neposredno učinkovite (glede na določbe tretjega odstavek 3.a člena Ustave Republike Slovenije), v to definicijo pa niso vključeni podzakonski predpisi (ker ne smejo biti vključeni glede na drugi odstavek 38. člena Ustave Republike Slovenije – glede na tam navedeno določbo o »zakonu« ter z njim povezano ustaljeno ustavnosodno presojo Ustavnega sodišča Republike Slovenije od leta 1992 dalje[51] ter glede na določbe 87. in 153. člena Ustave Republike Slovenije). Predlagana določba upošteva tudi najnovejšo precedenčno odločbo Ustavnega sodišča Republike Slovenije[52], ki je okrepila pomen podrobne zakonske podlage za vse obdelave osebnih podatkov (kot je to bilo to razvito v ustavnosodni presoji Ustavnega sodišča Republike Slovenije že od leta 1992 dalje).

Definicija »varnosti države« je pomembna za uporabo določb o varnosti države v ZVOP-2 ter določb področnih zakonov glede varnosti države, kadar določajo obdelavo osebnih podatkov: gre le za del področja ti. notranje varnosti, ki torej po tej definiciji ne vključuje javne varnosti, temveč klasično varnost države (obveščevalno in protiobveščevalno delovanje).

K 7. členu:

V predlaganem 7. členu so določena temeljna načela za zakonito obdelavo osebnih podatkov (pravne podlage), ki zlasti sledijo določbam prvega odstavka 6. člena Splošne uredbe, delno pa tudi sledijo

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

smerem iz dosedanjega 9. in 10. člena ZVOP-1. Bistvena razlika je, da so sedaj pravne podlage za obdelave osebnih podatkov v javnem in v zasebnem sektorju urejene v skupnem členu, s tem da je najprej poudarjena prva pravna podlaga – namreč prvi odstavek 6. člena Splošne uredbe.

Tako prvi odstavek 7. člena določa, da se osebne podatke lahko obdeluje le, če to omogočajo pravne podlage iz 6. člena Splošne uredbe. Konkretno pravne podlage zlasti iz prvega odstavka 6. člena Splošne uredbe, delno pa tudi drugega in tretjega odstavka 6. člena (urejanje obdelav osebnih podatkov s področnimi zakoni). Besedilo »le, če to omogočajo« upošteva določbo drugega odstavka 38. člena Ustave Republike Slovenije o varstvu tajnosti osebnih podatkov.

Predlagani drugi 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) ter ob upoštevanju (c) in (e) točk prvega pododstavka prvega odstavka člena 6 Splošne uredbe. Upošteva tudi merila iz drugega odstavka člena 6 Splošne uredbe ter drugega dela tretjega odstavka člena 6 Splošne uredbe.

Predlagani tretji odstavek določa posebne določbe glede možnosti uporabe privolitve v javnem sektorju (za oblastne naloge in pristojnosti). Najprej je določeno, da mora to možnost določati zakon, v drugih primerih poslovanja javnega sektorja, ko gre za neoblastno poslovanje, pa zadostuje podlaga iz tega tretjega odstavka. Za razliko od dosedanjega drugega odstavka 9. člena ZVOP-1 je sedaj določeno, da lahko ne samo nosilci javnih pooblastil, ampak izrecno celotni javni sektor obdelujejo osebne podatke tudi na podlagi privolitve[53], ki pa mora biti določena v zakonu (npr. narodnost, verska pripadnost – 61. člen ter prvi in drugi odstavek 41. člena Ustave Republike Slovenije). Če pa take možnosti ne določa zakon, pa lahko javni sektor obdeluje osebne podatke na podlagi privolitve le, če ne gre za izvrševanje zakonskih (dejansko: oblastvenih[54]) nalog ali pristojnosti javnega sektorja v smislu odločanja o človekovih pravicah ali temeljnih svoboščinah ali obveznostih, v okviru posameznikove podatkovne samoodločbe, da pač razkrije svoje osebne podatke določenemu krogu ljudi v določenemu subjektu javnega prava ozir. le temu subjektu javnega prava. To prostovoljno razkritje zahteva, da se poda privolitev.

Predlagani četrti odstavek pomeni izvedbo (f) točke prvega odstavka člena 6 Splošne uredbe. Po njej se izjemoma, lahko obdelujejo neposredno na tej pravni podlagi, določeni v tem zakonu, osebni podatki, kadar je to nujno za izvrševanje drugih nalog javnega sektorja, drugi osebni podatki, ki niso določeni v zakonu – in se z obdelavo ne poseže v upravičen interes posameznika, na katerega se osebni podatki nanašajo, kar vključuje človekove pravice in temeljne svoboščine ter če pri tem ne gre za izvajanje zakonskih pristojnosti, nalog ali obveznosti javnega sektorja. Primer je npr. kontaktiranje posameznika preko telefona za izvedbo določene storitve javnega sektorja. Predlagana določba pa ne omogoča niti začasnega omogočanja določanja osebnih podatkov v podzakonskih predpisih (zlasti v pravilnikih), je kvečjemu – glede na njeno izjemnost možni »sprožilec«, da pristojno ministrstvo po izvedeni začasni konkretni obdelavi osebnih podatkov (če je to potrebno), pripravi spremembe ali dopolnitve ustreznega zakona, tako da je spoštovano pravilo iz drugega odstavka tega člena predloga zakona (ki temelji na drugem odstavku 38. člena Ustave Republike Slovenije v zvezi s 87. členom

[53] 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).«

[54] Za okvirno opredelitev neoblastvenih delovanj glejte smiselno: Sklep Upravnega oddelka Vrhovnega sodišča RS, opr. št. I Up 231/2016, 1. 2. 2017: »11. Delovanje Varuha niti z vidika splošne opredelitve njegovih nalog in pristojnosti niti z vidika ravnanja v konkretnem primeru očitno ne ustreza značilnostim oblastvenega delovanja. Njegovo ravnanje je usmerjeno v nadzor nad delovanjem nosilcev oblasti in se tudi izraža v ukrepih, ki so usmerjeni prav zoper navedene oblastvene subjekte in ne druge osebe, nosilce človekovih pravic in temeljnih svoboščin. Še več, tudi samo delovanje Varuha je tako po zakonski kot po konceptualni opredelitvi neoblastno in le omejeno formalizirano […].«

Ustave Republike Slovenije)[55]. Predlagana določba temelji tudi na (c) in (e) točki prvega pododstavka prvega odstavka člena 6 Splošne uredbe in je primerljiva dosedanji določbi četrtega odstavka 9. člena ZVOP-1, katere uporabo sicer sodna praksa slovenskih sodišč nekoliko omejuje[56]. Gre torej za nadgradnjo vsebine dosedanjega četrtega odstavka 9. člena ZVOP-1. Predlagane določbe drugega odstavka so splošne, sistemske narave (*lex generalis*), določena področna izvedba pa je vsebovana v 124. členu predloga zakona (obdelava osebnih podatkov za izvajanje določenih dejavnosti osebe javnega sektorja).

Predlagani peti odstavek določa, da se v javnem sektorju lahko obdelujejo osebni podatki, ki so potrebni za uresničevanje zakonitih interesov javnega sektorja, če pri tem ne gre za izvajanje zakonskih pristojnosti, nalog ali obveznosti javnega sektorja ter če nad temi interesi ne prevladajo človekove pravice in temeljne svoboščine ali interesi posameznika, na katerega se nanašajo osebni podatki. Gre za rešitev, ki je že obstajala v ZVOP-1 v četrtem odstavku 9. člena in ima pomen za določene mejne situacije, kjer pa je vedno predpogoj predhodna ocena upravljavca, ali bi določena dejanja obdelave osebnih podatkov lahko pomenila ali ne pomenila, da vseeno prevladajo človekove pravice (ne samo varstvo osebnih podatkov, lahko domneva nedolžnosti, pravice narodnih skupnosti ipd.).

Predlagani šesti odstavek podrobneje določa eno od pravnih podlag za obdelavo osebnih podatkov v zasebnem sektorju (ostale so določene v prvem odstavku 7. člena) – namreč obdelavo na podlagi področnih zakonov. Tako je določeno, da je treba v zakonu določiti namen obdelave osebnih podatkov in vrste osebnih podatkov, ki se obdelujejo, kategorije posameznikov, na katere se nanašajo osebni podatki, uporabnike osebnih podatkov oziroma namene, za katere se jim lahko posreduje osebne podatke, posamezna dejanja obdelave in postopke obdelave ter druge ukrepe za zagotovitev zakonite, poštene in pregledne obdelave.

Predlagani sedmi odstavek določa obdelavo osebnih podatkov v druge namene[57] kot pravilo za delovanje (odločanje) javnega in zasebnega sektorja glede možnosti obdelav osebnih podatkov v druge namene po četrtem odstavku člena 6 Splošne uredbe. Po predlagani določbi obdelava osebnih podatkov za drug namen kot za tistega, za katerega so bili zbrani, v javnem sektorju ni dopustna, razen če to določa ta **področni** zakon**.**

K 8. členu:

Predlagani 8. člen ureja pogoje za obdelavo osebnih podatkov otrok v primeru uporabe storitev informacijske družbe določa v skladu z 8. členom Splošne uredbe (po vzorcu iz Zakona o zasebnosti otrok na spletu Združenih držav Amerike – (*Children's Online Privacy Protection Act - COPPA*) iz leta 1998). Otrok je v tem primeru v skladu z odprtimi določbami Splošne uredbe naveden kot mladoletna oseba, ki je stara 15 let ali več. Kar tudi pomeni (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[58]: »Otrok, ki dopolni 15 let, lahko sam sklepa pravne posle, če zakon ne določa drugače.«

Po predlaganem drugem odstavku privolitev mladoletne osebe ne sme biti pogojevana s pretiranimi pogoji s strani upravljavca, npr. da bi bila omogočena udeležba mladoletnih oseb v igri, ponujanje nagrade, vključitve v družbeno omrežje ali druge podobne dejavnosti, tako da bi mladoletna oseba morala posredovati več osebnih podatkov (kršitev načela sorazmernosti), kot je potrebno za namen opravljanje takšne dejavnosti. V Francoski republiki je tako v Zakonu o varstvu osebnih podatkov

[55] Glejte ustaljeno ustavnosodno presojo Ustavnega sodišča Republike Slovenije o nedopustnosti določanja osebnih podatkov, namenov obdelave ipd. v podzakonskih predpisih: Odločba US, št. U-I-115/92, 24. 12. 1992; objava: OdlUS I, 105 in Uradni list RS, št. 3/93; Odločba US, št. U-I-229/03, 9. 2. 2006; objava: OdlUS XV, 13 in Uradni list RS, št. 21/06; Odločba US, št. U-I-245/05, 7. 2. 2007; objava: Uradni list RS, št. 15/07; delno tudi Odločba US, št. U-I-463/06, 18. 1. 2007; objava: Uradni list RS, št. 8/07.

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

[57] 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.

[58] Uradni list RS, št. 15/17.

Francoske republike določeno, da je starost za mladoletnika za podajo privolitve za uporabo storitev informacijske družbe 15 let, dodano pa je v okviru prostega polja zakonodajne presoje določeno, da kadar gre za mladoletnika pod starostjo 15 let, je privolitev zakonita le, če jo skupaj podata mladoletnik in oseba, ki ima starševsko odgovornost za mladoletnika. Poleg tega je kot zakonska specifičnost predpisano tudi, da mora upravljavec s področja storitev informacijske družbe pogoje poslovanja in druge komunikacije (tudi posredovanje informacij) z mladoletnikom izvajati na jasen in preprost način, tako da mladoletnik to vsebino razume na enostaven način. Določena razdelava glede storitev informacijske družbe in mladoletnikov je narejena tudi v amandmiranem Predlogu Zakona o varstvu osebnih podatkov 2018 Irske (z dne 15. 2. 2018) v drugem odstavku 30. člena, da namreč storitve informacijske družbe ne vključujejo storitev preventivne ali svetovalne narave – namreč ne vključujejo pomoči mladoletnikom. Za take primere ni zahtevana privolitev mladoletnika.

K 9. členu:

V 9. členu je predlagana posebna ureditev glede varstva osebnih podatkov umrlih posameznikov, na katere so se nanašali v preteklosti zbrani in obdelani osebni podatki. Gre že za tradicionalno slovensko ureditev (glejte veljavni 23. člen ZVOP-1) z vidika zadržanja dosedanje višje stopnje varstva osebnih podatkov. Podobna ureditev obstaja ali pa bo prenovljena vsaj v Avstriji in v Estoniji. Predlagana ureditev torej predstavlja zadržanje dosedanje ureditve, vendar z nekoliko posodobljena vsebino – tudi ob upoštevanju dejstva, da Splošna uredba določa, da ne posega v tovrstne nacionalne ureditve obdelave osebnih podatkov umrlih oseb (uvodna navedba št. 27 Splošne uredbe).

Predlagani prvi odstavek določa, da se **o**sebni podatki umrlih posameznikov varujejo po tem zakonu in drugih zakonih (npr. Obligacijski zakonik, Zakon o varstvu dokumentarnega in arhivskega gradiva ter arhivih).

Predlagani drugi odstavek določa, da upravljavec podatke o umrlem posamezniku posreduje le tistim uporabnikom, ki so za obdelavo osebnih podatkov pooblaščeni z zakonom (s področja javnega ali zasebnega sektorja) in tistim osebam, ki izkažejo pravni interes za uveljavljanje pravic pred osebami javnega sektorja.

Predlagani tretji odstavek določa, da ne glede na določbe drugega odstavka 10. člena ZVOP-2 upravljavec osebne podatke o umrlem posamezniku posreduje zakoncu, zunajzakonskemu partnerju ali partnerju iz partnerske zveze (izenačen s prej navedenimi), otrokom ali staršem ali dedičem, če umrli ni tega pisno prepovedal ali če drug zakon ne določa drugače.

Predlagani četrti odstavek določa, da če drug zakon ne določa drugače, lahko upravljavec podatke o umrlem posamezniku posreduje tudi katerikoli drugi osebi, ki namerava te podatke uporabljati za zgodovinske raziskovalne, znanstvene raziskovalne, statistične ali arhivske namene, kar je celo širše od področne ureditve iz 100. do 102. člena predloga zakona.

Predlagani peti odstavek je neposredna pravna podlaga (upravičenje) za izjemno objavo podatkov umrlih v knjigah, učbenikih, enciklopedijh itd, se pa ne nanaša na klasične objave oziroma članke v medijih (za te primere načeloma veljajo določbe glede razmerja do svobode izražanja po 103. členu predloga zakona), po pridobitvah privolitev po določenem izključujočem vrstnem redu.

K 10. členu:

V predlaganem 10. členu je določena dodaten sklop osebnih podatkov, ki so dejansko po vsebini del posebne vrste osebnih podatkov, namreč podatkov o kazenskih obsodbah in kaznovanjih za prekrške. Predlagana ureditev izhaja iz 10. člena Splošne uredbe ter iz uvodnih navedbi št. 75 in 80, ki v zvezi s konceptom kazenske obtožbe iz prvega odstavka 6. člena Evropske konvencije omenjajo poleg kaznivih dejanj tudi prekrške (kar je del skupnega koncepta kaznivih ravnanj – npr. 27. člen Ustave Republike Slovenije). V prvem odstavku je tako določeno, da za podatke o vpisu ali izbrisu v ali iz kazenske evidence ali evidenc (posebej urejene zbirke osebnih podatkov – uradne evidence), ki se upravljajo na podlagi Zakona o prekrških ter za prenose teh osebnih podatkov velja, da gre za osebne podatke, ki se morajo obravnavati kot posebne vrste osebnih podatkov v skladu s prvim in tretjim odstavkom 9. člena Splošne uredbe.

Drugi odstavek najprej v prvem stavku določa, da za obdelave določenih (vrst) osebnih podatkov iz kazenskih evidenc ter njihove zakonsko določene namene obdelave, roke hrambe ter prenose osebnih podatkov javnemu ali zasebnemu sektorju iz teh evidenc veljajo pravila iz 250.a člena Zakona o izvrševanju kazenskih sankcij, 135. člena Zakona o kazenskem postopku ter 84. člena Kazenskega zakonika. Prav tako določa, da za obdelave določenih (vrst) osebnih podatkov iz prekrškovnih evidenc po Zakonu o prekrških veljajo primerljiva pravila iz Zakona o prekrških glede zakonsko določenih namenov obdelave, rokov hrambe ter prenosov javnemu ali zasebnemu sektorju. Zaključno je za obe vrsti evidenc tudi določeno, da za prenose teh osebnih podatkov iz navedenih evidenc organom drugih držav ali mednarodnim organizacijam (za zakonsko določene namene) veljajo tudi pravila po drugih zakonskih podlagah. Glede na to, da je torej sistemska pravna ureditev glede osebnih podatkov o kazenskih obsodbah in kaznovanjih za prekrške dejansko izenačena s posebnimi vrstami osebnih podatkov, ostane v veljavi dosedanja višja raven njihovega varstva, vključno z omejitvami dostopa do njih, tudi po dosedanji praksi Informacijskega pooblaščenca[59].

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 in to na način, da se kot identifikacijska znaka uporabita osebno ime in njihova enotna matična številka, za tujca pa njegovo osebno ime in njegova enotna matična številka ali drug ustrezen identifikacijski znak iz kazenske ali prekrškovne evidence. Tretji odstavek tudi posebej (področno) določa, da mora biti zlasti zagotovljeno, da se osebni podatki iz obeh evidenc in Centralnega registra prebivalstva ne obdelujejo nepooblaščeno, nezakonito razkrivajo ali drugače nepooblaščeno obdelujejo. Gre za poseben poudarek glede zagotavljanja varnosti osebnih podatkov.

Peti odstavek določa, da se povezovanje iz tretjega odstavka predlaganega člena se izvede tako, da je mogoče avtomatično posodabljanje podatkov v kazenskih evidencah in prekrškovnih evidencah oziroma tako, da povezovanje omogoča vsaj, da se v evidencah pri osebnih podatkih določenega ali določljivega posameznika pojavi samodejno opozorilo, da je pri njegovih podatkih v drugi zbirki osebnih podatkov prišlo do spremembe (ti. »*alert sistem*«).

K 2. poglavju – Postopek odločanja o pravicah posameznikov

V 2. poglavju I. dela Predloga zakona se urejajo določena postopkovna vprašanja glede zagotavljanja pravic posameznikov, na katere se nanašajo osebni podatki oziroma njihovega sistemskega institucionalnega varstva (pristojnosti Informacijskega pooblaščenca). Predlagani členi smiselno sledijo obstoječi ureditvi iz 30. in sledečih členov ZVOP-1 in tako urejajo postopek vložitve, obravnave, odločitve o zahtevah posameznika ter sodno varstvo.

K 11. členu:

Uvodni 11. člen določa sistemska pravila glede pravil postopka v zvezi z uveljavljanjem pravic posameznikov in posameznic, na katere se nanašajo osebni podatki. Splošna uredba določa okrepljeno odgovornost upravljavca za zagotavljanje informacij oziroma pravic posameznikom, katerih osebne podatke obdeluje. Navedeno temelji na premisi, da lahko le dobro informiran posameznik ustrezno zavaruje svoj pravice skozi postopke pred upravljavcem, Informacijskim pooblaščencem oziroma pred sodišči.

Člen tako določa obveznost upravljavca, da vzpostavi ustrezne ukrepe in postopke za sprejem, obravnavo in odgovarjanja na zahteve posameznikov po členih 15 do 22 Splošne uredbe ter po II. delu predloga zakona. Pri tem se smiselno izhaja iz ureditve obravnave vlog v Zakonu o splošnem upravnem postopku.

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

K 12. členu:

Predlagani 12. člen določa obvezne vsebine zahteve, kar so poleg same vsebine zahteve (za katero pravico gre, ter na katere osebne podatke se nanaša) še zlasti podatki, ki bodo upravljavcu potrebni (našteti so primeroma, vendar je treba pri njihovi uporabi upoštevati načelo sorazmernosti, kot je tudi specifično določeno v drugem stavku prvega odstavka), da enolično določi posameznika v svojih zbirkah. V kolikor zahteva ne vsebuje vseh teh elementov, mora upravljavec (v luči obveznosti olajšanja uveljavljanja pravic posamezniku omogočiti, da jo dopolni. Šele, če je posameznik tudi na poziv ne dopolni, lahko upravljavec zahtevo zavrže ali pa sporoči, da je ne bo obravnaval.

K 13. členu:

Predlagani 13. člen v prvem odstavku ureja načine preverjanja identitete vlagatelja zahteve (posameznika, na katerega se nanašajo osebni podatki) ali njegovega podpisa, kadar uporablja pravice po tem poglavju predloga zakona. Med drugim se v javnem ali zasebnem sektorju to lahko preveri preko elektronskega podpisa, ki je izenačen z lastnoročnim podpisom in velja v skladu z Uredbo (EU) št. 910/2014[60], z naprednim elektronskim podpisom, ki velja v skladu z Uredbo (EU) št. 910/2014 in se vlagatelja lahko preveri z vpogledom v ustrezno javno listino, ki vsebuje njegovo fotografijo, s potrditvijo zahteve v papirni obliki ali osebno, z vpogledom v ustrezno javno listino, ki vsebuje vlagateljevo fotografijo, ali na način osebne vročitve upravljavčeve odločitve o zahtevi na uradni naslov posameznika ali naslov, ki izhaja iz lastnih zbirk upravljavca. V osnovi pa vsak upravljavec sam odloči katero raven zanesljivosti sredstev elektronske identifikacije bo uporabil – glede na vsebino oziroma okoliščine konkretne obdelave osebnih podatkov.

K 14. členu:

Predlagani 14. člen določa, da mora upravljavec odgovor zagotoviti brez nepotrebnega odlašanja, vendar v vsakem primeru v enem mesecu po prejemu zahteve, razen če si v skladu s pravili Splošne uredbe določi podaljšanje tega roka. Kršitve teh rokov imajo lahko dejansko posledico, da se šteje, da je zahteva zavrnjena.

Navedeno ne pomeni, da lahko upravljavec izvajanje vseh pravic vedno zadrži do preteka meseca dni od prejema popolne zahteve. Takšno postopanje se šteje kot kršitev Splošne uredbe oziroma tega zakona in predstavlja podlago za prekrškovno odgovornost upravljavca.

K 15. členu:

Upravljavci iz javnega sektorja morajo o zahtevi odločiti s pisnim obvestilom (torej ne z upravno odločbo). Enako lahko odloči upravljavec iz zasebnega sektorja - s pisnim obvestilom (dopisom), ki ga posamezniku vroči na način, kot ga je ta zahteval oziroma kot je glede na vse okoliščine primerno.

Tretji odstavek določa splošno pravilo, po katerem se na zahtevo, ki je bila vložena po elektronski poti, poda odgovor v elektronski obliki.

K 16. členu:

V 16. členu je določen ugovor v primeru nepopolne odločitve upravljavca glede posredovanja osebnih podatkov. Predlagano je, da če posameznik po prejeti odločitvi upravljavca meni, da osebni podatki, ki jih je prejel, niso osebni podatki, ki jih je zahteval, ali da ni prejel vseh zahtevanih osebnih podatkov, lahko pred vložitvijo pritožbe (pri Informacijskem pooblaščencu) pri upravljavcu vloži obrazložen ugovor v roku osmih dni. Upravljavec mora o ugovoru odločiti kot o novi zahtevi v 5 delovnih dneh, če pa gre za zadeve iz direktivnega področja (66. člen predloga zakona) pa v 15 delovnih dneh, saj gre za lahko tudi za izmenjavo informacij med različnimi subjekti, ki so lahko tudi v tujini (druge države Evropske unije, tretje države, mednarodne organizacije) in gre tudi za vprašanje odzivnosti (tuji

[60] Uredba (EU) št. 910/2014 Evropskega parlamenta in Sveta z dne 23. julija 2014 o elektronski identifikaciji in storitvah zaupanja za elektronske transakcije na notranjem trgu in o razveljavitvi Direktive 1999/93/ES (UL L št. 257 z dne 28. 8. 2014, str. 73).

policijski organi, tuja kazenska sodišča…) in je lahko ustrezni predpisani rok za izvedbo odločitve le 15 delovnih dni.

K 17. členu:

V 17. členu je določeno, da če upravljavec ne odloči o zahtevi posameznika v roku iz 14. člena predloga zakona, lahko posameznik pri Informacijskem pooblaščencu vloži pritožbo zaradi molka upravljavca. Če upravljavec zahtevo zavrne, lahko posameznik pri upravljavcu, če gre za javni sektor oziroma pri Informacijskem pooblaščencu, če gre za zasebni sektor vloži obrazloženo pritožbo v roku 15 dni od prejema obvestila ali odločbe upravljavca. Po drugem odstavku pravica strank do pregledovanja dokumentov v zadevah odločanja o posameznikovi pritožbi po določbah Zakona o splošnem upravnem postopku, do pravnomočnosti odločbe Informacijskega pooblaščenca - ne more vključevati pregledovanja upravne zadeve v delu, ki se nanaša na dokumente, ki so predmet zahteve in drugih dokumentov zadeve, iz katerih bi se dalo razbrati ali sklepati na vsebino (že) zahtevanih osebnih podatkov. Smiselno enaka omejitev glede omejitev pravic do pregledovanja upravne zadeve velja tudi pri odločanju o zahtevi pri upravljavcu. Tretji odstavek določa da po koncu postopka iz drugega odstavka možnost pregleda vsebine zadeve le v skladu z dokončno odločbo Informacijskega pooblaščenca ali upravljavca. Četrti odstavek določa pravila do kdaj se v zvezi s potrebami postopka ne smejo uničiti, odsvojiti ali na drug način napraviti za nedostopne osebni podatki, kateri se obravnavajo.

K 18. členu:

V 18. členu je določen postopek obravnavanja pritožbe, da namreč odloča Informacijski pooblaščenec ter kaj so možni pritožbeni razlogi.

K 19. členu:

V 19. členu so določena pooblastila Informacijskega pooblaščenca v pritožbenem postopku, konkretno glede državnih nadzornikov za varstvo osebnih podatkov, tako glede uporabe pooblastil iz Splošne uredbe, Zakona o inšpekcijskem nadzoru, dostopa do dokumentacije ipd., sicer v skladu z omejitvami posegov v pravice s področij komunikacijske in prostorske zasebnosti iz drugega do četrtega odstavka 53. člena tega zakona. V četrtem 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, temeljne razloge odločitve ter pravni pouk.

K 20. členu:

20. člen določa, da je za izvedbe upravne izvršbe v zvezi z odločbami, izdanimi v pritožbenem postopku, pristojen Informacijski pooblaščenec. Po drugem odstavku se upravna izvršba opravi na predlog posameznika na podlagi izvršljive odločbe in sklepa o dovolitvi izvršbe, in sicer s prisilitvijo zoper upravljavca.

K 21. členu:

Bistvo 21. člena o zaračunavanju stroškov je, da se po prvem odstavku informacije in sporočila ter ukrepi iz I. dela zakona zagotavljajo brezplačno (kot to zahteva prvi stavek tretjega odstavka člena 15 Splošne uredbe). Po drugem odstavku pa so določene izjeme, da se v določenih primerih očitno neutemeljenih zahtev ali njihove pretiranosti lahko zaračunajo razumne pristojbine, pri čemer se upoštevajo administrativni stroški posredovanja informacij ali sporočila oziroma izvajanja zahtevanega ukrepa po tem delu zakona (npr. če se zahteva nanaša na posredovanje istih osebnih podatkov npr. trikrat v enem letu). V primerih, ko se izdaja kopija, ki ne vsebuje samo lastnih osebnih podatkov posameznika, ampak tudi osebne podatke drugih posameznikov (npr. posnetek videonadzora, ki ga je treba anonimizirati pred posredovanjem posamezniku, ker so na njemu tudi drugi posamezniki), ne gre več za (začetno) kopijo, ampak za dodatno kopijo, kjer je možno zaračunavanje.

Naslednji odstavki določajo, da izda pravilnik o zaračunavanju stroškov minister za pravosodje. Področje višine stroškov na področju seznanitve z lastno zdravstveno dokumentacijo in dokumentacijo umrlih pacientov ter povezana pravila o zaračunavanju bodo predpisana v istem pravilniku, jih je pa treba zaradi pravne varnosti in različnih pristojnosti ministrstev posebej omeniti glede na področno ureditev, namreč glede na četrti odstavek 41. člena Zakona o pacientovih pravicah[61].

K 22. členu:

Predlagani 22. člen ZVOP-2 določa omejitve pravic posameznikov. Po prvem odstavku je pravice posameznika iz tega dela zakona mogoče z zakonom izjemoma omejiti iz razlogov navedenih v prvem odstavku člena 23 Splošne uredbe (razlogi državne varnosti, obrambe, javne varnosti, preprečevanja, preiskovanja, odkrivanja ali pregona kaznivih dejanj ali izvrševanja kazenskih sankcij, vključno z varovanjem pred grožnjami javni varnosti in njihovim preprečevanjem, drugih pomembnih ciljev v splošnem javnem interesu Republike Slovenije, zlasti pomembnega gospodarskega ali finančnega interesa, vključno z denarnimi, proračunskimi in davčnimi zadevami, javnim zdravjem in socialno varnostjo, varstva neodvisnosti sodstva in sodnega postopka, preprečevanja, preiskovanja, odkrivanja in pregona kršitev etike v zakonsko urejenih poklicih, spremljanja, pregledovanja ali urejanja, povezanega, lahko tudi zgolj občasno, z izvajanjem javne oblasti, varstva posameznika, na katerega se nanašajo osebni podatki, ali človekovih pravic in temeljnih svoboščin drugih ter uveljavljanja civilnopravnih zahtevkov). Omejitve pa se lahko določijo samo pod pogojem, da je zakonska določba, ki določa takšno omejitev, v skladu z drugim odstavkom 7. člena predloga zakona. Prav tako je določena sistemska izjema, da se ne glede na določbe prvega odstavka in še zlasti v primerih obdelave osebnih podatkov v okviru strokovnih mnenj, izdelanih v skladu z določbami zakonov, ki urejajo sodne ali upravne ali nadzorne postopke, v primeru, kadar se posameznik, na katerega se nanašajo osebni podatki, navaja netočnost in neposodobljenih svojih osebnih podatkov, posamezniku mora dati na razpolago možnost za nasprotni prikaz dejstev, v okviru njegove pravice do ugovora. Upravljavec mora nasprotni prikaz dejstev priložiti dokumentom (posebni uradni zaznamek) ali ustrezno označiti na njih, kje se ta prikaz nahaja.

K 23. členu:

V 23. členu je posebej področno urejeno sodno varstvo pravic posameznika s področja varstva osebnih podatkov. V prvem odstavku je določeno, da ima posameznik, ki ugotovi, da so kršene njegove pravice, določene s tem zakonom ali Splošno uredbo, pravico do sodnega varstva ves čas, dokler kršitev (še) traja.

Po drugem odstavku je v primeru prenehanja kršitve možno vložiti posebno ugotovitveno tožbo, če ne obstaja drugo sodno varstvo.

V tretjem odstavku je določena vrsta sodnega postopka in sicer je to Zakon o upravnem sporu, kot je to urejeno v 34. členu ZVOP-1 že od leta 2004.

Po četrtem odstavku izhaja, da je javnost sodnega postopka načeloma izključena, saj gre za podvrsto splošne pravice do zasebnosti, namreč informacijsko zasebnost.

Po petem odstavku lahko posameznik, na katerega se nanašajo osebni podatki, v skladu s prvim odstavkom člena 80 Splošne uredbe, pisno pooblasti nevladno organizacijo s področja varstva osebnih podatkov ali zasebnosti, ki ima status nevladne organizacije v javnem interesu[62], da v njegovem imenu uveljavlja sodno varstvo po določbah tega člena.

Sodno odločanje Upravnega sodišča Republike Slovenije po predlaganem šestem odstavku nujno in prednostno (kot je bilo dosedaj enako določeno tudi v petem odstavku 34. člena ZVOP-1).

K 24. členu:

[61] Uradni list RS, št. 15/08 in 55/17.
[62] Navedene organizacije bodo priznane oziroma jim bo podeljen zahtevani status v skladu z določbami Zakona o nevladnih organizacijah iz leta 2018 (Uradni list RS, št. 21/18).

V 24. členu so določena posebna pravila glede načina uveljavljanja pravic posameznikov, na katere se nanašajo osebni podatki, kadar gre za določena zakonska področja iz predloga zakona, namreč iz 100.-104. člena (statistika, svoboda izražanja ipd.). Pravice zasebnosti se izvršujejo v skladu s področnimi zakoni (npr. Zakon o medijih), izjemoma pa tudi po določbah predloga zakona, kolikor je to v navedenih členih predpisano.

V tretjem odstavku 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[63].

K 25. členu:

Predlagani 25. člen določa področno izjemo glede uveljavljanja pravic posameznika preko zakonitega zastopnika glede vsebine posameznikove zdravstvene dokumentacije. Po predlagani ureditvi lahko upravljavec lahko izjemoma zavrne zahtevo posameznika iz I. dela zakona ali dostop do posameznikove zdravstvene dokumentacije, ki je vložena prek zakonitega zastopnika, če so podane konkretne in objektivne okoliščine, zaradi katerih bi bilo utemeljeno sklepati, da bi bile zaradi seznanitve z določenimi osebnimi podatki neposredno ali posredno prizadete koristi, pravice ali upravičeni interesi mladoletnih oseb ali oseb z omejeno ali odvzeto poslovno sposobnostjo ali drugih oseb, za katere tako določa zakon, in če te pravice in interesi pretehtajo nad interesi zakonitega zastopnika za seznanitev z osebnimi podatki.

K 3. poglavju: Varnost osebnih podatkov in ocena učinka

K 26. členu:
Predlagani člen nadomešča dosedanji pojem oziroma institut "zavarovanje osebnih podatkov" (24. člen ZVOP-1) s pojmom "varnost osebnih podatkov". Sprememba seveda ni samo izrazoslovna, ampak je vezana zlasti na spremenjene tehnološke realnost, ki so nastopile v času od uveljavitve ZVOP-1. Vsesplošna informatizacija postopkov obdelave osebnih podatkov je namreč poleg številnih prednosti prinesla tudi nekatere probleme, zlasti glede zagotavljanja varnosti obdelav.

Uvodna opredelitev 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 izvedeta ustrezne tehnične ukrepe, da se v čim večji meri prepreči kršitve varstva osebnih podatkov. Določbe veljajo kot specifični standard le za javni sektor,

Drugi odstavek primeroma našteva nekatere najbolj tipične varnostne ukrepe, tj. uporabo psevdonimiziranja oziroma šifriranja, izvajanje glavnih premis informacijske varnosti (zaupnost, celovitost, dostopnost sistemov), izdelovanje varnostnih kopij in sposobnost njihove obnove, ter zavarovanje osebnih podatkov med prenosom po elektronskem komunikacijskem omrežju. Novi, oziroma točneje, izrecno določeni sta tako zgolj alineja d), ki zahteva, da se navedene ukrepe varstva osebnih podatkov periodično pregleduje, ter tč. f) zadosti dolgo vodenje dnevniških sledi o dejanjih obdelave osebnih podatkov.

Konkretneje se varnostne ukrepe zagotavlja zlasti z namenskimi informacijskimi orodji, kot so

- orodja, tehnike in mehanizmov za zagotavljanje zaupnosti, celovitosti in razpoložljivosti komunikacijskih omrežij,
- orodja za preverjanje identitete uporabnikov,
- orodja za upravljanje pooblastil za dostop,
- orodja za zaščito pred zlonamernimi kodami,

[63] 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.

- orodja za beleženje dejavnosti kritične informacijske infrastrukture in pomembnih informacijskih sistemov, njihovih uporabnikov in administratorjev,
- orodja za zaznavanje poskusov vdorov in preprečevanje incidentov,
- orodja za šifriranje, anonimiziranje ali psevdonimiziranje osebnih podatkov.

Zadnja navedena novost (ti. »notranja sledljivost« obdelav osebnih podatkov) je določena v 7. točki drugega odstavka in je predlagana zlasti glede na izkušnje Informacijskega pooblaščenca iz prakse, kjer se pri številnih nadzornih postopkih pri večjih upravljavcih še vedno dogaja, da kljub izvajanju tveganih obdelav še vedno ne vodijo revizijskih sledi v takšni kvaliteti, ki bi v primeru zlorab omogočali odgovor na vprašanje, katera oseba je kdaj dostopala do katerih podatkov, kaj je z njimi naredila ipd.. Iz tega razloga se obveznost vodenja revizijskih sledi izrecno predpisuje v minimalnem roku 5 let od preteka leta, v katerem se je zgodila obdelava, razen če kakšen področni zakon določa drug rok. Predlagana določba tako pomeni izvedbo 32. (ukrepi varnosti obdelave), 33. (obveščanje o kršitvah varstva osebnih podatkov), 17. (izkazovanje dejanske izvršitve ali omogočanje izvrševanja pravice od izbrisa ozir. pravice do pozabe) in delno tudi 25. člena (olajšanje izvajanje vgrajenega in privzetega varstva osebnih podatkov) Splošne uredbe.

K 27. členu:

Predlagani člen podobno kot 26. člen določa specifičnosti za javni sektor glede ocene učinka glede obdelav osebnih podatkov v javnem sektorju. Prvi odstavek določa da v primerih, kadar bi lahko obdelava osebnih podatkov v javnem sektorju, ki se določa z zakonom, zlasti kadar gre za uporabo novih tehnologij in upoštevaje naravo, obseg, okoliščine in namen te obdelave, vsebovala obdelavo osebnih podatkov večjega števila posameznikov, na katere se nanašajo osebni podatki ali pa veliko tveganje za človekove pravice in temeljne svoboščine posameznikov, mora upravljavec pred začetkom obdelave opraviti oceno učinka predvidenih dejanj obdelave na varstvo osebnih podatkov v skladu s 35. členom Splošne uredbe. Drugi odstavek določa posebno vrsto vsebinske (notranje) legitimnosti, da mora namreč predlagatelj zakona pripraviti predhodno oceno učinka iz prvega odstavka, še preden je predlog zakona dostopen javnosti.

K 4. poglavju – Posebne določbe

3. poglavje I. dela ureja določena tehnična in vsebinska vprašanja, ki omogočajo lažje delovanje sistema varstva osebnih podatkov. Urejen je postopek posredovanja osebnih podatkov, vprašanje uporabe povezovalnih znakov, vprašanje sledljivosti posredovanj osebnih podatkov ipd.

K 28., 29. in 30. členu:

Navedeni trije členi urejajo vprašanje posredovanja osebnih podatkov drugemu upravljavcu, zaradi namenov, ki so pod njegovo kontrolo. V praksi gre pri tem zlasti za zahteve odvetnikov, policije, državnih tožilstev in sodišč za posredovanje podatkov, relevantnih za odločanje ali delovanje v konkretni zadevi.

Izhodiščno pravilo za posredovanje je, da gre zgolj za eno od oblik obdelave osebnih podatkov, in da mora torej zanjo obstajati veljavna pravna podlaga, ki upravljavca zavezuje ali mu vsaj dovoljuje posredovanje. Naloga, da določi to pravno podlago, ter da njeno podanost ustrezno izkaže, je na prosilcu za podatke. Ta mora imetniku podatkov poslati zahtevek, v katerem utemelji svojo pravno podlago. Šele na podlagi takšnega dopisa pa je potem mogoče pripraviti zaprošene podatke in jih tudi posredovati.

Predlagani 29. člen je neke vrste »zrcalna slika« 28. člena – zasebni sektor posreduje določene podatke uporabnikom iz javnega sektorja ali celo iz zasebnega sektorja, če gre za nalogo javnega sektorja po prvem odstavku 29. člena.

V šestem odstavku 30. člena so določena pravila glede ti. »zunanje sledljivosti« obdelave osebnih podatkov, namreč glede posredovanj osebnih podatkov s strani upravljavcev uporabnikom. Po

sedmem odstavku mora upravljavec za vsako posredovanje osebnih podatkov zagotoviti, da je mogoče pozneje ugotoviti, kateri osebni podatki so bili posredovani, komu, kdaj in po kateri pravni podlagi, za kateri namen oziroma iz katerih razlogov oziroma za potrebe katerega postopka, razen če drug zakon za posredovanje posameznih vrst podatkov ne določa drugače. Ureditev je podobna kot v dosedanjem tretjem odstavku 22. člena ZVOP-1. Predlagana določba je tako izvedba 33. (ukrepi varnosti obdelave), 34. (obveščanje o kršitvah varstva osebnih podatkov), 17. (izkazovanje dejanske izvršitve ali omogočanje izvrševanja pravice od izbrisa ozir. pravice do pozabe) in 25. (olajšanje izvajanje vgrajenega in privzetega varstva osebnih podatkov) Splošne uredbe. V zvezi z navedenim se v sedmem odstavku 30. člena izvedbeno zahteva tudi vodenje revizijskih sledi o posredovanjih – za dobo petih let.

Osmi odstavek 30. člena določa, da določbe sedmega in osmega odstavka o zunanji sledljivosti ter revizijski sledi veljajo tudi za obdelovalce, če so z zakonom ali pogodbo zavezani posredovati določene osebne podatke, kar pa vključuje tudi sodne odredbe ali inšpektorske ali druge nadzorne zavezujoče odredbe na podlagi in v mejah zakona.

K 31. členu:

V navedenem členu se ohranja obstoječa rešitev iz drugega odstavka 18. člena ZVOP-1. Pravica do vpogleda v osebni dokument tako ostaja definirana sorazmerno široko (vedno, ko je potrebno potrditi identiteto posameznika), medtem ko pravica fotokopiranja tega dokumenta ostaja pridržana bankam in drugim finančnim institucijam.

Po predlagani določbi lahko (občasno po drugem zakonu: mora[64]) upravljavec osebnih podatkov pred vnosom določenih podatkov ali njihovo spremembo ali dopolnitvijo v zbirki (osebnih podatkov) preveriti točnost identifikacijskih osebnih podatkov z vpogledom v osebno izkaznico, potni list ali vozniško dovoljenje posameznika, na katerega se nanašajo, ki vsebuje tudi fotografijo posameznika, ob tem pa tudi z vpogledom v kakšno drugo javno listino (ki ne vsebuje fotografije). Kot je razvidno, je krog dokumentov načeloma določen (razširijo jih lahko drugi zakoni), pomembno je, da je sedaj izrecno omenjeno vozniško dovoljenje. Te določbe ne posegajo v določbe zakonov, ki urejajo posamezne osebne dokumente glede dopustnosti kopiranja osebnega dokumenta.

K 32. členu:

V navedenem členu se glede povezovalnih znakov (EMŠO, davčna številka, ZZZS številka) ohranja obstoječe tradicionalne sistemske omejitve iz 20. člena ZVOP-1 pri povezovanju z nekaterimi zbirkami osebnih podatkov (evidence), in sicer, da je treba poleg EMŠO-a ozir. davčne številke kot vezni kriterij vnesti vsaj še en drug podatek (osebno ime, rojstni datum, idr.). Navedeno služi kot varovalka pred prehitrim in napačnim pripisovanjem dejstev iz teh evidenc napačni osebi. Prepovedi iz prvega odstavka 32. člena so bile vsebovane že v četrtem odstavku 8. člena Zakona o varstvu osebnih podatkov iz leta 1999 ter v veljavnem prvem odstavku 20. člena ZVOP-1, vključene pa so bile v navedena zakona kot povezava s sprejemanjem Zakona o centralnem registru prebivalstva[65] leta 1998 - namreč kot varovalka v povezavi s takratnimi idejami, da bi bilo treba (v Zakonu o centralnem registru prebivalstva) ukiniti enotno matično številko občana, ker naj bi le-ta omogočala preveliko moč državi in preveč ogrožala zasebnost ljudi.

K 33. členu:

V navedenem členu je opredeljena obveznost upravljavca da mora spoštovati načelo najkrajšega roka hrambe oziroma do spoštovanja obveznosti vgrajenega in privzetega varstva osebnih podatkov, ni pa predlagan splošen (zakonsko določen) rok hrambe za primere, ko področni zakoni, pogodbe ipd. tega

[64] Npr. drugi odstavek 39. člena Zakona o notariatu (Uradni list RS, št. 2/07 – uradno prečiščeno besedilo, 33/07 – ZSReg-B, 45/08 in 91/13).
[65] Izvirno: Uradni list RS, št. 1/99.

ne določajo[66], saj je to odvisno od konkretnih situacij in zakonsko predpisani rok bi bil prenevaren (verjetno predolg za določene »rutinske« obdelave). Upravljavec je zlasti dolžan redno preverjati, ali sta nabor in rok hrambe podatkov še vedno sorazmerna ter o tem voditi dokumentacijo za potrebe nadzor s strani Informacijskega pooblaščenca

K 5. poglavju – Pooblaščene osebe za varstvo osebnih podatkov

V 5. poglavju I. dela Predloga zakona se podrobneje ureja institute pooblaščene osebe za varstvo osebnih podatkov (v angleščini: Data Protection Officer; s kratico: DPO), kodeksov ravnanja oz. certificiranja. Pripadajoče določbe Splošne uredbe (tj. 37. do 43. člen) namreč niso v celoti neposredno uporabljive oziroma učinkovite, temveč na nekaterih mestih zahtevajo oziroma dovoljujejo podrobnejše urejanje v nacionalnih zakonih o varstvu osebnih podatkov.

Institut **pooblaščene osebe za varstvo osebnih podatkov** (v nadaljevanju: pooblaščene osebe) je ena od **večjih novosti** Splošne uredbe. Uvaja se jo po vzoru iz nemške prakse, kjer takšno osebo oziroma način delovanja poznajo že več kot 30 let. V samem bistvu gre za to, da morajo tisti upravljavci, ki izvajajo bolj obsežne oziroma tvegane obdelave, določiti namensko osebo, katere glavna naloga bo svetovanje in pomoč upravljavcu glede zagotavljanja skladnosti s Splošno uredbo in drugimi predpisi s področja varstva osebnih podatkov, obenem pa še skrb še za komunikacijo z državnim nadzornim organom za varstvo osebnih podatkov (Informacijskim pooblaščencem) v morebitnih postopkih nadzora oz. uveljavljanja pravic posameznikov, na katere se nanašajo osebni podatki. Pooblaščena oseba je lahko bodisi zaposleni, bodisi zunanji strokovnjak oz. podjetje. Imeti mora ustrezen dostop do postopkov obdelave osebnih podatkov pri upravljavcu ter obenem zadostno stopnjo neodvisnosti, da lahko nudi strokovno utemeljene nasvete oziroma drugo pomoč; skratka, ne sme biti primarno podrejena zasledovanju poslovnih oziroma drugih ciljev upravljavca. V ta namen se z zakonom se ureja pogoje za njeno imenovanje ter njene naloge, še zlasti pa njen položaj ter pooblastila.

K 34. členu:

Predlagani člen podaja opredelitev pooblaščene osebo. To je neodvisna oseba, ki naj upravljavcu ali obdelovalcu pomaga pri sistematičnem obvladovanju tveganj oziroma kršitev varstva osebnih podatkov. Z njenim imenovanjem upravljavec izkaže, da se vprašanj varstva osebnih podatkov loteva sistematično in z ustreznimi kadrovskimi in finančnimi vložki.

Pri tem je posebej poudarjeno, da so naloge pooblaščene osebe omejene zgolj na svetovanje in pomoč upravljavcu ali obdelovalcu in da torej ne pomenijo prevzem odgovornosti za zagotavljanje skladnost obdelav osebnih podatkov, ki jih Splošna uredba v 24. členu sicer poverja upravljavcu oziroma obdelovalcu. Upravljavec oziroma obdelovalec ostaneta odgovorna za zagotavljanje skladnosti obdelave osebnih podatkov z določbami Splošne uredbe, Direktive, ZVOP-2, področnih zakonov, prav tako pa se odgovornosti za kršitve skladnosti ne more rešiti s sklicevanjem na neustrezno delo pooblaščene osebe.

K 35. členu:

Imenovanje pooblaščene osebe vsebinsko in stroškovno ni nujno (in zato tudi ne smiselno) za vse upravljavce in obdelovalce. Temu primerno predlagani člen (po vzoru člena 37 Splošna uredbe) imenovanje pooblaščene osebe ne predpisuje za vse zavezance, temveč le:

- za upravljavce in obdelovalce v javnem sektorju, ker se njihove obdelave praviloma izvajajo neodvisno od privolitve posameznika in jih je treba že zaradi tega presojati strožje;

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

- za tiste upravljavce iz zasebnega sektorja, 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, ter
- Za tiste upravljavce iz zasebnega sektorja, ki izvajajo obsežne obdelave posebnih vrst osebnih podatkov iz 12. člena predloga zakona ali osebnih podatke iz 13. člena zakona (tj. dosedanje občutljive osebne podatke).

Medtem ko pri upravljavcih iz javnega sektorja dvoma glede potrebe po imenovanju pooblaščane osebe ni, morajo upravljavci iz zasebnega sektorja opraviti presojo, ali tveganost njihovih obdelav zahteva imenovanje pooblaščene osebe.

Prav tako morajo to presojo opraviti tudi obdelovalci (seveda smiselno le tisti, ki so del zasebnega sektorja, ker je pri javnopravnih ta obveznost velja že po samem zakonu). Tako je možno, da bosta k imenovanju pooblaščene osebe zavezana oba, lahko pa samo eden od njiju. Npr. v primeru, ko manjši upravljavec uporablja določeno storitev obdelovalca, ki sicer je invazivna, vendar je ne uporablja v velikem obsegu, ta upravljavec ne bo zavezan k imenovanju pooblaščene osebe, obdelovalec, ki pa isto storitev ponuja številnim upravljavcem in jo zato opravlja v velikem obsegu, pa bo.

Natančnejša merila glede tega, kdaj se določene obdelave štejejo v temeljne dejavnosti, ter kdaj gre za obsežne in bolj invazivne obdelave, so podrobneje pojasnjena v Smernicah Evropskega odbora za varstvo podatkov[67] na to temo.

Ocenjuje se, da bo v praksi velika večina upravljavcev in obdelovalcev iz zasebnega sektorja prosta obveznosti določitve pooblaščene osebe. Bodo pa še vedno lahko pooblaščeno osebo imenovali na prostovoljni podlagi, torej v primeru, če ocenjujejo, da jo potrebujejo, in na ta način izkažejo kakovost njihovih obdelav osebnih podatkov. Zakon tudi ne predvideva dodatnih primerov, ko bi bilo imenovanje obvezno, lahko pa takšno možnost določijo posamezni področni zakoni.

Primeri subjektov iz zasebnega sektorja, ki bodo morali določiti pooblaščeno osebo:

Primer št 1:

Gospodarska družba Družbeno omrežje d.o.o., ki ponuja splošno dostopno socialno omrežje, ki zbira številne podatke o zasebnem življenju posameznika in iz njih izdeluje podrobne profile, oz. ki te profile daje na voljo spletnim oglaševalcem.

Primer št. 2:

Gospodarska družba Mali račun d.d., ki preko kartic zvestobe podrobno spremlja nakupe velikega števila kupcev ter jih nato s pomočjo analiz uvršča v posamezne segmente, zaradi izdelave ciljnih oglasov in ponudb.

Primer št. 3:

Zasebni zdravstveni zavod Moj zdravnik d.o.o., ki vodi zdravstvene kartoteke večjega števila okoliških občanov oziroma ki podpira tudi storitve spletnega naročanja na zdravstvene storitve.

Primeri subjektov iz zasebnega sektorja, ki jim ne bo treba določiti pooblaščene osebe:

Primer št. 1:

Manja Novak, Frizerstvo, s.p., stalno izvaja frizerske storitve, ima še dve zaposleni osebi, obdeluje sama seznam stalno naročenih strank dvakrat mesečno (okoli 100 oseb), o njih obdeluje le osebno ime, telefonsko številko ter datum predvidene oprave storitve; ne obdeluje kakšnih podatkov (v obliki opomb) glede zdravstvenih problemov nekaterih strank z lasišči, niti podatkov o rojstnih dnevih za

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

določene najbolj stalne stranke, saj zna oboje na pamet ipd.. Pooblaščene osebe ji zaradi majhne tveganosti in istočasne neobsežnosti obdelave osebnih podatkov ni treba določiti.

Primer št. 2:

Odvetnik Danko Majer, ima le manjše število strank, nima nekega pomembnega registra strank, niti nima stalnih strank, ki bi bile fizične osebe, pretežno bolj pravno svetuje, pred sodišči le občasno zastopa stranke in to bolj glede sosedskih sporov (nujne poti ipd.), odškodninsko zadevo v zvezi z zdravstvenim incidentom ima le na kaka 3 ali 4 leta, pa še takrat pretežno poskusi z izvedbo poravnave. Pooblaščene osebe mu zaradi majhne tveganosti in neobsežnosti obdelave osebnih podatkov ni treba določiti.

Primer št. 3:

Folksy Side of It, s.p., lastnica izdeluje majhne figurice škratov kot občasno popoldansko obrt, sprejema naročila preko svetovnega spleta in tudi plačila na ta način, ima mesečno med 15-20 strank, ne vodi posebnih seznamov osebnih podatkov njenih strank, teh podatkov ne združuje, v kratkem roku - po preteku reklamacijskih rokov njihove osebne podatke (zlasti e-pisma) podatke zbriše, le zaradi davčnih in računovodskih obveznosti zadrži ločeno podatke o plačilih za njene izdelke. Pooblaščene osebe ji glede na neobsežnost obdelave ter na hitro brisanje večine osebnih podatkov ni treba določiti.

Primer št. 4:

Pek Anrej Kostel, s.p., prodaja običajno rogljičke na stojnici, ima dogovor z več domovi upokojencev, ki so (kot domovi upokojencev njegove stalne stranke) ter z nekaj fizičnimi osebami, da jim v sobotah dostavlja rogljičke. Podatke o kontaktih domov upokojencev ter kontaktne podatke fizičnih oseb (osebno ime, naslov, datum dostave in običajna količina rogljičkov) obdeluje v Microsot Excel tabeli, ki jo ne posodablja dovolj pravočasno in niso kaj posebej urejeni, niso tudi v njej dodani podatki o plačilih, to za njega ločeno opravlja računovodja, ki enkrat mesečno pride k njemu in si prepiše samo relevantne podatke za določen mesec. Pooblaščene osebe mu glede na težjo povezljivost osebnih podatkov, njihovo delno neposodobljenost (netveganost) ipd. ni treba določiti.

Primer št. 5:

Vaški pek Renato Lavinar ima stalne stranke v vasi, kar vključuje skoraj vse vaščane in vaščanke in jim prodaja pekarske izdelke. V službenem računalniku upravlja seznam stalnih strank, ki so mu v preteklosti na običajni način (ustne pogodbe pretežno) povedale, da potrebujejo njegove izdelke na določen dan v tednu. Gre za manj kot 60 oseb, seznam uporablja le za dostavo izdelkov ter za njihova plačila njemu konec meseca, za kar ima poseben seznam. Pooblaščene osebe mu ni treba določiti za te obdelave osebnih podatkov, ki dejansko niso tvegane, obsežne (množične), tudi zato ker ima dva ločena seznama z osebnimi podatki, ki ju ročno primerja enkrat mesečno. Poleg tega pa si je sam naredil (glede na podlagi običajnih medčloveških komunikacij ter prostovoljno njemu danih informacij posameznikov in posameznic, na katere se nanašajo osebni podatki) še tretji seznam, kjer je skoraj za vse svoje stalne stranke iz vasi navedel še datum rojstva, god, obletnice porok, datume rojstev otrok njegovih strank - skupaj s podatki iz prvega seznama in te stranke stalno kontaktira, jim pošilja ponudbe, včasih po lastni volji dostavi določene izdelke kot darilo za določene obletnice, pošiljal je tudi že pakete z izdelki tudi v tujino, če je kak vaščan šel na delo v tujino... Ta tretji seznam in povezana obdelava osebnih podatkov sta pa že bolj tvegana in obsežnejša in verjetneje je, da mora določiti pooblaščeno osebo.

Zgornji primeri, ki razlagalno opisujejo komu ni treba imenovati pooblaščene osebe, so relevantni tudi za uporabo ozir. razlago določb o evidenci dejavnosti obdelav pač kateri upravljavci ne izpolnjujejo teh kriterijev in jim torej ni treba imeti ne evidence dejavnosti obdelav in niti določiti pooblaščene osebe (glejte peti odstavek 30. člena Splošne uredbe).

Predlagani tretji odstavek določa možnost imenovanja namestnika pooblaščene osebe za čas zadržanosti ali odsotnosti pooblaščene osebe, seveda pa namestnik deluje po navodilih pooblaščene osebe (drugi stavek sedmega odstavka 36. člena ZVOP-2), za namestnike so tudi nekoliko olajšani

pogoji glede njihove določitve (prvi stavek sedmega odstavka 36. člena ZVOP-2). Odgovornost za namestnikovo delo pri tem ves čas ostaja na pooblaščeni osebi.

Po predlaganem četrtem odstavku morata upravljavec ali obdelovalec, ki sta imenovala pooblaščeno osebo, v roku osmih dni od imenovanja vpisati njene kontaktne podatke po členu 30 Splošne uredbe v svoji evidenci dejanj obdelave, jih javno objaviti na primeren način (npr. na spletni strani) ter jih sporočiti Informacijskemu pooblaščencu (zaradi nadzora nad spoštovanjem obveznosti imenovanja, zaradi česar seznam tudi ni javen).

K 36. členu:

V predlaganem členu so določeni pogoji za imenovanje pooblaščene osebe za varstvo podatkov. Za upravljavce iz zasebnega sektorja neposredno veljajo usmeritve iz petega odstavka člena 37 in drugega stavka šestega odstavka člena 38 Splošne uredbe, medtem ko se za javni sektor na podlagi pooblastila iz drugega oziroma tretjega odstavka 6. člena Splošne uredbe poleg teh usmeritev še nekateri dodatni pogoji. Ti so po mnenju predlagatelja nujni in razumni, saj je treba zagotoviti ustrezno zaupanje v pooblaščene osebe, npr. obstoj poslovne sposobnosti, nekaznovanost, delovne izkušnje ipd[68].

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

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

2. poslovno sposoben,

3. ima vsaj univerzitetno izobrazbo ali končan magistrski študijski program (po področni zakonodaji je to: izobrazba, pridobljena po študijskem programu druge stopnje, oziroma izobrazba, ki ustreza ravni izobrazbe, pridobljene po študijskem programu druge stopnje, in je v skladu z zakonom, ki ureja slovensko ogrodje kvalifikacij, uvrščena na 8. raven ali izobrazba, pridobljena po študijskem programu druge stopnje, oziroma izobrazba, ki ustreza ravni izobrazbe, pridobljene po študijskem programu druge stopnje, in je v skladu z zakonom, ki ureja slovensko ogrodje kvalifikacij, uvrščena na 9. raven),

4. ima ustrezne kompetence z vidika varstva osebnih podatkov, kar se izkazuje lahko s potrdili sedanjega ali preteklega delodajalca ali delodajalcev da ima tri leta delovnih izkušenj s področja varstva osebnih podatkov ali izvedena ustrezna usposabljanja v Sloveniji ali mednarodna usposabljanja glede varstva osebnih podatkov, za kar ima podeljen ustrezen certifikat (glejte tudi začasne izjeme glede sorodnih delovnih področij v tretjem odstavku 150. člena ZVOP-2, katere omogočajo da širši krog ljudi začasno pridobi status pooblaščene osebe),

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.

Poleg tega je v drugem odstavku določeno še, da mora biti pooblaščena oseba javnopravnega upravljavca zaposlena pri tem upravljavce, s čimer se omejuje pretirano zanašanje na zunanje ponudnike in obenem utrjuje zavedanja o pomenu varstva osebnih podatkov. Izjeme od te zahteve določajo naslednji odstavki.

V tretjem odstavku je za ti. širši javni sektor (torej javni sektor brez sektorja država) izjemoma dovoljeno, da za pooblaščeno osebo, če je ni mogoče določiti znotraj osebe javnega sektorja v skladu

[68] Delno podoben vsebinski pristop je sprejela tudi Kraljevina Belgija, ki je tudi samostojno določila pravno podlago za pogoje za določitev pooblaščene osebe – vendar na način, da je za to dano pooblastilo v obliki delegirane zakonodaje za Kraljevo (dejansko: vladno) uredbo v zakonu (peti odstavek 63. člena Zakona o varstvu fizičnih oseb glede obdelave osebnih podatkov Kraljevine Belgije iz leta 2018).

z ZVOP-2 ali določiti skupne pooblaščene osebe z drugimi upravljavci ali obdelovalci javnega sektorja, s pogodbo v pisni obliki določijo tudi posameznika ali posameznico iz zasebnega sektorja ali pravno osebo iz zasebnega sektorja.

Četrti odstavek še dodatno upošteva specifike s področja vzgoje in izobraževanja (razpršenost tovrstnih subjektov, morebitno manjše število zaposlenih pri posameznih subjektih, nemožnost dodatnega zaposlovanja, lahko tudi manjša finančna sredstva) in tako omogoča, da če je za pooblaščeno osebo upravljavca ali obdelovalca na področju vzgoje in izobraževanja določena oseba, ki izpolnjuje pogoje za strokovnega delavca na področju vzgoje in izobraževanja, se šteje, da izpolnjuje pogoj iz 4. točke prvega odstavka tega člena ter da se upravljavci ali obdelovalci na področju vzgoje in izobraževanja lahko dogovorijo tudi za določitev skupne pooblaščene osebe, tako da s pogodbo v pisni obliki določijo tudi posameznika ali posameznico iz zasebnega sektorja ali pravno osebo iz zasebnega sektorja v skladu s petim odstavkom tega člena.

Peti odstavek pojasnjuje, da lahko zasebni sektor za pooblaščeno osebo upravljavca ali obdelovalca s pogodbo v pisni obliki imenuje tudi posameznika ali posameznico, ki ni zaposlena pri upravljavcu ali obdelovalcu, ali pravno osebo, podano je torej splošno pooblastilo za zunanje izvajalce, ob tem je tudi določeno, da je pooblaščena oseba lahko le individualno določena, kar pomeni, da ne more biti kolektivnega subjekta/organa, v primeru pravne osebe pa, da mora določena fizična osebe iz te pravne osebe imeti položaj vodilnega člana.

Po šestem odstavku mora vodilna oseba pravne osebe izpolnjevati vse pogoje iz prvega odstavka, razen seveda pogoja državljanstva.

Sedmi odstavek nekoliko olajšuje posamezne pogoje glede oseb, ki bodo nudile pomoč pooblaščenim osebam. Pooblaščeni osebi namreč pri opravljanju njenih nalog pomagajo tudi druge osebe, ki so pri tem vezane na njena navodila. Te osebe morajo izpolnjevati pogoje za imenovanje za pooblaščeno osebo, razen državljanstva in delovnih izkušenj. To pomeni, da je pooblaščena oseba funkcionalno in organizacijsko vedno le ena (ima pa lahko namestnika, ki jo v času odsotnosti polno nadomešča, vendar deluje po njenih navodilih in ni treba da izpolnjuje vse pogoje iz prvega odstavka tega člena), je ti. »vodilna oseba« in da torej tudi ni možno ustanoviti kolektivne pooblaščene osebe (kolegijski subjekt ali kolegijski »organ«). Ta vodilna oseba je hierarhično nadrejena ostalim članom skupine in odgovorna za delo.

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

V devetem odstavku je prepoved iz devetega odstavka podrobneje razdelana za javni sektor. Po njej se za javni sektor šteje, da ima določena oseba konflikt interesov, če ima položaj predstojnika ali drugega funkcionarja v subjektu javnega sektorja, če je član organov upravljanja ali nadzora pri upravljavcu ali obdelovalcu, če njene druge naloge vključujejo odločanje o obdelavi osebnih podatkov pri upravljavcu ali obdelovalcu, ali če zastopa upravljavca oziroma obdelovalca v sodnih ali arbitražnih postopkih v zvezi z vprašanji varstva osebnih podatkov. V primeru, da pooblaščena oseba izve za situacijo, ki predstavlja ali bi lahko predstavljala konflikt interesov, mora o tem takoj pisno obvestiti upravljavca oziroma obdelovalca. Upravljavec oziroma obdelovalec mora v tem primeru bodisi odpraviti konflikt bodisi pooblaščeno osebo razrešiti. Enako ravna v primeru, če se na drug način seznani z obstojem ali verjetnostjo obstoja konflikta interesov. Vse navedeno velja tudi za osebe, ki pooblaščeni osebi pomagajo pri opravljanju njenih nalog.

Določbe devetega odstavka o razrešitvi konflikta interesov veljajo smiselno tudi za zasebni sektor (zadnji stavek tega odstavka).

K 37. členu:

V predlaganem členu je določena možnost imenovanja skupne pooblaščene osebe za varstvo podatkov. Več upravljavcev iz javnega sektorja ali več upravljavcev iz zasebnega sektorju lahko, upoštevaje njihovo delovno področje, organizacijsko strukturo in velikost, imenuje tudi skupno pooblaščeno osebo (ne more pa del javnega sektorja skupaj z delom zasebnega sektorja imenovati skupne pooblaščene osebe). Pri tem morajo zagotoviti, da je pooblaščena oseba še vedno sposobna opravljati svoje naloge v zvezi z vsemi upravljavci ali obdelovalci, za katere je imenovana. Upoštevana je torej možnost, da zaradi strogosti pogojev in pa zahtevnosti nalog pooblaščene osebe obstaja skrb, da bodo morale pooblaščeno osebo za polni delovni čas imenovati tudi takšni subjekti, ki je v resnici ne rabijo večino časa v letu. Zato se daje družbam v povezani družbi, državnim organom, ter društvom ipd. možnost, da določijo skupno pooblaščeno besedo.

Zakon torej z vidikov ekonomičnosti (stroški) in racionalnosti (izkušnje) omogoča izbiro (imenovanje) zunanjih pooblaščenih oseb. Tako omogoča tudi fleksibilnost, da lahko zlasti skupine gospodarskih družb, društva ipd. določijo eno pooblaščeno osebo, ki skrbi za notranje varstvo osebnih podatkov v več subjektih.

Za odvetnike, ki so kot del pravosodja v širšem smislu samostojni in neodvisni (svobodni) poklic (prvi odstavek 137. člena Ustave Republike Slovenije) je dodan poseben odstavek, po katerem se lahko individualno dogovorijo z Odvetniško zbornico Slovenije, da jim le-ta določi pooblaščeno osebo. Precejšnje število odvetnikov sicer ne izvaja sistematičnih obdelav osebnih podatkov kot njihove temeljne dejavnosti in tako ne bodo potrebovali pooblaščene osebe, kar pa bodo morali samostojno presoditi glede na njihovo dejansko situacijo. Posebni peti odstavek je določen tudi za notarje (javna služba po drugem odstavku 137. člena Ustave Republike Slovenije), omogoča, da lahko notarji v dogovoru z Notarsko zbornico Slovenije določijo skupno pooblaščeno osebo, ni pa nujno da je zaposlena na Notarski zbornici Slovenije.

K 38. členu:

Predlagani člen določa naloge pooblaščene osebe za varstvo podatkov. Po prvem odstavku pooblaščena oseba opravlja naloge iz člena 39 Splošne uredbe, zlasti pa glede ocene tveganj obdelav osebnih podatkov v zbirkah. Po drugem odstavku pooblaščena oseba sodišča ali državnega tožilstva ne sme opravljati navedenih nalog v zvezi z obdelavami osebnih podatkov, izvršenih v okviru izvajanja neodvisnega sodniškega odločanja oziroma izvajanja neodvisnega sodnega postopka (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[69] (3. člen) in Zakon o državnem tožilstvu[70] (19. člen). Pooblaščena oseba sme opravljati te naloge samo glede zadev sodne uprave (npr. kadri, finance, poslovna razmerja) in državnotožilske uprave ter glede izvajanja varnosti osebnih podatkov. Prav tako je za izvršitelje in za stečajne upravitelje določeno, da jim ni treba imenovati pooblaščene osebe za obdelave osebnih podatkov, ki jih opravljajo za izvrševanje neodvisnega sodniškega odločanja ali po odredbi sodišča. Izvršitelji in stečajni upravitelji veljajo nekako za ti. »podaljšano roko sodišč s splošno pristojnostjo«. Tako stečajni upravitelj ni stranka postopka, pač pa organ postopka zaradi insolventnosti, ki je pri opravljanju dejanj zaradi insolventnosti podrejen drugemu procesnemu organu sodišča, to je sodniku, ki oblastno vodi (!) stečajni postopek[71]. Stečajni upravitelj ima položaj organa v stečajnem postopku. Stečajni postopek predstavlja sodni postopek, ki je namenjen predvsem zagotavljanju varstva upnikov stečajnega dolžnika in zagotavljanju čim višjega poplačila njihovih terjatev do stečajnega dolžnika. Vodenje tega postopka pod sodnim nadzorom mora že v principu vsem udeležencem postopka zagotavljati zakonitost samega postopka in s tem spoštovanje načela pravne države (2. člen Ustave Republike Slovenije) v teh postopkih. Vloga stečajnega upravitelja je dvojna, je tako zakoniti zastopnik stečajnega dolžnika in hkrati eden od

[69] Uradni list RS, št. 94/07 – uradno prečiščeno besedilo, 45/08, 96/09, 86/10 – ZJNepS, 33/11, 75/12 – ZSPDSLS-A, 63/13, 17/15 in 23/17 – ZSSve.
[70] 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.
[71] Glejte sklep Višjega sodišča v Ljubljani, opr. št. Cst 12/2016, 13. 1. 2016.

organov stečajnega postopka, poleg tega pa je glede njegovega delovanja veljavno tudi merilo javnega zaupanja[72].

Izvršitelj pa je nosilec javnih pooblastil in opravlja javno službo. Njegova uradna opravila določa Zakon o izvršbi in zavarovanju, ki določa tudi nadzor nad delom izvršitelja in pogoje za imenovanje in razrešitev. Izvršitelju že zakon določa dolžnost pridobiti vrsto osebnih podatkov o dolžniku, ki so nujno potrebni za uspešno izvedbo izvršbe (glejte 4. člen Zakona o izvršbi in zavarovanju). Pridobitev in obdelava teh podatkov so neločljivi del njegove javne službe, ki jo mora opravljati skladno z Zakonom in Pravilnikom o službi izvršitelja, ki podrobneje tudi določa način vodenja teh podatkov. Nadzor nad njegovih delom/poslovanjem opravlja Ministrstvo za pravosodje, nadzor nad njegovih delom v konkretnih sodnih postopkih pa je tudi predmet sodne kontrole (preko zahteve za odprave nepravilnosti, ki jo imajo stranke sodnega postopka). Z vidika ustavnega prava je stališče ustavnosodne presoje glede delovanja izvršitelja naslednje: »15. […] Iz ustave ne izhaja zahteva, da bi vsa **(materialna) dejanja v okviru sodnega postopka**[73] moral opraviti sodnik. Pri dejanjih neposrednega opravljanja izvršbe ne gre za sojenje kot odločanje o spornih pravicah in obveznostih, zato z vidika skladnosti z Ustavo ureditev, da ta dejanja opravljajo (zasebni) izvršitelji ni sporna. […]«[74] Bistven del te odločbe, zakaj priznati izjemo glede določitve pooblaščenih oseb tudi za izvršitelje je, da delujejo kot del (za potrebe uradnega izvajanja) sodnega postopka in po odredbi sodnika ali sodnice.

Za Ustavno sodišče Republike Slovenije pa je primerljivo (kot za neodvisna sodišča) v tretjem odstavku določeno, da pooblaščena oseba Ustavnega sodišča Republike Slovenije ne sme opravljati navedenih nalog v zvezi z obdelavami osebnih podatkov, izvršenih v okviru odločanja Ustavnega sodišča Republike Slovenije, kot jih opredeljujejo Zakon o ustavnem sodišču ali drugi zakoni (npr. drugi odstavek 5.č člena Zakona o referendumu in ljudski iniciativi). Pooblaščena oseba sme opravljati te naloge samo glede zadev sodne uprave Ustavnega sodišča (sodna uprava Ustavnega sodišča ter tudi zadeve s področja odločanja upravne seje Ustavnega sodišča) ter glede izvajanja varnosti osebnih podatkov.

Po četrtem odstavku pooblaščena oseba Varuha človekovih pravic ne sme opravljati navedenih nalog v zvezi z obdelavami osebnih podatkov, izvršenih v okviru delovanja Varuha človekovih pravic, kot jih opredeljuje Zakon o varuhu človekovih pravic ali drug zakon, ki ureja pristojnosti ali naloge varuha človekovih pravic (npr. 5. člen izvedbenega dela Zakona o ratifikaciji Opcijskega protokola h Konvenciji proti mučenju in drugim krutim, nečloveškim ali poniževalnim kaznim ali ravnanju[75]). Varuh ima namreč položaj posebnega ustavnega organa (159. člen Ustave Republike Slovenije) ki kot *sui generis* ustavni organ izven trodelbe vej oblasti neoblastveno izvaja nadzor glede uresničevanja in varstva človekovih pravic ter temeljnih svoboščin v Republiki Sloveniji in to neodvisno in samostojno (4. člen Zakona o varuhu človekovih pravic). Pooblaščena oseba za varstvo podatkov Varuha človekovih pravic sme opravljati te naloge samo glede zadev obdelav osebnih podatkov s področja zagovorništva otrok – 25.a-25.d člen Zakona o varuhu človekovih pravic (glede na posebno občutljivost področja ter dejstvo, da ne gre za običajno nadzorno vlogo Varuha človekovih pravic, ampak za ti. »upravno pomožno delovanje« Varuha človekovih pravic) ter glede izvajanja varnosti osebnih podatkov.

K 39. členu:

V predlogu člena so glede na posebne ustavne položaje ali določene ustavne vrednote določena pravila glede določitve pooblaščenih oseb za varstvo osebnih podatkov pri posameznih državnih organih.

V prvem odstavku najprej določeno, da na Ustavnem sodišču Republike Slovenije Ustavno sodišče določi eno pooblaščeno osebo, ki opravlja naloge v skladu s tretjim odstavkom 38. člena predloga zakona. V drugem odstavku je določeno, da mora Vrhovno sodišče Republike Slovenije določiti (le)

[72] Glejte sklep Višjega sodišča v Ljubljani, opr. št. Cst 426/2017, 25. 7. 2017.
[73] Poudarilo Ministrstvo za pravosodje.
[74] Glejte odločba US, št. U-I-339/98, 21. 1. 1999; objava: Uradni list RS, št. 72/98, Uradni list RS, št. 11/99 in OdlUS VIII, 13.
[75] Uradni list RS, št. 114/06 – Mednarodne pogodbe, št. 20/06.

eno pooblaščeno osebo, ki opravlja naloge za vsa sodišča s splošno pristojnostjo in specializirana sodišča v Republiki Sloveniji – torej centralizirani pristop. V tretjem odstavku je določen centraliziran pristop tudi za vsa državna tožilstva ter za Državnotožilski svet, da namreč Vrhovno državno tožilstvo Republike Slovenije določi eno pooblaščeno osebo, ki opravlja naloge pooblaščene osebe zakona za vsa državna tožilstva v Republiki Sloveniji ter za Državnotožilski svet kot samostojni pravosodni državni organ. V četrtem odstavku je določeno, da Varuh človekovih pravic (kot državni organ) določi eno pooblaščeno osebo, ki opravlja naloge v skladu s četrtim odstavkom 50. člena tega zakona.

V četrtem odstavku je določeno strogo pravilo, po katerem mora vsak minister ali ministrica določiti svojo pooblaščeno osebo, ki je zaposlena na tem ministrstvu – v tem primeru se upošteva pravilo ministrske odgovornosti ter povezane parlamentarne odgovornosti ministrov (drugi stavek 110. člena in drugi stavek prvega odstavka 114. člena Ustave Republike Slovenije in 4. člen Zakona o Vladi Republike Slovenije[76]). Za organe v sestavi ministrstev je določeno, da se lahko določi posebno pooblaščeno osebo, kar bo v praksi verjetno veljalo le za večje organe v sestavi.

Za področja obveščevalno-varnostne dejavnosti je v petem odstavku določeno, da predstojnik organizacije (Slovenska obveščevalno-varnostna agencija, Obveščevalno varnostna služba Ministrstva za obrambo) s tega področja določi eno pooblaščeno osebo in njenega namestnika znotraj organizacije s tega področja, ki opravlja tiste naloge iz člena 39 Splošne uredbe, za katere tako določi predstojnik, med njih pa so po zakonu obvezno vključene naloge glede izvajanja varnosti osebnih podatkov ter posredovanja osebnih podatkov Vladi Republike Slovenije, Predsedniku Republike Slovenije, policiji, državnim tožilstvom ali sodiščem ali pristojnemu delovnem telesu Državnega zbora Republike Slovenije, čezmejne obdelave in prenosi osebnih podatkov.

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

K 40. členu:

Prvi odstavek predlaganega člena določa, da morata upravljavec ali obdelovalec pooblaščeni osebi zagotovita pogoje za učinkovito in neodvisno opravljanje njenih nalog po 38. členu ZVOP-2, zlasti, da je pooblaščena oseba:

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

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

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

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

5. da ima neposredni dostop do vodstva upravljavca ali obdelovalca, če oceni, da je to zaradi pomembnosti določene obdelave osebnih podatkov nujno potrebno, zlasti kadar gre za tvegane obdelave, obdelave posebnih vrst osebnih podatkov, podatke iz 13. člena ZVOP-2, množične obdelave in vpliv na človekove pravice, temeljne svoboščine ali interese posameznikov, na katere se nanašajo osebni podatki ali za očitno neustreznost ukrepov zavarovanja osebnih podatkov, neposredni dostop vključuje možnost predstavitve stališč ali ocen o neustreznosti varstva osebnih podatkov.

Po drugem odstavku morata upravljavec ali obdelovalec zagotoviti, da pooblaščena oseba pri izvajanju svojih nalog ne prejema nobenih navodil. Pooblaščena oseba o svojem izvedenem delu

[76] 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.

neposredno in neodvisno poroča vodstvu upravljavca ali obdelovalca (omogočen torej neposreden neoviran pristop ter zagotovljen neodvisen način dela).

Po tretjem odstavku ima pooblaščena oseba pravico da kadarkoli zahteva njeno razrešitev z navedbo konkretnih razlogov. Predlagana ureditev je en od elementov zagotavljanja neodvisnega delovanja pooblaščenih oseb.

K 6. poglavju – kodeksi ravnanja in certifikacija

Kodeksi ravnanja ter certifikacija sta prav tako nova instituta v domačem pravu varstva osebnih podatkov. Z njima se uvaja dodatne možnosti samoregulacijo upravljavcev na področju osebnih podatkov, še zlasti v dejavnostih, kjer je že sedaj prisotne veliko samoregulacije.

Modernizacija pravil varstva osebnih podatkov ima za posledico tudi, da so postala ta pravila znatno številčnejša, obsežnejša in vse bolj zapletena. Temu primerno se povečuje tudi potreba po nadzoru nad izvrševanjem teh pravil, ki pa jih, glede na vseprisotnost in obsežnost obdelav osebnih podatkov v današnji družbi, ni v celoti več mogoče zagotoviti skozi delo državnega nadzornega organa (Informacijski pooblaščenec).

Posledično se po zgledu številnih drugih področjih državno regulacijo dopolnjuje z instrumenti samoregulacije, kot so prostovoljne zaveze podjetij, da bodo pri svojem poslovanju spoštovala določene kodekse ravnanja, oziroma, da bodo svoje poslovne procese predala v neodvisno zunanjo revizijo certifikacijski agenciji, ki jim bo v primeru skladnosti tudi izdaja ustrezni certifikat. Takšna potrdila imajo številne prednosti; poleg olajšanega izvajanja inšpekcijskega nadzora predvsem vzbujajo zaupanje posameznikov, na katere se nanašajo osebni podatki, da upravljavci oziroma obdelovalci njihove podatke obdelujejo v skladu s pravili, ter da temu posvečajo zadostna sredstva.

Ta razdelek predloga zakona ureja obe pojavni obliki takšne samoregulacije, in sicer tako kodekse ravnanja kot tudi certifikacijo. Pri kodeksih ravnanja sicer ne implementira možnosti zunanjega nadzora s strani pooblaščenih organizacij. Pri certifikaciji to prepušča tako Informacijskemu pooblaščencu kot morebitnim zunanjim certifikacijskim organizacijam, ki jih za to pooblasti nacionalni akreditacijski organ (Slovenska akreditacija). Za vsebine certifikacij (standarde) se v veliki meri zanaša na standarde, sprejete na evropski ravni, in odobrene s strani Informacijskega pooblaščenca

Kodeksi ravnanja so tako avtonomne zbirke dobrih praks za varstvo osebnih podatkov na določenih poslovnih področjih (npr. neposrednem trženju, zdravstvu, šolstvu, športu, idr.), ki jih pripravijo področna združenja na teh področjih, dajo potrditi pri Informacijskem pooblaščencu, nato pa priporočijo za rabo svojim članom. Njihova raba je povsem prostovoljna, njihova glavna prednost pa je, da lahko v znatni meri zagotovi skladnost obdelav s pravili Splošne uredbe, oziroma da v primeru nadzora Informacijskega pooblaščenca znatno olajšajo dokazovanje takšne skladnosti. Zakon ureja zlasti postopek potrjevanja teh kodeksov.

Še za stopnjo večjo veljavo pa ima **certificiranje**, ki pomeni predložitev praks obdelave osebnih podatkov v zunanjo recenzijo neodvisni instituciji, ter pridobitev ustreznega certifikata. Zakon ureja pogoje za oblikovanje certifikacijskih mehanizmov na področju varstva osebnih podatkov, ter za akreditacijo certifikacijskih organov pri domačem akreditacijskem organu (Slovenska akreditacija).

K 41. členu:

V predlaganem členu se tako ureja kodekse ravnanja - podana je pravna podlaga, ki omogoča uporabo kodeksov ravnanja, tj. pravil dobre prakse na področju posameznih vrst obdelav osebnih podatkov, ki jih pripravijo relevantna domača ali tuja združenja podjetij v določenem sektorju, in so že prilagojena posebnostim manjših, srednjih oziroma večjih podjetij. Člen predvideva uporabo kodeksov, ki so potrjeni na različnih nivojih nadzornih organov; tako s strani posameznega državnega nadzornega organa, kot tudi širše, s strani Evropskega Odbora za varstvo osebnih podatkov po členu 68 Splošne uredbe kot s strani Evropske komisije. Pri tem Evropska komisija potrjuje tiste kodekse, ki se nanašajo na obdelave, ki potekajo v več državah članicah, pri čemer mora predhodno pridobiti tudi mnenje Odbora.

Člen hkrati ne preprečuje, da ne bi mogel Informacijski pooblaščenec razveljaviti uporabe določenega kodeksa, če oceni, da ni oziroma da ni več ustrezen. Navedeno izhaja iz sodbe Sodišča Evropske unije v *primeru Maximillian Schrems* (ozir. ti. *Facebook primer*)[77], 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 42. členu:

V predlaganem členu se ureja certificiranje obdelav osebnih podatkov. V prvem odstavku je tako določena definicija certificiranja, ki za potrebe tega zakona pomeni prostovoljni postopek ugotavljanja, ali so dejanja obdelave osebnih podatkov s strani upravljavcev in obdelovalcev skladna z merili iz določenega mehanizma certificiranja (vsebinski kriterij) ter da se o ugotovitvi takšne skladnosti se upravljavcu ali obdelovalcu izda certifikat (oblastveni kriterij). Predmet certificiranja je lahko zbirka, njena delovanja obdelave ter informacijski sistem - Klub zvestobe trgovinske gospodarske družbe, sistem SISBON, eAsistent informacijski sistem za šole, informacijski sistem za bolnišnico.

Po drugem odstavku merila posameznega certifikacijskega mehanizma odobri z odločbo Informacijski pooblaščenec v skladu s petim odstavkom člena 42 Splošne uredbe ali Evropski Odbor za varstvo osebnih podatkov v skladu s petim odstavkom člena 42 Splošne uredbe ter v zvezi s členom 63 Splošne uredbe. Zoper odločbo Informacijskega pooblaščenca iz prejšnjega stavka pritožba ni dopustna, je pa dopusten upravni spor pred Upravnim sodiščem Republike Slovenije.

Po predlaganem tretjem odstavku se izdani certifikat lahko uporabi za izkazovanje, da so dejanja obdelave osebnih podatkov s strani upravljavca ali obdelovalca skladna s Splošno uredbo, pri čemer pa sklicevanje na certifikat ne posega v odgovornosti upravljavca ali obdelovalca za skladnost njunih delovanj obdelave osebnih podatkov s Splošno uredbo in ne posega v naloge in pristojnosti Informacijskega pooblaščenca za ugotavljanje te skladnosti.

Po četrtem odstavku Informacijski pooblaščenec pripravlja in upravlja seznam pravnomočnih certifikacijskih mehanizmov, ki jih je odobril in ta seznam sprotno objavlja na svoji spletni strani.

K 43. členu:

V predlaganem členu se v skladu s 121. členom Ustave Republike Slovenije 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[78] (torej tudi pooblastilo na podlagi zakona). Dodatne zahteve glede certifikacije v skladu s točko b prvega odstavka in tretjim odstavkom člena 43 Splošne uredbe določi Informacijski pooblaščenec.

Po drugem odstavku pred izdajo pooblastila zunanjemu certifikacijskemu telesu Slovenska akreditacija v skladu s prvim odstavkom člena 43 Splošne uredbe o vlogi zainteresiranega subjekta obvesti Informacijskega pooblaščenca, ki preveri izpolnjevanje dodatnih zahtev v skladu s točko b prvega odstavka in tretjim odstavkom člena 43 Splošne uredbe in o tem izda odločbo. Zoper to odločbo pritožba ni dopustna, je pa dopusten upravni spor pred Upravnim sodiščem Republike Slovenije.

Po tretjem odstavku Slovenska akreditacija na lastno pobudo ali na predlog Informacijskega pooblaščenca prekliče pooblastilo za certificiranje zunanjemu certifikacijskemu telesu, če je ugotovljeno, da pogoji za pooblastilo niso ali niso več izpolnjeni, ali, da so bili ukrepi, ki jih je v postopku certifikacije izvedlo pooblaščeno certifikacijsko telo, v neskladju s Splošno uredbo.

Predlagan je torej spodbujevalni mehanizem za varstvo osebnih podatkov, ki je le na razpolago in katerega je šteti, da utegne trajati daljše obdobje, preden bo v Republiki Sloveniji dejansko uporaben.

[77] Sodba SEU, C-362/14, 6. 10.2015.
[78] Uradni list RS, št. 59/99.

K 7. poglavju – Nadzorni organ za varstvo osebnih podatkov Republike Slovenije

7. poglavje I. dela predloga zakona ureja položaj in temeljne pristojnosti in naloge Informacijskega pooblaščenca kot nadzornega organa za varstvo osebnih podatkov Republike Slovenije, tako njegove nadzorne pristojnosti, vključno s preiskovalnimi pristojnostmi, sodelovalne pristojnosti in svetovalne naloge.

K 44. členu:

Predlagani 44. člen predloga zakona v prvem odstavku ponovno potrjuje obstoječe in ustrezno stanje, da je nadzorni organ za varstvo osebnih podatkov Republike Slovenije Informacijski pooblaščenec, kot ga določa Zakon o informacijskem pooblaščencu[79]. Informacijski pooblaščenec je (javnopravno) samostojni in neodvisni državni organ (ki pa nima funkcije tribunala, saj o njegovih odločitvah razsojajo Upravno sodišče Republike Slovenije ali prekrškovni oddelki okrajnih sodišč). Nadalje je v drugem odstavku določeno, da pri Informacijskem pooblaščencu delujejo poleg informacijskega pooblaščenca in namestnikov tudi državne nadzornice oziroma državni nadzorniki za varstvo osebnih podatkov, ki opravljajo pristojnosti inšpekcijskega nadzora in druge naloge glede varstva osebnih podatkov po določbah Splošne uredbe, ZVOP-2 in drugih zakonov ali predpisov. V tretjem odstavku je določeno, da imajo informacijski pooblaščenec (funkcionar, predstojnik tega državnega organa) in njegovi namestniki enaka pooblastila in pristojnosti, kot velja za nadzornike iz prejšnjega odstavka – torej vsi lahko izvajajo nadzore glede varstva osebnih podatkov. Četrti odstavek pa določa, da ima tudi določeno strokovno osebje Informacijskega pooblaščenca enaka pooblastila in pristojnosti, kot to velja za nadzornike, če izpolnjuje pogoje za delo nadzornika, seveda če informacijski pooblaščenec to posamično določi. V tem primeru opravljajo pristojnosti inšpekcijskega nadzora. Peti odstavek določa, da so informacijski pooblaščenec, njegovi namestniki, državni nadzorniki ter strokovno osebje iz četrtega odstavka uradne osebe – kadar izvršujejo nadzorne pristojnosti in pooblastila po tem predlogu zakona. Podana je tudi skupna okrajšava, ki se nadalje uporablja: nadzorne osebe.

K 45. členu:

V 45. členu ZVOP-2 so določene temeljne pristojnosti Informacijskega pooblaščenca. V prvem odstavku je določeno, da Informacijski pooblaščenec samostojno in neodvisno[80] 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 določeno, da je Informacijski pooblaščenec pristojen za inšpekcijske nadzore in čezmejne inšpekcijske nadzore.

V petem 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 46. členu:

[79] Uradni list RS, št. 113/05 in 51/07 – ZUstS-A.
[80] Glejte: Pirc Musar, Nataša, *Neodvisni nadzor in varstvo osebnih podatkov*, Pravna praksa, št. 35/2006, str. 6-10.

V predlaganem 46. členu so določene izjeme glede pristojnosti Informacijskega pooblaščenca glede dometa inšpekcijskih nadzorov na določenih sistemskih področjih. Namreč glede tistih obdelav osebnih podatkov, izvršenih v okviru izvajanja neodvisnega sodniškega odločanja, kot to opredeljuje Zakon o sodiščih (3. člen), odločanja strokovnih sodelavcev in sodniških pomočnikov po odredbah sodnika, kot to tudi opredeljuje Zakon o sodiščih (53.a člen in drugi odstavek 54. člena)[81] ali po določbah drugih zakonov, ki določajo njihovo samostojno delovanje (brez posebne odredbe sodnika[82]), nato obdelav osebnih podatkov, izvršenih v okviru opravljanja samostojne državnotožilske funkcije po Zakonu o državnem tožilstvu (vsebine iz 19. člena v zvezi s 3. členom, vendar omejeno – kot je določeno v predlagani zakonski določbi, zlasti osredotočenje na odločanje o kazenskem pregonu in njegovo uveljavljanje, vključno z nastopanjem na sodiščih), obdelav osebnih podatkov, izvršenih v okviru odločanja Ustavnega sodišča Republike Slovenije, kot jih opredeljujejo Zakon o ustavnem sodišču (21. člen).

Po drugem odstavku lahko Informacijski pooblaščenec vpogleda (pomeni da je pristojen za inšpekcijski nadzor) tudi v vso dokumentacijo Varuha človekovih pravic, predkazenskega postopka ali obveščevalno-varnostne dejavnosti, zaščitenih prič, prijaviteljev korupcije ter varnostnega preverjanja. Ne glede na tretji in četrti odstavek prejšnjega člena pa Informacijski pooblaščenec pri opravljanju inšpekcijskega in prekrškovnega nadzora na navedenih področjih sme zabeležiti identifikacijskih osebnih podatkov oziroma kopirati nobene dokumentacije glede obdelav osebnih podatkov, izvršenih v okviru nadzornega delovanja Varuha človekovih pravic, kot jih opredeljujejo zakoni, ki določajo njegove pristojnosti ali pooblastila, razen glede obdelav osebnih podatkov s področja zagovorništva otrok, obdelav osebnih podatkov na področjih predkazenskega postopka ali obveščevalno-varnostne dejavnost, samo v delu, kjer je izvedena identifikacija zapisana tajnih delavcev oziroma sodelavcev v skladu z zakonom, ki ureja kazenski postopek, zakonom, ki ureja obrambo, ali zakonom, ki ureja Slovensko obveščevalno-varnostno agencijo, obdelav osebnih podatkov na področju zaščitenih prič v skladu z zakonom, ki ureja zaščito prič, samo v delu, kjer je izvedena identifikacija zaščitene priče, ali prijaviteljev korupcije po zakonu, ki ureja integriteto in preprečevanje korupcije ter obdelav osebnih podatkov varnostno preverjanih oseb v skladu z zakonom, ki ureja tajne podatke samo v delu, kjer je izvedena identifikacija virov ugotavljanja oziroma preverjanja prejetih osebnih podatkov, ki jih organom, pristojnim za varnostno preverjanje, posredujejo pristojni organi v skladu z zakonom, ki ureja obrambo, ali zakonom, ki ureja Slovensko obveščevalno-varnostno agencijo.

Glede sodne oblasti nadzor glede varstva osebnih podatkov v zvezi s sodnim odločanjem preprečujejo ustavne določbe, konvencijske določbe ter določbe Splošne uredbe – namreč neodvisno odločanje sodstva (prvi odstavek 23. člena in 125. člen Ustave Republike Slovenije, prvi odstavek 6. člena Evropske konvencije o človekovih pravicah ter tretji odstavek člena 55 Splošne uredbe). Podobno (primerljivo) velja za državna tožilstva glede na samostojnost državnih tožilcev po 135. členu Ustave Republike Slovenije, saj gre po ustavnosodni presoji za delno primerljiv (funkcionalno) samostojni sistem[83] napram sistemu neodvisnega sodnega odločanja – zlasti v delu, ki se nanaša na kazenski pregon.

Pri izjemah glede nadzora v zvezi z varstvom osebnih podatkov v razmerju do Varuha človekovih pravic se izhaja iz spoštovanja *sui generis* ustavnega položaja Varuha človekovih pravic po 159. členu Ustave Republike Slovenije in njegove neoblastne nadzorne funkcije[84].

[81] Tudi v skladu z omejitvami ne-sodniškega odločanja v razmerju do pristojnosti neodvisnih sodnikov iz sodbe Evropskega sodišča za človekove pravice v primeru *Ezgeta proti Hrvaški*, št. 40562/12, 7. 9. 2017, zlasti razdelki 38.-45. sodbe.

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

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

[84] Sklep Upravnega oddelka Vrhovnega sodišča RS, opr. št. I Up 231/2016, 1. 2. 2017: »11. Delovanje Varuha niti z vidika splošne opredelitve njegovih nalog in pristojnosti niti z vidika ravnanja v konkretnem primeru očitno ne ustreza značilnostim oblastvenega delovanja. Njegovo ravnanje je usmerjeno v nadzor nad delovanjem nosilcev oblasti in se tudi izraža v ukrepih, ki so usmerjeni prav zoper navedene oblastvene subjekte in ne druge osebe, nosilce človekovih pravic in temeljnih svoboščin. …«

Po tretjem odstavku je Informacijski pooblaščenec ne glede na prvi odstavek tega člena pristojen za opravljanje inšpekcijskega nadzora z vsemi ostalimi delovnimi področji organov ali funkcionarjev iz prvega odstavka, zlasti v zvezi z zadevami sodne uprave, državnotožilske uprave, uprave Ustavnega sodišča Republike Slovenije ter glede izvajanja ukrepov in postopkov s področja varnosti osebnih podatkov ter sledljivosti obdelav in posredovanj osebnih podatkov šestem odstavku 30. člena in 7. točki drugega odstavka 26. člena predloga zakona glede vseh državnih organov iz prvega odstavka tega člena, razen če gre za izmenjave podatkov med sodišči in med državnimi tožilstvi. Navedena področja ne spadajo med temeljna »odločevalna« oziroma »oblastvena« področja navedenih državnih organov oziroma so nekoliko bolj tehnične narave in je ta zakonodajni pristop (polna nadzorna pristojnost Informacijskega pooblaščenca) upravičen. Prav tako ni za izločena področja sodnega delovanja, ki so izločena po prvem odstavku, predlagan kakšen poseben (*sui generis*) nadomestni nadzorni sistem (mehanizem) glede varstva osebnih podatkov (npr. poseben organ pri Sodnem svetu), saj se npr. za sodstvo šteje, da je presoja zakonitosti obdelave določenih osebnih podatkov v sodnih postopkih del običajne postopkovne zakonodaje v zvezi z uporabo pravnih sredstev oziroma vprašanje dokaznega prava.

Ne glede na navedeno izbrana izločena področja po prvem odstavku ne ostanejo brez zunanjega nadzora glede posegov v človekove pravice in temeljne svoboščine, pa četudi naknadnega (nadzor sodnega odločanja po 24. členu Zakona o varuhu človekovih pravic[85]). Varuh človekovih pravic je namreč po 159. členu Ustave Republike Slovenije ter po 1. členu Zakona o varuhu človekovih pravic poseben ustavni organ, ki na neoblastven in neformalen način izvaja nadzore na vseh[86] področjih človekovih pravic in temeljnih svoboščin.

K 47. členu:

V predlaganem 47. členu so določene naloge Informacijskega pooblaščenca glede posvetovanj o uvedbah obdelav osebnih podatkov. Po prvem odstavku Informacijski pooblaščenec daje predhodna mnenja ministrstvom Vlade Republike Slovenije, Državnemu zboru Republike Slovenije ter Državnemu svetu Republike Slovenije o usklajenosti določb predlogov zakonov, podzakonskih aktov ter drugih predpisov z ZVOP-2, Splošno uredbo in drugimi zakoni ter predpisi, ki urejajo osebne podatke. Kadar se vrste obdelav, ki jih ureja predlagani predpis, nanašajo na situacije iz 27. člena predloga zakona, mora predlagatelj predpisa v okviru posvetovanja Informacijskemu pooblaščencu predložiti tudi oceno učinka iz sedmega odstavka člena 25. člena Splošne uredbe. V četrtem odstavku je določeno, da kadar zakon določa, da Informacijski pooblaščenec poda soglasje k predlogu predpisa, se smiselno uporabljajo določbe drugega odstavka. V tretjem odstavku je z vidikov načel transparentnosti in legitimnosti določeno, da mora biti Mnenje Informacijskega pooblaščenca del javno dostopnega gradiva predloga predpisa iz prvega odstavka tega člena, skupaj z odzivom organa ali nosilca javnega pooblastila. V šestem odstavku je določeno, da lahko Informacijski pooblaščenec samostojno odloči, da posreduje tudi naknadno mnenje organu ali nosilcu javnega pooblastila iz prvega odstavka tega člena, če oceni, da je bilo njegovo mnenje neutemeljeno neupoštevano (npr. v postopku obravnave predloga zakona v Državnem zboru Republike Slovenije).

K 48. členu:

Predlagani 48. 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

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

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

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 62. členu 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 5. člena predloga zakona. Tako so člani (vodstvo, funkcionarji) ali strokovno osebje (javni uslužbenci) nadzornega organa druge države članice Evropske unije dolžni izvajati nadzor tako, da nadzor vodi Informacijski pooblaščenec (so začasno del njegove »ekipe«). Člani ali osebje drugega nadzornega organa krijejo svoje stroške.

V četrtem odstavku je urejena nasprotna situacija, če Informacijski pooblaščenec (funkcionar, namestniki ali državni nadzorniki) izvajajo skupni nadzor na ozemlju druge države članice Evropske unije ali v okviru njenih pristojnosti (pristojnosti njenega nadzornega organa za varstvo osebnih podatkov). Tudi v tem primeru vodi nadzor nadzorni organ druge (pristojne) države članice, predstavniki Informacijskega pooblaščenca pa krijejo svoje stroške skupnega nadzora.

K 49. členu:

Predlagani 49. 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 50. členu:

V 50. členu je določen obseg inšpekcijskega nadzora, po katerem v njegovem okviru nadzorni organ Informacijski pooblaščenec (torej nadzorne osebe) izvajajo naslednja delovanja:

nadzorujejo skladnost obdelave osebnih podatkov z določbami Splošne uredbe, tega zakona in drugih predpisov, ki urejajo obdelavo osebnih podatkov.

K 51. členu:

V 51. členu je določeno neposredno opravljanje inšpekcijskega nadzora s strani državnih nadzornikov, informacijskega pooblaščenca in namestnikov informacijskega pooblaščenca ter tudi strokovnega osebja (če izpolnjuje pogoje za nadzornike) v mejah pristojnosti Informacijskega pooblaščenca (kot državnega nadzornega organa po tem zakonu, Zakonu o Informacijskem pooblaščencu in drugih zakonih). Po drugem odstavku se sme oddaljeni (posredni) nadzor izvajati samo v primerih in pod pogoji iz tega zakona.

K 52. členu:

Po predlaganem 52. členu nadzorne osebe izkazujejo pooblastilo in svojo identiteto (namen obdelave osebnih podatkov) za opravljanje nalog inšpekcijskega nadzora s službeno izkaznico, ki vsebuje fotografijo nadzornika, informacijskega pooblaščenca ali namestnika informacijskega pooblaščenca, njegovo osebno ime, strokovni ali znanstveni naslov ter navedbo organa in pooblastil. Obliko in vsebino službene izkaznice podrobneje predpiše minister za pravosodje v podzakonskem predpisu.

K 53. členu:

V 53. členu so glede na 49. člen predloga zakona podrobneje urejena preiskovalna pooblastila Informacijskega pooblaščenca, ozir. njegovih uradnih oseb (državni nadzornik, namestniki informacijskega pooblaščenca, informacijski pooblaščenec ter strokovno osebje Informacijskega pooblaščenca, ki izpolnjuje pogoje za nadzornika in je za dejanja nadzora posamično pooblaščeno) upravičeni:

Predlagani člen tako ureja pooblastila nadzornih oseb v okviru postopkov inšpekcijskega nadzora, tj. postopkov nadzora nad spoštovanjem skladnosti obdelave osebnih podatkov s pravili Splošne uredbe ter določbami tega zakona in drugih zakonov, ki urejajo obdelavo in varstvo osebnih podatkov.

Prvi odstavek določa, da lahko nadzorna oseba pri opravljanju inšpekcijskega nadzora poleg uporabe preiskovalnih pooblastil iz prvega odstavka 58. člena Splošne uredbe oziroma pooblastil po zakonih, ki urejata inšpekcijski postopek ter splošni upravni postopek, tudi:

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

2. pregleduje poslovne knjige, pogodbe, listine, poslovno korespondenco, poslovne evidence in druge podatke, ki se nanašajo na obdelavo osebnih podatkov s strani upravljavca ali obdelovalca samega ali druge pravne ali fizične osebe po njunem pooblastilu, oziroma na prenos osebnih podatkov v tretjo državo ali posredovanje uporabnikom osebnih podatkov iz tretjih držav s strani upravljavca ali obdelovalca oziroma druge pravne ali fizične osebe po njunem pooblastilu (v nadaljnjem besedilu: poslovne knjige in druga dokumentacija), ne glede na njihovo tajnost ali drugo vrsto zaupnosti ter ne glede na nosilec, na katerem so zapisani ali shranjeni;

3. vstopi in pregleduje prostore, zemljišča, prevozna sredstva in opremo in sredstva za obdelavo osebnih podatkov (v nadaljnjem besedilu: prostori in oprema), v oziroma s katerimi upravljavec ali obdelovalec sam ali drugo podjetje ali posameznik po njunem pooblastilu opravlja obdelavo osebnih podatkov, za katero izhaja verjetnost kršitve določb tega zakona, Splošne uredbe oziroma drugih predpisov, ki urejajo varstvo osebnih podatkov;

4. zavaruje in pregleduje elektronske in z njimi povezane naprave ter nosilce elektronskih podatkov, vključno s preko omrežja dosegljivimi informacijskimi sistemi, na katerih so shranjeni podatki (v nadaljnjem besedilu: elektronska naprava), glede katerih izhaja verjetnost, da se na njih nahajajo podatki, iz katerih izhaja verjetnost kršitve določb tega zakona, Splošne uredbe oziroma drugih predpisov, ki urejajo varstvo osebnih podatkov (dokazni standard);

5. odvzame ali pridobi ustrezne kopije, forenzične kopije ali izvlečke iz poslovnih knjig in druge dokumentacije v kakršni koli obliki z uporabo fotokopirnih sredstev ter računalniške opreme upravljavca ali obdelovalca oziroma Informacijskega pooblaščenca. Če zaradi tehničnih ali časovnih razlogov ni mogoče narediti kopij na kraju samem, lahko odnese poslovne knjige in drugo dokumentacijo za čas, potreben, da se naredijo kopije. O tem naredi uradni zaznamek;

6. zapečati poslovne prostore ter poslovne knjige in drugo dokumentacijo za čas trajanja postopka in v obsegu, potrebnem za njegovo izvedbo. O tem se naredi uradni zaznamek.

7. zaseže predmete ter poslovne knjige in drugo dokumentacijo za največ 20 delovnih dni, če je to potrebno za izvedbo postopka. O tem naredi potrdilo o zasegu, v katerem mora biti navedeno, kateri predmeti so bili zaseženi, njihov opis, navedba kraja, kjer so bili najdeni, ter razlog za zaseg.

8. brez predhodne najave in brez navzočnosti upravljavca ali obdelovalca, njegovega zakonitega zastopnika oziroma pooblaščenca pregleduje vsebine in preveri način delovanja zavezančevih spletnih strani in drugih javno dostopnih storitev informacijske družbe, če je to nujno zaradi varovanja človekovih pravic, temeljnih svoboščin ali interesov posameznikov, na katere se nanašajo osebni podatki in obstaja utemeljena bojazen, da teh pooblastil dejanj pozneje ne bo mogoče izvesti ali da bo njegova izvedba pozneje otežkočena;

9. izvaja druga pooblastila, določena z zakonom.

Splošna uredba za pooblastila iz prejšnjega odstavka uporablja izraz »preiskovalna pooblastila«. Pri tem predvideva, da jih države članice določijo same, upoštevaje posebnosti svoje postopkovne

zakonodaje, sama pa določa zgolj njihov minimalen nabor (prvi odstavek 58. člena) ter nekatera temeljna načela za njihovo urejanje (uvodna navedba št. 129). Države morajo tako nadzornemu organu podeliti *»učinkovita pooblastila«* za opravljanje njegovih nalog, pri čemer morajo biti ta pooblastila določena tako, da se izvajajo *»nepristransko, pravično in v razumnem roku [ter] v skladu z ustreznimi postopkovnimi zaščitnimi ukrepi, določenimi v pravu Unije in pravu držav članic«*, tako da je vsak na njihovi podlagi izveden ukrep *»ustrezen, potreben in sorazmeren«*. Pri tem določa tudi minimalni nabor teh pooblastil, in sicer v prvem odstavku 58. člena.

Predlagani člen pri določanju preiskovalnih pooblastil tako izhaja iz nabora pooblastil po že omenjenem 58. členu Splošne uredbe oziroma nabora splošnih inšpekcijskih pooblastil po 19. členu Zakona o inšpekcijskem nadzoru[87]. Tam našteta nabora pa nadgrajuje še z nekaterimi dodatnimi pooblastili, ki bodo glede na prakso nekaterih drugih primerljivih organov ter glede na zahteve Splošne uredbe potrebna za učinkovito izvajanje nalog Informacijskega pooblaščenca. Glede na naravo zavezancev, ki bodo večidel gospodarske družbe, oz. glede na naravo nadzorovane dejavnosti – obdelave osebnih podatkov, torej informacij - je namreč **za računati, da bodo številna preiskovalna dejanja Informacijskega pooblaščenca nujno usmerjena v elektronsko komunikacijo članov nadzorovanega subjekta, oziroma drugih elektronskih podatkov, s katerimi razpolaga ta subjekt**. Pri tem pa se nujno odpirajo vprašanja ustavnopravne narave, kot so prostorska oz. komunikacijska zasebnost upravljavca, oziroma odvetniška zaupnost. Ta vprašanja predlog rešuje po vzoru podobnih postopkov na drugih področij, še zlasti po vzoru preiskovalnega postopka Javne agencije Republike Slovenije za varstvo konkurence po Zakonu o preprečevanju omejevanja konkurence[88], v zvezi s katerim obstaja že tudi določena (ustavno)sodna praksa.
Prvi odstavek se tako sklicuje na že omenjena obstoječa pooblastila Informacijskega pooblaščenca po Splošni uredbo oziroma ZIN, ter obenem našteva njegova dodatna pooblastila. Prva in druga alineja določata dostop do obdelovanih osebnih podatkov oziroma dokumentacije v zvezi z obdelavo osebnih podatkov, ne glede na stopnjo njune zaupnosti, kar je seveda nujni pogoj in izhodišče za izvajanje nadzora. Tretja in četrta alineja določata dostop do prostorov in opreme oz. elektronskih naprav zavezanca, kar so danes ključne tarče preiskave, zato sta seveda dodatno razdelana v nadaljnjih odstavkih. Peta do sedma alineja določajo začasni zaseg oziroma zapečatenje dokumentacije in drugih predmetov na sedežu zavezanca, kar so nujna orodja za učinkovito izvajanje bolj obsežnih inšpekcij. Osma alineja ureja posebna pravila pri nadzoru storitev zavezancev, ki so javno dostopne.

Iz narave opravljanja reguliranih dejavnosti izhaja, da imajo državni nadzorni organi pravico nenapovedanega obiska na sedežu upravljavca, vstopa v njegove poslovne prostore, pregleda dokumentacije, ter zahtevanja pooblastil. Vendar se to nanaša zgolj na predele poslovnih prostorov, ki niso skriti oz. zaprti, oz. za dokumentacijo, ki ni shranjena na elektronskih nosilcih. Ustavno sodišče je namreč glede tega že odločilo, da »*tudi pravna oseba, ki je umetna tvorba pravnega reda, namreč uživa ustavno varovano pravico do zasebnosti, ki jo sicer Ustava kot človekovo pravico zagotavlja fizičnim osebam. [..] Ustavnopravno varstvo pravice do zasebnosti pravnih oseb je sicer prilagojeno naravi te pravice in naravi pravne osebe, ki jo fizične osebe ustanovijo zaradi uresničevanja svojih pravic, na gospodarskem področju za uresničevanje pravice do svobodne gospodarske pobude. Pravna oseba uživa pravico do prostorske zasebnosti v poslovnih prostorih, ki niso splošno dostopni javnosti. [..] Državni organi smejo zato zaradi izvrševanja nadzora nad gospodarsko dejavnostjo tudi brez sodne odločbe vstopati v poslovne prostore pravnih oseb, ki niso odprti za javnost, ter si jih vizualno ogledati, brez odpiranja skritih predelov ter zasegov stvari in opreme, ki se tam nahajajo. Za dopustnost [podrobnejše preiskave] pravne osebe pa je treba prav tako zahtevati jamstvo vnaprejšnje sodne odločbe iz drugega odstavka 36. člena Ustave*«[89]. Pregled skritih delov poslovnih prostorov ali opreme, ter pregled elektronskih naprav, nosilcev, ter storitev za shranjevanje podatkov, je tako lahko dopusten le na podlagi soglasja zavezanca oziroma predhodne odredbe sodišča.

Iz tega razloga se v drugem in tretjem odstavku določa primere, ko mora Informacijski pooblaščenec pred izvedbo posameznega preiskovalnega dejanja pridobiti bodisi odredbo sodišča. V četrtem, petem

[87] Uradni list RS, št. 43/07 – uradno prečiščeno besedilo in 40/14.
[88] Uradni list RS, št. 36/08, 40/09, 26/11, 87/11, 57/12, 39/13 – odl. US, 63/13 – ZS-K, 33/14, 76/15 in 23/17.
[89] Odločba Ustavnega sodišče št. U-I-40/12 z dne 11. 4. 2013.

in šestem odstavku pa so določeni postopek izdaje te odredbe, pogoji za njeno izdajo ter pristojno sodišče, po vzoru že omenjenih Zakona o preprečevanju omejevanja konkurence, Zakona o trgu vrednostnih papirjev, oziroma deloma tudi Zakonu o kazenskem postopku. Tako mora uradna oseba v primeru, da soglasja ne more pridobiti, oziroma če vnaprej računa, da ga ne bo mogla pridobiti oziroma da bi pridobivanje soglasja lahko škodilo postopku, za preiskavo pridobiti odredbo preiskovalnega sodnika, za to pa mora izkazati visok standard utemeljenih razlogov za sum, da je nadzorovani upravljavec huje kršil pravila varstva osebnih podatkov (v smislu, da bi mu za to bilo mogoče v skladu s kriteriji iz drugega odstavka 83. člena Splošne uredbe naložiti tudi višjo globo), da se bo s predlaganih preiskovalnim ukrepom našlo dokaze o takšni kršitvi, ter da takšnih dokazov drugače ne bi bilo mogoče pridobiti (t.i. strogi test sorazmernosti). Ukrepi preiskave službene e-pošte, službenih računalnikov in strežnikov, ipd. se tako *ab initio* ne morejo uporabljata za minorne kršitve Splošne uredbe, za katere bi bilo npr. primerno, da se namesto globe izreče opomin.

Šesti in sedmi odstavek po vzoru Zakona o pravdnem postopku[90] ter Zakona o kazenskem postopku[91] določata postopek pregleda dokumentacije, ki naj bi bila zaobjeta z odvetniško zaupnostjo. Takšno dokumentacijo se zapečati, nakar se jo preda s strani sodišča imenovanemu izvedencu, ki jo pregleda in odbere dele dokumentacije, ki niso zaobjeti z odvetniško zaupnostjo. Te dele dokumentacije se izroči Informacijskemu pooblaščencu, da jih lahko pregleda, ostali del pa se vrne zavezancu.

K 54. členu:

V 54. členu so urejena popravljalna pooblastila in ukrepi državnega nadzornika za varstvo osebnih podatkov, namestnika informacijskega pooblaščenca in samega informacijskega pooblaščenca (predstojnika Informacijskega pooblaščenca). V prvem odstavku je urejeno, da imajo navedene uradne osebe, ki pri opravljanju inšpekcijskega nadzora ugotovijo kršitev določb Splošne uredbe, ZVOP-2 ali drugega zakona ali predpisa, ki ureja varstvo osebnih podatkov, pristojnost, poleg uporabe popravljalnih pooblastil iz Splošne uredbe, takoj:

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

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

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

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

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

Predlagani drugi odstavek pomeni nadgradnjo določb dosedanjega drugega odstavka 54. člena ZVOP-1[92]. Po predlaganem drugem odstavku ukrepov iz prvega odstavka ni mogoče odrediti zoper osebo, ki v elektronskem komunikacijskem omrežju opravlja storitev izključnega prenosa podatkov, vključno z začasnim shranjevanjem podatkov in drugimi delovanji v zvezi s podatki, ki so izključno v

[90] Uradni list RS, št. 73/07 – uradno prečiščeno besedilo, 45/08 – ZArbit, 45/08, 111/08 – odl. US, 57/09 – odl. US, 12/10 – odl. US, 50/10 – odl. US, 107/10 – odl. US, 75/12 – odl. US, 40/13 – odl. US, 92/13 – odl. US, 10/14 – odl. US, 48/15 – odl. US, 6/17 – odl. US in 10/17.

[91] Uradni list RS, št. 32/12 – uradno prečiščeno besedilo, 47/13, 87/14, 8/16 – odl. US, 64/16 – odl. US, 65/16 – odl. US, 66/17 – ORZKP153,154 in 1/19 – skl. US.

[92] Drugi odstavek 54. člena ZVOP-1 je bil predpisan leta 2004 kot reakcija na nekdanjo »afero udba.net« iz leta 2003 – kot ukrep preprečevanja vzpostavljanja cenzure ali preprečevanja nastanka samocenzure (ker to nedopustno posega v svobodo izražanja in v svobodo komuniciranja). Glejte tudi: Makarovic, Bostjan, *Foreign Internet content restriction in the Republic of Slovenia: Artificial borders within the Internet to protect personal data?*, Journal of Computer, Media and Telecommunications Law, Volume 8, Number 5, 2003, str. 371-374.

funkciji opravljanja ali olajšanja prenosa podatkov po omrežjih, če ta oseba sama nima interesa, povezanega z vsebino teh podatkov, in ne gre za osebo, ki lahko sama ali skupaj z omejenim krogom z njo povezanih oseb učinkovito nadzoruje dostop do teh podatkov, kot je bilo že dosedaj določeno v drugem odstavku 54. člena ZVOP-1. Ukrepa prav tako ni mogoče odrediti zoper ponudnika gostovanja, če le-ta ni bil predhodno seznanjen s protipravnostjo vsebine, ki so jo zagotovili njegovi uporabniki. Zadnji stavek še posebej poudarja zaupnost (in posredno tudi svobodo) komuniciranja, saj določa, da prejšnje določbe ne vključujejo zahteve, da bi se ponudniki gostovanja, shranjevanja ipd. morali seznaniti z vsebino podatkov, če to prepoveduje drug zakon.

Predlagana je torej ureditev, ki naj bi preprečevala nastanek zlasti slučajnega vzpostavljanja cenzure ozir. spodbujanja samocenzure (svoboda izražanja in svoboda komuniciranja)[93], posredno pa gre tudi ukrep proti vzpostavljanju ti. totalne nadzorovalne družbe. Ta varovalni ukrep je tudi nekoliko povezan z 9., 10. in 11. členom Zakona o elektronskem poslovanju na trgu[94] – sodno odrejeni »*take down*« sistem ter tudi novejša praksa na ravni Evropske unije na področjih razprav o odgovornosti ponudnikov družbenih omrežij za ti. lažne novice (»*fake news*«) in ti. prirejanje volitev preko njih (»*election rigging*«).

K 55. členu:

V prvem odstavku 55. člena je določen postopek odločitve, da se postopek nadzora ne uvede. Nadzornik v primerih, kadar je iz prijave posameznika, na katerega se nanašajo osebni podatki očitno, da glede na podatke iz prijave ni možno sklepati na kršitev varstva osebnih podatkov po Splošni uredbi, ZVOP-2 ali drugem zakonu oziroma predpisu, ki ureja obdelavo in varstvo osebnih podatkov, s posebno odločitvijo odloči, da se postopek inšpekcijskega nadzorstva ne uvede, ta odločitev pa se zaznamuje v spisu zadeve (posebna vrsta uradnega zaznamka). Enako velja, ko je prijavo podala druga oseba. Nadzornik mora v obrazložitvi odločitve navesti kratke razloge za neuvedbo postopka. Pri tem se izhaja iz pomena varstva osebnih podatkov kot človekove pravice (2. člen predloga zakona) in zagotavljanja pravne varnosti ter enakega obravnavanja (22. člen Ustave Republike Slovenije[95]). V tretjem odstavku pa je določena ureditev, po kateri v primerih kadar prijavo iz prvega odstavka 55. člena poda posameznik, na katerega se nanašajo osebni podatki in prijava izpolnjuje formalne zahteve po določbah zakona, ki ureja splošni upravni postopek, nadzornik, namestnik informacijskega pooblaščenca ali informacijski pooblaščenec s sklepom odloči, da se inšpekcijski postopek ne uvede. V obrazložitvi sklepa se navedejo razlogi za neuvedbo postopka ter pravni pouk. Sklep pa se vroči prijavitelju.

K 56. členu:

Predlagani 56. člen določa pravice prijavitelja. V prvem odstavku je določeno obveščanje prijavitelja, po določbi morajo nadzorne osebe vsakega prijavitelja po opravljenem nadzoru in sprejetem zadnjem ukrepu oziroma ustavitvi postopka obvestiti o vseh pomembnejših ugotovitvah in dejanjih iz postopka inšpekcijskega nadzora.
Po drugem odstavku lahko prijavitelj, ki meni, da obstaja domnevna kršitev varstva osebnih podatkov v zvezi z osebnimi podatki, ki se nanašajo nanj, v skladu s prvim odstavkom člena 80 Splošne uredbe pisno pooblasti nevladno organizacijo s področja varstva osebnih podatkov ali zasebnosti, ki ima

[93] Glejte: Makarovic, Bostjan, *The new Slovenian personal data protection act: Statutory limits to injunctive regulation of the internet*, Computer & Security Law Report (2005), 21, Elsevier Ltd., str. 322-327, še posebej str. 326-327, mag. Makarovič, Boštjan, *Ustavno varstvo zasebnosti komunikacijskih naprav v inšpekcijskih in prekrškovnih postopkih*, Zbornik - 6. dnevi prekrškovnega prava - DPP, 2011, str. 151 ter *Komentar Ustave Republike Slovenije – Dopolnitev A*, ur.: prof. dr. Šturm, Lovro, Fakulteta za državne in evropske študije, Ljubljana, 2011 (*Komentar 37. člena Ustave Republike Slovenije*, mag. Klemenčič, Goran, str. 522-524, robne št. 4-6, str. 529-530, robne št. 17-18).
[94] Uradni list RS, št. 96/09 – uradno prečiščeno besedilo in 19/15.
[95] Glede obrazložitve sklepa se smiselno sledi sicer odločitvi o obrazložitvi državnega organa glede na zavezo iz 22. člena Ustave Republike Slovenije iz najnovejše odločbe Ustavnega sodišča RS, št. Up-326/14, 6. 12. 2017, zlasti 16. točka odločbe; objava: Uradni list RS, št. 6/18.

status nevladne organizacije v javnem interesu, da v njegovem imenu vloži prijavo po prejšnjem členu tega zakona.

K 57. členu:

V prvem odstavku 57. člena ZVOP-2 je določeno splošno pravno sredstvo zoper odločitve Informacijskega pooblaščenca, da namreč zoper odločbo ali sklep Informacijskega pooblaščenca ni dovoljena pritožba, dovoljen pa je upravni spor. Informacijski pooblaščenec kot samostojni in neodvisni državni organ za varstvo osebnih podatkov torej ne sme imeti (nad seboj) drugostopenjskega upravnega organa, torej pritožbenega organa[96].

Po drugem odstavku lahko v skladu s prvim odstavkom člena 80 Splošne uredbe posameznik, na katerega se nanašajo osebni podatki in je bil prijavitelj, pisno pooblasti nevladno organizacijo s področja varstva osebnih podatkov ali zasebnosti, ki ima status nevladne organizacije v javnem interesu, da v njegovem imenu uveljavlja sodno varstvo po določbah prvega odstavka 23. člena predloga zakona.

K 58. členu:

V 58. členu predloga zakona je urejeno ukrepanje ob zaznavi kaznivih dejanj ali prekrškov. V prvem odstavku je določeno, da če nadzorna oseba pri izvrševanju svojih pristojnosti ugotovi, da obstaja sum storitve prekrška, ki je v pristojnosti Informacijskega pooblaščenca, izvede postopek po Zakonu o prekrških in po določbah Splošne uredbe. V drugem odstavku je določeno, da če nadzornik pri izvrševanju svojih pristojnosti ugotovi, da obstaja sum storitve kaznivega dejanja ali prekrška iz pristojnosti drugega prekrškovnega organa, poda kazensko ovadbo v skladu z Zakonom o kazenskem postopku oziroma izvede ustrezne postopke v skladu z Zakonom o prekrških.

Predlagani tretji odstavek vzpostavlja podobne omejitve kot v inšpekcijskem postopku (drugi odstavek 54. člena predloga zakona) tudi za prekrškovni postopek. Tako nadzornik, namestnik informacijskega pooblaščenca in informacijski pooblaščenec zaradi ugotavljanja dejstev in okoliščin oziroma zbiranja dokazov v prekrškovnem postopku ne smejo uporabiti svojih pooblastil zoper tretje osebe (ponudniki storitev gostovanja ipd., kot so navedeni v drugem odstavku 54. člena predloga zakona), ki so zgolj ponujale posredovalne storitve osebi, osumljeni storitve prekrška.

Predlagani četrti odstavek nadzorniku, namestniku informacijskega pooblaščenca in informacijskemu pooblaščencu v primeru obravnave posebej hudih kršitev zakona oziroma Splošne uredbe omogočata prebitje komunikacijske zasebnosti posameznika (37. člen Ustave Republike Slovenije) na podlagi odredbe sodnika s sodišča za prekrške (pristojnega sodnika okrajnega sodišča). Predlagana ureditev tako določa, da morajo ponudniki prenosa (ISP), začasnega shranjevanja, oziroma gostovanja ne odgovarjajo za kršitve, ki so jih povzročili njihovi uporabniki (prejemniki storitev), Informacijskemu pooblaščencu, če le-ta pridobi sodno odredbo, predati določene identifikacijske podatke o teh uporabnikih po vsebinskih določbah drugega zakona (Zakon o elektronskem poslovanju na trgu[97]) in ustaviti kršitev, pod pogojem predhodne odredbe prekrškovnega sodišča. Informacijski pooblaščenec lahko torej od ponudnikov prenosa (ISP), začasnega shranjevanja, oziroma gostovanja s sodno odredbo zgolj zahteva identifikacijske podatke o dejanskem kršitelju (tiste s katerimi razpolagajo). Ker je iz narave ureditve jasno, da se podatki vedno pridobivajo v zvezi z neko določljivo komunikacijo, se za pridobitev podatkov zahteva sodna odredba, kjer sodišče za vsak primer posebej preverja nujnost, primernost in sorazmernost ukrepa v luči 37. in 38. člena Ustave Republike Slovenije (glejte tudi odločbo Ustavnega sodišča RS iz leta 2013[98]). Takšna sodna odredba temu primerno tudi ne more biti izdana v inšpekcijskem postopku, ampak le v prekškovnem postopku, in še to le, če gre za prekrške, se glede na vrednote, katere varujejo, štejejo za hude prekrške, kot je to opredeljeno v četrtem odstavku (sum obstoja velikega tveganja za človekove pravice ali temeljne svoboščine posameznika v

[96] Glejte: odločba US, št. P-5/11, 2. 6. 2011; objava: Uradni list RS, št. 52/11.
[97] Uradni list RS, št. 96/09 – uradno prečiščeno besedilo in 19/15.
[98] Odločba US, št. U-I-40/12, 11. 4. 2013; objava: Uradni list RS, št. 39/13.

zvezi z možnostjo hude kršitve varstva osebnih podatkov – koncept ti. hudega prekrška s področja človekovih pravic in temeljnih svoboščin).

Peti odstavek ureja obvezno (in ustrezno) obveščanje posameznika, čigar podatki so bili tako pridobljeni, o tem, da so bili osebni podatki pridobljeni.

K 59. členu:

V 59. členu je določeno varovanje tajnosti osebnih podatkov, v okviru nadzornih postopkov Informacijskega pooblaščenca. Po prvem odstavku so dolžni državni nadzornik za varstvo osebnih podatkov, informacijski pooblaščenec in namestnik informacijskega pooblaščenca dolžni varovati tajnost osebnih podatkov, s katerimi se seznanijo pri opravljanju inšpekcijskega nadzora, preiskovalnih pooblastil, popravljalnih ali prekrškovnih pooblastil tudi po prenehanju delovnega razmerja ali funkcije.

Po drugem odstavku dolžnost iz prvega odstavka velja tudi za vse javne uslužbence pri Informacijskem pooblaščencu ali druge osebe, ki sodelujejo pri postopkih po tem zakonu.

K 60. členu:

V predlaganem 60. členu so določeni javnost dela Informacijskega pooblaščenca, informiranje javnosti ter dodatna svetovanja. Po prvem odstavku Informacijski pooblaščenec lahko poleg nalog iz 57. člena Splošne uredbe tudi:

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 pogojih poslovanja oziroma njihovih predlogov s predpisi s področja varstva osebnih podatkov;

6. daje neobvezna mnenja, pojasnila in stališča o vprašanjih s področja varstva osebnih podatkov in jih objavlja na spletni strani ali na drug primeren način;

7. pripravlja in daje neobvezne smernice in priporočila glede varstva osebnih podatkov na posameznem področju;

8. po potrebi daje izjave za javnost o izvedbi posamičnih zadev po tem zakonu;

9. izvaja konference za medije v zvezi z delom Informacijskega pooblaščenca ter prepise izjav ali posnetke izjav s konferenc za medije objavi na spletni strani;

10. obdeluje kontaktne podatke za izvajanje izobraževanj, posvetovanj, javnih dogodkov;

11. na spletni strani objavlja druga pomembna obvestila.

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

K 8. poglavju: Zunanji nadzor delovanja nadzornega organa

Informacijski pooblaščenec je vzpostavljen kot neodvisni nadzorni organ glede na obveznosti iz drugega odstavka 38. člena Ustave Republike Slovenije (»nadzor«), prvega odstavka 51. člena Splošne uredbe, prvega odstavka 45. člena Direktive ter 15. člen spremenjene Konvencije št. 108. Je samostojni in neodvisni organ v izvršilni veji oblasti (glejte tudi drugi odstavek 120. člena Ustave Republike Slovenije) in neodvisno izvršuje svoje pristojnosti glede varstva osebnih podatkov. Njegovo delovanje je primarno podvrženo naknadnemu sodnemu nadzoru (upravni spor), ker pa ima zelo široke pristojnosti je treba zakonsko zagotoviti tudi dodatne zunanje nadzorne mehanizme (sistem zavor in ravnovesij) glede njegovega delovanja, tako da se ne bo postavljalo vprašanje "Kdo bo varoval varuhe?"[99].

K 61. 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 62. členu:

V 62. členu je določen dodatni (drugi) zunanji kontrolni mehanizem – določitev pristojnosti Varuha človekovih pravic. Določeno je da Varuh človekovih pravic opravlja svoje naloge na področju varstva osebnih podatkov v razmerju do državnih organov, organov samoupravnih lokalnih skupnosti in nosilcev javnih pooblastil v skladu z Zakonom o varuhu človekovih pravic – torej gre za rezervni (generalni) kontrolni mehanizem, ki deluje neoblastno z lastnimi nadzori na področju varstva osebnih podatkov kot ene od človekovih pravic iz Ustave Republike Slovenije. V drugem odstavku je določeno, da je varstvo osebnih podatkov posebno delovno področje varuha.

K 63. členu:
Kot dodatna izpeljava kontrolnega mehanizma (kot tretji zunanji kontrolni mehanizem) je določeno glede pristojnosti zakonodajne oblasti, da stanje na področju varstva osebnih podatkov in izvrševanje določb tega zakona, v skladu z 61. členom tega zakona, spremlja pristojno delovno telo državnega zbora.

Po drugem odstavku pristojno delovno telo Državnega zbora Republike Slovenije za nadzor obveščevalnih in varnostnih služb (Komisija za nadzor obveščevalnih in varnostnih služb Državnega zbora Republike Slovenije) lahko sodeluje z Informacijskim pooblaščencem, na lasten predlog ali na pobudo Informacijskega pooblaščenca, kadar je v določenih primerih potrebna zaupna izmenjava informacij o ugotovitvah ločenih nadzornih postopkov (iz pristojnosti Informacijskega pooblaščenca ali iz pristojnosti Komisije) ali glede sprememb zakonov ali drugih predpisov (iz delovnega področja Informacijskega pooblaščenca ali Komisije).

K 9. poglavju: Prenosi določenih osebnih podatkov državam članicam Evropske unije, tretjim državam ali mednarodnim organizacijam

Dva člena 9. poglavja urejata načine posredovanj osebnih podatkov iz Republike Slovenije v druge države ali v mednarodne organizacije – ko gre za obdelave osebnih podatkov, ki jih Slovenija ureja popolnoma samostojno. Predlagana ureditev sledi ureditvi iz Splošne uredbe.

[99] "*Quis custodiet ipsos custodes?*"

K 64. členu:

Predlagani 64. člen določa za določena področja, ki so popolnoma samostojno v pristojnosti Republike Slovenije (9. in 10. člen) posebna pravila za prenose osebnih podatkov v druge države ali mednarodne organizacije.

K 65. členu:

Predlagani 56. člen predloga zakona določa posebna pravila za primere, ko se osebni podatki iz prejšnjega člena posredujejo v tretjo državo ali mednarodno organizacijo, za katero ne obstaja sklep o ustreznosti iz 45. člena Splošne uredbe oziroma niso bili sprejeti ustrezni zaščitni ukrepi. Te določbe ne veljajo za II. del predloga zakona, ki ima določena samostojna pravila za posredovanje osebnih podatkov.

K II. delu predloga zakona: OBDELAVA OSEBNIH PODATKOV ZA NAMENE PREPREČEVANJA, PREISKOVANJA, ODKRIVANJA ALI PREGONA ZARADI KAZNIVIH DEJANJ, IZVRŠEVANJA NALOG IN POOBLASTIL POLICIJE, VARNOSTI DRŽAVE, OBRAMBE DRŽAVE TER IZVRŠEVANJA KAZENSKIH SANKCIJ

II. del predloga zakona v pravni red Republike Slovenije prenaša določbe *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* (v nadaljnjem besedilu: Direktiva).

Zakonodajni pristop, da se področje ureja v posebnem delu sistemskega Zakona o varstvu osebnih podatkov, je podoben zakonodajnim pristopom Nemčije, Avstrije, Slovaške, izhaja pa tudi iz pristopa Republike Slovenije iz časa priprave Predloga Direktive. Vsebinski pristop, da se v tem »policijsko ter kazensko pravosodnem« delu zakona izhaja iz uporabe določenih standardov (določb) Splošne uredbe sledi pristopu Zvezne republike Nemčije, ki je v Zakonu o prilagoditvi in izvajanju zakonodaje o varstvu osebnih podatkov EU (iz leta 2017) izvedla razširitev določb Splošne uredbe na določena vprašanja, ki jih ureja sicer Direktiva (zaradi pravne varnosti in enakosti na področju varstva osebnih podatkov), v III. Delu zakona Nemčije je namreč določena izvedba določb Direktive (EU) 2016/680 in določbe v njem, ki so enake ali podobne istim, ki so v Splošni uredbi ali v predhodnih delih zakona izhajajo iz pristopa, po katerem je nacionalnemu zakonodajalcu prepuščeno, kako bo izvedel določbe navedene Direktive in lahko tako tudi uporabi (z vidika pravne varnosti) splošni sistem (splošno sistemsko raven) urejanja varstva osebnih podatkov po (nekoliko prilagojenih) določbah iz Splošne uredbe. To je tudi pristop predlagatelja predloga zakona.

K 1. poglavju: Splošne določbe 1. poglavje II. dela

1. poglavje II. dela določa splošne določbe za uporabo ti. »direktivnega dela« zakona, kar med drugim vključuje definicijo področja, posebna pravila glede ozemeljske veljavnosti, uporabo prava ipd.

K 66. členu:

V predlaganem členu je v skladu z določbami prvega odstavka 1. oziroma 2. člena Direktive določeno področje uporabe tega dela zakona. II. del zakona se tako uporablja za primere, ko pristojni državni organi (policija, državna tožilstva, kazenska sodišča, ministrstvi za pravosodje oz. notranje zadeve, urad za preprečevanje pranja denarja ter financiranja terorizma ter druge pristojni organi) obdelujejo osebne podatke za namene preprečevanja, preiskovanja, odkrivanja ali pregona kaznivih dejanj ali izvrševanja kazenskih sankcij, vključno z varovanjem pred grožnjami javni varnosti in njihovim preprečevanjem. .

Obdelave s strani teh istih organov ali subjektov za druge namene, npr. namene zaposlovanja ali javnih naročil, se še vedno izvajajo v skladu s pravili Splošne uredbe oziroma ostalih delov predloga zakona.

K 67. členu:

Prvi odstavek predlaganega člena določa subsidiarno uporabo I. dela predloga zakona za primere, ko določbe tega dela ne določajo drugače.

K 68. členu

Predlagani člen omejuje ozemeljsko veljavo določb II. dela na primere, ko pristojni organi iz 66. člena izvajajo svoje pristojnosti na ozemlju Republike Slovenije. Edina izjema so obdelave s strani teh organov na misijah v tujini, vendar le, če merodajno mednarodno pravo določa uporabo slovenske zakonodaje za varstvo osebni podatkov.

K 69. členu

Predlagani člen definira relevantne izraze. Pri tem izhaja zlasti iz 3. člena Direktive, obenem pa dodaja še druge potrebne definicije, npr. definicijo privolitve.

K 70. členu

Predlagani člen določa temeljna načela varstva osebnih podatkov, s čimer prenaša določbe prvega oziroma četrtega odstavka 4. člena Direktive.

K 71. členu:

Predlagani člen tako določa obveznost razvrščanja in s tem ločene obravnave osebnih podatkov po vrstah ter kakovosti, sicer 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 vrednostni ali 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.

K 72. členu:

Predlagani člen določa posebna pravila glede zagotavljanja točnosti, popolnosti, posodobljenosti ter zanesljivosti osebnih podatkov, še zlasti v policijskih evidencah.

Po prvem odstavku se osebni podatki, ki so netočni, nepopolni, ki niso posodobljeni ali jih je treba izbrisati, ne smejo ne prenašati ne pripraviti za avtomatiziran priklic iz zbirk, upravljavci pa morajo v ta namen pred prenosom z uporabo vseh razumnih ukrepov ustrezno preveriti kakovost osebnih podatkov. Glede osebnih podatkov, ki so že na razpolago za avtomatiziran priklic, se je treba neprestano prizadevati za ohranjanje njihove točnosti in posodobljenosti.

Po drugem odstavku je pri vsakem posredovanju, čezmejni obdelavi ali prenosu osebnih podatkov treba po možnosti osebnim podatkom priložiti informacije, na podlagi katerih lahko uporabnik oceni oceno aktualnost, pravilnost, popolnost in zanesljivost. V tretjem odstavku je določeno, da če uporabnik, Informacijski pooblaščenec ali pooblaščena oseba za varstvo osebnih podatkov na podlagi sporočila posameznika, na katerega se nanašajo osebni podatki, ugotovijo (katerikoli od njih), da so bili posredovani osebni podatki, ki ne ustrezajo zahtevam iz prvega odstavka tega člena, mora pošiljatelj to nemudoma sporočiti uporabniku. Ta pa mora nemudoma izvesti izbris nezakonito posredovanih podatkov, popravek netočnih podatkov, dopolnitev nepopolnih podatkov ali omejitev obdelave.

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

Po petem odstavku se posebej določa obveznost obveščanja posameznikov v primeru, da upravljavec zazna, da je naprej posredoval netočne, nepopolne, neposodobljene oziroma nezanesljive podatke, ter mu s tem omogoči nadaljnje ukrepanje pri uporabnikih takšnih podatkov.

K 73. členu:

Predlagani člen določa načelo zakonitosti.

V prvem odstavku določa pravila zakonitosti obdelave osebnih podatkov, po kateri je obdelava osebnih podatkov zakonita le, če

1. je to potrebno za namene iz prvega člena tega poglavja, in
2. tako določa področni zakon, ki mora pri tem določiti vsaj samo obdelavo, vrste obdelovanih osebnih podatkov ter namen obdelave, če je mogoče, pa še tudi druge ustrezne vidika te obdelave.

V drugem odstavku določa pravila zakonitosti obdelave posebnih vrst osebnih podatkov, po kateri je obdelave teh podatkov zakonite le, če:

1. je to nujno potrebna za varovanje življenja ali telesa ali zdravja posameznika, na katerega se osebni podatki nanašajo, ali druge osebe, kadar posameznik, na katerega se osebni podatki nanašajo, fizično ali poslovno ni sposoben dati svoje privolitve,
2. je posameznik, na katerega se nanašajo občutljivi osebni podatki, te javno objavil, brez očitnega ali izrecnega namena, da omeji namen obdelave osebnih podatkov,
3. 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,
4. tako določa drug zakon za namen arhiviranja v javnem interesu oz. za znanstvenoraziskovalne ali statistične namene, ali
5. tako določajo zakoni, ki urejajo izvajanje obveščevalnih in protiobveščevalnih dejavnosti države[100]).

K 74. členu:

Predlagani člen določa uporabo javno objavljenih »navadnih« oziroma posebnih vrst osebnih podatkov za izvajanje namenov iz 66. člena predloga zakona.

Če posameznik, na katerega se nanašajo osebni podatki, javno objavi svoje posebne vrste osebnih podatkov in pri tem ne izrazi izrecnega oz. drugače očitnega namena, da omeji namen njihove obdelave, je njihova obdelava zakonita, če je v skladu z nameni iz 66. člena tega zakona.

Za »navadne osebne podatke« (tj. vse osebne podatke, ki ne spadajo v posebne vrste osebnih podatkov), ki jih posameznik javno objavi, je njihova obdelava za namene iz 66. člena tega zakona dopustna tu v primeru, če je posameznih izrecno oziroma drugače očitno omejil namen njihove uporabe.

[100] Zakon o Slovenski obveščevalno-varnostni agenciji (Uradni list RS, št. 81/06 – uradno prečiščeno besedilo) in 32.-34. ter 36. člen Zakona o obrambi (Uradni list RS, št. 103/04 – uradno prečiščeno besedilo in 95/15).

K 75. členu:

Predlagani člen določa pravila za obdelavo osebnih podatkov za druge namene ter tudi s tem povezan prenos osebnih podatkov v tretje države oziroma mednarodne organizacije.

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 to zaradi namena iz 66. člena predloga zakona določa področni zakon, ki pri tem izpolnjuje pogoje za zakonitost obdelave iz 73. člena predloga zakona.

K 76. členu:

Predlagani člen na splošno ureja prenos, posredovanje ali čezmejna obdelava osebnih podatkov, obdelanih skladno z določbami tega dela, za namen, ki ni naveden v 66. členu tega zakona, in določa, da je taka obdelava dovoljena le, če je to izrecno določeno v zakonu (zakon, obvezujoča mednarodna pogodba ali pravni akt ali odločitev Evropske unije, ki sta enakovredna zakonu in se v Republiki Sloveniji uporabljata neposredno) ter če je uporabnik po svojih predpisih pooblaščen za obdelavo teh osebnih podatkov za ta drug namen.

Po drugem odstavku mora v primeru, če za obdelavo osebnih podatkov veljajo posebni pogoji v skladu s področnim zakonom (npr. zaščitene priče), mora pristojni pošiljatelj uporabnika osebnih podatkov obvestiti o teh pogojih in o tem, da jih je treba upoštevati. Pri čezmejni obdelavi uporabnikom v druge države članice Evropske unije ali v ustanove in druge organe, vzpostavljene skladno s 4. in 5. poglavjem V. naslova Pogodbe o delovanju Evropske unije, se ne smejo uveljavljati pogoji, ki za ustrezni prenos podatkov ne veljajo tudi v Republiki Sloveniji.

K 77. členu:

Predlagani člen določa omejitve avtomatizirane obdelavo osebnih podatkov za potrebe tega dela tega zakona. Gre za področno specifično ureditev. Njeno bistvo je, da mora avtomatizirano obdelavo osebnih podatkov določati zakon in da mora biti možno in dejansko izvedeno naknadno preverjanje rezultatov avtomatizirane obdelave.

Četrti odstavek določa, da je prepovedano profiliranje, če bi to vodilo do diskriminacije posameznikov, na katere se nanašajo osebni podatki.

K 78. členu:

Predlagani člen ureja dnevnike (žurnale) obdelav osebnih podatkov, s tem je zagotovljena posebna vrsta sledljivosti obdelav osebnih podatkov v zvezi nameni iz 66. člena ZVOP-2.

K 79. členu:

Predlagani člen določa obveznost izdelave ocene učinkov na varstvo osebnih podatkov.

Za večje in z vidika obdelave osebnih podatkov bolj invazivne nove projekte obdelav osebnih podatkov bo potrebno že v fazi načrtovanja obdelave pripraviti poseben dokument z oceno vseh učinkov na pravice posameznikov, katerih podatki se bodo obdelovali. Takšen dokument je v praksi poimenovan kot »Ocena učinkov v zvezi z varstvom osebnih podatkov« (»*Data Protection Impact Assessment – DPIA*«).

Bistvo DPIA-e ni v popisu obdelav osebnih podatkov oziroma iskanju pravne podlage za njih, ampak v identifikaciji, kategorizaciji ter ovrednotenju tveganj, ki bi lahko nastala pri obdelavah, ter potem iskanju rešitev, ki bi, vsaka posebej oziroma vse skupaj, prispevale k zmanjšanju tako najdenih tveganj ter k obdelavi osebnih podatkov v skladu z načelom sorazmernosti.

Podrobnosti za izvedbo ocene razlaga Informacijski pooblaščenec v svojih smernicah iz novembra 2017[101].

K 80. členu

[101] Glejte: https://www.ip-rs.si/fileadmin/user_upload/Smernice_o_ocenah_ucinka__DPIA__nov2017.pdf

Predlagani člen določa obveznost predhodnega posvetovanja z Informacijskim pooblaščencem pred vzpostavitvijo novih zbirk osebnih podatkov za namene iz 66. člena predloga zakona. Upravljavec mora k izvedbi tega posvetovanja pristopiti pravočasno, tj. še pred vzpostavitvijo teh zbirk.

K 81. členu

Predlagani člen določa izjemo glede pogojev za izvedbo preiskovalnega pooblastila preiskave uradnih prostorov zavezancev iz 66. člena predloga tega zakona. Za razliko od splošne ureditve iz 53. člena predloga zakona, ki za takšen poseg zahteva predhodno odredbo Okrožnega sodišča, zaradi zavarovanja prostorske in komunikacijske zasebnosti upravljavca, to pri preiskavah službenih prostorov policijskih in drugih organov iz tega poglavja ni potrebno – gre namreč za državne prostore, namenjene opravljanju uradnih (oblastnih) delovanj države ozir. javnega sektorja. Delo teh organov oziroma njihovih zaposlenih mora zaradi represivne narave njihovih pooblastil biti še posebej transparentno, kar posledično zmanjšuje njihovo pričakovano zasebnost v obziru do službenih prostorov. Informacijski pooblaščenec zato za preiskavo skritih delov njihovih prostorov ne bo rabil sodne odredbe, ampak se bo lahko zanašal že na pooblastila iz Zakona o inšpekcijskem nadzoru ter na smiselno uporabo določb 53. člena predloga zakona.

K 82. členu

Predlagani člen ureja eno ključnih novosti Direktive v primerjavi s prejšnjih Okvirnim sklepom - iz Splošne uredbe prevzeta obveznost upravljavca, da ves čas izvajanja obdelav skrbi za skladnost teh obdelav s pravili te uredbe oziroma drugih predpisov o varstvu osebnih podatkov, ter da to izvajanje tudi ustrezno dokumentira.

Upravljavec mora v ta namen v svojih internih aktih določiti postopke in ukrepe za zagotovitev skladnosti (kar je dosedaj veljalo zgolj za ukrepe za zavarovanje osebnih podatkov oz. za (pogodbeno) obdelavo - drugi odstavek 25. člena ozir. drugi odstavek 11. člena ZVOP-1). V primeru bolj tveganih obdelav mora določiti tudi splošno politiko varstva osebnih podatkov, ki naj vključuje ukrepe kot so ozaveščanje in usposabljanje svojih zaposlenih, upravljanje njihovih pooblastil za dostop do oz. za obdelavo podatkov, določitev odgovornih oseb za posamezne zbirke osebnih podatkov ter pravila za izvajanje revizij. Primerne postopek oziroma ukrepe, oziroma vsebino politike varstva osebnih podatkov določi na podlagi tveganosti posamezne obdelave. Pri najbolj tveganih ukrepih se priporoča uporaba katerega od veljavnih mednarodnih standardov na tem področju.

Upravljavec mora tako predpisane ukrepe tudi ves čas izvajati in o tem voditi vso potrebno dokumentacijo, s katero lahko skladnost dokazuje tudi za nazaj. Ta dokumentacija naj vsebuje zlasti evidenco obdelav pri upravljavcu, oceno učinkov teh obdelav za varstvo osebnih podatkov (izdelano po ustrezni metodologiji, upoštevaje tveganost obdelave), popis sredstev obdelave, popis dostopnih pravic zaposlenih, pogodbenih partnerjev in drugih uporabnikov, ter rezultate rednih revizij skladnosti obdelave podatkov. Upravljavec lahko za pripravo in hrambo te dokumentacijo pooblasti tudi pooblaščeno osebo za varstvo osebnih podatkov, najame zunanje strokovnjake, oziroma pridobi ustrezno in za to namenjeno programsko opremo.

K 83. členu

Predlagani člen določa obveznost upravljavca, da že pri snovanju novih obdelav preveri, katere podatke resnično potrebuje za učinkovito izvajanje posamezne obdelave, ter potem te obdelave zasnuje tako, da ne zahtevajo zbiranja dodatnih podatkov (vgrajeno varstvo osebnih podatkov).

Obenem mora upravljavec mora svoje obdelave v čim večji meri zasnovati tudi tako, da v vsakem posamičnem primeru pridobijo in obdelajo samo tiste podatke, ki so potrebni v tem primeru. To pri obdelavah, ki se izvajajo s sredstvi informacijske tehnologije pomeni še zlasti, da se pred začetkom vsake obdelave ne naloži vseh podatkov, ki bi bili potrebni za tipično obdelavo te vrste, ampak, kolikor je le mogoče, zgolj tiste podatke, ki jih potrebuje ta konkretna obdelava (privzeto varstvo osebnih podatkov).

K 84. členu

Predlagani člen za primer, ko več pristojnih organov skupaj obdeluje osebne podatke za namene iz 66. člena, določa obveznost, da ti organi svoje medsebojne odnose uredijo s pisnim sporazumom. Prav tako določa, da se lahko posamezniki, katerih osebni podatki se pri tem obdelujejo, glede svojih pravic obrnejo na kateregakoli od teh skupnih upravljavcev.

K 85. členu

Predlagani člen ureja možnost odstopa izvedbe posameznih dejanj obdelave zunanjemu subjektu (obdelovalcu).

Tako kot že dosedaj lahko upravljavec posamezna opravila v zvezi z obdelavo osebnih podatkov pogodbeno preda (zaupa) obdelovalcu (dosedanjemu "pogodbenemu obdelovalcu). Podobno kot dosedaj mora njuna medsebojna razmerja še vedno urediti v pisni pogodbi ali v drugem dogovoru, 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. Prav tako se lahko pogodbena obdelava določi na podlagi izrecnega zakonskega pooblastila, ki določi upravljavca in obdelovalca in vsaj okvirno opredeli naloge ozir. zamejitve nalog obdelovalca.

Upravljavec ne sme skleniti takega dogovora ali pogodbe z obdelovalcem, ki ni sposoben dati zagotovil, da bo lahko zagotovil spoštovanje teh obveznosti. Prav tako obdelovalec ne sme dalje prenesti posameznih opravil na druge obdelovalce, brez da bi mu upravljavec do izrecno dovolil, ali vsaj bil s tem seznanjen in imel možnost nasprotovati izbiri podobdelovalca.

Določeno je tudi, da obdelovalec obvezno nudi pomoč upravljavcu glede zagotavljanje varnosti osebnih podatkov, sporočanja in urejanja problemov glede kršitve varnosti osebnih podatkov, pri izdelavo ocene učinka glede varstva osebnih podatkov ter glede posvetovanje z Informacijskim pooblaščencem glede ocene učinkov. Ostale obveznosti zagotavljanja skladnosti so na upravljavcu samem; če želi pomoč obdelovalca pri tem, se to seveda lahko dogovori v pogodbi, ne sem pa biti obdelovalec prisiljen, da skladnost varstva osebnih podatkov pretežno ali skoraj v celoti zagotavlja sam, v tem primeru dejansko postane obdelovalec.

Vsebina pogodbe ali drugega dogovora med upravljavcem in obdelovalcem ostaja podobna kot dosedaj, seveda z dodanimi novostmi Splošne uredbe.

V praksi je treba v vsakem konkretnem primeru presoditi, ali gre pri pravnem poslu (tudi) za obdelavo osebnih podatkov. Za primer: ne gre za (pogodbeno) obdelavo, če določen subjekt javnega ali zasebnega sektorja izvaja samo hrambo strežniške infrastrukture (daje na razpolago prostore oziroma opremo) za drug subjekt (javnega ali zasebnega sektorja), če pri tem ne more vpogledati v osebne podatke, jih priklicati, spreminjati, izbrisati, arhivirati ter izvajati drugih dejanj obdelave osebnih podatkov. V tem primeru se torej ne izvaja (pogodbena) obdelava osebnih podatkov, subjekt ni obdelovalec (in ni niti upravljavec).

Za primer: ne gre za pogodbeno obdelavo, če določen subjekt javnega ali zasebnega sektorja izvaja samo hrambo strežniške infrastrukture (daje prostore oziroma opremo na razpolago) za drug subjekt (javnega ali zasebnega sektorja), če ne more niti vpogledati v osebne podatke, jih priklicati, spreminjati, izbrisati, arhivirati ter izvajati drugih dejanj obdelave osebnih podatkov. V tem primeru se torej ne izvaja pogodbena obdelava osebnih podatkov, subjekt ni obdelovalec (in ni niti upravljavec).

K 86. členu

Predlagani člen določa vsebino evidence dejavnosti obdelav.

Čeprav Direktiva po zgledu Splošne uredbe črta obveznost prijave zbirk osebnih podatkov Informacijskemu pooblaščencu, je to na področju policijskih obdelav nekoliko omejeno, saj je zaradi represivne naloge policijskih in drugih kazenskopravnih pooblastil potreba po transparentnosti obdelav še toliko večja.

Člen tako določa obvezno vsebino evidenc dejavnosti obdelave tako za same organe (upravljavce) kot tudi njihove pogodbene obdelovalce. Kasnejši členi glede pravic posameznikov pa določajo pravico posameznika, da se seznani s podatki iz te evidence.

K 2. poglavju: Pravice posameznika, na katerega se nanašajo osebni podatki

Predlagano 2. poglavje posebej ureja pravice in postopek glede pravic posameznikov, na katere se nanašajo osebni podatki.

K 87. členu

Predlagani člen določa pristojnost Informacijskega pooblaščena za reševanje pritožb posameznikov zoper obdelave osebnih podatkov s strani organov iz 66. člena predloga.

K 88. členu

Predlagani člen ureja področje dajanja splošnih informacij posamezniku, na katerega se nanašajo osebni podatki.

Zagotoviti je treba najmanj:

1. naziv in kontaktne podatke upravljavca;

2. po potrebi tudi kontaktne podatke pooblaščene osebe (glede na konkretne okoliščine zadeve ali zahtevka);

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

4. obstoj pravice do vložitve prijave pri Informacijskem pooblaščencu ter kontaktne podatke Informacijskega pooblaščenca;

5. navesti obstoj pravice dostopa do vsebine osebnih podatkov in do tega, da upravljavec popravi ali izbriše podatke ali omeji obdelavo podatkov posameznika, na katerega se osebni podatki nanašajo.

Po drugem odstavku mora poleg informacij iz prvega odstavka upravljavec posamezniku, na katerega se nanašajo podatki, v posebnih primerih na njegovo zahtevo po prvem odstavku zagotoviti tudi določene (navedene) dodatne informacije, da lahko s tem omogoči izvajanje pravic tega posameznika:

1. pravno podlago obdelave;

2. rok hrambe osebnih podatkov ali, če to izjemoma ni možno, merila za določitev tega roka v skladu z 33. členom tega zakona;

3. po potrebi navesti kategorije uporabnikov osebnih podatkov, tudi uporabnikov v tretjih državah in mednarodnih organizacijah;

4. po potrebi druge informacije, zlasti če so bili osebni podatki pridobljeni brez vednosti posameznika, na katerega se nanašajo.

K 89. členu:

V predlaganem členu je urejena pravica posameznika do dostopa do osebnih podatkov, ki jih o njem obdelujejo pristojni organi iz 66. člena zakona.

V prvem odstavku so določene posebne seznanitvene pravice posameznika, na katerega se nanašajo osebni podatki, do pridobitve posebnih informacij o vsebini teh podatkov.

V drugem odstavku za pridobitev informacij iz prvega odstavka veljajo enaki roki oz. iz 12. člena Splošne uredbe. Omejitve pravice do pridobitve informacij so dovoljene le pod pogoji, navedeni v 91. členu predloga zakona.

V tretjem odstavku je določeno, da v primeru neizdaje informacij v skladu z drugim odstavkom mora upravljavec posameznika, na katerega se nanašajo podatki, nemudoma pisno obvestiti o zavrnitvi ali omejitvi informacij in razlogih, na katerih to temelji. Ta določba se ne uporablja, če je zagotovitev teh informacij v nasprotju z enim od namenov iz četrtega odstavka 92. člena predloga zakona. Upravljavec mora posameznika, na katerega se nanašajo podatki, obvestiti o možnosti vložitve pritožbe na organ za varstvo podatkov.

V četrtem odstavku je določeno, da mora upravljavec dokumentirati razloge za odločitev o neizdaji informacij v skladu z drugim odstavkom. Ti podatki morajo biti dostopni Informacijskemu pooblaščencu in pooblaščeni osebi.

V petem odstavku je določeno, da če glede posameznih zbirk osebnih podatkov področni zakon določa posebna pravila dostopa, potem ta pravila prevladajo (navedeni drugi področni zakon torej prevlada – npr. Zakon o nalogah in pooblastilih policije, zakoni, ki urejajo sodne postopke).

K 90. členu:

V predlaganem členu je ločeno (področno) urejena pravica do popravka ali izbrisa osebnih podatkov in do omejitve obdelave.

Po prvem odstavku ima vsak posameznik, na katerega se nanašajo osebni podatki, pravico, da od upravljavca zahteva takojšnji popravek svojih netočnih osebnih podatkov in dopolnitev nepopolnih ali neposodobljenih osebnih podatkov. Popravek ali dopolnitev se lahko po potrebi izvede z dodatno priloženo izjavo ali posebnim uradnim zaznamkom, če je naknadna sprememba nezdružljiva z namenom dokumentiranja glede na fazo določenega postopka (podatkov se torej ne spremeni, ampak se jim le priloži uradni zaznamek o izjavi). Upravljavec je dolžan dokazati točnost ali posodobljenost osebnih podatkov, če osebni podatki niso bili pridobljeni izključno na podlagi navedb posameznika, na katerega se podatki nanašajo.

Po drugem odstavku mora upravljavec osebne podatke nemudoma izbrisati na lastno pobudo ali na podlagi zahtevka posameznika, na katerega se podatki nanašajo, če:

1. osebni podatki niso več potrebni za namene, za katere so bili pridobljeni ali drugače obdelani;

2. so bili osebni podatki obdelani nezakonito ali

3. je izbris osebnih podatkov potreben zaradi izpolnitve druge obveznosti po zakonu ali po pravnomočni sodni odločbi (npr. pravnomočna oprostilna kazenska sodba). Po tretjem odstavku lahko namesto izbrisa osebnih podatkov upravljavec njihovo obdelavo omeji, če:

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

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

Po četrtem odstavku mora upravljavec posameznika, na katerega se nanašajo osebni podatki, pisno obvestiti o zavrnitvi popravka ali izbrisa osebnih podatkov ali o omejitvi obdelave in o razlogih za zavrnitev. Upravljavec mora posameznika, na katerega se nanašajo podatki, obvestiti o možnosti vložitve prijave Informacijskemu pooblaščencu in o njegovih kontaktnih podatkih. Po petem odstavku mora upravljavec morebitni popravek nepravilnih osebnih podatkov sporočiti pristojnemu organu, ki mu je prenesel ali drugače poslal (čezmejna obdelava, posredovanje) te osebne podatke.

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

Po šestem 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.

K 91. členu

Predlagani člen določa pogoje za omejitve pravic posameznika, na katerega se nanašajo osebni podatki. Navedeni pogoji so podobni tistim iz določb 23. člena Splošne uredbe, pri čemer so zaradi represivne narave področja nekoliko postroženi, in sicer je omejevanje dovoljeno le iz najbolj utemeljenih razlogov (skupaj 5 v primerjavi z 11 iz Splošne uredbe), prav tako pa je treba v vsakem posameznem primeru omejevanja pravic posebej preveriti, da je takšno omejevanje v tem primeru resnično nujno, in obenem sorazmerno v razmerju do razloga za omejevanje.

K 92. členu

Predlagani člen konkretizira obveznosti zagotavljanja varnosti obdelave osebnih podatkov.

V prvem odstavku se ureja ta obveznost za vse obdelave iz tega dela, in sicer pod enakimi kriteriji kot veljajo po 32. členu Splošne uredbe – torej upoštevaje množičnost in tveganost obdelave, stanje možnih ukrepov, ter stroške njihovega izvajanja.

V drugem odstavku se določajo dodatni ukrepi, ki jih je treba podvzeti v zvezi z avtomatiziranimi obdelavami.

K 93. členu

Predlagani člen ureja ti. »obvestilo o kršitvi« ("*breach notification*"), po vzoru Zakona o elektronskih komunikacijah[102] (81. člen) ter tudi Zakon o informacijski varnosti[103] (npr. tretji odstavek 31. člena). Gre za pravilo da morajo upravljavci v primeru odkritih varnostnih napadov oz. drugih incidentov, ki kršijo varnost ali varstvo osebnih podatkov le-te sporočiti Informacijskemu pooblaščencu, da ta lahko ukrepa in določi primerne ukrepe za ustavitev oziroma razrešitev varnostnega incidenta.

Pri tem Informacijskega pooblaščenca ne bo potrebno obveščati o vsakem odkritem (ali osumljenem) varnostnem incidentu, ampak zgolj o tistih, za katere je verjetno, da so oz. še bodo povzročili tveganje za posege v človekove pravice in temeljne svoboščine posameznikov. Ključna razlika bo zlasti v primerih napadov na dosegljivost informacijskega sistema (ti. »*availability napadi*«, med njimi zlasti DDOS), kjer gre za varnostni incident, ni pa nujno, da je prišlo tudi do kršitve varstva osebnih podatkov.

Rok za obveščanje je čim prej po odkritju incidenta ("brez nepotrebnega odlašanja") – realno najpozneje v 72 urah, po tem pa le, če za zamik obstajajo opravičljivi razlogi. Bistvo tega roka je, da lahko Informacijski pooblaščenec čim prej odredi morebitne ukrepa za zagotovitev varnosti osebnih podatkov, kot tudi v tem, da v primeru najresnejših kršitev skupaj z upravljavcem oziroma obdelovalcem, pri katerem je prišlo do incidenta, premisli, ali je potrebno o njem obvestiti tudi končne uporabnike, zato da lahko izvedejo ustrezne ukrepa za zaščito njihovih osebnih podatkov.

Obveščati je zatorej treba tudi v primerih, ko upravljavec incidenta še ni povsem raziskal, in ko tudi morda še ne ve dokončno, ali sploh je, ter v kakšnem obsegu, prišlo do zlorabe (zlasti odtujitve) osebnih podatkov. Takšen pristop izvira iz izkušenj z informacijsko-varnostne sfere, saj bi čakanje na dokončno raziskanost incidenta lahko povzročilo znatno dodatno škodo posameznikom zaradi zlorab njihovih podatkov v vmesnem času.

Dodatna novost pa je še v tem, da mora upravljavec takoj po odkritju varnostne grožnje pristopiti k zavarovanju dokazov o dogodku, za primer, če bi bilo kasneje potrebno za ugotavljanje okoliščin in dometa vloma.

[102] Uradni list RS, št. 109/12, 110/13, 40/14 – ZIN-B, 54/14 – odl. US, 81/15 in 40/17.
[103] Uradni list RS, št. 30/18.

Posamezne vidike notifikacijske dolžnosti je že obravnavala Delovna skupina po členu 29 Direktive 95/46/ES, in o tem izdala ustrezne smernice[104].

K 94. členu

Predlagani člen v primerih suma hujših varnostnih incidentov glede kršitve varnosti osebnih podatkov upravljavca obvezuje, da o incidentu obvesti tudi svoje uporabnike (posameznike, na katere se nanašajo osebni podatki), zato da lahko izvedejo ustrezne zaščitne ukrepe, še zlasti ukrepe za preprečitev kraje identitete.

K 3. poglavju: Prenos osebnih podatkov tretjim državam ali mednarodnim organizacijam ter čezmejne obdelave osebnih podatkov

3. poglavje ureja prenose osebnih podatkov v tretje države ali mednarodne organizacije, drugače kot je to urejeno v Splošni uredbi.

K 95. členu:

Predlagani člen ureja splošna pravila za prenos osebnih podatkov ter glede čezmejne obdelave (za posredovanja osebnih podatkov med državami članicami Evropske unije).

Prenos je dopusten, če so upoštevane določbe tega dela zakona in:

1. je prenos potreben za namene iz 88. 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 88. člena tega zakona;

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

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

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

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

V petem odstavku je določeno, da se prenos osebnih podatkov državam Evropske unije, tretjim državam ali mednarodnim organizacijam iz razlogov varnosti države ureja v zakonih, ki urejajo izvajanje obveščevalnih in protiobveščevalnih nalog države.

V šestem odstavku je tudi izveden prvi odstavek 14. člena Konvencije št. 108, ki omogoča, da Informacijski pooblaščenec zaustavi prenose v tretje države ali mednarodne organizacije ali celo države Sveta Evrope ali Evropske unije, če obstaja dejansko in resno tveganje (kumulativna pogoja) obida določb o varstvu osebnih podatkov iz navedene Konvencije. Po sedmem odstavku zoper odločitev Informacijskega pooblaščenca iz prejšnjega odstavka ni dovoljena pritožba ali začasna

[104] Glejte: WP250 z dne 3.10.2017, Guidelines on Personal data breach notification under Regulation 2016/679.

odredba, dopusten pa je upravni spor. Osmi odstavek pa določa, da Informacijski pooblaščenec tovrstno določitev objavi v Uradnem listu Republike Slovenije ter o tem neposredno obvesti Evropsko komisijo, pravo Evropske unije mu pa tudi omogoča, da o tem obvesti tudi Evropski odbor za varstvo podatkov oziroma na tem forumu odpre razpravo.

K 96. členu:

Predlagani člen ureja sistem prenosa osebnih podatkov na podlagi sklepa o ustreznosti varstva osebnih podatkov, ki ga izda Evropska komisija na podlagi tretjega odstavka člena 36 Direktive (izvedbeni akt), če pač odloči, da zadevna tretja država, njena regija oziroma eden ali več specifičnih sektorjev (javni sektor, zasebni sektor, deli zasebnega sektorja, deli javnega sektorja) v tej tretji državi ali zadevna mednarodna organizacija nudi ustrezno stopnjo varstva osebnih podatkov. Za tak prenos podatkov ni potrebna posebna odobritev nobenega drugega organa (ni potrebna naknadna odobritev). Ta Sklep Evropske komisije, sprejet v skladu s petim odstavkom člena 36 Direktive, ki se nanaša na preklic, spremembo ali odložitev izvajanja že izdanega sklepa po tretjem odstavku člena 36 Direktive ne vpliva na že izvedene prenose osebnih podatkov tretji državi, regiji oziroma enemu ali več specifičnim sektorjem v tretji državi oziroma mednarodni organizaciji v skladu s 106. in 107. členom tega zakona, niti ne vpliva na obveznosti iz področnih mednarodnih pogodb.

K 97. členu:

Predlagani člen ureja prenos osebnih podatkov z uveljavljanjem ustreznih ukrepov varstva osebnih podatkov, če:

1. so v ustreznem pravnem aktu, ki je pravno obvezujoč, določeni ustrezni ukrepi za varstvo osebnih podatkov ali

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

V predlaganem drugem odstavku je določeno, da če v skladu z 2. točko prvega odstavka obstajajo ustrezni ukrepi za določene vrste prenosov, mora upravljavec o teh kategorijah prenosov obvestiti Informacijskega pooblaščenca, ki lahko odredi prepoved prenosa osebnih podatkov. Po tretjem odstavku je treba prenose v skladu z 2. točko prvega odstavka dokumentirati, dokumentacijo, ki vključuje datum in čas prenosa, informacije o pristojnemu organu uporabniku, utemeljitev prenosa in prenešene osebne podatke, pa je treba na zahtevo dati na razpolago Informacijskemu pooblaščencu.

K 98. členu:

V predlaganem členu so določene izjeme (glede na člen 38 Direktive), ki urejajo dodatne možnosti prenosa osebnih podatkov, če ne obstajajo podlage po prejšnjih dveh členih predloga

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 66. členu ZVOP-2, ali

5. v posameznem primeru za uveljavljanje, izvajanje ali obrambo pravnih zahtevkov v povezavi z nameni, navedenimi v 66. 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 prejšnjega člena tega zakona (obveznosti dokumentiranja ter preverjanja).

K 99. členu:

Predlagani člen izvaja člen 39 Direktive glede izjemnih prenosov osebnih podatkov določenim uporabnikom v tretjih državah – in to neposredno, mimo običajnega sodelovanja (posredništva) preko centralnega pristojnega organa tretje države (pot centralnega pristojnega organa) in mimo običajnih (v prejšnjih členih, v področnih zakonih, mednarodnih pogodbah določenih) pravnih poti – pač po tem členu, kjer gre v bistvu za ti. »tiktakajoča bomba« situacijo (»*ticking bomb situation*«). Prvi odstavek v uvodnem besedilu definira prenosnike osebnih podatkov le kot upravljavce (torej ne gre za obdelovalce), znotraj njih pa gre lahko le za pristojne državne organe Republike Slovenije. Uvodni kriterij je, da mora biti prenos nujno potreben za opravljanje konkretnih nalog uporabnika v tretji državi (npr. nujni prenos policijske informacije za takojšnjo policijsko akcijo v tretji državi, akcija banke glede preprečevanja pranja denarja ipd.). V 1. do 4. točki so določeni kumulativni pogoji, ki omogočajo tovrsten izjemni prenos, s tem da 4. točka določa, da mora upravljavec (državni organ) iz Republike Slovenije določiti vezanost organa (uporabnika) iz tretje države, da bo osebne podatke uporabil le za določen namen in tudi sorazmerno v okviru tega namena.

Drugi odstavek določa, da se za prenose iz prvega odstavka uporabljajo pogoji iz drugega in tretjega odstavka predprejšnjega. člena.

Tretji odstavek pa določa še dodatno izjemno pot prenosa osebnih podatkov – obvezujoče (ratificirane in objavljene) mednarodne pogodbe s področja pravosodnega sodelovanja v kazenskih zadevah in policijskega sodelovanja. Določba je pojasnilne narave (»lahko«), kar pomeni, da če je čas da se podatke pošlje po običajni poti in to (le) centralnemu pristojnemu organu druge države, se to izvede (po običajni predpisani poti).

K III. delu predloga zakona: Področne ureditve obdelave osebnih podatkov

III. del predloga zakona določa področne ureditve, ki so po svojem pomenu v bistvu področni zakoni (npr. področje videonadzora in obdelave osebnih podatkov). Pri tem sledi dosedanjemu zakonodajnemu pristopu iz ZVOP-1 (urejanje videonadzora, biometrije ipd.).

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

1. poglavje III. dela vsebuje določbe glede obdelav osebnih podatkov za znanstvenoraziskovalne, zgodovinskoraziskovalne, statistične in arhivske namene. Vzpostavljeno je ustrezno ravnotežje med vrednotami varstva osebnih podatkov in prej navedenimi področji.

K 100. členu:

Predlagani 100. 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[105], v Zakonu o državni statistiki[106] (kjer bi morda vseeno bilo potrebno urediti področno povezovanje zbirk) ter v Zakonu o raziskovalni in razvojni dejavnosti[107] (ki pa bi ga bilo treba širše spremeniti ozir. dopolniti z vidika urejanja varstva osebnih podatkov).

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

Po prvem odstavku lahko upravljavec ne glede na prvotni namen zbiranja osebne podatke, vključno s posebnimi vrstami osebnih podatkov, nadalje obdeluje za znanstvene raziskovalne, zgodovinske raziskovalne in statistične namene. Urejena je torej obdelava v druge namene glede na določbe (b) točke prvega odstavka člena 5 in člena 89 Splošne uredbe. Obdelava za te druge namene, ki so v posebnem javnem interesu, je dopustna v okviru naslednjih pravnih podlag:

- če je posameznik, na katerega se osebni podatki nanašajo za takšno obdelavo podal predhodno pisno privolitev, pri obdelavah v znanstvenoraziskovalne namene pa še posebej specificirana privolitev glede namena raziskave (torej posebna vrsta privolitve, določena na sistemski način v ZVOP-2),
- če raziskava ni nezdružljiva s prvotnim namenom obdelave osebnih podatkov,
- aliče 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 z navedbo ustreznih podatkov,
- podatke o neposrednih izvajalcih raziskave (osebno ime, naziv, prebivališče, razmerje do nosilca raziskave in šifra raziskovalca);
- podatke o znanstveno raziskovalnem področju (opisno in po klasifikaciji Agencije za raziskovalno dejavnost Republike Slovenije);
- namene oziroma cilje raziskave;
- metode dela v zvezi z osebnimi podatki,
- vrste osebnih podatkov, ki bi jih želeli pridobiti od upravljavca, ter kategorije posameznikov, na katere se nanašajo ti podatki;
- obliko, v kateri želijo prejeti osebne podatke (predvsem izvorni osebni podatki, psevdonimizirani osebni podatki, osebni podatki v obliki, ki ne zahteva identifikacije, anonimizirani podatki);
- da namenov oziroma ciljev raziskave ni mogoče doseči brez obdelave zaprošenih osebnih podatkov, z že anonimiziranimi osebnimi podatki oziroma z osebnimi podatki v manj izvirni obliki, ali da bi bilo to povezano z nesorazmernim naporom ali stroški (primernost in nujnost obdelave),
- da bi predvidene koristi od raziskave bistveno pretehtale nad posledicami, ki bi lahko nastale posameznikom, na katere se nanašajo osebni podatki (sorazmernost obdelave),
- način objave rezultatov raziskave,
- navedbo morebitnih specifičnih etičnih pravil znanstvenoraziskovalnega, zgodovinskoraziskovalnega ali statističnega področja (opcijsko pravilo) ter
- način objave raziskave oziroma njene bodoče dostopnosti oziroma navedbo kroga oseb ali subjektov, ki bodo imeli dostop do nje.
-

Predlagani so torej kumulativni strogi pogoji, kdaj lahko pridobijo osebne podatke brez privolitve, posebnega (področnega) zakona, brez anonimizacije, natančneje – raziskovalec se mora opredeliti,

zakaj anonimizacija ne bi bila ustrezno sredstvo. Etična pravila lahko raziskovalec oziroma raziskovalna organizacija navede, če je k njim zavezana.

Po tretjem odstavku raziskovalec mora elaborat vsebovati oceno učinkov, ki mora vsebovati tudi navedbo zaščitnih ukrepov (npr. varovanje dokumentacije, način pošiljanja gradiv z osebnimi podatki, ukrepe glede onemogočanja dostopa nepooblaščenim osebam…).

Četrti odstavek določa, da ima upravljavec pravico zavrniti posredovanje osebnih podatkov pod zakonsko določenimi pogoji ter tudi možnost predhodnega sodelovanja pri dopolnitvi elaborata.

Peti odstavek določa, kdaj upravljavec in izvajalec raziskave obvestita posameznika o njegovi možnosti ugovora glede obdelave osebnih podatkov.

Po šestem odstavku se osebne podatke po opravljeni raziskavi praviloma uniči.

Sedmi 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 osmem odstavku so določena posebna pravila za posameznika glede njegovih pravic s področja varstva osebnih podatkov, zlasti glede dostopa do njihove vsebine.

V devetem odstavku je določeno, da določbe 79. člena ZVOP-2 ne posegajo v (področne) določbe Zakona o varstvu dokumentarnega in arhivskega gradiva ter arhivih[108].

K 101. členu:

V 101. členu je določena obdelava naslovov za kontaktiranje posameznikov v znanstvene raziskovalne, zgodovinske raziskovalne in statistične namene. Po prvem odstavku se v okviru obdelave osebnih podatkov za namene znanstvenega raziskovanja, zgodovinskega raziskovanja ali statističnega raziskovanja upravljavcu izjemoma dovoljuje tudi obdelovati osebne podatke ciljne skupine posameznikov za potrebe pridobitve privolitev za obdelavo njihovih osebnih podatkov ali zaradi pridobitve dodatnih podatkov ali pojasnil za prej navedene namene.

Po drugem odstavku lahko upravljavec lahko na podlagi zbirk, s katerimi zakonito razpolaga v okviru zakonitega opravljanja dejavnosti, proti plačilu stroškov obdelave osebnih podatkov kontaktira posameznike z namenom pridobivanja privolitev za potrebe drugega uporabnika in za izvrševanje namenov iz prejšnjega odstavka:

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

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

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.

V petem odstavku je določeno, da določbe 101. člena predloga zakona ne posegajo v (področne) določbe Zakona o varstvu dokumentarnega in arhivskega gradiva ter arhivih[109], za področje arhivov namreč tudi veljajo (podrejeno) možnosti npr. znanstvenega raziskovanja ter zgodovinskega raziskovanja.

K 102. členu:

V predlaganem 102. členu je določena obdelava podatkov za namene arhiviranja v javnem interesu. Po prvem odstavku je obdelava osebnih podatkov za namene arhivskega delovanja je dovoljena, če je v javnem interesu in določeno z zakonom. Upravljavec mora v skladu z zakonom določiti ukrepe za varnost osebnih podatkov ter primerne in posebne ukrepe za varstvo interesov posameznika, na katerega se nanašajo osebni podatki, zlasti glede posebnih vrst osebnih podatkov.

Po drugem odstavku posameznik, na katerega se nanašajo osebni podatki, nima pravice do seznanitve z lastnimi osebnimi podatki v arhivskem gradivu po členu 15 Splošne uredbe le, če bi dajanje informacij ali kopij njegovih osebnih podatkov zahtevalo očitno nesorazmeren napor, niti ne sme zahtevati popravka osebnih podatkov zaradi netočnosti ali neposodobljenosti v skladu s členom 16 Splošne uredbe[110]. Posameznik, na katerega se nanašajo osebni podatki nima pravice zahtevati izvedbe izbrisa v skladu s pravico do pozabe iz člena 17 Splošne uredbe ipd..

Po tretjem odstavku se ne glede na določbe drugega stavka prejšnjega odstavka v primeru, kadar posameznik, na katerega se nanašajo osebni podatki in le-ta navaja netočnost in neposodobljenosti svojih osebnih podatkov, posamezniku dati na razpolago možnost za nasprotni prikaz dejstev. Pristojni arhiv mora nasprotni prikaz dejstev priložiti dokumentom ali ustrezno označiti na njih, kje se ta prikaz nahaja (posebna vrsta uradnega zaznamka).

Po četrtem odstavku posameznik, na katerega se nanašajo osebni podatki, nima pravice zahtevati omejitev obdelave po 18. členu, pravice do prenosljivosti osebnih podatkov po 20. členu ter izvajati pravice do ugovora po 21. členu Splošne uredbe.

K 2. poglavju III. dela:

2. poglavje III. dela ureja razmerja med človekovo pravico do varstva osebnih podatkov (38. člen Ustave Republike Slovenije) ter svobodo izražanja iz prvega odstavka 39. člena in dostopom do informacij javnega značaja iz drugega odstavka 39. člena Ustave Republike Slovenije.

K 103. členu:

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

V 103. členu predloga zakona 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[111]. 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[112]) področje, ki ga je treba nekoliko bolje varovati pred posegi države.

V prvem odstavku je glede na določbe prvega odstavka 39. člena Ustave Republike Slovenije zagotovljeno uresničevanje svobode izražanja, kar vključuje svobodo izražanja misli, govora in javnega nastopanja, tiska in drugih oblik javnega obveščanja in izražanja v okvirih pravnega reda Republike Slovenije. Vsakdo lahko svobodno zbira, sprejema in širi vesti in mnenja ter v njih vsebovane osebne podatke, ki so v ta namen potrebni in upravičeno obdelovani. Prvi odstavek (ozir. določbe celotnega člena) so formulirane tako, da se ne nanašajo samo na registrirane medije ali npr. akreditirane novinarje, ampak na celotno skupnost, ki izvaja svobodo izražanja (npr. tudi delovanje blogerjev, pisma bralcev, pisanje knjig…), torej ni mišljeno samo izvajanje svobode izražanja po določbah Zakona o medijih[113]. Posredno (posledično) pa pokriva predlagani člen tudi področje svobode komuniciranja[114] po 37. členu Ustave Republike Slovenije.

V drugem odstavku je natančneje določena varstvo svobode izražanja v razmerju do varstva osebnih podatkov za namene obveščanja javnosti s strani medijev, književnega, umetniškega ali znanstvenega ustvarjanja, zaradi resne kritike, obrambe kakšne pravice ali varstva upravičene koristi ter izobraževanja, ki ga izvajajo izobraževalne organizacije ali izobraževanja preko javno dostopnih publikacij, kar vključuje pravice medijev in drugih, da se osebni podatki uporabijo, objavijo ali drugače razkrijejo za namene uresničevanja svobode izražanja pod naslednjimi pogoji:

1. če je posameznik za uporabo, objavo ali razkritje podal privolitev (ki se dokazuje po določbah ZVOP-2 o dokumentiranju delovanj obdelave),

2. če je posameznik osebne podatke že javno objavil ali dal na razpolago javnosti (uporaba pravice do informacijske samoodločbe),

3. če so osebni podatki na zakonit način že bili dostopni javnosti (npr. starejše objave v okviru izvrševanja svobode izražanja),

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),

---

[111] 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....«.

[112] Uradni list RS št. 33/94 – Mednarodne pogodbe, št. 7/94, Uradni list RS, št. 102/03 – Mednarodne pogodbe, št. 22/03, Uradni list RS, št. 49/05 – Mednarodne pogodbe, št. 7/05, Uradni list RS, št. 48/09 – Mednarodne pogodbe, št. 12/09, Uradni list RS, št. 46/10 – Mednarodne pogodbe, št. 8/10 in Uradni list RS, št. 1/15 – Mednarodne pogodbe, št. 1/15.

[113] 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.

[114] 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.

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[115] (ta določba ne posega nujno v pravico do pozabe – če gre za zelo staro objavo),

6. če so bili osebni podatki pridobljeni na drug zakonit način (jih npr. nekdo drug zakonito objavil, raziskovalno novinarstvo, povzetek objave iz čezmejne obdelave ipd.),

7. če javni interes po obveščanju javnosti, pravica do obveščenosti ter svoboda izražanja prevladajo nad upravičenimi interesi varstva zasebnosti in drugih osebnostnih pravic posameznika (zlasti določbe Zakona o dostopu do informacij javnega značaja), ali

8. če tako določa drug zakon (npr. drugi in tretji odstavek 178. člena Zakona o državnem tožilstvu[116]).

Po tretjem odstavku uveljavljanje pravic v zvezi z določbami tega člena zagotavlja samo sodna oblast (sodišča) v skladu z določbami zakonov, ki urejajo svobodo izražanja in sodne postopke ali urejajo sodno varstvo (po določbah Zakona o medijih, po splošnih določbah Zakona o pravdnem postopku, Zakona o kazenskem postopku, delno pa tudi Zakona o upravnem sporu – ne gre pa več za posebno upravnosodno varstvo kot je to v 34. členu ZVOP-1).

Četrti odstavek določa, da upravljavci ali obdelovalci ne smejo subjektom svobode izražanja nezakonito posredovati, nezakonito razkriti ali nezakonito omogočiti nepooblaščenega dostopa do vsebine osebnih podatkov.

Le v petem odstavku je določena delna 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 v povezavi s četrtim odstavkom tega člena izvaja Informacijski pooblaščenec.

K 104. členu:

Podobno kot za varstvo svobode izražanja v 103. členu predloga zakona je v predlaganem 104. členu predloga zakona določena posebna ureditev tudi za varstvo ozir. uresničevanje druge človekove pravice, namreč dostopa do informacij javnega značaja (drugi odstavek 39. člena Ustave Republike Slovenije) v razmerju do človekove pravice do varstva osebnih podatkov, povzeto: obveljajo dosedanja pravila iz Zakona o dostopu do informacij javnega značaja[117].

Po prvem odstavku 86. člena ZVOP-2 lahko zavezanci po Zakonu o dostopu do informacij javnega značaja javnosti posredujejo osebne podatke, če so ti po zakonu javni ali če je za njihovo razkritje podan prevladujoč javni interes ali ne obstaja zakonsko določena izjema po določbah Zakonu o dostopu do informacij javnega značaja ali npr. Zakona o zunanjih zadevah (drugi odstavek 45.a člena)[118].

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 osebni podatki iz dokumentov, ki niso zajeti v prvem odstavku tega člena, in predstavljajo informacijo javnega značaja, na način delnega dostopa praviloma v anonimizirani obliki. V primerih,

[115] Glede pomembnosti osebnih podatkov, ki so vsebovani v mnenjih v okviru svobode izražanja ter načelni neprimernosti uporabe pravic izbrisa ali do pozabe po Splošni uredbi v takih primerih glejte: Voigt, Paul, von dem Bussche, Axel, *The EU General Data Protection Regulation (GDPR) : A Practical Guide*, Springer International Publishing AG, Cham, 2017, str. 159-160, razdelek 5.5.2.3..

[116] 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.

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

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

kjer zasledovanje navedenih ciljev na ta način ni mogoče, pa jih objavijo v psevdonimizirani obliki v skladu s Splošno uredbo. To vključuje tudi osebne podatke iz sodb sodišč Republike Slovenije (tudi prve stopnje), kjer bo v praksi najverjetneje izvedena lahko (najbolj) le psevdonimizacija s strani sodstva.

K 105. členu:

V predlaganem 105. 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 13. ali 14. členu Splošne uredbe in po določbah Zakona o splošnem upravnem postopku[119] (npr. šesti odstavek 143. člena o vabljenju k stranski udeležbi).

K 3. poglavju III. dela:

Predlagano 3. poglavje ureja uporabo osebnih podatkov za neposredno trženje (direktni marketing). Predvidena področna ureditev sledi tradiciji urejanja tega področja v zakonu o varstvu osebnih podatkov (glejte 72.-73. člen ZVOP-1) in je v predlogu zakona določena predvsem iz razloga zagotavljanja čim večje stopnje pravne (in poslovne) varnosti.

K 106. členu:

Predlagani 106. člen predloga zakona ureja pravice in dolžnosti upravljavca na področju neposrednega trženja, kar je posebna zakonska ureditev (področna obdelava v druge namene v zvezi z upravičenimi interesi upravljavca po sicer nejasni in sporno formulirano oziroma interpretirani določbi (f) točke prvega odstavka člena 6 Splošne uredbe) - glede na možnosti iz zadnjega stavka uvodne navedbe št. 47, ki je načeloma opcijska (»Obdelava osebnih podatkov za neposredno trženje se lahko šteje za opravljeno v upravičenem interesu.«).

Predlagani člen tako ureja pravice in dolžnosti upravljavca na področju neposrednega trženja, oziroma še točneje, ureja podrobnejša pravila glede možnosti uporabe osebnih podatkov, zbranih za neke druge namene, tudi za namen neposrednega trženja. S tem pomembno dopolnjuje Splošno uredbo, v kateri posebnih pravil za to sicer zelo pomembno področje ni, saj glede tega obstaja le uvodna navedba št. 47, ki je načeloma opcijska (»Obdelava osebnih podatkov za neposredno trženje se lahko šteje za opravljeno v upravičenem interesu.«). V svojem bistvu je primerljiv določbam dosedanjega 72. člena ZVOP-1, s tem da so določeni izrazi usklajeni z izrazoslovjem Splošne uredbe (tako se npr. za obdelavo posebnih vrst osebnih podatkov navaja kot pravna podlaga izrecna privolitev in ne pisna privolitev).

Bistveni namen predlaganega prvega odstavka je podjetjem in drugim organizacijam omogočiti (oz. ohraniti) izrecno zakonsko podlago za osnovno (nesegmentirano, neindividualizirano) neposredno trženje obstoječim strankam, torej posameznikom, ki so z njimi že opravili nek nakup ali drugo podobno transakcijo, pa pri tem pustili svoje kontaktne podatke, ali pa za trženje posameznikom, katerih kontaktne podatke so pridobili iz javnih virov. V teh primerih lahko upravljavec te kontaktne podatke uporabi za nadaljnje trženje svojih izdelkov, storitev oz. zaposlitev, brez da bi rabil izkazovati, da ima za to zakonite interese (v smislu točke (f) prvega odstavka 6. člena Splošne uredbe), oziroma, da da je namen neposrednega trženja združljiv z namenom, za katerega so bili podatki že prvotno zbrani (v smislu četrtega odstavka 6. člena Splošne uredbe). S tem predlog zakona sledi obstoječi ureditvi iz 72. člena ZVOP-1, s čemer obenem tudi ohranja pravno podlago za morebitne obstoječe zbirke kontaktnih podatkov, zbrane tekom večletnega opravljanja dejavnosti. To imetnikom takšnih zbirk zagotavlja pravno varnost, saj so, dokler lahko pokažejo na vir podatkov (tržna transakcija ali javni vir), lahko prepričani v obstoj pravne podlage za njihovo nadaljnjo hrambo in uporabo za neposredno trženje. Pri tem je pa seveda potrebno poudariti, da lahko upravljavec na tej (zakonski)

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

podlagi za oblikovanje trženjskih sporočil uporabo zgolj v členu določene kontaktne podatke svojih strank (osebno ime, naslov bivališča, telefonska številka, e-poštni naslov), ne pa tudi drugih podatkov, še zlasti pa ne podatkov o nakupovalnih in podobnih navadah stranke.

Uporaba drugih osebnih podatkov za potrebe neposrednega trženja, oziroma uporaba kontaktnih podatkov, pridobljenih na drug način, pa je urejena v predlaganem drugem odstavku. Ta določa, da mora upravljavec za takšno uporabo zagotoviti katero od veljavnih pravnih podlag po Splošni uredbi, npr. privolitev posameznika ali (in še zlasti) obstoj lastnih zakonitih interesov za izvajanje takšnega trženja, nad katerimi pa ne smejo prevladati interesi zadevnega posameznika. Obstoj te pravne podlage mora upravljavec seveda ustrezno in utemeljeno dokumentirati, česar mu pri osnovnih (tj. kontaktnih) podatkih po prvem odstavku ne bo treba, saj tam zadostuje že dokazilo o viru podatkov. S tem se, seveda pod pravili iz Splošne uredbe, dovoljuje tudi naprednejše oblike neposrednega trženja, kot so segmentiranje, profiliranje, remarketing, in podobno.

Tretji odstavek ureja pravila igre pri pošiljanju trženjskih sporočil, ki seveda morajo biti ustrezno označena kot taka, prav tako pa mora biti posamezniku dana jasna možnost, da se odjavi od njihovega nadaljnjega prejemanja (opt-out). Teh informacij pa posamezniku ni treba posredovati, če jih že ima (četrti odstavek).

V predlaganem petem odstavku je določena prepoved glede uporabe osebnih podatkov s področja neposrednega trženja za področje političnega trženja (volitve, referendumi), s čimer je izrecno določena neskladnost med poslovnim in političnim namenom obdelave osebnih podatkov. Odločitev za takšno rešitev izvira zlasti iz nedavnih afer »Cambridge Analytics« ter »Deutsche Post«. Povezana določba v šestem odstavku tudi določi prepoved prodaje teh podatkov drugim osebam za namene političnega trženja.

V sedmem odstavku se ureja razmerje z ureditvijo neposrednega trženja (tudi: neželene komunikacije) po zakonu, ki ureja elektronske komunikacije (tj. Zakon o elektronskih komunikacijah, ZEKom-1). V skladu s slednjim lahko fizična ali pravna oseba z uporabo elektronskih komunikacij trži svoje izdelke ali storitve posameznikom le na podlagi njihove privolitve (prvi oziroma tretji odstavek 158. člena ZEKom-1), z eno in edino izjemo, da sme tudi brez privolitve poslati trženjsko e-poštno sporočilo istim posameznikom, ki so pri njej v preteklosti kaj kupili in pri tem pustili e-poštni naslov (drugo odstavek 158. člena ZEKom-1). Takšna ureditev je seveda bistveno strožja od te po predlaganem členu, saj ne dopušča trženja po e-pošti tudi na javno dostopne e-poštni naslove oz. po drugih elektronskih kanalih na kakšni drugih podlagi kot pa na podlagi privolitve (torej ne dovoljuje zanašanja na zakonite interese). Predlagatelj seveda razume restriktivnost zakonodajalca pri sprejemu ZEKom-1, zlasti njegove želje, da zaščiti naročnike storitev pred nezaželenimi klici in e-poštnimi sporočili. Vendar pa obenem šteje, da bi bilo primerneje pravne podlage za pridobivanje podatkov za oblikovanje in naslavljanje trženjskih sporočil urediti v zakonu, ki ureja varstvo osebnih podatkov, načine obrambe pred nezaželenimi elektronskimi sporočili pa v zakonu, ki ureja elektronske komunikacije. Tako šteje, da naj se kot pravne podlage štejejo vse, ki so določene v prvem in drugem odstavku tega člena, medtem ko naj se omejitve pošiljanja trženjskih sporočil z uporabo elektronskih komunikacij ureja v 158. členu ZEKom-1 (po začetku veljave prihajajoče Uredbe o zasebnosti in elektronskih komunikacijah pa v tej).

K 107. členu:

Predlagani člen določa posebno pravico do ugovora ozir. prekinitve dogovorjenega dela od upravljavca glede njegovih osebnih podatkov, ki se obdelujejo za namene neposrednega trženja. Enak člen je vsebovan v določbah dosedanjega 73. člena ZVOP-1. Po vsebini gre za ti. »opt-out« določb**o.**

K 4. poglavju III. dela:

4. poglavje III. dela zakona ureja pomembno področno ureditev – videonadzor. Vsebina ima pomen ti. »področne zakonodaje« in razreši konflikt med pravico do varstva osebnih podatkov napram izvajanju videonadzora.

K 108. členu:

S 108. členom se začne posebno (četrto) poglavje III. dela predloga zakona, ki velja za področno ureditev (kot da bi bila poseben zakon). Določbe tega poglavja veljajo za vse uvedbe videonadzora v Sloveniji, razen če kak področni zakon posebej (podrobno) ureja videonadzor, prav tako pa ta področna ureditev pomeni, da videonadzora ni možno uvesti z uporabo sistemskih pravnih podlag za obdelavo osebnih podatkov (glejte 7. člen predloga zakona)[120], Prav tako splošne določbe tega člena veljajo za vse ureditve videonadzora v tem poglavju.

V 108. členu se tako urejajo splošne določbe o videonadzoru in obdelavi osebnih podatkov. Člen je pretežno enak določbam dosedanjega 74. člena ZVOP-1, z določenimi dodatnimi rešitvami (pravno-tehnična definicija videonadzora v petem odstavku, šestmesečni rok v sedmem odstavku). Podatki, ki se obdelujejo po petem odstavku so: posnetek posameznika (slika), datum in čas posnetka. Prav tako lahko zbirka posnetkov vsebuje tudi zvok, če je v tem ali drugem zakonu tako posebej določeno.

K 109. členu:

Predlagani 109. člen določa uporabo videonadzora glede dostopa v uradne službene oziroma poslovne prostore. V predlagani določbi se prevzema vsebina dosedanjega 95. člena ZVOP-1.

K 110. členu:

V 110. členu je urejen videonadzor v zvezi z večstanovanjskimi stavbami, podrobno kot je to določeno v dosedanjem 76. členu ZVOP-1. Tretji odstavek posebej poudarja pomen (pisne) privolitve, četrti in peti odstavek definirata za ta kontekst posebej kdo je upravljavec ter kje se sme izvajati videonadzor, osmi odstavek pa določa, da je izjemoma dovoljeno omogočiti združitev videonadzornega sistema z napravami, ki jih uporabljajo lastniki za potrebe vstopa v večstanovanjsko stavbo, kot sta na primer domofon ali video domofon, razen če te naprave omogočajo snemanje ali spremljanje dogajanja v območju izvajanja videonadzora na posamezni napravi. Spremljanje dogajanja v območju izvajanja videonadzora mora onemogočiti upravljavec videonadzora. V šestem odstavku obstoječi prepovedi videonadzora glede hišniškega stanovanja ter delavnice za hišnika ni dodana tudi prepoved videonadzora prostorov za čistilke in čistilce, saj v tem primeru ne gre za znatno polje utemeljenega pričakovanja zasebnosti, niti ne obstaja specifična pravna ureditev prostorov za čistilke ali čistilce[121]. Vendar to z vidika splošnega načela sorazmernosti ne preprečuje, da se pri oceni učinkov oceni, da ni primerno uporabiti videonadzornega sistema v zvezi s prostori za čistilke ali čistilce, kar bo verjetno upoštevno v večini primerov, zlasti z vidika spoštovanja osebnega dostojanstva po 34. členu Ustave Republike Slovenije.

K 111. členu:

V predlaganem 111. členu ZVOP-2 je urejen videonadzor znotraj delovnih prostorov, gre za nekoliko drugačno ureditev glede vstopov v uradne službene oziroma poslovne prostore kot v 109. členu predloga ZVOP-2, tukaj gre namreč za snemanje znotraj delovnih prostorov. Člen je pretežno enak 77. členu dosedanjega ZVOP-1, s tem da je v prvem odstavku sedaj omenjeno tudi področje (namen) preprečevanja ali odkrivanja kršitev na področju iger na srečo. V tretjem odstavku pa je dodano, da je spremljanje neposrednega dogajanja pred kamerami pod pogoji iz prvega in drugega odstavka dopustno le, če ga izvaja pooblaščeno varnostno osebje ali drugo posebej pooblaščeno ter ustrezno usposobljeno osebje upravljavca (npr. glede na specifično delovno področje posebej pooblaščeni in

[120] Glejte npr.: sodba Upravnega sodišča RS, opr. št. I U 1843/2015, 15. 6. 2017, 11.-13. točka.
[121] Glejte npr. prvi odstavek 5. člena Stanovanjskega zakona (Uradni list RS, št. 69/03, 18/04 – ZVKSES, 47/06 – ZEN, 45/08 – ZVEtL, 57/08, 62/10 – ZUPJS, 56/11 – odl. US, 87/11, 40/12 – ZUJF, 14/17 – odl. US in 27/17) o hišniških stanovanjih in delavnicah za hišnike.

usposobljeni uslužbenci Arhiva Republike Slovenije). Posebna dodana vrednost je v petem odstavku, kjer je določeno, da se mora pred uvedbo videonadzora v osebi javnega ali zasebnega sektorja delodajalec posvetovati z reprezentativnimi sindikati pri delodajalcu ter svetom delavcev ali delavskim zaupnikom (dosedaj je bilo to določeno le glede reprezentativnih sindikatov pri delodajalcu), kar je »jamstveni« prispevek k dodatnemu spoštovanju človeškega dostojanstva z uporabo mehanizmov participacije s področja socialne države (2. člen Ustave Republike Slovenije). To pomeni, da delodajalec pridobiva le mnenje sindikata ali drugega predstavnika delavcev, da ne gre za soglasje. Delodajalec po prejetju mnenja v tem postopku posvetovanja[122] dokončno odloči o uvedbi ali neuvedbi videonadzora v delovnih prostorih, gre torej le za obveznost proučitve morebitnih nasprotnih argumentov, ne pa za vezanost na mnenje (posvetovanje namreč vsebinsko ne pomeni zahteve po soglasju).

V sedmem odstavku je na podoben način kot pri videonadzoru in večstanovanjskih stavbah (drugi odstavek 110. člena) določen tudi način uvedbe videonadzora v poslovnih zgradbah, kjer je lahko več lastnikov.

K 112. členu:

V 112. členu je urejena nova vrsta videonadzora, namreč izvajanje videonadzora na javnih površinah, kar dosedaj ni bilo urejeno v ZVOP-1. Določbe so načeloma previdno in sorazmerno napisane, upoštevajo delno dejansko stanje, njihov namen pa ni podpiranje ali promocija ali razvoj ti. »totalne nadzorovalne družbe«. Po prvem odstavku je videonadzor na javnih površinah dovoljen le v izjemnih primerih, kadar je to nujno potrebno, ker obstaja resna in utemeljena nevarnost za življenje ali zdravje ljudi, varnost premoženja ali varovanje tajnih podatkov in tega namena ni mogoče doseči z milejšimi sredstvi (prvi strogi kriterij/skupek pogojev kumulativne narave). Prav tako je dovoljen za potrebe varovanja prostorov, zgradb ali območij, ki jih je potrebno varovati na podlagi zakona ter objektov, prostorov in oseb, katere varuje policija in sicer samo v obsegu in trajanju, ki je za dosego teh namenov nujno potreben (drugi in nekoliko milejši kumulativni kriterij). Predlagane določbe prvega dela stavka glede resne in utemeljene nevarnosti za življenje ali zdravje ljudi ter varnost premoženja po naravi stvari veljajo tako za javni sektor kot za zasebni sektor[123] in tako določajo meje možnih posegov v pravico do varstva osebnih podatkov.

Po drugem odstavku se videonadzor lahko izvaja le glede tistih delov javne površine in v obsegu, kjer je potrebno varovati interese iz prvega odstavka 112. člena ZVOP-2.

V tretjem odstavku je podana še pravnoorganizacijska omejitev, po kateri lahko videonadzor na javnih površinah izvaja le oseba javnega ali zasebnega sektorja, ki upravlja z javno površino ali na njej zakonito opravlja dejavnost.

K 5. poglavju III. dela:

V 5. poglavju III. dela se ureja eno najpomembnejših področij (iz področnih ureditev) predloga zakona, namreč področje biometrije. Biometrija omogoča avtomatizirano obdelavo osebnih podatkov in je eno najnevarnejših področij obdelave osebnih podatkov, ki lahko v primeru (pre)široke obdelave s strani javnih organov pripelje do ti. »totalne nadzorovalne družbe«, v primeru obdelave s strani zasebnega sektorja pa k razosebljenju posameznika. Zato so v predlogu zakona na to temo podane podrobne določbe.

[122] Glejte npr.: sodba Vrhovnega sodišča RS, opr. št. VIII Ips 32/2015, 8. 4. 2015, 14. točka.
[123] Glejte tudi posvetovanje o obdelavi osebnih podatkov in videonadzoru, ki se izvaja v okviru Evropskega odbora za varstvo podatkov (zlasti str. 15-16): https://edpb.europa.eu/our-work-tools/public-consultations/2019/guidelines-32019-processing-personal-data-through-video_en

K 113. členu:

S 113. členom se začne 5. poglavje III. dela predloga zakona – urejanje biometrije oziroma biometričnih ukrepov. Kot je že bilo uvedeno v ZVOP-1 leta 2004, je zakonodajni pristop glede biometrije dokaj zadržan in garantističen, kar pomeni – načeloma nenaklonjen uporabi biometrije[124]. Ne glede na navedeno predlagane rešitve nekoliko omogočajo širšo uporabo biometrije (za zasebni sektor), kot je to dosedaj bila urejena v ZVOP-1.

113. 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 139. členu ZVOP-2.

K 114. členu:

V predlaganem 114. členu se urejajo biometrični ukrepi v zasebnem sektorju. Po prvem odstavku lahko zasebni sektor izvaja biometrične ukrepe le, če so nujno potrebni za opravljanje dejavnosti, za varnost ljudi ali premoženja ali za varovanje tajnih podatkov ali poslovne skrivnosti v skladu z določbami tega člena. Po drugem odstavku sme biometrične ukrepe izvajati nad svojimi zaposlenimi ter nad tistimi osebami, ki so zaposlene pri pogodbenih partnerjih upravljavca, če je to potrebno za namene varovanja interesov iz prvega odstavka in so bili te osebe o tem predhodno pisno obveščene. Po tretjem odstavku zasebni sektor lahko izvaja biometrične ukrepe tudi nad svojimi strankami pod naslednjimi pogoji:, da tako za namene varovanja interesov iz prvega odstavka določa zakon in so stranke podale pisno privolitev ter se na ta način preprečuje nastanek hude škode, kar je pomembna izjema od strogega pristopa k dovoljeni uporabi biometrije. V četrtem odstavku je kot varovalni organizacijski ukrep določeno da mora upravljavec osebnih podatkov, ki namerava izvajati biometrične ukrepe, še pred uvedbo ukrepov posredovati Informacijskemu pooblaščencu opis nameravanih ukrepov in razloge za njihovo uvedbo. V petem odstavku je določeno, da je Informacijski pooblaščenec dolžan po prejemu posredovanih informacij iz četrtega odstavka dolžan v dveh mesecih odločiti, ali je nameravana uvedba biometričnih ukrepov v skladu s tem zakonom, predvsem s pogoji iz prvega stavka prvega odstavka tega člena. Rok se ob upoštevanju zapletenosti predvidene obdelave lahko podaljša za največ dva meseca. Po šestem odstavku sme upravljavec osebnih podatkov izvajati biometrične ukrepe šele po prejetju 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 139. členu predloga zakona.

K 115. členu:

Predlagani 115. člen določa posebno (dodatno) prepoved glede uporabe biometrije za zasebni sektor. Predlagano je, da zasebni sektor ne sme zahtevati, pridobiti ali nadalje obdelovati osebnih podatkov v

[124] Glejte tudi četrti odstavek 9. člena Splošne uredbe, po katerem »Države članice lahko ohranijo ali uvedejo dodatne pogoje, tudi omejitve, glede obdelave genetskih, biometričnih ali podatkov v zvezi z zdravjem.«

zamenjavo za določene storitve, pa četudi so te storitve (npr. storitve informacijske družbe) brezplačne. Za javni sektor ni dane izrecne prepovedi v posebnem členu, saj predlagatelj ocenjuje, da je z vidika (vsaj) 34. in 38. člena Ustave Republike Slovenije nepredstavljivo, da bi javni sektor (pa četudi bi to vprašanje morda vseeno poskusil urediti v zakonu) lahko zahteval biometrične podatke od ljudi za določene komercialne (trženjske) storitve. Drugače seveda velja (je dopustno), ko gre za vprašanje izpolnjevanja zakonskih obveznosti (npr. s področja državne uprave – 120. člen Ustave Republike Slovenije) – dajanje fotografij za osebne dokumente ipd.

Določen je tudi ustrezni prekršek v 140. členu predloga zakona.

Predlagana ureditev v tem členu ne pomeni, da je podana sistemska opredelitev glede vprašanja zamenjave osebnih podatkov za določene (četudi brezplačne) storitve - za področja varstva in obdelave osebnih podatkov. O teh vprašanjih se bo odločalo na podlagi splošnih pravil tega zakona in Splošne uredbe (sorazmernost, poštenost, namenska obdelava...).

K 116. členu:

V 116. členu predloga zakona je določena obdelava osebnih podatkov v okviru evidentiranja vstopov in izstopov iz službenih prostorov, podobno kot je to že urejeno v 82. členu ZVOP-1. Po prvem odstavku oseba javnega ali zasebnega sektorja lahko za zagotavljanje varnosti ljudi in premoženja, ter reda v njenih prostorih ali v prostorih, ki jih ima v uporabi od posameznika, ki namerava vstopiti ali izstopiti iz tega prostora, zahteva, da navede vse ali nekatere osebne podatke iz drugega odstavka tega člena ter razlog vstopa ali izstopa. Po potrebi pa lahko osebne podatke preveri tudi z vpogledom v osebni dokument posameznika. Po drugem odstavku se v zbirki o vstopih in izstopih iz službenih prostorov lahko o posamezniku vodijo samo naslednji osebni podatki, kadar je to potrebno: osebno ime, številka in vrsta osebnega dokumenta, naslov prebivališča, zaposlitev, vrsta in registrska številka vozila ter datum, ura in razlog vstopa ali izstopa v ali iz prostorov. Po tretjem odstavku evidenca iz prejšnjega odstavka velja za uradno evidenco v skladu z Zakonom o splošnem upravnem postopku (drugi odstavek 179. člena), če je potrebno pridobiti podatke iz nje z vidika koristi mladoletnika ali za izvrševanje pristojnosti policije ter obveščevalno-varnostne dejavnosti. Po četrtem odstavku se osebni podatki iz evidence iz drugega odstavka tega člena se lahko hranijo največ tri leta (rok hrambe) od vpisa, nato se zbrišejo ali na drug način uničijo, če zakon ne določa drugače.

Predlagani člen ima določen tudi prekršek za kršitve v 141. členu predloga zakona.

K 117. členu:

V 117. členu je določeno, da se lahko osebni podatki iz javne knjige, urejene z zakonom (npr. zemljiška knjiga), uporabljajo le v skladu z namenom[125], 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 142. členu predloga zakona.

K 118. členu:

Predlagani 118. člen o povezovanju uradnih evidenc in javnih knjig predstavlja nadaljevanje in v določeni meri tudi nadgradnjo obstoječe ureditve povezovanja zbirk osebnih podatkov iz 84. člena ZVOP-1. Glavna vsebina ureditve tako ostaja enaka kot dosedaj, in sicer, da se omejuje vsako količinsko ozir. kakovostno znatnejše povezovanje uradnih evidenc med sabo ali z zunanjimi evidencami zgolj na tiste primere, ko sta to posebej dovolila zakonodajalec oziroma v (najbolj tveganih) primerih tudi Informacijski pooblaščenec.

[125] 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.

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

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

Ekstremni primer, ki ga ta ureditev preprečuje, je t.i. nastanek/omogočanje »totalne nadzorovalne družbe«. Preprečevalni pristop izhaja iz francoske »afere SAFARI« iz leta 1974[126], ko so se v Francoski republiki izvrševale zakonodajne priprave, da se preko povezovanj množice informatiziranih zbirk osebnih podatkov doseže nastanek ene (centralne; centralizirane) zbirke osebnih podatkov, za povezovanje pa bi se uporabila takratna francoska enotna matična številka občana (INSEE koda). Projekt je bil na koncu preklican zaradi nasprotovanja javnosti oziroma razumevanja, da uvedba takšne totalne družbe nadzora nikakor ne more biti dopustna v razmerah, ki niso ne izredno niti vojno stanje, pa še takrat bi lahko tovrstna ureditev bila dopustna le začasno in v skladu z načelom sorazmernosti.

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

Definicija povezovanja je zdaj urejena v samem členu (tretji odstavek), pri čemer je po novem določena tehnološko nevtralno ozir. bolj splošno, tako da lahko vključuje različne tehnične načine izvajanja povezovanja zbirk, ki so se pojavila v zadnjih desetih letih. Definicija se namesto na sam način povezovanja osredotoča zlasti na obseg in pogostost povezovanja, ter tveganja, ki pri tem nastajajo. Bistveno vprašanje pri presoji, ali določeno dostopanje do uradne zbirke šteje za povezovanje je, ali zaradi takšne povezave nastanejo znatno večja tveganja za pravice posameznika. Tako je vseeno, ali se povezovanje izvede samodejno oz. brez zahteve uporabnika (npr. da informacijski sistemi medsebojno čez noč posodabljajo osebne podatke ob spremembah kot v primeru Centralnega registra prebivalstva) ali pa na zahtevo uporabnika (primer eSociala, kjer sistem na zahtevo uporabnika z uporabo različnih centralnih gradnikov pridobi osebne podatke posameznika iz 44 zbirk). Posledice pa so v praksi iste. Prav tako je vseeno, ali se prejeti podatki združijo šele pri uporabniku ali na kakšnem mestu pred njim (primer rešitve ti. »Pladenj«). Prav tako se kot povezovanje šteje tudi vodenje različnih zbirk pri istem upravljavcu ali obdelovalcu, razen če so organizacijsko in tehnično ustrezno ločene, saj bi sicer kršitev pravil varstva osebnih podatkov na eni

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

od povezanih zbirk lahko imela posledice še za ostale povezane zbirke. Smiselno eneko velja tudi v primeru, če isti pogodbeni obdelovalec vodi različne zbirke za različne upravljavce. Če te zbirke niso ustrezno ločene, je tudi treba govoriti o povezovanju.

Tako kot dosedaj pa se za povezovanje ne štejejo primeri, ko se pooblaščeni uporabnik v okviru upravnega ali drugega individualnega postopka prijavi v zbirko osebnih podatkov, iz katere je pooblaščen pridobiti osebne podatke posameznika (primeri aplikacij za posamične poizvedbe v centralnih registrih, kot je e-RISK v primeru Centralnega registra prebivalstva ali e-Poizvedbe na področju zdravstvenega zavarovanja). V takšnem primeru ni posebej povečanih tveganj za pravice in svoboščine posameznika. Ključna razlika med povezovanjem zbirk osebnih podatkov in posameznim pridobivanjem osebnih podatkov je v tem, da se posamezniku v primeru povezanih zbirk podatkov pred vsako posamično poizvedbo v zbirko podatkov ni treba posebej prijavljati v vsako zbirko osebnih podatkov.

Vse navedeno za upravljavce, ki bi želeli povezovati svoje zbirke z uradnimi evidencami ali javnimi knjigami (kar vključuje tako povezavo med samimi uradnimi evidencami, povezavo med javnimi knjigami, povezavo med evidencami in javnimi knjigami, povezavo uradnih evidenc z drugimi zbirkami, povezavo javnih knjig z drugimi zbirkami kot tudi povezavo uradnih evidenc in javnih knjig z drugimi zbirkami), nalaga določene pripravljalne obveznosti. Intenzivnost teh obveznosti je odvisna od tveganosti podatkov zbirki, s katero se želi povezovati.

Za povezovanje z vsebinsko najbolj tveganimi uradnimi evidencami (zlasti: evidence posebnih vrst osebnih podatkov, evidencami premoženjskih in dohodkovnih podatkov) bo moral upravljavec po novem od zakonodajalca dobiti izrecno odobritev (torej določitev v zakonu)[127], da sme pridobivati podatke s pomočjo povezovanja (torej, ob premisleku tveganj, ki lahko nastopijo zaradi tega) preko sprejetja določb v področnem zakonu (npr. Zakon o sodnem registru).

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

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

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

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

Ker obstajajo določeni režimi povezovanja s ključnimi uradnimi evidencami ipd., ki ne zadostijo tem pogojem, je v prehodnih določbah določeno štiriletno prehodno obdobje za uskladitev z novimi pravili. Navedeno postroženje bo tako nastopilo le postopoma. V vmesnem času bodo lahko bolj tvegana

[127] Glejte tudi sodbo Upravnega sodišča RS, opr. št. I U 1715/2011, 18. 4. 2012, kjer je med drugim navedeno: […] Sodišče meni, da je zakonodajalec s tem, ko je ministrstvu zgolj dal možnost take povezave, ni pa navedel, da se te zbirke morajo povezati, predvidel, da tako povezovanje lahko pride v poštev, če ni katere druge ovire, ki bi tako povezovanje preprečila. V konkretnem primeru pa tak zadržek obstaja, to je določilo 199. člena ZZK-1, ki onemogoča tak način povezovanja. V ponovljenem postopku bo morala tožena stranka upoštevati stališča sodišča glede uporabe materialnega prava, kot so navedena v tej sodbi. […]«

povezovanja potekajo na istovrstni zakonski podlagi kot manj tvegana (se pravi, zakon mora določati vsaj možnost pridobivanja podatkov iz zadevnih uradnih evidenc), pri čemer pa se še vedno mora pridobiti dovoljenje Informacijskega pooblaščenca (četrti odstavek člena, za katerega prehodno obdobje ne velja).

V roku štirih let bo torej treba poskrbeti za prilagoditev zakonske podlage, sicer bo lahko nastopila situacija, da bo Informacijski pooblaščenec povezovanje prepovedal.

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

- eSociala I/O modul in namenski spletni servisi – JE POVEZOVANJE, velja strožja ureditev po prvem odstavku
- eSociala asinhroni modul (uporabnik na center za socialno delo (CSD) prek ISCSD2 sistema in Pladnja posreduje zahtevo bankam, banke gredo po zahtevek na pladenj, vsak zahtevek obdelajo ročno in poizvedbe ne spustijo v svoj sistem, pripravijo podatke in jih čez nekaj časa odložijo na Pladenj, kjer so na voljo uporabniku na CSD-ju) – JE POVEZOVANJE, velja strožja ureditev po prvem odstavku;
- pridobivanje podatkov zaradi odločanja o vlogah za dodelitev neprofitnih stanovanj po 11.a členu Stanovanjskega zakona – JE POVEZOVANJE, velja strožja ureditev po prvem odstavku, v prehodnem obdobju je potrebno prilagoditi zadevni člen, da bo izrecno dovoljeval povezovanje kot način pridobivanja podatkov;
- informacijski sistem TIRS, ki inšpektorju omogoča, da v tem sistemu brez posebne prijave v CRP za določeno osebo iz CRP pridobi njene podatke ali hkrati pridobi podatke za večje število oseb – JE POVEZOVANJE; zanj velja milejši režim po drugem odstavku;
- aplikacije e-RISK, e-Poizvedbe, eMRVL - dostop do podatkov v registru MRVL – NI POVEZOVANJE, če pa se posamezne evidence povezujejo preko spletnih servisov, npr. prekrškovna evidenca redarskih služb, pa JE POVEZOVANJE;
- spletni servis, kjer se uporabnik na občini pred poizvedbo posebej avtenticira za dostop do zbirke osebnih podatkov in dobi podatke hkrati za več posameznikov – paketna poizvedba (npr. vsi, ki imajo 50 let) – JE POVEZOVANJE; odvisno od podatkov, ki se pridobivajo, velja strožji ali milejši režim;
- spletni servis, kjer se uporabnik na občini pred poizvedbo posebej avtenticira za dostop do zbirke osebnih podatkov in pridobi podatke za enega posameznika (posamična poizvedba) – NI POVEZOVANJE;
- spletni servis, kjer se uporabnik na občini pred poizvedbo posebej avtenticira za dostop do zbirke osebnih podatkov hkrati za več posameznikov (oseba na občini pripravi podatke, naredi izvoz, zapeče podatke na CD ali jih odloži na neko mesto za prevzem - JE POVEZOVANJE odvisno od podatkov, ki se pridobivajo, velja strožji ali milejši režim.

K 9. poglavju III. dela predloga zakona:

Institut strokovnega nadzora je urejen v večjem številu drugih zakonov, vendar navedeni zakoni ne urejajo vprašanj obdelave (ali varstva) osebnih podatkov. Zato so ta vprašanja (kot že v ZVOP-1) urejena v posebnem poglavju predloga zakona.

K 119. členu:

V 119. členu je določena uvodna določba za posebno poglavje (9. poglavje) III. dela predloga zakona o strokovnem nadzoru in obdelavi osebnih podatkov. V tem poglavju so določena pravila obdelave osebnih podatkov pri opravljanju strokovnega nadzora, če področni zakoni ne določajo drugače. S predlaganim poglavjem se upošteva možnost pravne praznine na tem področju, saj veljavni področni zakoni ne vsebujejo vedno določb o obdelavi osebnih podatkov pri opravljanju strokovnega nadzora. Predlagano poglavje je uporabno predvsem na področju socialnega varstva in zdravstva, kjer imajo npr. državni organi ali nosilci javnega pooblastila v njihovih področnih zakonih običajno določeno le pristojnost oziroma obveznost opravljanja strokovnega nadzora, ni pa tudi nujno določeno vsebinsko (materialno), kaj konkretno lahko izvajalec strokovnega nadzora pri njegovem opravljanju opravi glede dostopa do vsebine osebnih podatkov, za kar pa je treba določiti ustrezno ureditev tudi v zvezi s 7. členom predloga zakona (načelo zakonitosti glede obdelave osebnih podatkov).

K 120. členu:

V 120. členu so ponovljene dosedanje konkretne določbe o obdelavi osebnih podatkov v okviru strokovnega nadzora, kot je to določeno že v 88. členu ZVOP-1. S tem členom so povezane prekrškovne določbe v 144. členu predloga zakona.

K 121. členu:

V 121. členu je določeno obveščanje posameznika (prvi odstavek) in dodatna obdelava osebnih podatkov v okviru strokovnega nadzora (drugi odstavek), kot je to določeno v 89. členu ZVOP-1.

K 122. členu:

V 122. 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 147. členu ZVOP-2.

K 10. poglavju III. dela predloga zakona:

V 10. poglavju III. dela predloga zakona sta urejeni dve področji delovanj obdelav osebnih – objave kontaktnih podatkov za potrebe izvajanja uradnih ali drugih postopkov ali poslovanj (tako za zasebni kot za javni sektor) ter obdelava osebnih podatkov za izvajanje določenih neoblastnih delovanj javnega sektorja.

K 123. členu:

Predlagani 123. člen določa objavo kontaktnih podatkov za potrebe uradnih postopkov, kot je to določeno že v drugem odstavku 106. člena ZVOP-1.

K 124. členu:

V 124. členu se ureja posebna pravna podlaga za obdelavo osebnih podatkov za izvajanje določenih dejavnosti javnega sektorja, zlasti za organiziranje določenih običajnih uradnih dogodkov. Konkretneje gre za ureditev vprašanja kako pridobiti (in nadalje obdelovati) osebne podatke za udeležbo na državnih proslavah in drugih uradnih dogodkih (tudi medijske konference, izdaje raznih knjig ipd.).

V tem primeru ne gre za izvrševanje oblastvenih[128] nalog ali pristojnosti javnega sektorja v smislu odločanja o človekovih pravicah ali temeljnih svoboščinah ali obveznostih, gre ali za uporabo javno dostopnih podatkov ali za podatke, pridobljene ob opravljanju uradnih nalog javnega sektorja ali pa za delovanje ob upoštevanju posameznikove podatkovne samoodločbe, da pač razkrije svoje osebne podatke določenemu krogu ljudi v določenemu subjektu javnega prava ozir. le temu subjektu javnega

[128] Za okvirno opredelitev neoblastvenih delovanj državnega organa glejte smiselno: Sklep Upravnega oddelka Vrhovnega sodišča RS, opr. št. I Up 231/2016, 1. 2. 2017: »11. Delovanje Varuha niti z vidika splošne opredelitve njegovih nalog in pristojnosti niti z vidika ravnanja v konkretnem primeru očitno ne ustreza značilnostim oblastvenega delovanja. Njegovo ravnanje je usmerjeno v nadzor nad delovanjem nosilcev oblasti in se tudi izraža v ukrepih, ki so usmerjeni prav zoper navedene oblastvene subjekte in ne druge osebe, nosilce človekovih pravic in temeljnih svoboščin. Še več, tudi samo delovanje Varuha je tako po zakonski kot po konceptualni opredelitvi neoblastno in le omejeno formalizirano […].«

prava. To prostovoljno razkritje, ki običajno ne zahteva podaje (izrecne) privolitve, je podobno določbi (e) točki drugega odstavka 9. člena Splošne uredbe – prostovoljno razkritje posebne vrste osebnih podatkov. V isti smeri je določeno, da so tej pravni podlagi enakovredni tudi osebni podatki, pridobljeni iz javnega vira ter osebni podatki, pridobljeni na drug zakonit ali običajen način (npr. izmenjava e-poštnih naslovov z istega delovnega področja ipd.). Urejena je torej pravna podlaga za npr. zbiranje in obdelavo osebnih podatkov seznamov obiskovalcev državnih proslav, seznam novinarjev z elektronskimi naslovi, seznamov državljanov Republike Slovenije za udeležbo na prireditvah na diplomatsko-konzularnih predstavništvih ali drugih državljanov ali diplomatov za uradne sprejeme, vodenje osebnih imen staršev zaradi vabil na ti. »nadstandardne« šolske aktivnosti – npr. eAsistent. Običajni osebni podatki, ki se bodo zbirali in nadalje obdelovali v skladu z načelom sorazmernosti in glede na okoliščine posamezne situacije ozir. dogodka, so npr.: osebno ime, znanstveni ali strokovni naslov, naslov elektronske pošte, telefonska številka, naslov institucije ali izjemoma naslov domačega prebivališča, morebitna zaposlitev ali funkcija ali članstvo v določenem klubu ipd.). Navedeni osebni podatki se bodo zbirali z običajno prakso – posameznikom bo zlasti dana možnost, da se glede na običajno prakso samo-opredelijo – posredujejo svoje osebne podatke. Zbirke osebnih podatkov, ki nastanejo na tej podlagi pa morajo biti ločene od zbirk osebnih podatkov, ki nastanejo pri izvrševanju zakonitih pristojnosti, nalog ali obveznosti. Predlagana določba torej pomeni neposredno pravno podlago za obdelavo osebnih podatkov v javnem sektorju. Določba je ti. *lex specialis* v razmerju do ti. *lex generalis* v četrtem odstavku 7. člena ZVOP-2.

K IV. delu predloga zakona:

IV. del predloga zakona ureja kazenske določbe za izvajanje predloga zakona, tako z vidika kaznovalnih določb Splošne uredbe, ki potrebujejo zakonsko izvedbo, kot z vidika drugih prekrškov, katere lahko Republika Slovenija samostojno predpiše.

K 125. členu:

Predlagani 125. 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 45. člena predloga zakona) 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 125. člena predloga zakona). Predlog zakona torej predpisane (opise; znake) kršitev iz Splošne uredbe opredeli kot prekrške v smislu Zakona o prekrških, njihove sankcije pa kot sankcije za prekrške (slovensko kaznovalno pravo pozna v okviru kaznivih ravnanj le kazniva dejanja in prekrške). Predlagana določba tudi določa, da se 17. člen Zakona o prekrških ne uporablja (sistemska določba prekrškovnega prava glede določanja razpona glob s predpisi Republike Slovenije).

V drugem odstavku je sistemsko določeno, da se pri odločanju Informacijskega pooblaščenca ter prekrškovnih sodišč (zahteva za sodno varstvo) o višini izrečene globe za kršitve, predpisane v četrtem do šestem odstavku 83. člena Splošne uredbe, v skladu z določbami prvega odstavka člena 83 Splošne uredbe in Zakona o prekrških, ob obravnavanju konkretnih okoliščin posameznega primera tudi upošteva, da globa ne sme biti nesorazmerno breme ali neprimerljivo breme za upravljavce ali obdelovalce glede na druge primerljive kršitve človekovih pravic in temeljnih svoboščin, ki se kaznujejo za prekrške, ali je obstajal namen koristoljubnosti ali namen škodovanja posameznikom, na katere se nanašajo osebni podatki, v primeru izvajanja popravljalnih ukrepov s strani upravljavca ali obdelovalca njihovo učinkovitost ali samostojno ukrepanje še pred uvedbo nadzora, glede fizičnih oseb pa se zlasti upošteva splošna raven dohodkov v Republiki Sloveniji ter njihov ekonomski položaj. Prav tako je treba upoštevati pri tem odločanju za vse obdelovalce ali

upravljavce ali gre za ponavljajoče kršitve in pomen, ki bi ga za odvračanje teh kršitev imela izbira vrste ali višine globe. Pri tem se upošteva pooblastilo iz uvodnega dela besedila drugega odstavka člena 83 Splošne uredbe ter zlasti (c) in (k) točke navedenega odstavka. Na ta način se onemogoča, da bi bile v neskladju s temeljnim ustavnim načelom sorazmernosti (2. v zvezi s tretjim odstavkom 15. člena Ustave Republike Slovenije) izrečene nesorazmerno visoke globe (kot že navedeno, je delno primerljiva ureditev zaradi pretiranosti glob v ustavnosodni presoji pred Ustavnim sodiščem Republike Avstrije, poleg tega pa je Avstrija zaradi sorazmernosti kaznovanja z globami leta 2018 spremenila Zakon o varstvu osebnih podatkov)[129].

V predlaganem tretjem 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 četrtem odstavku je določeno, da Informacijski pooblaščenec lahko za prekrške po določbah Splošne uredbe in iz predloga zakona v hitrem postopku izreče globo v kateri koli višini v razponu, kot je določena v določbah Splošne uredbe in predloga zakona, v znesku, ki je nižji ali višji od najnižje predpisane globe. To pomeni, da se 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 126. in 127. členu predloga zakona, uporabljajo ne glede na določbe o pristojnosti (da imajo tak način odločanja zakonsko določena le sodišča) iz šestega odstavka 26. člena Zakona o prekrških.

K 126. členu:

V predlaganem 126. 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 127. členu:

V predlaganem 127. 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 128. členu:

V predlaganem 128. členu so predpisane kršitve in kazni za prekrške za določena delovanja v neskladju z I. delom predloga zakona, zlasti glede notranje in zunanje sledljivosti osebnih podatkov.

K 129. členu:

Za področje svobode izražanja (ki je po 103. členu predloga zakona skoraj v celoti izvzeto iz dometa predloga zakona in tako tudi nadzora Informacijskega pooblaščenca – v korist svobode izražanja) je v predlaganem 130. členu predpisan poseben prekršek, ki se nanaša na nezakonito razkritje osebnih podatkov. Ta ureditev pa omogoča tudi nekaznivost, če kak drug zakon določi varstvo oseb, ki izdajo podatke (žvižgači, viri informacij).

K 130. členu:

[129] Avstrija je s spremembo Zakona o varstvu osebnih podatkov (Zakon o deregulaciji varstva osebnih podatkov) dne 20. aprila 2018 (Datenschutz-Deregulierungs-Gesetz 2018, BGBl. I Nr. 24/2018) določila, da se v primeru predpisanih glob za kršitve po Splošni uredbi najprej izrekajo opozorilne sankcije, šele v primeru ponovitev pa globe po Splošni uredbi (spremembe 11. člena), prav tako pa je sedaj določeno, da nosilci javnih pooblastil niso odgovorni za prekrške po Splošni uredbi (spremembe 35. člena).

V 130. členu so predpisane kršitve (prekrški) glede določb predloga zakona o uporabi povezovalnega znaka ter avtomatiziranem odločanju. Predpisane globe so glede na občutljivost varovanih vrednot nekoliko višje, tudi za posameznike – od 200 do 2000 evrov.

K 131. členu:

V 131. členu so predpisani določeni prekrški s področij iz II. dela tega zakona, namreč bistvene kršitve glede nezakonite obdelave osebnih podatkov ter nezakonitega dostopanja do njihove vsebine, določeni so torej prekrški glede zakonskih izvedbenih določb v zvezi z določbami Direktive.

K 132. členu:

V 132. členu so določeni prekrški glede kršitve splošnih določb prve področne ureditve po predlogu zakona, namreč določb o neposrednem trženju.

K 133. členu:

V 133. členu so določeni prekrški glede kršitve splošnih določb druge področne ureditve po predlogu zakona, namreč splošnih določb o videonadzoru, katere med drugim vključujejo ne-objavo obvestila o izvajanju videonadzora ipd. Globe so razumno (sorazmerno) predpisane.

K 134. členu:

V predlaganem 134. 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 135. členu:

V predlaganem 135. 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 133. in 134. členu predlogu zakona, ker se upošteva pomembnejši zasebnopravni kontekst stanovanjskih razmerij.

K 136. členu:

V 136. 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 133. in 134. členu predloga zakona, ker se upošteva pomembnejši kontekst varstva delavcev v delovnih prostorih.

K 137. členu:

V 137. členu so določeni prekrški glede kršitev določb o videonadzoru na javnih površinah (nov prekršek). Glede na kontekst (javne površine; javni prostor), kjer je večja nevarnost nastanka ti. totalne nadzorovalne države ozir. družbe je višina glob za prekrške nekoliko višja, vseeno pa primerljiva globam po 136. členu predloga zakona.

K 138. členu:

V predlaganem 138. členu je določen prvi prekršek s področja tretje področne ureditve – biometrije. Globe so razumno (sorazmerno) predpisane za kršitve določb glede biometrije v javnem sektorju.

K 139. členu:

V predlaganem 139. členu je določen drugi prekršek s področja področne ureditve biometrije. Globe so razumno (sorazmerno) predpisane za kršitve določb glede biometrije v zasebnem sektorju.

K 140. členu:

Predlagani 140. člen določa poseben prekršek glede kršitev določb o prepovedi trženja biometričnih osebnih podatkov v zasebnem sektorju (115. člen predloga zakona). Predpisane globe so opazno višje od drugih glob s področja biometrije, saj gre pri ukrepih »zamenjave biometričnih osebnih podatkov za storitve« za večjo nevarnost (tveganost) za pravice ljudi, za njihovo razosebljenje, krajo identitete ipd.

K 141. členu:

V predlaganem 141. členu je določen prekršek s področja četrte področne ureditve, namreč kršitev določb o evidenci vstopov in izstopov. Glede na kontekst (običajni vstopi in izstopi v prostore) so globe razumno (sorazmerno) predpisane – nižje kot npr. v 133. in 134. členu predloga zakona.

K 142. členu:

V predlaganem 142. členu je določen prekršek s področja pete področne ureditve, namreč kršitev določb o javnih knjigah (njihovi namenski uporabi). Globe so razumno (sorazmerno) predpisane za kršitve zakonskih določb.

K 143. členu:

V predlaganem 143. členu so določeni prekrški s področja šeste področne ureditve glede povezovanj uradnih evidenc in javnih knjig (glede na prvi odstavek, drugi odstavek in tretji odstavek 118. člena predloga zakona). Globe so glede na kontekst predpisane v nekoliko večji višini.

K 144. členu:

V predlaganem 144. členu so določeni prekrški glede sedme področne ureditve – opravljanja strokovnega nadzora. Globe so predpisane nekoliko nižje, saj gre za področje, ki še ni dovolj normirano v področni zakonodaji.

12. K V. delu Predloga ZVOP-2:

Predlagani V. del predloga zakona ureja prehodne in končne določbe, Prehodne določbe so zlasti pomembne z vidika pozitivnih vplivov na gospodarstvo, lokalno samoupravo in javne zavode.

K 145. členu:

Predlagani 145. člen ureja začasno ureditev glede pooblaščenih oseb za varstvo osebnih podatkov glede vprašanja delovne dobe, izobrazbe ter izkušenj z določenih delovnih področij, poseben položaj

za občine ter za vzgojno-izobraževalne zavode ter možnost začasnega (rok devetih mesecev) uresničevanja te obveznosti na drug način. Gre za nov institut in potrebna je prehodna doba.

K 146. členu:

Predlagani 146. člen določa ureditev glede dosedanjih postopkov ali odločanja Informacijskega pooblaščenca, najprej je glede prekrškovnih postopkov, ki so se začeli pri Informacijskem pooblaščencu ali na sodiščih pred uveljavitvijo ZVOP-2 določeno, da se končajo ZVOP-1 iz leta 2004, razen če je ta ZVOP-2 za storilca milejši (vsebinsko, ne samo redakcijsko spremenjeni znaki prekrška ali kršitve, ukinjen prekršek). Glede postopkov inšpekcijskega nadzora, ki so se začeli na podlagi ZVOP-1 je določeno, da se nadaljujejo v skladu z ZVOP-2.

K 147. členu:

V prvem odstavku 147. člena je določeno prehodno obdobje za izvrševanje šestega odstavka 28. člena predloga zakona - upravljavci ali obdelovalci, ki za izvajanje svojega delovanja pridobivajo osebne podatke iz registrov ali evidenc s področja upravnih notranjih zadev, morajo v dveh letih od uveljavitve tega zakona vzpostaviti ustrezne varnostne mehanizme, kot jih določi Ministrstvo za notranje zadeve.

Predlagani člen v drugem odstavku določa prehodne določbe glede pridobivanja podatkov iz uradnih evidenc in javnih knjig ter povezovanja – glede na 118. člen ZVOP-2 (štiriletno prehodno obdobje). To pomeni, da imajo upravljavci na razpolago štiri leta, da si v svojem področnem zakonu glede na kriterije iz prvega odstavka 118. člena predloga zakona zagotovijo zakonsko ureditev povezovanja. V vmesnem času veljajo obstoječa povezovanja za zakonita.

K 148. členu:

Določene so prehodne določbe za uvedbo certificiranja po ZVOP-2 – in to šele od 1. 1. 2022, saj se izhaja iz dejstva, da je treba izdati merila– merila na ravni Evropske unije, ki se bodo še nekaj časa usklajevala ter merila, ki jih izda Informacijski pooblaščenec. Realno to pomeni nekaj več kot dvoletni rok za začetek delovanja določb o postopkih akreditacije in temu sledi tudi predlagana prehodna določba.

K 149. členu:

Predlagani 150. člen določa, da upravljavci in obdelovalci, ki so Informacijskemu pooblaščencu že poslali podatke o pooblaščenih osebah, tega niso dolžni storiti ponovno, če se podatki niso spremenili.

K 150. členu:

Predlagani 150. člen omogoča daljšo uporabo obstoječega Pravilnika o službeni izkaznici državnega nadzornika za varstvo osebnih podatkov.

K 151. členu:

Predlagani 151. člen določa prenehanje veljavnosti podzakonskih predpisov, za določene (npr. zaračunavanje) pa določa njihovo začasno uporabo do uveljavitve novih podzakonskih predpisov (katere izda minister za pravosodje).

K 152. členu:

Predlagani 152. člen določa, da minister za pravosodje izda pravilnik iz četrtega odstavka 21. člena v roku treh mesecev od uveljavitve tega zakona.

K 153. členu:

Predlagani 153. člen določa prenehanje veljavnosti dosedanjega ZVOP-1 (iz leta 2004, s spremembami do leta 2007[130] ter ob upoštevanju vpliva Splošne uredbe iz leta 2016[131]).

K 154. členu:

V končni določbi je v 154. členu predlagano, da začne novi Zakon o varstvu osebnih podatkov (ZVOP-2) veljati 30 dni po objavi v Uradnem listu Republike Slovenije, kar pomeni v drugi polovici leta 2019. Rok tridesetih dni je predlagan z vidika pravne varnosti, tako da se uporabnikom zakona da nekaj časa za seznanitev z vsebino sprejetega zakona ter pripravo za njegovo uporabo, po drugi strani pa se upošteva, da se Splošna uredba o varstvu podatkov uporablja že od maja 2018 in je za šteti, da so uporabniki pravne ureditve varstva osebnih podatkov z bistvenimi novimi rešitvami že seznanjeni zlasti preko (preostale) vsebine veljavnega ZVOP-1 iz leta 2004 ter Splošne uredbe o varstvu podatkov iz leta 2016.

[130] Uradni list RS, št. 86/04, 113/05 – ZInfP, 51/07 – ZUstS-A, 67/07 in 94/07 – uradno prečiščeno besedilo.
[131] UL L št. 119 z dne 4. 5. 2016, str. 1), zadnjič popravljena s Popravkom (UL L št. 127 z dne 23. 5. 2018, str. 2.